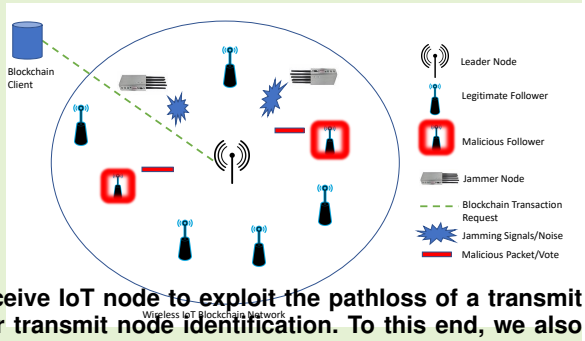
Countering Active Attacks on RAFT-based IoT Blockchain Networks

Hasan Mujtaba Buttar*, Waqas Aman*, M. Mahboob Ur Rahman, Qammer H. Abbasi

***Abstract*— This paper considers an Internet of Things (IoT) blockchain wireless network consisting of a leader node and various follower nodes which together implement the RAFT consensus protocol to verify a blockchain transaction, as requested by a blockchain client. Further, two kinds of active attacks, i.e., jamming and impersonation, are considered on the IoT blockchain network due to the presence of multiple *active* malicious nodes in the close vicinity. When the IoT network is under a jamming attack, we utilize the stochastic geometry tool to derive the closed-form expressions for the coverage probabilities for both uplink and downlink IoT transmissions (which eventually translate to blockchain transaction success rate). On the other hand, when the IoT network is under an impersonation attack, we propose a novel method that enables a receive IoT node to exploit the pathloss of a transmit IoT node as its fingerprint to implement a binary hypothesis test for transmit node identification. To this end, we also provide the closed-form expressions for the probabilities of false alarm, missed detection, and miss-classification. Finally, we present detailed simulation results that indicate the following: i) the coverage probability (and hence blockchain transaction success rate) improves as the jammers' locations move away from the IoT network, ii) the three error probabilities decrease (i.e., chances of corruption of the blockchain ledger data due to false data injection by malicious node decrease) as a function of the quality of the link between the transmit and receive IoT node.**



***Index Terms*— Authentication, Blockchain, Coverage Probability, Downlink, Uplink, IoT Blockchain Wireless Networks, Impersonation, Jamming, Pathloss, RAFT consensus, Security, Stochastic Geometry.**

I. Introduction

Blockchain technology consists of a decentralized, distributed ledger that allows multiple parties to securely and transparently record and verify transactions. It uses a series of cryptographic algorithms to create a tamper-proof and immutable record of every transaction in the network. Each block in the chain contains a timestamp, a unique cryptographic hash, and a reference to the previous block, creating a chain of interconnected blocks. Once a block is added to the chain, it cannot be altered or deleted without changing all subsequent blocks, making the blockchain an extremely secure and transparent system for storing and sharing data. Blockchain technology has numerous potential applications, including cryptocurrency, supply chain management, healthcare, voting systems, and more [1].

One pivotal component of blockchain technology are the consensus techniques that establish trust among blockchain entities, and enable updates in the distributed ledger's states. The blockchain consensus methods could be broadly categorized into two classes [2]. The first class of methods is based on pure computation that asks the participating nodes to solve a mathematical puzzle in order to prove that they are eligible for mining work, e.g., proof-of-work (PoW) [3] and proof-of-stakes (PoS) [4]. The second class of methods relies on pure communications between joining nodes whereby the successful voting by a majority of nodes through the communication channel leads to the achievement of consensus, i.e. Byzantine fault tolerant (BFT) method [5], Paxos [6], and RAFT [7]. Private blockchains use second class of consensus methods due to their low-complexity, high throughput and small confirmation delay [8]. Among them, RAFT method has become ubiquitous as it reduces the degree of non-determinism by decomposing the nodes into two types of roles: there is one leader node while others are follower nodes.

Having introduced the essentials of blockchain technology in detail, we discuss next the recent research interest to investigate potential integration of blockchain with wireless networks. Recently, there has been growing interest in utilization of blockchain technology in next-generation wireless networks for various system configurations, and for a multitude of problems [9]. The potential integration of blockchain technology with the next-generation wireless networks is anticipated to help wireless networks provide support for processing at the edge, automation, and distributed trust [10]. Thus, research which study various aspects of a wireless blockchain network

H. M. Buttar and M. M. U Rahman are with the electrical engineering department, Information Technology University, Lahore 54000, Pakistan (e-mail: mahboob.rahman@itu.edu.pk).

W. Aman is with Hamad Bin Khalifa University, Qatar (e-mail: waman@hbku.edu.qa).

Q. H. Abbasi is with the Department of Electronics and Nano Engineering, University of Glasgow, Glasgow, G12 8QQ, UK (e-mail: Qammer.Abbasi@glasgow.ac.uk).

* implies equal contribution by the authors.

have started to emerge. As an example, [11] studies the impact of optimal node deployment on blockchain transaction throughput. Authors in [12] maximize the blockchain transaction rate (and thus the revenue of miners) using the Stackelberg game approach. [13] provides a closed-form expression of the signal to interference plus noise ratio, throughput and transmission successful probability for a wireless blockchain network. [14] investigates the potential of blockchain for doing resource management in 6G cellular networks, for the following use-case scenarios: device-to-device, IoT, and network-slicing. Dynamic spectrum sharing is studied in [15], where reinforcement learning is utilized to analyze the resource-sharing structure and spectrum-sharing process in a blockchain system combined with 6G hybrid cloud. Authors in [16] study the dynamics of block propagation and provide a closed-form expression for block propagation time, in blockchain-based vehicular ad-hoc networks. The work [17] minimizes the latency in storing data by intelligent transaction migration policy by exploiting the Markov process and deep deterministic policy gradient. The authors in [18] focus on blockchain-based wireless local area networks and provide a new medium access control protocol known as block access control. Finally, the authors in [19] propose Blockchain Enabled Radio Access Network whereby they provide a security framework for mutual authentication based on digital signatures/secret keys. They also provide design guidelines for switching, routing, and quality of service management.

Though blockchain technology is a promising solution for wireless IoT networks, nevertheless wireless IoT blockchain networks are vulnerable to different attacks (due to broadcast nature of wireless medium) [20]. Such attacks on IoT blockchain networks lead to the failure of the consensus process that is responsible for integrity of the transactions in the blockchain. For example, in a RAFT-based blockchain network, RAFT consensus protocol will fail if several follower nodes do not cast their votes due to communication failure, or if dishonest votes are cast by malicious actors [21].

