ReND: Toward Reasoning-based BLE Neighbor Discovery by Integrating with Wi-Fi Fingerprints

Ziwei Li[†], Zhaoqi Yang[‡], Bowen Hu[‡], Tong Li[‡]*, Bo Wu[§], Yukuan Ding[¶], Dulin Xu[‡], and Ke Xu[†‖]
Tsinghua University[†], Renmin University of China[‡], Tencent[§], Delft University of Technology[¶] Zhongguancun Laboratory[‖]

***Abstract*—This paper proposes the novel concept of reasoning-based Bluetooth Low-Energy (BLE) neighbor discovery, an indirect paradigm of device-to-device sensing to address challenges (e.g., interference and power limitations) where direct sensing falls short. Inspired by the classical Rule of Syllogism, reasoning-based BLE neighbor discovery abstracts the device-to-device sensing as the presence detection of a BLE signal in a certain space. It deduces the presence of the BLE signal according to the presence of the Wi-Fi signal through the historical correlation between BLE and Wi-Fi. To demonstrate the feasibility of this new neighbor discovery paradigm, we report the design and evaluation of a prototype called ReND. By leveraging the complementary strengths of Wi-Fi and BLE, ReND reduces up to 91.3% and 65.9% of the 50^{th} and 95^{th} percentile BLE neighbor discovery latency, respectively. We further discuss the feasibility and incentive of ReND in the Polygon's Mumbai Testnet public blockchain.**

***Index Terms*—neighbor discovery, syllogism, fingerprint, blockchain**

I. Introduction

Device-to-device Bluetooth Low-Energy (BLE) neighbor discovery, serves as a fundamental stage for enabling diverse Internet of Everything (IoE) scenarios, including marketing activities such as advertising, promotions, and scheduling, as well as interactive applications like seamless access systems and robot navigation [1]. It mainly employs a neighbor discovery protocol [2], including the roles of a scanner and a broadcaster, where one device tries to establish contact with another device in the Bluetooth signal range. The user experience of applications is usually significantly affected by the neighbor discovery latency [3], which is measured from the point when both devices enter the range of reception, to the point when the scanner captures the complete packet in a broadcast event. This paradigm of neighbor discovery falls into the category of "direct sensing".

BLE neighbor discovery in the paradigm of "direct sensing" faces two foundational challenges. First, minimizing the neighbor discovery latency may require increased power consumption as a trade-off. In 2019, Kindt et al. [2] introduced tight latency bounds that surpassed previous approaches for BLE neighbor discovery parameter settings. They concluded that there were no further possibilities for improving the relationship between latency and duty cycle [4]. Second, Bluetooth signal interference may still significantly impact the neighbor discovery latency even when the scanner runs in a high-power mode (see §II-A).

However, in this paper, we argue that there is still ample potential for improvement, especially in practical scenarios. When abstracting the neighbor discovery problem as the presence detection of the BLE Beacon in a certain space, considering the ubiquity of Wi-Fi APs, we have seen the possibilities of reasoning about the presence of BLE Beacon from the presence of Wi-Fi fingerprints, which is denoted by a list of Wi-Fi APs nearby the BLE Beacon. Thus we design `ReND`, a *Reasoning-based Neighbor Discovery* paradigm that makes full use of the complementarity between Wi-Fi and BLE. In the case of a long BLE neighbor discovery latency, ReND accelerates the discovery by deducing the presence of the BLE Beacons according to the presence of Wi-Fi fingerprints through the historical correlation between them.

Essentially, ReND is a kind of "indirect sensing" that leverages the Rule of Syllogism [5] to address wireless sensing challenges where direct sensing falls short (see §II-B). The logical foundation of syllogisms includes a major premise, a minor premise, and a conclusion. For example, given the major premise: "Device B is near Device A", and the minor premise: "Device A is found", then we can deduce the conclusion: "Device B is found". From the perspective of syllogistic reasoning, the major premise of ReND highlights the mapping relationship between BLE signals and Wi-Fi signals. The minor premise of ReND involves the matching of Wi-Fi fingerprint information. The conclusion of ReND is therefore the discovery of BLE signals.

