Towards a Trusted and Cryptocurrency-Enabled Decentralized Wireless Community Network

PaperID: 348

***Abstract*—In the context of the telecom network trending towards centralization, a relatively decentralized and citizen-centric, non-profit network architecture known as a Wireless Community Network (WCN) has emerged. However, WCN faces challenges related to unintentional shifts towards centralization, the lack of automation and verifiability to handle increasing volumes of information, and the absence of real-time and more flexible incentive mechanisms to incentivize a diverse range of contributors based on the quality of their contributions. As the network expands, maintenance becomes more challenging for small volunteer teams, potentially compromising network performance, reliability, and overall trustworthiness. With the development of decentralized physical infrastructure network (DePIN), this paper proposes a decentralized wireless community network (DeWCN) system, designing a governance platform, presenting incentive-driven oracle design methodologies for verifiable common resource pools, and proposing additional network tools to enhance functionality and efficiency. Our work contributes to the DePIN domain, specifically addressing the mesh network direction within the telecom sector and eliminating the need for specialized devices.**

***Index Terms*—Decentralized Wireless Network, DePIN, Community Network, Blockchain**

I. Introduction

With the declining costs of consumer wireless equipment, the deployment of non-centralized, non-profit, self-managed, and collaborative Internet Service Providers (ISPs) at local or regional levels emerges as a viable grassroots initiative. This development is epitomized by the Wireless Community Network (WCN), which stands as a compelling alternative to the monopolistic dominance of wired metropolitan networks. WCN's primary objectives encompass the reduction of Internet expenses, the expansion of network accessibility, and the promotion of network neutrality, thereby challenging conventional network paradigms and offering a more inclusive and equitable online environment.

However, WCNs often experience unintentional centralization shifts, which affect various aspects of network operation and management. Firstly, the technical maintenance of networks increasingly depends on a subset of technically adept members, prompting a move towards centralization in technical governance [1]. Similarly, the implementation of economic models within these networks shows a propensity for centralization [2]. The distribution of data exchange workloads also exhibits central tendencies, with edge nodes bearing significantly different burdens compared to central nodes [3]. To boost network performance, the integration of backbone links and the introduction of supernodes are common strategies, further evidencing infrastructure centralization [4]. Moreover, the necessity for networks to acquire traffic from external ISPs showcases a centralization in traffic management [5]. As networks expand, maintenance becomes harder for small volunteer teams, potentially compromising network performance, reliability, and the overall trust in the WCN.

Moreover, WCNs encounter governance and management challenges necessitating automation and verifiability to ensure seamless operations amidst rising information volumes. A diverse array of contributors provides various assets, including upstream bandwidth, router devices, and resources for intelligent applications. To foster sustainable growth, incentivizing these contributors based on the quality of their contributions is paramount [1].

The emergence of decentralized physical infrastructure networks (DePIN) represents a pivotal shift in the Web3 and blockchain domains, aiming to revolutionize traditional IoT business models. By integrating blockchain, IoT, and tokenomics, DePIN offers a decentralized approach to building IoT networks and applications, promising efficiency and cost-effectiveness [6]. DePIN leverages cryptocurrency and smart contracts for governance and sustainability, enabling community-driven networks. Adapting the design philosophy of DePINs to WCNs can address the aforementioned issues. However, in the telecom sector, numerous DePIN projects focus on technologies like WiFi, 5G, and Bluetooth, which require specialized equipment for network maintenance and do not involve multi-hop message transmission, such as the Helium Network [7]. A DePIN solution specifically tailored for mesh networks like WCNs is conspicuously absent.