Contributions. This work considers a RAFT-based IoT blockchain network that comprises a leader node and many follower nodes which together verify a blockchain transaction upon request from a blockchain client. To the best of the authors' knowledge, this work is the first that considers the two most prominent kinds of active attacks (jamming and impersonation) on the IoT blockchain networks. Specifically, two main contributions of this paper are as follows:

- When the IoT blockchain network is under jamming attack, we utilize the stochastic geometry tool to derive the coverage probabilities for both uplink and downlink IoT transmissions (which eventually translate to blockchain transaction success rate). In simulations, we thoroughly study the impact of important system parameters, e.g., transmit power of legitimate and jamming nodes, intensity and relative geometry of the jamming nodes, etc. on the coverage performance.
- When the IoT blockchain network is under impersonation attack, we propose a novel counter-method that enables a receive IoT node to exploit the pathloss of a transmit IoT node as its fingerprint to construct a two-step testing approach (i.e. maximum likelihood test followed by the binary hypothesis test). Further, we provide closed-form expressions for the three error probabilities, i.e., false alarm, missed detection and miss-classification. Note that the probability of missed detection translates to the probability of corruption of the blockchain ledger data due to false data injection by malicious node.

Outline. Section II describes the selected related work. Section III provides a detailed description of the considered system model. Section IV considers the scenario of a jamming attack on the IoT blockchain network. Section V considers the scenario of an impersonation attack on the IoT blockchain network. Section VI provides selected numerical results. Finally, Section VII concludes the paper.

Notations. Unless specified otherwise, $|.|$ and $\|.\|$ denote the modulus and the 2-norm respectively, $\mathbb{E}(.)$ is the expectation operator, boldface letters such as $\mathbf{X}$ represents a vector and $\mathcal{CN}$ means complex normal.

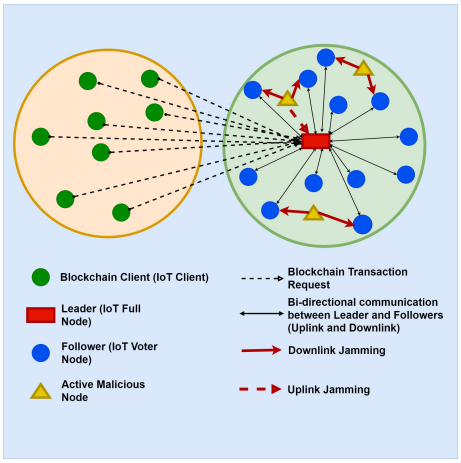


Fig. 1. System Model

II. Related work

The literature on blockchain-assisted wireless networks as well as blockchain systems with wireless IoT verifier nodes is continuously expanding. Thus, due to space constraints, only selected related work is discussed below. The interested reader is referred to the relevant survey papers [22], [23], [24] for a more detailed overview of the recent progress in the field. Specifically, the survey article [22] summarizes the works that have been proposed by the researchers to realize secure IoT networks by using machine learning and blockchain tools. The second survey article [23] summarizes works that utilize blockchain for various configurations of wireless cellular networks, e.g., THz networks, mm-wave networks, D2D communication, HetNets, full-duplex networks, aerial networks etc. Finally, the third survey article [24] provides a comprehensive discussion of the existing blockchain consensus protocols, and their sub-types, e.g., proof of work, proof of stakes, proof of elapsed time, proof of activity, Paxos, RAFT, and many more.

There have been quite a few works which do analytical performance analysis of the blockchain networks under various system configurations and assumptions. For example, [25]

does performance analysis of a wireless blockchain network using stochastic geometry tool. Specifically, they utilize the stochastic geometry tool find the optimal deployment of the full/leader node in order to maximize the coverage performance of the wireless blockchain system. [26] focuses on RAFT consensus protocol and utilizes tools from probability theory in order to do reliability analysis of the RAFT consensus protocol. For example, they derive the probability density function of the logarithmic consensus failure rate. [27] proposes a machine learning aided scheme where authors begin with proof of work consensus protocol and propose to split a blockchain into multiple sub-chains in order to reduce the mining time of the blockchain transaction. The splitted sub-transactions are later merged together.

Another direction of research is to investigate novel and efficient blockchain consensus protocols. For example, [28] proposes a new variant of the classical RAFT protocol whereby the leader node is re-elected every once in a while. More precisely, the IoT node with better computational capability is more likely to be elected as the new leader. [29] also proposes a new blockchain consensus protocol whereby the participating IoT nodes are ranked in a hierarchical manner for their reputation according to a novel methodology that the authors develop. [30] utilizes blockchain to store and trade information between the IoT nodes of an air to ground IoT network. Specifically, authors propose a novel consensus method to achieve a required quality of service. To this end, authors also utilize the mathematical tool of stochastic geometry in order to systematically figure out number of ground IoT nodes in order to provide a required coverage.

There have been quite a few works which discuss attacks as well as undesired scenarios a wireless IoT blockchain network could run into. For example, [31] propose a solution to the forking problem, an undesired phenomenon in a wireless blockchain system. Here, due to wireless channel fading, occasionally there is a large transmission delay and sometime transmission failure occurs. When this happens, it results in an inconsistency in the blockchain ledger where few nodes start to work on new blockchain transaction while the other (with communication failure) keep working on old transaction. [32] considers interferers which transmit undesired signals to harm the ongoing communication within a wireless IoT blockchain network, and studies the impact of density of number of interfering nodes on the blockchain transaction rate. [33] considers jamming attacks on a wireless blockchain system that is being used for record keeping of medical health records. Here, the authors propose frequency-hopping spread spectrum (FHSS) as anti-jamming solution where the IoT nodes switch to a new channel at a different frequency as soon as a jamming attack is detected. Finally, the work [21] considers a RAFT-based wireless blockchain network when a single jammer is present nearby, and derives the probability of achieving a successful blockchain transaction.

At the same time, the parallel domain of physical layer security has evolved rapidly whereby physical layer authentication has emerged as a promising method for countering impersonation attacks [34]. Specifically, to counter the impersonation attacks at the physical layer, researchers have proposed various channel and hardware-based features, e.g., [35], [36], [37] propose distance, angle of arrival and position, [38] and [39] propose channel impulse response, and [40] and [41] exploits the lack of hardware reciprocity, [42] exploits carrier frequency offset as features or device fingerprints to carry out authentication. Inline with the previous work, this work counters impersonation attacks by exploiting the pathloss of the transmit IoT nodes as features for authentication.

III. System Model & Background

A. System Model

The RAFT-based IoT blockchain network comprises two parts, a wireless consensus network, and IoT clients, as shown in Fig. 1. The two parts may or may not be geographically isolated. Fig. 1 illustrates the communication network topology and the IoT nodes' roles interchangeably for different business models. Any IoT node in the network can play a client's role that sends out transaction-requests or a leader/follower in the consensus process. The followers and malicious nodes' locations in a 2-dimensional free space are modeled as Poisson point process (PPP), while the leader (full node) is fixed at the geo-center of consensus network.

Adversary capabilities and behavior modeling. We consider that malicious nodes are active malicious nodes who are capable of launching jamming and impersonation attacks. We assume that malicious nodes either launch jamming attacks or impersonation attacks in a given time. In jamming mode, malicious nodes continuously transmit noise/jamming signals in the available spectrum of communication for both uplink and downlink transmissions in order to destroy the voting process in IoT wireless blockchain networks. Thus, it is critically important to explore the blockchain transactions success rate in the form of coverage probability in the presence of radio jamming [21]. On the other hand, in impersonation mode, the malicious nodes aim to represent themselves as legitimate nodes and cast votes to select a leader. Therefore, it is important to counter impersonation attacks by using a physical layer authentication mechanism.