By introducing logical inference processes into BLE neighbor discovery, the discovery latency can be reduced in many cases. First, it is essential to maintain a delicate tradeoff between latency and power consumption. Typically, to conserve power, longer broadcast intervals and lower duty cycles are used, but this may result in unexpected long discovery latency [3]. In this case, ReND can be applied to accelerate BLE neighbor discovery with a lower power budget (see §IV). This benefit can be attributed to the complementarity between Wi-Fi and BLE in discovery patterns (see §II-B). Second, wireless interference leads to packet loss, especially

This work was supported in part by the Science Fund for Creative Research Groups of the National Natural Science Foundation of China under No. 62221003, the National Natural Science Foundation of China under No. 62202473, the Key Program of the National Natural Science Foundation of China under No. 61932016 and No. 62132011, the National Science Foundation for Distinguished Young Scholars of China under No. 62425201. Tong Li is the corresponding author (tong.li@ruc.edu.cn).

in environments with a high density of Bluetooth signals, such as crowded malls [3]. In this case, ReND can be also applied to accelerate BLE neighbor discovery regardless of Bluetooth signal interference. This benefit can be attributed to the complementarity between Wi-Fi and BLE in wireless interference (see §II-B).

The ReND system comprises two subsystems: FiND and FingerprintHub. FiND, the core of ReND, provides the fingerprint-based neighbor discovery protocol that accelerates BLE neighbor discovery via Wi-Fi fingerprints. It relies on massive location data (e.g., Wi-Fi fingerprints and Beacon IDs) for inference according to the Rule of Syllogism (see §III-A). FingerprintHub, a blockchain-based platform that overcomes both the *trust issues* and *incentive issues* by embedding incentive mechanisms through smart contracts, enables the value transfer and circulation of location data, facilitating secure and transparent data sharing and publishing (see §III-B).

With the aid of a cloud server and a blockchain system, we successfully integrated a prototype of the ReND system into the Android platform. Through performance evaluation, ReND has demonstrated remarkable reductions in neighbor discovery latency. Specifically, ReND reduces 73.9%-91.3% and 46.3%-65.9% of the 50^{th} and 95^{th} percentile latency, respectively. ReND can also evolve healthily with more data providers contributing high-quality data (see §IV).

II. Background and Motivation

A. Background

Rule of Syllogism. In the field of natural sciences, reasoning is widely recognized as the process of concluding from given premises, and it is also considered an act, method, or skill of deducing new information or conclusions through logical and inferential rules. In reasoning, a classic form is a syllogism, often called Rule of Syllogism [5]. The Rule of Syllogism consists of three parts: major premise (first premise), minor premise (second premise), and a conclusion. As shown in Fig. 1, two premises are composed of three parts, namely major term (P), middle term (M), and minor term (S). The major premise is composed of major term and middle term while minor premise is composed of middle term and minor term, where each term can serve as a subject and predicate in the premise. Due to different positions of major term, middle term, and minor term in premise, different syllogistic reasoning cases are formed [5]. As shown in Fig. 1, "Metal is conductive" is the major premise, and "Iron is a type of metal" is minor premise. In the major premise, M (Metal) serves as the subject, and P (conductive) serves as the predicate, i.e., M–P. In the minor premise, S (Iron) serves as the subject and M (Metal) serves as the predicate, i.e., S–M. According to the Rule of Syllogism, we conclude: S–P ("Iron is conductive").

Challenges of BLE Neighbor Discovery. The current neighbor discovery technologies mainly employ a *direct sensing* paradigm. In the case when device A (acts as the scanner) tries to discover device B (acts as the broadcaster), direct neighbor discovery means device B is discovered by device A,

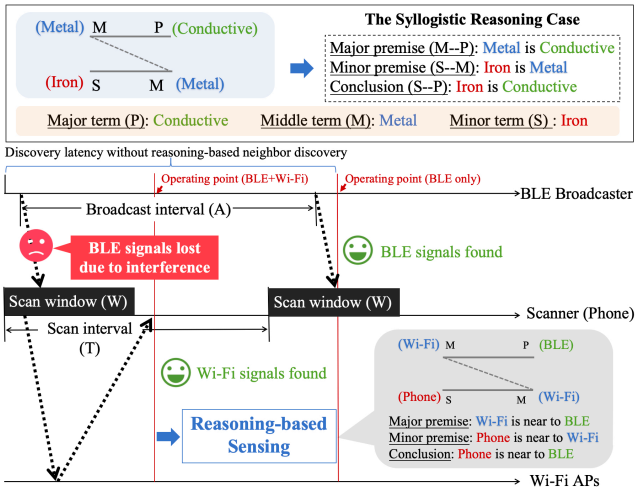


Fig. 1: Reasoning-based neighbor discovery under the Rule of Syllogism.

only if device A has received the advertised wireless packets from device B. However, direct sensing may fall short in the following cases.