In this paper, we introduce the concept of a Decentralized Wireless Community Network (DeWCN) and extend the work presented in [8] inspired by the development of DePIN. Our methodology operates at the application layer of the OSI model, ensuring compatibility with diverse wireless devices and routing protocols employed in WCNs. This compatibility eliminates the necessity for specialized equipment and facilitates seamless deployment on existing infrastructures. Our primary contributions encompass:

- We explore the three fundamental considerations for constructing DePINs for wireless community networks, as outlined by [9].
- We design a governance platform for DeWCNs, utilizing the Raft consensus algorithm [10], and investigate potential Byzantine faults that impact the platform.
- We present oracle design methodologies for DeWCNs and outline two specific oracles for verifiable common resource pool.

- We propose additional network tools, such as a cross-chain bridge, auction manager, and state channel network manager, to enhance the network's efficiency.

Organization: §II presents the design paradigm of DeWCN. §III designs a governance platform. §IV outlines the methodology for designing oracles. §V introduces network tool design. §VI evaluates our method on a specific network. §VII conclusion and future work.

II. DeWCN Design Paradigm

A. Network Structure

We base our network structure model on Guifi.net[1], the world's largest WCN, as shown in Fig. 1.

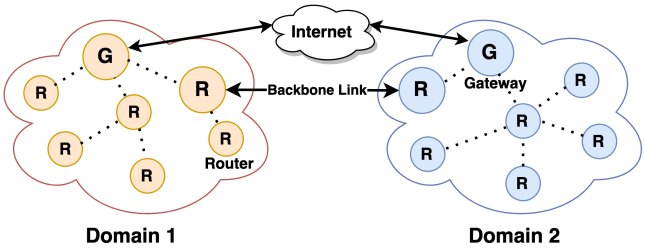

Fig. 1. Network Structure of DeWCN

This model facilitates network growth by allowing new participants to extend coverage through rooftop router installations. Dynamic routing protocols like OSPF enable the network to adapt and expand. We model the network as consisting of multiple domains, each hosting diverse devices. These domains connect via directional links, such as parabolic antennas and fiber optics, with backbone nodes ensuring robust inter-domain links. Within domains, connectivity relies on semi-directional and omni-directional antennas.

B. Considerations for Developing DeWCN [9]

1) Hardware Considerations: Our system is designed to seamlessly integrate with existing WCNs, using current network devices and layout to significantly improve manageability, automation, and incentives in the sharing economy. It eliminates the necessity for custom routing hardware but requires routers capable of running OpenWRT[2]. The initial setup involves both hardware installation, such as deploying antennas, and software installation, like installing our designed system, with all subsequent processes being passive and automated. As the network infrastructure of WCNs is already established, there's no need to tackle cold-start issues through incentives. We transition away from traditional token systems, preferring a model where real-time incentives are generated via direct payments from service users to the network.

2) Threshold-Scale Considerations: Our system benefits from the long-range capabilities of wireless transmission, making it location-insensitive. As local demand increases, new router resources emerge in under-covered areas. While network density is crucial for ensuring continuous coverage in WCNs, our system requires a higher density of network nodes compared to typical WCN requirements. By utilizing the broadcast nature of wireless communication and requiring nodes to connect using semi/omni-directional antennas, our network enables the sensing of nearby nodes' positions, resource contributions, latency, and other factors. This setup is designed to collectively observe the behavior of nodes within a specific area, with the purpose of constructing an oracle and delivering reliable parameters to upper-level applications.

3) Demand Generation Considerations: From the perspective of bandwidth sharing, WCNs demonstrate a natural resource-sharing relationship that includes both upstream and downstream connections. Each node plays the role of identifying resource providers and recipients. In our system, bandwidth sales take place at a local level, where every node acts as an independent seller of network resources. This decentralized approach enables resource seekers to choose access points based on factors such as network conditions and pricing. As a result, there is a direct flow of value from the demand for resources to their supply.