B. RAFT Consensus Protocol

RAFT consensus algorithm begins by first electing a leader. It is the leader node who receives log entries/transaction-details from the blockchain client. The leader node is assumed to have higher computational capability as well as higher reliability, and is responsible to manage the new log entries and makes sure that the blockchain ledger stays consistent. In contrast, followers are passive nodes that only respond to the request of the leader. It is only the leader who can insert the transaction-details into the blockchain ledger. The RAFT consensus mechanism is triggered as follows. Firstly, the leader receives the transaction information from a client and performs some necessary actions to form a block. Secondly, the leader will communicate with follower nodes via a downlink (DL) broadcasting channel to request to verify and approve the block. When followers successfully receive the leader's message, they verify the block and send their voting message on the multi-access uplink (UL) channel to the leader.

Lastly, the leader will count the votes, and consensus is said to be achieved if the leader gains the majority (i.e., more than 50% followers verify/approve the block).

This paper focuses on communication inside the RAFT consensus network, on both DL and UL.

IV. Jamming Attack on IoT Blockchain Network

In the RAFT consensus algorithm, a client transmits transaction requests to the leader node to make consent with the followers by considering that all follower nodes are honest. This section finds success/coverage probability defined as receiving Signal to Interference and Noise Ratio (SINR) is greater than its predefined threshold between a leader and associated follower. All followers operate in the same frequency band, so they cause increased interference that ultimately degrades the received SINR and lowers the success probability. Different protocols were employed in the private blockchain networks to avoid interference and collision among the follower nodes, such as centralized radio resource allocation and Carrier Sense Multiple Access (CSMA) or transmission interval made large enough so that collision is negligible.

A. Coverage Probability for Downlink IoT Transmissions

When the leader transmits, then a typical follower receives the following baseband signal:

$$y = \sqrt{P}Hs + \sum_{j\in\phi_J} \sqrt{P_j}H_j s + n, \tag{1}$$

where P (P_j) is the transmit power of the leader (j-th jammer) node, s is the transmitted symbol, $H = h/\sqrt{R^{\alpha}}$ ($H_j = h_j/\sqrt{R_j^{\alpha}}$) represents the wireless propagation from the leader (jammer) to the follower, and R (R_j) is the random distance between the leader (jammer) and the follower node. Further, for the leader-follower link, $R^{-\alpha}$ is the large-scale fading/pathloss component, α is the pathloss exponent, $h \sim \mathcal{CN}(0,1)$ is the small-scale fading component. Moreover, $\sqrt{I_J} = \sum_{j\in\phi_J}\sqrt{P_j}H_j s$ is the aggregate interference amplitude due to multiple jammers where ϕ_J indicates that the jammers are distributed in a 2-dimensional free-space as PPP. Finally, $n \sim \mathcal{CN}(0,\sigma^2)$ is the additive white Gaussian noise with power σ^2.

We consider an interference-limited scenario (i.e., the interference is much larger than the noise). This allows us to consider the signal-to-interference ratio (SIR) as the performance metric. The SIR of a typical follower associated with the leader node is given as:

$$SIR^{DL} = \frac{P|h|^2R^{-\alpha}}{I_J}, \tag{2}$$

where $I_J = \sum_{j\in\phi_J} P_j|h_j|^2\|\mathbf{X}_j\|^{-\alpha}$ is the aggregate interference power, $h_j \sim \mathcal{CN}(0,1)$ is the small-scale fading component on the jammer-follower channel, and $\mathbf{X}_j$ is the random location of j-th jammer or Poisson point (note that $\|\mathbf{X}_j\| = R_j$).

The IoT transmission from the leader to any given follower node on the DL will be considered successful only when the received SIR is greater than a pre-specified threshold β_D [43]. Thus, the transmission success probability, or, the coverage probability for the DL ($\mathcal{P}_c^{DL}$) is defined as follows:

$$\mathcal{P}_c^{DL}(\alpha,\beta_D) = \mathcal{P}\Big[SIR^{DL} > \beta_D\Big] = \mathcal{P}\Big[\frac{P|h|^2R^{-\alpha}}{I_J} > \beta_D\Big]. \tag{3}$$

Now, we assume that a typical follower is at distance r from the leader, then the coverage probability can be expressed as:

$$\mathcal{P}_c^{DL}(\alpha,\beta_D) = \mathbb{E}_R\Big[\mathcal{P}\Big[SIR^{DL} > \beta_D \mid R = r\Big]\Big], \tag{4}$$

$$= \int_{r>0}^{\infty} \mathcal{P}\Big[SIR^{DL} > \beta_D \mid r\Big] f_R(r)dr,$$

where $f_R(r)$ is the probability density function (PDF) of R, and is given as [44] [1]:

$$f_R(r) = 2\pi\rho r\exp(-\rho\pi r^2), \tag{5}$$

where ρ is the intensity/density of the IoT nodes. We now need to compute $\mathcal{P}\big[SIR^{DL} > \beta_D \mid r\big]$ which can be expressed as:

$$\mathcal{P}\Big[SIR^{DL} > \beta_D \mid r\Big] = \mathcal{P}\Big[|h|^2 > \frac{r^{\alpha}\beta_D}{P}I_J\Big]. \tag{6}$$

As $|h|^2 \sim \exp(1)$, we can write:

$$\mathcal{P}\Big[|h|^2 > \frac{r^{\alpha}\beta_D}{P}I_J\Big] = \mathbb{E}_{I_J}\Big[\exp(-\frac{r^{\alpha}\beta_D}{P}I_J)\Big] = \mathcal{L}_{I_J}(\frac{r^{\alpha}\beta_D}{P}), \tag{7}$$

where $\mathcal{L}_{I_J}(s)$ denotes the Laplace transform of the aggregate interference I_J which is computed in Appendix (with variable $s = \frac{r^{\alpha}\beta_D}{P}$).