Case 1: There exists a trade-off between latency and power consumption. BLE neighbor discovery faces a trade-off between latency and power consumption. Neighbor discovery latency depends on the broadcaster's broadcast interval (A), the scanner's scan window (W), and the scanner's scan interval (T). Power consumption is directly proportional to the scan duty cycle ($D = \frac{W}{T}$) and inversely proportional to A. To conserve power, modern applications often use a large A (e.g., $>$ 1000 ms) and a low D (e.g.,$<$ 10%), but this can lead to unacceptable discovery latency (e.g., $>$ 5 seconds) due to interleaved activity [2]. Applying a smaller A (e.g., 20 ms is the smallest value in the Android system) or a higher D (e.g., at most 100%) significantly reduces the neighbor discovery latency. However, the latency is still unacceptable in the case of wireless interference [6], as we will discuss next.

Case 2: There exists wireless interference. Currently, BLE Beacons (iBeacon, Eddystone, AltBeacon, aBeacon, HiBeacon, etc.) operating in the 2.4 GHz ISM frequency band are extensively used in public spaces. The increasing number of Bluetooth-equipped devices, particularly wearables, due to the Internet of Things has led to a rise in wireless interference. This interference adversely affects the performance of BLE neighbor discovery. For instance, in a medium-sized shopping mall, the simultaneous existence of over 20 BLE signals can significantly impact the neighbor discovery latency even with a small A and a large D (see §IV).

B. Motivation

Complementarity Between Wi-Fi and BLE. The two modes of Wi-Fi and BLE show complementarity in both wireless interference and discovery patterns. **First**, Wi-Fi and BLE show complementarity in wireless interference. Although both BLE and Wi-Fi operate in the 2.4GHz ISM band, the 3 channels (i.e., channels 37 (2402MHz), 38 (2426MHz), and

39 (2480MHz)) used by BLE neighbor discovery are almost unaffected by Wi-Fi interference (e.g., channels 1-11 (2412-2472MHz)). **Second**, Wi-Fi and BLE show complementarity in discovery patterns in two aspects: (a) Wi-Fi not only supports BLE-like passive scanning but also supports active scanning during which the client radio transmits a probe request and listens for a probe response from an AP. Generally, a passive scan takes more time in neighbor discovery, since the client must listen and wait for a beacon versus actively probing to find an AP. (b) Wi-Fi always returns discovery results (although might be from a previous scan if the current scan has not been completed or succeeded) [7], while BLE may return nothing.

Reasoning-based Sensing Under the Rule of Syllogism. The challenges of BLE neighbor discovery ultimately stem from the limitations of the direct sensing approach. Therefore, it becomes crucial to explore alternative methods of *indirect sensing* to facilitate connectivity and overcome these challenges. Inspired by the Rule of Syllogism, we propose a novel concept of *reasoning-based sensing* to enable an indirect paradigm of device-to-device neighbor discovery. Reasoning-based sensing also consists of a major premise, a minor premise, and a conclusion. For example, when integrating Wi-Fi fingerprints into BLE neighbor discovery (see Fig. 1), the reasoning-based sensing paradigm works as follows. Given the major premise: "A list of Wi-Fi APs (i.e., Wi-Fi fingerprints) is near to a BLE Beacon", and the minor premise: "Phone is near to the Wi-Fi APs". When the Wi-Fi APs are matched, we can deduce the conclusion: "Phone is near to the BLE Beacon". In this case, the scanner (i.e., Phone) doesn't need to receive the advertised wireless packets from the BLE Beacon, which is even not required to support the Bluetooth communication mode. Fig. 1 also shows that applying reasoning-based sensing moves the *operating point* forward, potentially accelerating the wireless sensing progress.

III. ReND Overview

Founded on the concept of reasoning-based neighbor discovery, we introduce the ReND system. Essentially, ReND falls into the category of *multimodal sensing* that incorporates Wi-Fi-based sensing with BLE-based sensing. Its goal is to reduce BLE neighbor discovery latency with a low power budget even under fierce Bluetooth signal interference. Fig. 2 shows the framework of the ReND system. ReND comprises two subsystems, namely FiND and FingerprintHub. The collaboration between FiND and FingerprintHub within ReND creates a comprehensive demonstration of the application of the reasoning-based sensing concept in the real world.