C. System Overview

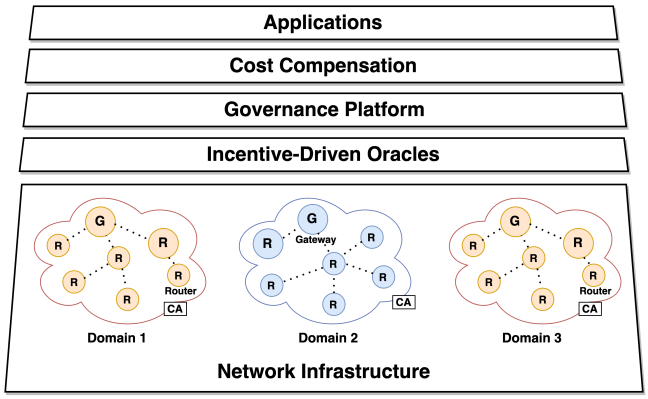

Fig. 2. DeWCN Overview

The Overview of the DeWCN, as depicted in Fig. 2, involves deploying a governance platform based on existing WCN infrastructure. The oracle executes on the platform to manage the inflow and outflow of resources in the common resource pool and provide trusted parameters for upper layers. We introduce a series of management tools to enhance network efficiency and expand its functionality. User-customized applications are deployed atop the entire system, shielding users from the internal details within the system.

D. Desired Properties of the System

1) Desired Properties of Governance Platform: A trusted governance platform should have the following properties:

- Timely Response: Legitimate transactions are executed within a set timeframe.
- Consistency: Governance nodes achieve consensus on transaction content, sequence, and results.
- Fault Tolerance: The system tolerates crash faults and is Byzantine fault tolerant.

[1]https://guifi.net/
[2]https://openwrt.org/

- Parameter Trustworthiness: Inputs accurately represent the network's real state, preventing fabrication.
- Result Verifiability: Nodes can verify governance outcomes based on inputs and gavernance rules.

2) Desired Properties of Oracle:

- Resource Efficiency: The oracle uploads real data in a trustworthy manner without significantly impacting network performance, including minimizing network load.
- Multiple Witnesses: Community members collectively witness events on the oracle.
- Incentive Compatibility: Oracle data is obtained through nodes' strategic interactions, encouraging truth-telling as the optimal strategy for participants.

III. Governance Platform

A. Overview

We achieve a balance between decentralization and centralization by partitioning the network into regions. Through social consensus, representatives are chosen from each network partition to form a governance group. This group collectively operates consensus protocols, state machines, and persists consensus data to maintain a trusted governance platform and implement global rules that cover aspects like trust management and cost compensation. Each representative node is responsible for executing their region's regional rules, including access authorization, load balancing, and aggregating information to propose new proposal.

B. Network Partition

In DeWCN, involving every node in governance is impractical due to the network's dynamic and distributed nature. We propose a partitioning strategy that leverages node connectivity and geographical proximity, utilizing the k-means clustering algorithm alongside a novel distance metric D:

$$D_{ij} = \frac{d(i,j)}{1 + \gamma \cdot A_{ij}} \tag{1}$$

where $A_{ij} = 1$ signifies an adjacency relationship between nodes i and j, and a normalized Euclidean distance $d(i,j)$ is used to account for physical proximity. Here, γ is a positive adjustment parameter used to modulate the impact of adjacency on the distance measure.

By applying k-means clustering with this distance metric, we can effectively partition the DeWCN into clusters, thereby facilitating easier management and enhancing the network's efficiency.

C. Trust and Reputation System

The dynamically evolving WCN network requires continuous adjustments to the consensus group and monitoring of network anomalies and node attacks. We incorporate a trust and reputation system to assess risks and provide a basis for node decision-making. Trust is a subjective assessment of a node's behavior, based on its historical interactions and independently calculated by each node. In contrast, reputation represents a collective assessment of a node's past behavior. It is calculated transparently through smart contracts, aggregating trust evaluations from other nodes.

Governance rules and application rules determine the evaluation set E, representing all interactions eligible for trust and reputation assessment. Reputation values include governance group reputation and regional reputations, with the scopes of evaluation chosen as subsets $E_g, E_r \subseteq E$ respectively. Trust values are local, selected by each node i from the subset $E_i \subseteq E$ on their own.