Putting back the result of Appendix to Eq. 4 we get the following final expression of coverage probability for DL:

$$\begin{aligned}\mathcal{P}_c^{DL}(\alpha,\beta_D) = 2\pi\rho_{r\geq 0}\exp\Bigg(\frac{\pi\rho_J\gamma_j\beta_D r^{\alpha}}{(\alpha/2)-1}\Bigg[z_2^{(2-\alpha)}\\ {}_2F_1(1,1-\frac{2}{\alpha},2-\frac{2}{\alpha},-\gamma_J\beta_D(\frac{r}{z_2})^{\alpha}) - z_1^{(2-\alpha)}\\ {}_2F_1(1,1-\frac{2}{\alpha},2-\frac{2}{\alpha},-\gamma_J\beta_D(\frac{r}{z_1})^{\alpha})\Bigg] - \rho\pi r^2\Bigg)rdr.\end{aligned} \tag{8}$$

B. Coverage Probability for Uplink IoT Transmissions

To achieve the consensus, followers send the voting message on the multi-access UL channel for confirmation after receiving a DL message. Consensus will be achieved if more than 50% from the followers successfully verify the transaction on the UL channel. So, we need to compute the success probability on the UL channel. We assume that CSMA is the medium access technique adopted by the followers and transmission on UL is available all the time (i.e., no idle channel). Then the coverage probability for a typical follower node on the UL is given as [43]:

$$\mathcal{P}_c^{UL}(\alpha,\beta_U) = \mathcal{P}\Big[SIR^{UL} > \beta_U\Big] = \mathcal{P}\Big[|h^U|^2 > \frac{R_U^{\alpha}\beta_U}{P_F}I_J^U\Big], \tag{9}$$

[1] We consider the elected leader node at the origin of considered space.

where β_U is a predefined threshold for UL, h^U is the channel gain, R_U is the distance from a typical follower to the leader on UL, P_F is the transmit power of a typical follower, and I_J^U is the aggregated interference to the leader. CSMA makes sure that there is no interference from the other follower nodes on the UL, thus, the interference/jamming is due to the jammers only. This makes the coverage probability formulation the same as we do for DL. We compute UL success probability using the same procedure as above, and we get:

$$\mathcal{P}_c^{UL}(\alpha,\beta_U) = 2\pi\rho_{r\geq 0}\exp\Bigg(\frac{\pi\rho_J\gamma_j^U\beta_U r_U^\alpha}{(\alpha/2)-1}\Bigg[z_2^{(2-\alpha)} \\ {}_2F_1(1,1-\frac{2}{\alpha},2-\frac{2}{\alpha},-\gamma_j^U\beta_U(\frac{r_U}{z_2})^\alpha) - z_1^{(2-\alpha)} \\ {}_2F_1(1,1-\frac{2}{\alpha},2-\frac{2}{\alpha},-\gamma_j^U\beta_U(\frac{r_U}{z_1})^\alpha)\Bigg] - \rho\pi r_U^2\Bigg) r_U dr_U, \tag{10}$$

where ρ_J is the intensity of jammer nodes and $\gamma_j^U = P_j/P_F$.

C. Overall Coverage Probability

Consensus is achieved when followers successfully receive the leader's request to verify the transaction-detail over the DL channel and respond to the leader over the UL channel. So, we derive the joint coverage probability in an IoT blockchain network as follows [45][2]:

$$\mathcal{P}_c = \mathcal{P}[SIR^{UL} > \beta_U].\mathcal{P}[SIR^{DL} > \beta_D] \tag{11}$$

V. Impersonation Attack on IoT Blockchain Network

In the RAFT consensus algorithm, due to the broadcast nature of wireless communication, the consensus algorithm may fail due to the impersonation attacks launched by nearby malicious/illegitimate node(s) (so-called Eve(s)). In impersonation attacks, malicious nodes try to claim themselves as legitimate nodes/followers by utilizing a forged character in order to destroy the consensus mechanism.

In this work, we provide a physical layer authentication mechanism to counter impersonation by illegitimate nodes. We, in this work, exploit the pathloss of the transmitter node as a device fingerprint to counter the impersonation. We assume a realization[3] of PPP, specifically, M follower (legitimate) nodes $\{F_i\}_{i=1}^M$ and N Eve (malicious/illegitimate) nodes $\{E_j\}_{j=1}^N$ are considered in a 2-Dimensional space, and a leader is placed at the center of the considered region. We assume that the transmitter nodes transmit with a fixed transmit power so that the leader can compute the pathloss. We also assume that the malicious nodes are transmitting with the same transmit power in order to stay stealth in the region [4]. The pathloss Ψ in dB of a transmitter at the distance d from the receiver is given as: $\Psi[dB] = 10\alpha\log_{10}(d)$, where α is the pathloss exponent.

A. The Proposed Authentication Method

We assume that CSMA is the approach used by the followers and malicious nodes to cast their votes. We assume that malicious node E_j could cast a vote, pretending to be a legitimate follower node when the channel is completely idle by the followers and hence, no collision. The leader is supposed to authenticate each received casting vote and correctly achieved the consensus. Furthermore, we assume that the leader already has the ground truths of legitimate nodes which he gets via prior training on a secure channel. The ground truth vector can be denoted by $\mathbf{\Psi} = \{\Psi_1, ..., \Psi_M\}^T$. As discussed earlier, we will authenticate the transmitter based on the pathloss feature. So the noisy measurement of pathloss $z = \Psi + n$ at a given time-slot is obtained, where Ψ is the pathloss and $n \sim \mathcal{N}(0,\sigma^2)$ is the noise/estimation error. To counter the impersonation by malicious nodes, we first do a maximum likelihood (ML) test as follows:

$$i^* = \max_i \quad f(z \mid \Psi_i), \tag{12}$$

where $f(z \mid \Psi_i)$ is the likelihood function or conditional PDF. Equivalently, we can write 12 as:

$$(TS^*, i^*) = \min_i \quad |z - \Psi_i|, \tag{13}$$

where TS^* is the minimum value of test statistics and i^* returns the index of the transmitter node which is decided through ML. Next, we decide on impersonation through binary hypothesis testing as follows:

$$\begin{cases} H_0(\text{no impersonation}): & TS^* = \min_i |z(t) - \Psi_i| < \epsilon \\ H_1(\text{impersonation}): & TS^* = \min_i |z(t) - \Psi_i| > \epsilon \end{cases}, \tag{14}$$

where ϵ is a small test threshold and is a design parameter that decides whether a vote from a follower node is accepted or not. Then: $TS^* \gtrless_{H_0}^{H_1} \epsilon$.

The hypothesis H_0 inferred that the legitimate node transmits the vote. Alternatively, the hypothesis H_1 implies that an illegitimate node transmits a vote. Further, we present closed-form expressions for the error probabilities. We have three types of errors resulting from the above tests. These errors are: false alarm, missed detection, and miss-classification. The probability of false alarm ($\mathcal{P}_{fa}$) is the probability that a legitimate follower casts a vote, but the leader identifies it as a malicious node. The probability of missed detection ($\mathcal{P}_{md}$) is the probability that a malicious node casts a vote, but the leader identifies it as a vote of a legitimate node. Last, the probability of miss-classification ($\mathcal{P}_{mc}$) is the probability that when no impersonation is detected but a wrong transmitter node is decided among the legitimate transmitters.

We, in this work, follow the Neyman-Pearson lemma [46] where a small test threshold ϵ for a pre-defined false alarm rate

[2]Note that coverage probability analysis is only a performance monitor amid the jamming attack. One potential anti-jamming method is frequency hopping spread spectrum, but this is outside the scope of this work.

[3]Typically, in physical layer authentication, one needs to know the exact number of transmitting nodes in order to evaluate its performance. Therefore, in this part, we take a single realization of PPP in order to fix the total number of nodes (both, malicious and legitimate).