FiND. Serving as the core component of ReND, FiND provides a fingerprint-based neighbor discovery protocol that accelerates BLE neighbor discovery using Wi-Fi fingerprints. As shown in Fig. 2, FiND employs the rules of syllogism for reasoning, taking "A BLE Beacon is near to a Wi-Fi fingerprint" as the major premise, and "The Wi-Fi fingerprint is found" as the minor premise. If the fingerprint is matched

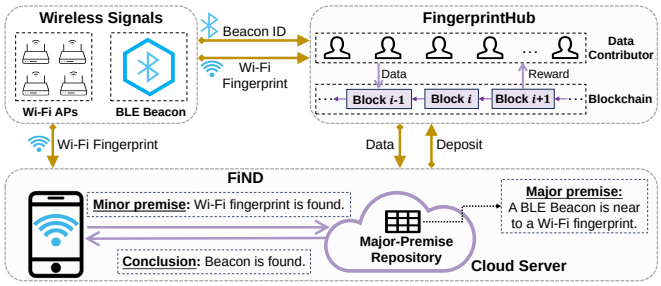


Fig. 2: The framework of ReND.

at the Cloud Server, then we derive the conclusion "The BLE Beacon is found".

FingerprintHub. The FiND subsystem heavily relies on the Major-Premise Repository which contains a substantial volume of Wi-Fi fingerprints and Beacon IDs for reasoning-based sensing. Due to the propagation characteristics of wireless signals, these datasets typically require periodic updates to maintain their relevance and accuracy. To build the Major-Premise Repository, we introduce FingerprintHub, a blockchain-based, large-scale intelligent platform designed for collecting Wi-Fi fingerprint data. As shown in Fig. 2, FingerprintHub leverages crowdsourced users to collect location data (e.g., the mapping between Wi-Fi fingerprints and Beacon IDs). It adopts a *smart contract* to address the urgent concerns of trust in the data collection process. Additionally, it acquires a deposit to reward crowdsourced users based on a carefully designed *Automated Incentive Allocation Mechanism*, facilitating the transfer of the value of location data.

A. Design of FiND

The Workflow of FiND. FiND employs a phone to deduce Beacon ID by leveraging Wi-Fi fingerprints and a remote cloud server. Here's the basic workflow involved.

Step 1: The phone initiates BLE scanning for a specific duration, whose failing to locate Beacon will proceed to Step 2. **Step 2**: The phone acquires the Wi-Fi fingerprint by either performing Wi-Fi scanning or retrieving historical records from the cache. **Step 3**: The Phone sends a request containing the Wi-Fi fingerprint to the Cloud Server. This fingerprint infers that "The Phone is near a list of Wi-Fi APs". **Step 4**: The Cloud Server, utilizing the Wi-Fi fingerprint from the *Major-Premise Repository*, queries the Beacon ID and employs *Syllogistic Reasoning* to obtain a result. This result is then sent as a response to the Phone. Consequently, the Phone discovers the BLE Beacon "indirectly" through the FiND system.

Major-Premise Repository. The Major-Premise Repository is implemented by a mapping table on the cloud server to store the mapping information between Wi-Fi fingerprints and Beacon IDs. Each record represents a major premise that "A BLE Beacon is near a Wi-Fi fingerprint". Note that the mapping table is initially empty in the FiND system, thus it does not accelerate BLE neighbor discovery. When a user successfully discovers a Beacon device in the first step

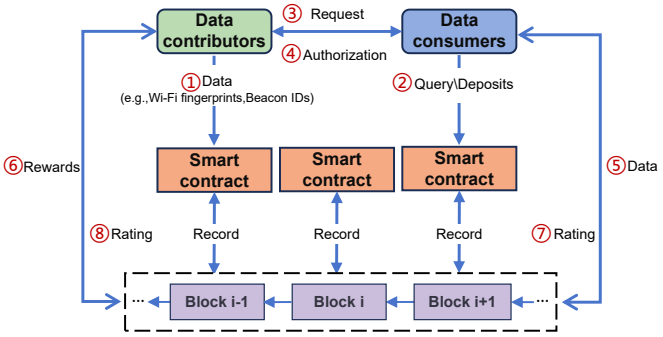


Fig. 3: The basic workflow of Smart Contract Mechanism.

mentioned above, the user is allowed to collect the Wi-Fi fingerprint and Beacon ID and upload the mapping of them to the Cloud Server. In this case, the user becomes a Data Contributor as specified in the FingerprintHub subsystem.