For each node $i, j \in N_{\text{peers}}$, where nodes can be routers, user devices, etc., the trust value of node j by node i, denoted as $T_{i,j}$ with a default value of 0, is derived from their past interactions, which may be either positive or negative. We refer to the formula from [11]. The ageing function for the n-th interaction I_n of nodes i and j is formulated as:

$$I_{i,j}^n = \sum_{k=1}^{n} \gamma^{n-k} I(e_{i,j}^k) \omega_i(e_{i,j}^k) \delta_{i,j}^k, e_{i,j}^k \in E \tag{2}$$

$$I(e_{i,j}) = \begin{cases} 1, & \text{if } e_{i,j} \in E_{T_i} \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

$$\delta_{i,j} = \begin{cases} \delta_{\text{pos}}, & \text{if positive interaction} \\ \delta_{\text{neg}}, & \text{otherwise} \end{cases} \tag{4}$$

where $\gamma^{n-k} \in (0,1)$ represents the ageing factor, $0 < \delta_{\text{pos}} < -\delta_{\text{neg}}$ indicates the asymmetry between positive and negative interactions, and $\omega_i(e_{i,j}^k) \in (0,1)$ represents the importance for node i to interaction $e_{i,j}^k$. Finally, the output of Eq. 1 is limited to the trust value from 0 to 1:

$$T_{i,j} = a e^{-b e^{-c I_{i,j}^n}}, \quad a, b, c \in \mathbb{R} \tag{5}$$

Reputation is an aggregation of trust. We divide time into logical intervals of Δ_T, starting from 0. In each Δ_T, node i evaluates its interactions with j over the past Δ_T to determine if they were positive, and then sends a message to system:

$$TX_{\text{rep}} = [j | \delta_{i,j,t} | Sig_i] \tag{6}$$

The reputation value of j is updated every Δ_T using the formula:

$$Rep_{j,n} = \sum_{t=1}^{n} \gamma^{n-t} \sum_{i=0}^{N_t} \delta_{i,j,t} \ln(N_t) \tag{7}$$

where N_t is the number of nodes evaluating the trust of node j in the t-th interval Δ_T.

Additionally, to elect nodes with higher stability in consensus member elections, we introduce the concept of stability reputation. Similar to reputation, it involves periodic transmission of the following message:

$$TX_{\text{stb}} = [j | \sigma_{i,j,t} | Sig_i] \tag{8}$$

$$\sigma_{i,j,t} = \begin{cases} \sigma_{\text{pos}}, & \text{if stable} \\ \sigma_{\text{neg}}, & \text{otherwise} \end{cases} \tag{9}$$

The stability reputation value of j is updated every Δ_T using the formula:

$$Stb_{j,n} = \sum_{t=1}^{n} \mu^{n-t} \sum_{i=0}^{N_t} \sigma_{i,j,t} \ln(N_t) \tag{10}$$

where $\mu^{n-t} \in (0,1)$ and $0 < \sigma_{\text{pos}} < -\sigma_{\text{neg}}$.

D. Consensus Algorithm

The consensus algorithm is key to our governance platform, ensuring execution of committed transactions by the state machine. We selected Raft as our base algorithm after comparing the communication efficiencies of Byzantine Fault Tolerance (BFT) and Crash Fault Tolerance (CFT) algorithms. Despite this, challenges like malicious behavior and performance issues can impact its effectiveness. Assuming the consensus group experiences only crash faults, we will explore bridging the gap between CFT and BFT in a later section. We modify Raft's leader election to a two-phase mechanism.

1) Consensus Member Election: When the current consensus member of a specific domain exceed the timeout period, the system automatically initiates a new member election. The system first employs a top-k algorithm to identify the k nodes with the highest stability reputation, forming a candidate node set C. Subsequently, selects node i with a probability given by

$$Prob_i = \frac{\text{Rep}_i}{\sum_{j \in C} \text{Rep}_i} \tag{11}$$

Then, the membership change is executed.