[4]High power transmission will easily identify the transmitter as a malicious node. To get success in impersonating the legitimated nodes, malicious nodes transmit with the same power as legitimate nodes do.

$\mathcal{P}_{fa}$ is chosen such that missed detection probability $\mathcal{P}_{md}$ is minimized. First, the probability of false alarm is given as:

$$\begin{aligned}\mathcal{P}_{fa} &= \mathcal{P}(H_1|H_0) = \sum_{i=1}^{M} \mathcal{P}(TS^* > \epsilon|F_i)\pi(i) \\ &= \sum_{i=1}^{M} 2Q(\frac{\epsilon}{\sigma})\pi(i) = 2Q(\frac{\epsilon}{\sigma})\sum_{i=1}^{M}\pi(i) = 2Q(\frac{\epsilon}{\sigma})\end{aligned} \tag{15}$$

where $\pi(i)$ is the prior probability of legal node F_i (we consider equal priors in our work), and $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{\frac{-t^2}{2}}dt$ is the complementary CDF of a standard normal distribution Thus, the threshold ϵ is computed as follows: $\epsilon = \sigma Q^{-1}(\frac{\mathcal{P}_{fa}}{2})$.

B. The Performance of the Proposed Method

The probability of missed detection $\mathcal{P}_{md}$ is computed as:

$$\begin{aligned}&\mathcal{P}_{md} = \mathcal{P}(H_0|H_1) = \mathcal{P}(TS^* < \epsilon|E_j) \\ &= \sum_{j=1}^{N}\sum_{i=1}^{M}\left[Q(\frac{\Psi_i - \Psi_j - \epsilon}{\sigma}) - Q(\frac{\Psi_i - \Psi_j + \epsilon}{\sigma})\right]\frac{\pi(j)}{M}\end{aligned} \tag{16}$$

where $\pi(j)$ is the prior probability of impersonator node E_j.

Since the probability of missed detection is a random variable, so the expected value $\bar{\mathcal{P}}_{md} := \mathbb{E}(\mathcal{P}_{MD})$ is as follows:

$$\begin{aligned}&\bar{\mathcal{P}}_{md} = \sum_{j=1}^{N}\frac{1}{\Delta}\pi(j). \\ &\left(\int_{\Psi_{min}}^{\Psi_{max}} \sum_{i=1}^{M} Q(\frac{\Psi_i - \Psi_j^{(E)} - \epsilon}{\sigma}) - Q(\frac{\Psi_i - \Psi_j^{(E)} + \epsilon}{\sigma})d\Psi_j^{(E)}\right) \\ &= \sum_{j=1}^{N}\frac{1}{\Delta}\pi(j). \\ &\left(\int_{\Psi_{min}}^{\Psi_{max}} \sum_{i=1}^{M} Q(\frac{\Psi_i - \Psi^{(E)} - \epsilon}{\sigma}) - Q(\frac{\Psi_i - \Psi^{(E)} + \epsilon}{\sigma})d\Psi^{(E)}\right)\end{aligned} \tag{17}$$

where we have assumed that the unknown pathloss $\Psi_j \sim U(\Psi_{min}, \Psi_{max})\ \forall j$, and $\Delta = \Psi_{max} - \Psi_{min}$.

Now, we investigate the authentication of the casted vote by identifying the transmitter identity using the ML-based approach. The error probability of miss-classified node $\mathcal{P}_{mc}$ resulting from Eq. 13 is given as:

$$\mathcal{P}_{mc} = \sum_{i=1}^{M}\mathcal{P}_{mc|i}.\pi(i) \tag{18}$$

where $\mathcal{P}_{mc|i}$ is the probability that the leader notice that the vote is cast by follower F_j but the vote is actually cast by follower F_i where $i \neq j$. For the hypothesis test above, $\mathcal{P}_{mc|i}$ is given as:

$$\mathcal{P}_{mc|i} = 1 - \left(Q(\frac{\tilde{\Psi}_{l,i} - \tilde{\Psi}_i}{\sigma}) - Q(\frac{\tilde{\Psi}_{u,i} - \tilde{\Psi}_i}{\sigma})\right) \tag{19}$$

where $\tilde{\Psi}_{l,i} = \frac{\tilde{\Psi}_{i-1}+\tilde{\Psi}_i}{2}$, $\tilde{\Psi}_{u,i} = \frac{\tilde{\Psi}_i+\tilde{\Psi}_{i+1}}{2}$. Additionally, $\tilde{\mathbf{\Psi}} = \{\tilde{\Psi}_1, ..., \tilde{\Psi}_M\} = \text{sort}(\mathbf{\Psi})$ where sort operation (.) sorts a vector in an increasing order. For the boundary cases, e.g., $i = 1, i = M$, $\tilde{\Psi}_{l,1} = \Psi_{min}$, $\tilde{\Psi}_{l,M} = \Psi_{max}$ respectively. Note that the proposed mechanism will be executed at the leader node, which becomes uplink transmission according to the discussion of Section IV. For the downlink, the mechanism will be executed at followers having a single ground truth of the leader node. In this case, we will have two error probabilities (i.e., false alarm and missed detection) with a kind of similar error expressions given above (i.e., except summation for N legitimate nodes). We omit the discussion of it for the sake of brevity.

The proposed feature-based authentication method to counter impersonation attacks is summarized as follows:

1) Training phase: The receive IoT learns the ground truth, i.e., the pathloss feature for all the transmit IoT nodes on a secure channel.

2) Testing phase: The receive IoT measures the pathloss for every incoming data packet and compares it against the ground truth by means of hypothesis testing in order to systematically accept/reject a received data packet.

VI. Results And Discussions

We use MATLAB $2019a$ for simulations. The important simulation parameters for generated figures are mentioned in TABLE I, unless otherwise stated.

Parameters	Configuration
P_L, P_F, P_j	30 dBm, 20 dBm, 10 dBm
Pathloss exponent α	3
ρ_F	$15/\pi(500)^2$
Area	$\pi(500m)^2$
M, N	5, 5

TABLE I
IMPORTANT SIMULATION PARAMETERS

A. Coverage probability performance of the IoT blockchain network under jamming attack

For the jamming attack, Monte-Carlo simulations are done whereby both legitimate and malicious nodes are deployed according to the PPP with ρ_F intensity for legitimate nodes, and ρ_J intensity for jammer/malicious nodes. The leader is placed at the origin.

Fig. 2 presents the joint coverage probability for the different SIR threshold values of β (in dB) and intensity of jammers ρ_J. We observe that the transaction success rate (i.e., $\mathcal{P}_c$) declines as the SIR threshold increases. Fig. 2 also reveals that increasing the jammer intensity severely degrades the transaction success rate.

Fig. 3 demonstrates the behavior of joint coverage probability against different radius values (i.e., effective area) of distributed jammers. Specifically, we set $\rho = \rho_J$, $z_1 = 0$ and vary z_2 from 0 to 300 by step of 20. We observe that the increase in the effective jamming area of jammers causes low SIR values that lower the transaction success rate. We can also see the degradation in the performance of success rate with an increase in the intensity of jammers ρ_J.