Syllogistic Reasoning. In the Cloud Server, the output of Syllogistic Reasoning is the result inferred based on the major premise and minor premise. Specifically, the major premise claims "A BLE Beacon is near a Wi-Fi fingerprint", and the minor premise: "The Wi-Fi fingerprint is found". When the fingerprint in the minor premise is matched to the fingerprint in the major premise, we can deduce the conclusion: "The BLE Beacon is found". Nevertheless, the fluctuating nature of wireless signals introduces instability in Wi-Fi fingerprints. To address this concern, we utilize fuzzy matching techniques to enhancing the robustness of FiND. One such technique is the utilization of the Jaccard index [8] to calculate the similarity coefficient between fingerprints: $J(A,B) = \frac{|A \cap B|}{|A \cup B|}$, where A and B represent the sets of current and historical fingerprints, respectively. The symbol $|\cdot|$ denotes the size of a set. In this paper, the fuzzy matching returns $\varnothing$ if all the records meet $J(A,B) < 0.5$. Otherwise, the fuzzy matching returns the record with the highest $J(A,B)$.

B. Design of FingerprintHub

The data-sharing market that is powered by FingerprintHub consists of two key participants: data contributors and consumers. Data contributors can provide Wi-Fi fingerprints and Beacon IDs for pursuing rewards. Data consumers can query data and apply for access to data by paying a designated deposit. To build a high-quality Major-Premise Repository for the FiND subsystem, two fundamental issues and challenges should be considered when designing FingerprintHub, namely the trust issue and the incentive issue.

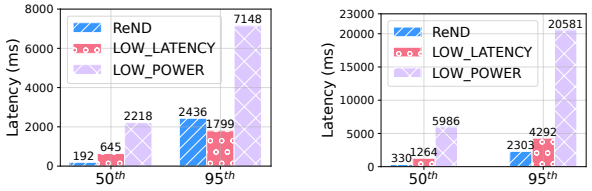
Smart Contract Mechanism. FingerprintHub adopts the smart contract to solve the trust issues. Fig. 3 illustrates the basic workflow of FingerprintHub. **Step 1**: Data contributors encrypt the Wi-Fi fingerprint data. Then data contributors call the smart contract to upload the Wi-Fi fingerprint data to the blockchain system. **Step 2**: Data consumers search for data of interest (Wi-Fi data packets) in an indexed manner using smart contracts. Data consumers may deposit funds as collateral for data value payment and reward distribution in the smart contract to initiate a data-sharing request. **Step 3**: A Data Consumer selects the most suitable data contributor and calls the smart contract to send a data-sharing request to the data contributor. **Step 4**: Upon receiving the request from the data consumer, the data contributor verifies the identity of the data consumer. Then the data contributor sends the encrypted authorization data back to the data consumer. **Step 5**: Once the data consumer receives the authorized encrypted data, the smart contract triggers the issuance of the corresponding Wi-Fi data packet from the blockchain to the data consumer. The data consumer then decrypts the Wi-Fi data packet, obtaining the data used for building the Major-Premise Repository. **Step 6**: After successful data acquisition, FingerprintHub triggers the smart contract, calling the reward distribution function to allocate rewards to the data contributor based on data quality and reward principles. **Step 7**: After obtaining the final data, data consumers can evaluate the data. **Step 8**: Data contributors can also score data consumers based on their relevant reputation to mitigate the risk of malicious behavior.

Automated Incentive Allocation Mechanism. FingerprintHub adopts the automated incentive allocation mechanism to solve the incentive issues. The effectiveness of the same set of data may vary significantly among different users due to factors such as user requirements for data accuracy, timing of data collection, and frequency of data acquisition. Therefore, traditional fixed pricing models are no longer sufficient to meet current demands. To achieve fairer and more efficient resource allocation, we have established a dynamic pricing mechanism based on data value. The data pricing model in FingerprintHub is as follows: we assume that each data provided by platform data providers consumes a certain token as the cost of publishing shared data (gas), denoted as c. In the FingerprintHub platform, we have established a unified billing standard, with the price of each data purchased by data consumers being r. Therefore, when data is purchased, the basic income for data providers is $e = (r - c) * n$, where n is the number of data purchased. After purchasing data and using it, data users rate each data packet based on its effectiveness. Here, we agree that the rating for each data packet in the same bundle is the same. The feedback rating from data users are divided into five levels, including extremely dissatisfied, dissatisfied, useless, satisfied and extremely satisfied. The corresponding values are -1, -0.5, 0, 0.5 and 1 respectively. We calculate the average of all ratings received by data providers as the utility increment of the pricing model, denoted as δ_u, where $-1 \leq \delta_u \leq 1$. The reward income based on feedback ratings from data users is denoted as e', where $e' = \delta_u \cdot r \cdot n$. Therefore, for data providers, the comprehensive income E is given by $E = e + e' = (r - c) \cdot n + \delta_u \cdot r \cdot n$.