2) Leader Election: Whenever a consensus node's stability reputation is updated and it identifies itself as having the highest value, it adjusts its election timeout to $10n$ms, $n > 0$. If it no longer holds the highest value, the node randomly selects an election timeout within the range of $10n$–$20n$ms. The heartbeat timeout is $n$ms. Upon transitioning to the candidate state and issuing a RequestVoteRPC, a node is granted a vote only if *votedFor* is null or *candidateId*, and the candidate's log and stability reputation are at least as current as the receiver's log and stability reputation. This mechanism ensures that nodes with greater stability have a higher probability of being elected.

E. Bridging Cryptocurrency with DeWCN

We introduce a cross-chain bridge between Conflux Network [12] and the consensus group, allowing nodes to stake tokens in the Conflux cross-chain bridge contract for use in DeWCN. The consensus group maintains balance in the cross-chain bridge via multi-signature signing. However, external factors like power outages can hinder the consensus process from reaching a quorum or cause domain partitioning. Despite this, even in the absence of formal consensus, each partition with its independent resource supply nodes can function as an independent sub-network. To address this, we introduce the state channel network to enable transaction facilitation through frequent small-scale trades during temporary partitions.

1) State Channel Network: Within each domain, nodes establish state channels on Conflux as an alternative payment solution. With the goal of reducing deposits and transaction fees, a state channel network is constructed, with the domain leader serving as the hub.

2) Cross Chain bridge: We design a cross chain bridge, with Conflux serving as the source and DeWCN as the destination. We achieve a two-way peg between the platforms through a $\lceil \frac{2}{3}n \rceil$-to-$n$ multi-signature wallet. Upon a node's deposit into the cross-chain bridge contract on Conflux, DeWCNs mints an equivalent quantity of token for the node. To initiate a withdrawal, node i generates $TX_{\text{wd}} = [i|amount|Sig_i]$, requiring signatures from at least $\lceil \frac{2}{3}n \rceil$ consensus members, resulting in $TX_{\text{confirm}} = [TX_{\text{wd}}|Sigs|SigOrder]$, where

$$Sigs = [hash(TX_{\text{wd}})|Sig_{i_1}|Sig_{i_2}|...|Sig_{i_{\lceil \frac{2}{3}n \rceil}}] \tag{12}$$

$$SigOrder = [i_1, i_2, ..., i_{\lceil \frac{2}{3}n \rceil}] \tag{13}$$

3) Switch Between Networks: When network communication becomes unreliable or untrusted, nodes can mutually agree to terminate ongoing transactions via signatures and shift towards micropayment transactions through state channels. They then send a message to the domain leader to vote for temporarily disconnecting from DeWCN, $TX_{\text{transform}} = [i|\text{StateChannel}|Sig_i]$. Once it receives votes from at least $\lceil \frac{2}{3}n \rceil$ nodes, the domain operates independently from DeWCN. If nodes deem that network trust is regained, another round of voting can occur to revert to DeWCN, via $TX_{\text{transform}} = [i|\text{DeWCN}|Sig_i]$. Each domain node independently decides whether to send $TX_{\text{transform}}$ based on private and common information.

F. Enhancing Raft with BFT

We categorize potential Byzantine behaviors that can impact the Raft consensus algorithm in our system into two types: external Byzantine behaviors originating from outside the consensus group, which include tampering, forgery, and selective forwarding by an outside node; and internal Byzantine behaviors involving members within the consensus group.

1) Algorithmic Solution: Tangaroa [13] is a Byzantine Fault Tolerant variant of the Raft consensus algorithm that discusses how Byzantine behaviors can break Raft, which can serve as guidance for solving internal Byzantine behaviors. By implementing additional measures, such as ensuring that each consensus node has independent internet connectivity, we can ensure the reachability of information between nodes, thereby avoiding external influences.