Fig. 4 presents the three computed coverage probabilities: UL, DL, and joint coverage probabilities against the jamming

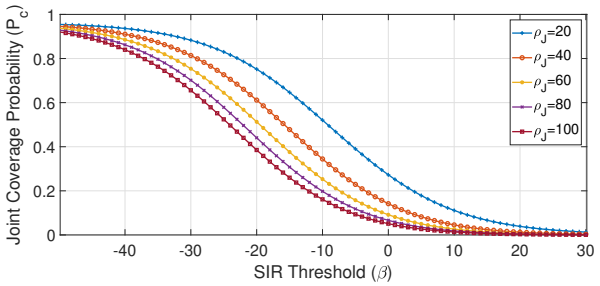


Fig. 2. Blockchain ransaction success probability vs SIR threshold β for different jammers densities

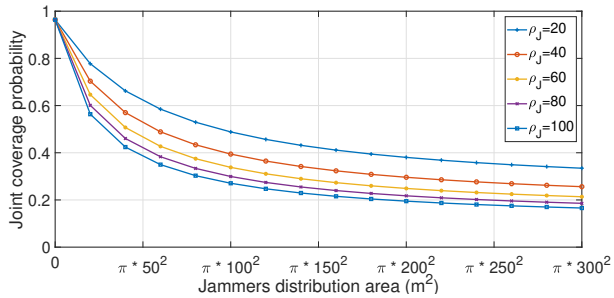


Fig. 3. Blockchain transaction success probability vs. jamming area

distance (i.e., z_1) from the origin or leader. We vary z_1 from $0m$ to $300m$ and keep $z_2 = z_1 + 50m$. In the upper two plots, the β varies from -30 dB to -20 dB from left to right, and from -10 dB to 0 dB in the lower two plots. We notice that the effective jamming area (or can be thought as jammers) moves away from the leader, making the interference lower at the leader and resulting in higher UL coverage probability. Followers are deployed in $\pi(500m)^2$ area, so moving of jamming distance from the origin produces low DL coverage probability as jammers are getting close to followers. On the other hand, joint coverage probability first enhances and then goes down. Note that we need coverage probabilities greater than 0.5 to achieve the consensus.

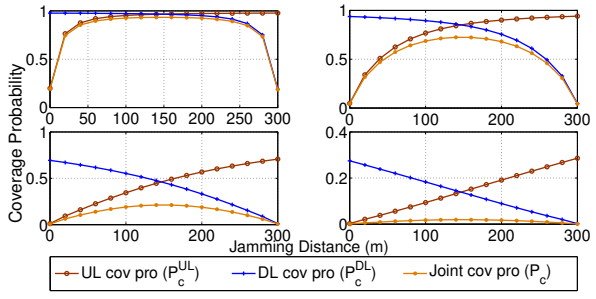


Fig. 4. Blockchain transaction success probability vs jamming distance

B. Authentication performance of the IoT blockchain network under impersonation attack

For impersonation attack analysis, we pick one realization of PPP for malicious and legitimate nodes where we have $M = N = 5$ number of malicious and legitimate nodes. We set the link quality as $LQ = 1/\sigma^2$, which means that more uncertainty in the estimation/noise implies poor link quality and vice versa. We plot the error probabilities (false alarm, missed detection, and miss classification) as functions of LQ (in dB) in Fig. 5. We observe from this figure that pathloss can be exploited to counter impersonation attacks in wireless blockchain networks. The design parameter ϵ can be set to achieve any desired level of security. We observe that we can not minimize both errors for a given link quality simultaneously. In other words, increasing ϵ improves false alarm but degrades missed detection. The lower plot of Fig. 5 shows the miss classification error against link quality and it demonstrates that it is not a function of ϵ, and that's why a single curve for all the three given choices of ϵ.

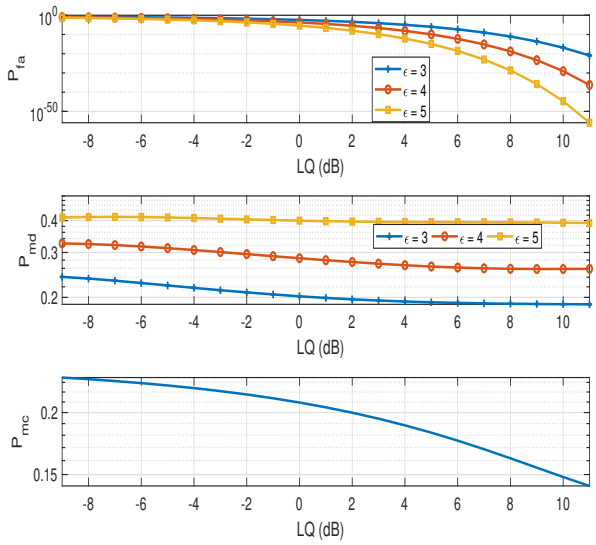


Fig. 5. Error Probabilities against $\boldsymbol{LQ}$. From top to bottom: Probability of false alarm $\boldsymbol{P_{fa}}$, probability of missed detection $\boldsymbol{P_{md}}$ and probability of misclassification $\boldsymbol{P_{mc}}$.

Fig. 6 shows the Receiver Operating Characteristic (ROC) curves comprises two error probabilities (P_d and P_{fa}). where $P_d = 1 - P_{md}$ is the detection probability is defined as the probability of correctly deciding malicious nodes. We sweep P_{fa} from zero to one and find P_{md} for different values of $1/\sigma^2$. As we can see improvements in link quality improves P_d. These curves can be used to set the system to the desired level of security where for a given link quality, one can find a value of false alarm for a desired value of detection.

VII. Conclusion

This paper studied active (jamming and impersonation) attacks on a RAFT-based IoT blockchain network. The impact of the jamming attack on the IoT blockchain network was evaluated via coverage probability analysis for both uplink and downlink IoT transmissions. On the other hand, the impersonation attack on the IoT blockchain network was countered by means of a novel, physical-layer method that exploited the pathloss of a transmit IoT node as its fingerprint to construct a binary hypothesis test for transmit node identification. To this end, closed-form expressions were

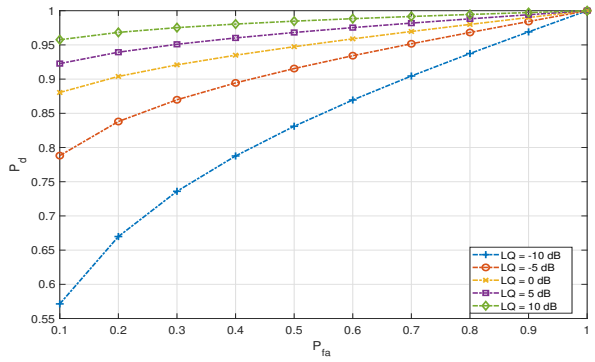


Fig. 6. Receiver Operating Characteristic (ROC) curves: the probability of detection $\boldsymbol{P_d}$ can be set to the desired level while compromising on probability of false alarm $\boldsymbol{P_{fa}}$

provided for the probabilities of false alarm, missed detection, and miss-classification. Simulation results showed that for the jamming attack, an increase in the threshold value reduces the coverage probability and high intensity of jammers produces low coverage probability, while for the impersonation attack, pathloss can be used as device fingerprint and above 95% of detection probability can be achieved with a minimum of 0.1 false alarm for a 10 dB link quality.