IV. Evaluation

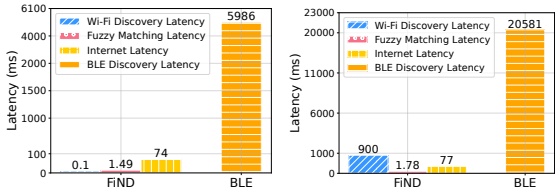
A. Experiment Setup

To verify the effectiveness of the ReND system in accelerating BLE neighbor discovery, we established a test environment utilizing an Android smartphone. The smartphone was connected to a remote server (e.g., Alibaba Cloud ECS2),



(a) Little interference (b) Fierce interference

Fig. 4: The evaluation of ReND with wireless interference.



(a) 50^{th} latency (b) 95^{th} latency

Fig. 5: Latency analysis in FiND.

with an average round-trip time (RTT) of 100 ms. At the same time, we developed a decentralized application to materialize FingerprintHub. This involves creating a front-end interface (running on the Android smartphone) for users to interact with smart contracts deployed on a blockchain network (e.g., Polygon [9]), thereby obtaining substantial location data through crowdsourcing. The Major-Premise Repository on the server obtains high-quality data, including a substantial volume of Wi-Fi fingerprints and Beacon IDs, from the blockchain network. We configured the Beacon advertising interval to 1000 ms. The distance between the broadcaster and the scanner is 5 meters. Additionally, we defined three BLE scan modes on the Android smartphone: LOW_POWER ($\frac{W}{T}$=10%), BALANCED ($\frac{W}{T}$=25%), and LOW_LATENCY ($\frac{W}{T}$=100%) [10]. When running ReND, the Android smartphone utilized the LOW_POWER mode.

B. Performance Improvement

Scenario 1: Little Interference. In a location free from Bluetooth interference, we strategically placed BLE Beacons and a phone in an open area where more than 10 Wi-Fi APs could be detected. The results depicted in Fig. 4(a) clearly illustrate the significant acceleration achieved in BLE neighbor discovery by implementing ReND with a low-duty cycle. Notably, when the phone operates in LOW_POWER mode, ReND effectively reduces the 50^{th} percentile latency by 91.3% and the 95^{th} percentile latency by 65.9%. This is because ReND makes the tradeoff between latency and power consumption less critical to BLE neighbor discovery.

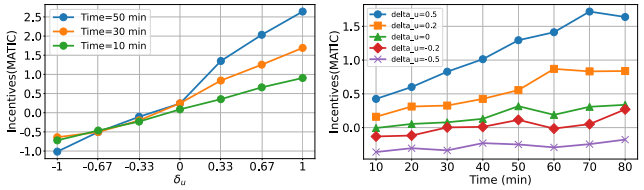
Scenario 2: Fierce Interference. In an office environment with fierce interference caused by the presence of more than 20 nearby randomly distributed BLE signals, we deployed both the BLE Beacons and the phone. Despite this challenging scenario, where over 10 Wi-Fi APs could still be detected, our findings presented in Fig. 4(a) and Fig. 4(b) showcase the stable and low-latency neighbor discovery achieved by ReND. In comparison, the traditional methods experience a decline in performance when faced with such fierce interference. Remarkably, even when compared to using the LOW_LATENCY mode, ReND excels by reducing the 50^{th} percentile latency by 73.9% and the 95^{th} percentile latency by 46.3%. This remarkable improvement can be attributed to ReND's ability to effectively leverage the complementary nature of Wi-Fi and BLE. By doing so, ReND can mitigate the negative impact of intense Bluetooth interference on BLE discovery latency, allowing for more reliable and efficient neighbor discovery.