2) Deployment Strategy: By introducing Raft management nodes supervised by consensus groups into the network, the permissions of all running devices belonging to consensus group members are transferred to the Raft management nodes. Consensus members no longer have the authority to operate the devices and are only permitted to experience crash faults.

3) Introduce of Trusted Hardware: Engraft [14] proposes a design paradigm that combines CFT protocols with Trusted Execution Environments (TEEs), like Intel SGX, to create a secure and efficient BFT consensus system, which is another solution worth considering.

IV. Incentive-Driven Oracle

A. Overview

Oracles serve as intermediaries between the real world and DeWCN, categorized into two primary types:

- **Common Resource Pool (CRP) Oracle:** Enables validation of resource utilization or contribution by nodes.
- **Behavior Oracle:** Provides reliable parameters for governance mechanisms and other applications.

This section outlines two specific algorithms for the CRP oracle and the methodology for designing behavior oracle.

B. CRP Oracle: Bandwidth

Proof of Traffic (PoT) [15] is a three-stage voting game paired with an incentive mechanism, involving a pair of traffic provider and consumer, along with witnesses. These witnesses, situated geographically close to the participants and leveraging the nature of wireless transmission, can attest to the volume of data exchanged between them.

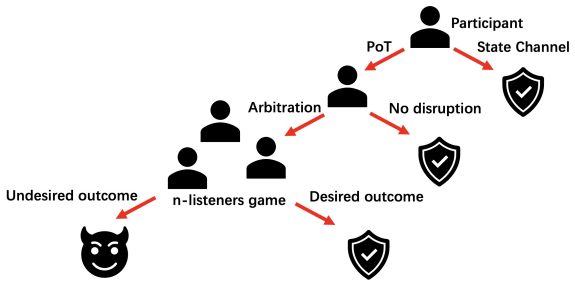

Fig. 3. The process of the PoT Mechanism

The process, illustrated in Fig. 3, initiates witness voting only when both the traffic provider and consumer agree to participate in PoT and if there is dishonesty from either side. The incentive mechanism ensures that all witnesses act honestly, maximizing their expected benefits, making it challenging for the dishonest party to prevail. Implementing PoT within DeWCN enables the verification of each node's traffic contributions or usage, providing trustworthy data for cost compensation mechanisms.

C. CRP Oracle: GPU Resource

Consumer i purchases resources from GPU provider j for training a deep learning model, using initial weights W_0, training set T, and validation set V. Applying the Directed Guiding Gradients method [16], the consumer sets a difficulty level R. Payments are made upon achieving each difficulty level R. Before starting, both consumer and provider sign an agreement detailing the transaction and submit TX_{task} to the platform for any future arbitration needs.

$$TX_{\text{task}} = [i|j|hash(W_0, T, V)|R|Sig_i|Sig_j] \quad (14)$$

Upon meeting a difficulty requirement, provider sends the updated weights W_k to consumer. If consumer verifies and approves W_k, they sign to confirm completion of that training round. Disputes are resolved by sending the full model weights and datasets to the consensus group for arbitration.

D. Behavior Oracle: Methodology

In DeWCN, user experience is significantly influenced by factors like node latency, bandwidth, jitter, and disconnection rates, as well as attributes such as location and connectivity, which, while crucial, do not directly pertain to the CRP. We define the oracle that can capture these parameters as the behavior oracle, and propose the following design approach. Leveraging the proximity of nodes, each node can sense information from nearby nodes. To determine the parameters of a node, the neighboring nodes collectively witness and report behaviors to the platform through a gamified process.

V. Network Tools

A. State Channel Network Manager

In general scenarios, the state channel network manager optimizes transaction paths. Given the interconnected nodes in WCN, the manager also has the capability to open and close state channels. It finds optimal paths to reduce costs and delays, thereby improving efficiency, and can instruct nodes to open new channels or close underused ones, optimizing resources.