This work opens up many exciting directions for future work. For example, when the structure of the jamming signal is exactly known, it is possible to boost blockchain transaction success probability further (for a given power of the jamming signal) by doing partial recovery of the data using power-domain non-orthogonal multiple access plus successive interference cancellation method [47]. Another promising direction is to utilize frequency-hopping spread spectrum techniques to dynamically switch between different frequency channels in order to make wireless blockchain networks more resilient to jamming attacks.

APPENDIX

The Laplace transform of interference I_J is defined as:

$$\mathcal{L}_{I_J}(s) = \mathbb{E}_{I_J}\Big[\exp(-sI_J)\Big], \tag{20}$$

$$\mathcal{L}_{I_J}(s) = \mathbb{E}_{\phi_j,\{|h_j|^2\}}\Big[\exp\Big(-s\sum_{j\in\phi_J} P_j|h_j|^2\|\mathbf{X}_j\|^{-\alpha}\Big)\Big]. \tag{21}$$

Next, we use the property of the exponential function that the sum of exponential powers is the product of exponentials and put the value of s back in the above expression to get:

$$\mathcal{L}_{I_J}(s) = \mathbb{E}_{\phi_j,\{|h_j|^2\}}\Big[\prod_{j\in\phi_J} exp\Big(-|h_j|^2\Big(\frac{P_j}{P}\Big)\beta_D\|\mathbf{X}_j\|^{-\alpha}r^{\alpha}\Big)\Big]. \tag{22}$$

Let $\gamma_j = P_j/P$, as ϕ_j is independent with $|h_j|^2$ we can take one expectation (i.e., $\mathbb{E}_{\{|h_j|^2\}}$) inside, which is given below:

$$\mathcal{L}_{I_J}(s) = \mathbb{E}_{\phi_j}[\prod_{j\in\phi_J} \mathbb{E}_{\{|h_j|^2\}}[exp(-|h_j|^2\gamma_j\beta_D(\frac{\|\mathbf{X}_j\|}{r})^{-\alpha})]]. \tag{23}$$

Indeed, Eq. 23 is the Probability Generating FunctionaL (PGFL) of PPP, which can be expressed as:

$$\mathcal{L}_{I_J}(s) = \exp\Big(-\rho_J\mathcal{A}1 - \mathbb{E}_{|h|^2}[exp(-|h|^2\gamma_j\beta_D(\frac{\|\mathbf{x}\|}{r})^{-\alpha})]d\mathbf{x}\Big), \tag{24}$$

where ρ_J is the intensity of jammer nodes, $\mathcal{A}$ is the effective 2D area where jammers signals are prominent or can affect the transmissions. Now, converting x into polar form as $x = (r_j, \theta)$ (j subscript is used in order to differentiate it from the earlier used r (distance of follower)), we have:

$$\mathcal{L}_{I_J}(s) = \exp\Big(-2\pi\rho_J\int_{z_1}^{z_2}\Big(1 - \mathbb{E}_{|h|^2}[exp(-|h|^2\gamma_j\beta_D(\frac{r_j}{r})^{-\alpha})]\Big)r_j dr_j\Big), \tag{25}$$

which can be written as:

$$\mathcal{L}_{I_J}(s) = \exp\Big(-2\pi\rho_J\int_{z_1}^{z_2}\Big(1 - \frac{1}{1+\Big(\gamma_j\beta_D(\frac{r_j}{r})^{-\alpha}}\Big)r_j dr_j\Big), \tag{26}$$

which can be further simplified as

$$\mathcal{L}_{I_J}(s) = \exp\Big(-2\pi\rho_J\int_{z_1}^{z_2}\Big(\frac{1}{1+\Big((\gamma_j\beta_D)^{-1}(\frac{r_j}{r})^{\alpha}}\Big)r_j dr_j\Big), \tag{27}$$

where z_1 and z_2 constitute the effective attacking area of the jammers, s.t., $z_1 < z_2$, or the area from where jammers can significantly affect the transmissions. To make the expression elegant let $u = \Big(r_j/r(\gamma_j\beta_D)^{1/\alpha}\Big)^2$, $z_l = \Big(\frac{z_1}{r(\gamma_j\beta_D)^{1/\alpha}}\Big)^2$ and $z_u = \Big(\frac{z_2}{r(\gamma_j\beta_D)^{1/\alpha}}\Big)^2$, then the above expression can be written as:

$$\mathcal{L}_{I_J}(s) = \exp\Big(-\pi\rho_J r^2(\gamma_j\beta_D)^{2/\alpha}\int_{z_l}^{z_u}\frac{1}{1+(u^{\alpha/2})}du\Big). \tag{28}$$

Integral is computed via Gauss-hypergeometric approximation, given as:

$$\mathcal{L}_{I_J}(s) = \exp\Big(\frac{\pi\rho_J\gamma_j\beta_D r^{\alpha}}{(\alpha/2)-1}\Big(z_2^{(2-\alpha)}{}_2F_1(1,1-\frac{2}{\alpha},2-\frac{2}{\alpha},-\gamma_j\beta_D(\frac{r}{z_2})^{\alpha}) - z_1^{(2-\alpha)}{}_2F_1(1,1-\frac{2}{\alpha},2-\frac{2}{\alpha},-\gamma_j\beta_D(\frac{r}{z_1})^{\alpha})\Big)\Big). \tag{29}$$

REFERENCES

[1] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019.

[2] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain." *Journal of Info. process. systems*, vol. 14, no. 1, 2018.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." [online]. Available: http://www.bitcoin.org/bitcoin.pdf.

[4] P. Vasin, "Blackcoin's proof-of-stake protocol v2," *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, vol. 71, 2014.

[5] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, no. 1999, 1999, pp. 173–186.

[6] L. Lamport, "The part-time parliament," in *Concurrency: the Works of Leslie Lamport*, 2019, pp. 277–317.

[7] 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.

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

[9] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5g and beyond networks: A state of the art survey," *arXiv preprint arXiv:1912.05062*, 2019.

[10] X. Li, P. Russell, C. Mladin, and C. Wang, "Blockchain-enabled applications in next-generation wireless systems: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 86–95, 2021.

[11] 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.

[12] W. Liu, B. Cao, L. Zhang, M. Peng, and M. Daneshmand, "A distributed game theoretic approach for blockchain-based offloading strategy," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[13] J. Zhuz, Y. Sun, L. Zhang, B. Cao, G. Feng, and M. A. Imran, "Blockchain-enabled wireless iot networks with multiple communication connections," in *ICC 2020-2020 IEEE Intl. Conf. on Commun. (ICC)*. IEEE, 2020, pp. 1–6.