C. Feasibility Analysis

Latency Breakdown in FingerprintHub. Before diving into the data-sharing process in FingerprintHub, we first investigated the overall performance of the FingerprintHub prototype on Polygon's Mumbai Testnet public blockchain. In FingerprintHub, the MATIC token is employed to assess incentives and balance between location data contributors and consumers [11]. Data contributors receive MATIC tokens post their initial data sharing. The system underwent a performance evaluation and after measuring 20,000 blocks, the average single block creation time was determined to be 2.48 seconds. We believe the response at the second level can satisfy the storage and sharing of Wi-Fi fingerprint data considering the low update frequency of the Major-Premise Repository. The data-sharing process in FingerprintHub encompasses three main phases: upload phase, request for data usage phase and the authorization and key exchange phase. The time expenses of these three stages were measured, revealing average durations of 10.28 seconds, 12.18 seconds, and 10.42 seconds, respectively. Notably, 80% of the total duration across these phases falls within the 37.5 seconds threshold.

Latency Breakdown in FiND. In this experiment, tests are conducted in an office environment with fierce interference caused by the presence of more than 20 nearby randomly distributed BLE signals. The scanning mode was consistently maintained in LOW_POWER mode. The overall latency of FiND includes Wi-Fi scan latency, fuzzy matching latency, and Internet latency, as presented in Fig. 5. "BLE" in the X-axis denotes the scenario when only using BLE scanning on the phone, and "FiND" in the X-axis denotes the scenario when applying FiND with only Wi-Fi scanning on the phone. It indicates that the Internet latency dominates the 50^{th} percentile latency of FiND. This is because the Wi-Fi fingerprints can be directly read from the system cache in most cases [7], resulting in a low Wi-Fi scan latency. However, the Wi-Fi scan latency dominates the 95^{th} percentile latency of FiND. This is because the phone has to redo an all-channel Wi-Fi scan when it fails to read a valid result in the cache. In both cases, it is demonstrated that the overall latency of FiND is much less than that of "BLE". This further validates the feasibility of applying FiND to accelerate BLE neighbor discovery.

Power Consumption. In this experiment, we investigate the power consumption of ReND. We compare three cases: low latency mode power consumption is 1.18mAh/30min, balanced mode power consumption is 0.448mAh/30min, and ReND



(a) Incentives under varying δ_u (b) Incentives under varying time

Fig. 6: Incentives with varying δ_u and participation time.

mode power consumption is 0.179mAh/30min. The results show that ReND achieves the lowest power consumption. In particular, ReND reduces power consumption by 84.8% and 60.0% compared to low latency and balanced, respectively. This reveals that ReND can accelerate BLE neighbor discovery with a low-duty cycle, making it suitable for applications with stringent power requirements.

D. Incentive Analysis

In FingerprintHub, we assess the equilibrium of data contributors by measuring their earnings and costs. Each data contributor incurs ∼0.063 MATIC as the cost of publishing a single data entry. To attract more participation in data sharing, we configure an earning base (i.e., 0.63 MATIC) for each data consumption. As described in §III-B, a data contributor's final balance comprises both base earnings and bonus earnings. As shown in Fig. 6(a) and 6(b), We evaluate the incentives for data contributors under varying δ_u and duration, in which the larger δ_u and more participation enable data contributors obtain more incentives. Conversely, when δ_u is negative, data contributors incur losses. Moreover, as the duration of data provision extends, earnings increase due to the possibility of the same data being purchased by multiple data consumers. Therefore, the experimental evaluation demonstrates that the FingerprintHub platform can evolve healthily in promoting data sharing, which can incentivize more data contributors to join this platform and contribute high-quality data.

V. Related Work

Neighbor Discovery Acceleration. Efficient neighbor discovery aims to achieve the shortest possible discovery latency for a given power budget. To this end, a large number of broadcast and scan setting approaches have been proposed for general wireless neighbor discovery, see [12], [13]. Different from these works that seek to find the optimized parameter settings of the BLE broadcasters and scanners, ReND further enlarges the solution space of BLE neighbor discovery optimization by integrating with Wi-Fi fingerprints.

Fusion Between Wi-Fi and BLE. A significant body of academic research has been devoted to the integration of Wi-Fi and BLE signals for various applications [14], [15]. Liu et al. [16] propose WiBeacon, a system that transforms commonly deployed WiFi access points into virtual BLE beacons with minimal software upgrades. To the best of our knowledge, no prior work has accelerated BLE neighbor discovery via Wi-Fi fingerprints.