B. Auction Manager

To address the issue of resource allocation in response to changes in supply and demand, there are two approaches that can be used: reverse auction and forward auction. Taking forward auction as an example, when a node serves two downstream nodes simultaneously and resources are scarce, the node can determine the resource allocation through an auction, such as a second-price auction. The auction manager initiates a second-price auction on the platform, waits for participants to make bids, and finally reveals the bids to determine the winner.

VI. Evaluations: GuifiSants Network

GuifiSants[3] is part of Guifi.net. We utilize topology data from publicly available datasets [17] to validate some of the proposed methods.

A. Network Partition Evaluation

We utilize relative distances for clustering, with the results shown in Fig. 4. We opt for $k = 3$, resulting in three partitions. Each area conducts independent elections to select consensus members, resulting in three members. These members then collectively elect a consensus leader.

[3]http://sants.guifi.net/

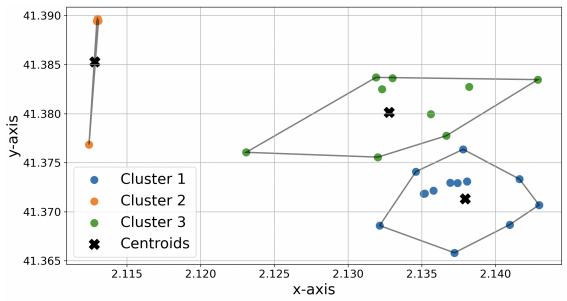

Fig. 4. The result of k-means clustering

B. Reputation Evaluation

To observe reputation growth trends within a domain, we simulate node behavior and calculate its reputation value using Eq. 7 with varying N_{peers}. The strategy for nodes involved initially engaging in positive interactions with others, followed by negative interactions, and ultimately colluding with a third of the nodes to artificially inflate scores. We introduce $\delta_{\text{pos}} = 15$, $\delta_{\text{neg}} = -0.8$ and $\gamma = 0.9$, Fig. 5 shows the results.

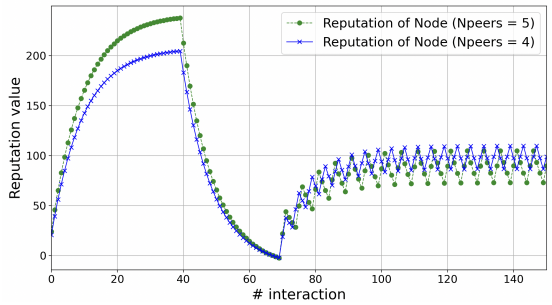

Fig. 5. The evaluation of reputation value

The results indicate that nodes' reputation increases follow logarithmic growth during positive interactions. However, due to the negative interactions among nodes, the reputation values experience a sharp decline. Furthermore, it is observed that even collusion with other nodes is not enough to restore the reputation. These findings highlight the effectiveness of our system in combating manipulative behaviors.

C. Leader Election Evaluation

We deploy a ETCD[4] cluster with three nodes on AWS EC2 and conduct 1000 tests of the modified leader election with $n = 100$. The results indicate that approximately 98% of the elected nodes have the highest value of stable reputation. demonstrating that our method maximizes the chances of electing stable nodes.

VII. Conclusion and Future Work

In this work, we design a DePIN solution called DeWCN for wireless community networks, following the DePIN approach. We design a distributed governance platform for transaction execution, introduce oracles for uploading trusted data to the platform, and propose deployment strategies for the platform. Additionally, we present various network tools that complement the DeWCN system. Moreover, we identify limitations in developing the platform based on the Raft consensus algorithm and provide suggestions for improvement. Our work significantly contributes to the DePIN domain, specifically addressing the mesh network direction within the telecom sector.

It is important to note that this work primarily focuses on the preliminary design of DeWCN. Future plans include refining the system architecture, designing oracles and governance protocols, and developing an open-source DeWCN application.