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

[15] L. Liu, W. Liang, G. Mang, and Z. Dong, "Blockchain based spectrum sharing over 6g hybrid cloud," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 2021, pp. 492–497.

[16] X. Zhang, W. Xia, X. Wang, J. Liu, Q. Cui, X. Tao, and R. P. Liu, "The block propagation in blockchain-based vehicular networks," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[17] L. Hou, X. Xu, K. Zheng, and X. Wang, "An intelligent transaction migration scheme for raft-based private blockchain in internet of things applications," *IEEE Commun. Lett.*, vol. 25, no. 8, pp. 2753–2757, 2021.

[18] Y. Li, B. Cao, L. Liang, D. Mao, and L. Zhang, "Block access control in wireless blockchain network: Design, modeling and analysis," *IEEE Trans. on Veh. Technol.*, pp. 1–1, 2021.

[19] H. Xu, L. Zhang, Y. Sun, and C.-L. I, "Be-ran: Blockchain-enabled open ran with decentralized identity management and privacy-preserving communication," 2021.

[20] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[21] H. Xu, L. Zhang, Y. Liu, and B. Cao, "Raft based wireless blockchain networks in the presence of malicious jamming," *IEEE Wireless Commun. Letters*, vol. 9, no. 6, pp. 817–821, 2020.

[22] N. Waheed et. al., "Security and privacy in iot using machine learning and blockchain: Threats and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 53, no. 6, pp. 1–37, 2020.

[23] E. M. Ghourab et. al., "Interplay between physical layer security and blockchain technology for 5g and beyond: A comprehensive survey," 2023.

[24] A. K. Yadav, K. Singh, A. H. Amin, L. Almutairi, T. R. Alsenani, and A. Ahmadian, "A comparative study on consensus mechanism with security threats and future scopes: Blockchain," *Computer Commun.*, vol. 201, pp. 102–115, 2023.

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

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

[27] S. Agrawal and S. Kumar, "Mlsmbqs: Design of a machine learning based split & merge blockchain model for qos-aware secure iot deployments."

[28] X. Xu, L. Hou, Y. Li, and Y. Geng, "Weighted raft: An improved blockchain consensus mechanism for internet of things application," in *2021 7th Intl. Conf. on Computer and Commun. (ICCC)*. IEEE, 2021, pp. 1520–1525.

[29] X. Wang and Y. Guan, "A hierarchy byzantine fault tolerance consensus protocol based on node reputation," *Sensors*, vol. 22, no. 15, p. 5887, 2022.

[30] Y. Zhu, G. Zheng, and K.-K. Wong, "Blockchain-empowered decentralized storage in air-to-ground industrial networks," *IEEE Trans. on Industrial Informatics*, vol. 15, no. 6, pp. 3593–3601, 2019.

[31] Q. Liu, Y. Xu, B. Cao, L. Zhang, and M. Peng, "Unintentional forking analysis in wireless blockchain networks," *Digital Commun. and Networks*, vol. 7, no. 3, pp. 335–341, 2021.

[32] D. K. Kamel, "Wireless iot with blockchain-enabled technology amidst attacks," *IRO Journal on Sustainable Wireless Systems*, vol. 2, no. 3, pp. 133–137, 2021.

[33] B. Mbarek, M. Ge, and T. Pitner, "An adaptive anti-jamming system in hyperledger-based wireless sensor networks," *Wireless Networks*, vol. 28, no. 2, pp. 691–703, 2022.

[34] W. Aman, S. Al-Kuwari, M. Muzzammil, M. M. U. Rahman, and A. Kumar, "Security of underwater and air–water wireless communication: State-of-the-art, challenges and outlook," *Ad Hoc Networks*, vol. 142, p. 103114, 2023.

[35] W. Aman, M. M. U. Rahman, J. Qadir, H. Pervaiz, and Q. Ni, "Impersonation detection in line-of-sight underwater acoustic sensor networks," *IEEE Access*, vol. 6, pp. 44 459–44 472, Aug. 2018.

[36] W. Aman, Z. Haider, S. W. H. Shah, M. M. U. Rahman, and O. A. Dobre, "On the effective capacity of an underwater acoustic channel under impersonation attack," 2020.

[37] M. M. U. Rahman, Q. H. Abbasi, N. Chopra, K. Qaraqe, and A. Alomainy, "Physical layer authentication in nano networks at terahertz frequencies for biomedical applications," *IEEE Access*, vol. 5, pp. 7808–7815, 2017.

[38] A. Mahmood, W. Aman, M. O. Iqbal, M. M. U. Rahman, and Q. H. Abbasi, "Channel impulse response-based distributed physical layer authentication," in *Proc. IEEE VTC*, Jun. 2017, pp. 1–5.

[39] S. Zafar, W. Aman, M. M. U. Rahman, A. Alomainy, and Q. H. Abbasi, "Channel impulse response-based physical layer authentication in a diffusion-based molecular communication system," in *2019 UK/ China Emerging Technol. (UCET)*, 2019, pp. 1–2.

[40] A. Mehmood, W. Aman, M. M. U. Rahman, M. A. Imran, and Q. H. Abbasi, "Preventing identity attacks in rfid backscatter communication systems: A physical-layer approach," in *2020 Intl. Conf. on UK-China Emerging Technologies (UCET)*, 2020, pp. 1–5.

[41] M. M. U. Rahman, A. Yasmeen, and Q. H. Abbasi, "Exploiting lack of hardware reciprocity for sender-node authentication at the phy layer," in *2017 IEEE 85th Veh. Tech. Conf. (VTC Spring)*. IEEE, 2017, pp. 1–5.

[42] M. M. U. Rahman, A. Yasmeen, and J. Gross, "Phy layer authentication via drifting oscillators," in *2014 IEEE Global Commun. Conf.* IEEE, 2014, pp. 716–721.

[43] X. Lu, M. Salehi, M. Haenggi, E. Hossain, and H. Jiang, "Stochastic geometry analysis of spatial-temporal performance in wireless networks: A tutorial," *IEEE Commun. Surveys & Tut.*, vol. 23, no. 4, pp. 2753–2801, 2021.

[44] A. M. Mathai, "An introduction to geometrical probability: Distributional aspects with applications," 1999.

[45] K. Yang, P. Wang, X. Hong, and X. Zhang, "Joint downlink and uplink network performance analysis with cre in heterogeneous wireless network," in *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2015, pp. 1659–1663.

[46] Q. Yan and R. Blum, "Distributed signal detection under the neyman-pearson criterion," *IEEE Trans. on Info. Theory*, vol. 47, no. 4, pp. 1368–1377, 2001.

[47] A. Ijaz, M. M. U. Rahman, and O. A. Dobre, "On safeguarding visible light communication systems against attacks by active adversaries," *IEEE photonics tech. letters*, vol. 32, no. 1, pp. 11–14, 2019.