Crowdsourced Data-Sharing Frameworks. The concept of crowdsourcing has been widely applied across numerous fields, resulting in a plethora of application cases [17], [18]. Utilizing blockchain technology enables the provision of a trust mechanism within data crowdsourcing platforms [19], [20]. Consequently, this paper implements FingerprintHub, a privacy-friendly and fully trusted location data crowdsourcing platform based on blockchain.

VI. Conclusion

In this paper, we for the first time discuss the possibility of one kind of "indirect sensing", called "reasoning-based sensing", and report its demonstration system called ReND. The evaluation of ReND not only confirms the performance improvement of integrating Wi-Fi fingerprints into BLE, but also establishes an architectural paradigm for reasoning-based sensing. We believe the proposition of the reasoning-based sensing concept holds significant importance in both academic and industrial realms.

References

[1] "Proximity beacon," https://altbeacon.org/, 2022.
[2] P. H. Kindt and S. Chakraborty, "On optimal neighbor discovery," in *ACM SIGCOMM*, 2019, pp. 441–457.
[3] T. Li, J. Liang, D. Wang, Y. Ding, K. Zheng, X. Zhang, and K. Xu, "On design and performance of offline finding network," in *IEEE INFOCOM*, 2023, pp. 1–10.
[4] K. Geissdoerfer and M. Zimmerling, "Bootstrapping battery-free wireless networks: Efficient neighbor discovery and synchronization in the face of intermittency," in *USENIX NSDI*, 2021, pp. 439–455.
[5] T. J. Smiley, "What is a syllogism?" *Journal of philosophical logic*, pp. 136–154, 1973.
[6] Y. Ding, T. Li, J. Liang, and D. Wang, "Blender: Toward practical simulation framework for ble neighbor discovery," in *ACM MSWiM*, 2022, pp. 103–110.
[7] "Android wi-fi scan," https://developer.android.com/guide/topics/connectivity/wifi-scan, 2020.
[8] P. Jaccard, "The distribution of the flora in the alpine zone." *New phytologist*, vol. 11, no. 2, pp. 37–50, 1912.
[9] "Polygon," https://polygon.technology/, 2023.
[10] "Android ble scan settings apis," https://developer.android.com/reference/android/bluetooth/le/ScanSettings, 2023.
[11] J. Kanani, S. Nailwal, and A. Arjun, "Matic whitepaper," *Polygon, Bengaluru, India, Tech. Rep., Sep*, 2021.
[12] N. Karowski, A. C. Viana *et al.*, "Optimized asynchronous multi-channel neighbor discovery," in *IEEE INFOCOM*, 2011, pp. 536–540.
[13] T. Meng, F. Wu *et al.*, "On designing neighbor discovery protocols: A code-based approach," in *IEEE INFOCOM*, 2014, pp. 1689–1697.
[14] R. C. Luo and T.-J. Hsiao, "Indoor localization system based on hybrid wi-fi/ble and hierarchical topological fingerprinting approach," *IEEE TVT*, vol. 68, no. 11, pp. 10 791–10 806, 2019.
[15] A. N. Nor Hisham, Y. H. Ng, C. K. Tan, and D. Chieng, "Hybrid wi-fi and ble fingerprinting dataset for multi-floor indoor environments with different layouts," *Data*, vol. 7, no. 11, 2022.
[16] R. Liu, Z. Yin, W. Jiang, and T. He, "Wibeacon: expanding ble location-based services via wifi," in *MobiCom*, 2021, p. 83–96.
[17] Z. Yang, C. Wu, and Y. Liu, "Locating in fingerprint space: wireless indoor localization with little human intervention," in *Mobicom*, 2012, p. 269–280.
[18] J. Xu, Z. Luo, C. Guan, D. Yang, L. Liu, and Y. Zhang, "Hiring a team from social network: Incentive mechanism design for two-tiered social mobile crowdsourcing," *IEEE TMC*, vol. 22, no. 8, pp. 4664–4681, 2023.
[19] B. Wu, Q. Li, K. Xu, R. Li, and Z. Liu, "Smartretro: Blockchain-based incentives for distributed iot retrospective detection," in *IEEE MASS*, 2018, pp. 308–316.
[20] B. Wu, K. Xu, Q. Li, Z. Liu, Y.-C. Hu, Z. Zhang, X. Du, B. Liu, and S. Ren, "Smartcrowd: Decentralized and automated incentives for distributed iot system detection," in *IEEE ICDCS*, 2019, pp. 1106–1116.