[4]https://github.com/etcd-io/etcd/

References

[1] Gabriele Gemmi, Llorenç Cerdà-Alabern, Leandro Navarro, and Leonardo Maccari. Toward smart community networks. *IEEE Network*, 37(2):128–134, 2023.

[2] Roger Baig, Lluís Dalmau, Ramon Roca, Leandro Navarro, Felix Freitag, and Arjuna Sathiaseelan. Making community networks economically sustainable, the guifi. net experience. In *Proceedings of the 2016 workshop on Global Access to the Internet for All*, pages 31–36, 2016.

[3] Leonardo Maccari and Renato Lo Cigno. A week in the life of three large wireless community networks. *Ad Hoc Networks*, 24:175–190, 2015.

[4] Davide Vega, Roger Baig, Llorenç Cerdà-Alabern, Esunly Medina, Roc Meseguer, and Leandro Navarro. A technological overview of the guifi. net community network. *Computer Networks*, 93:260–278, 2015.

[5] Primavera De Filippi and Félix Tréguer. Expanding the internet commons: The subversive potential of wireless community networks. *Journal of Peer Production, Issue*, (6), 2015.

[6] Xinxin Fan and Lei Xu. Towards a rollup-centric scalable architecture for decentralized physical infrastructure networks: A position paper. In *Proceedings of the Fifth ACM International Workshop on Blockchain-enabled Networked Sensor Systems*, pages 9–12, 2023.

[7] Amir Haleem, Andrew Allen, Andrew Thompson, Marc Nijdam, and Rahul Garg. A decentralized wireless network. *Helium Netw*, pages 3–7, 2018.

[8] Sungmin Choi, Tat Woo Tan, Zhuochen Xie, Yongqi Wu, and Xingjun Wang. Trusted resource sharing infrastructure for decentralized wireless community network. In *Proceedings of the 25th International Workshop on Mobile Computing Systems and Applications*, pages 1–1, 2024.

[9] Sami Kassab. Navigating the DePIN Domain. Research Report, Messari, 2023.

[10] Diego Ongaro and John Ousterhout. In search of an understandable consensus algorithm. In *2014 USENIX annual technical conference (USENIX ATC 14)*, pages 305–319, 2014.

[11] Guntur Dharma Putra, Volkan Dedeoglu, Salil S Kanhere, and Raja Jurdak. Trust management in decentralized iot access control system. In *2020 IEEE international conference on blockchain and cryptocurrency (ICBC)*, pages 1–9. IEEE, 2020.

[12] Chenxin Li, Peilun Li, Dong Zhou, Zhe Yang, Ming Wu, Guang Yang, Wei Xu, Fan Long, and Andrew Chi-Chih Yao. A decentralized blockchain with high throughput and fast confirmation. In *2020 {USENIX} Annual Technical Conference ({USENIX}{ATC} 20)*, pages 515–528, 2020.

[13] Christopher Copeland and Hongxia Zhong. Tangaroa: a byzantine fault tolerant raft, 2016.

[14] Weili Wang, Sen Deng, Jianyu Niu, Michael K Reiter, and Yinqian Zhang. Engraft: Enclave-guarded raft on byzantine faulty nodes. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 2841–2855, 2022.

[15] Sungmin Choi, Yongqi Wu, Guining Liu, Zhuochen Xie, Shengnan Zhang, and Xingjun Wang. Proof of traffic: An incentive mechanism for traffic sharing in decentralized wireless networks. In *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*, pages 1–7. IEEE, 2023.

[16] Yongqi Wu, Sungmin Choi, Guining Liu, and Xingjun Wang. Proof of directed guiding gradients: A new proof of learning consensus mechanism with constant-time verification. In *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–3. IEEE, 2023.

[17] Llorenç Cerdá-Alabern and Gabriel Iuhasz. Dataset for anomaly detection in a production wireless mesh community network. *Data in Brief*, page 109342, 2023.