# Zero-Knowledge Proof-based Verification System based on Environmental Sensing for Reliable Operation of AI-Driven Autonomous Robots

Arata Nakajima
*Ritsumeikan University*
*Graduate School of Information Science and Engineering*
Osaka, Japan
is0569fp@ed.ritsumei.ac.jp

Hideaki Miyaji Hiroshi Yamamoto
*Ritsumeikan University*
*College of Information Science and Engineering*
Osaka, Japan

***Abstract.*—The smart cities that collaborate with AI-driven autonomous robots are attracting attention for supporting various social activities in the real world. In facilities that provide such services, various systems managing the facility and robots may coexist in the common area. By enabling the systems to interoperate and share information about the status of the facility and robots, it becomes possible to realize a variety of services that support safety and security within the facility. However, while the operators of the facility want to monitor the detailed conditions of the robots, the operators of the robots are cautious about providing the information about the status of robots such as the moving trajectory and various sensor data. To resolve this dilemma, we propose a new system that enables estimation of the operational conditions of the robots by verifying the positions and trajectories at landmarks in the facility without disclosing their internal information. In the proposed system, we focus on the observation of environmental information that accurately reflects the real-world situation for estimating the proximity between the robot and each landmark. As the environmental information, both systems on robots and a facility measure CSI (Channel State Information) and acoustic information. In addition, by utilizing zero-knowledge proof (ZKP) technology, the system for the facility confirms the reliability of the process for estimating the proximity of the robots to the landmark without exchanging detailed internal information. Through the proof-of-concept experiment, applying the proposed system achieved high-accuracy proximity detection with both methods (CSI and acoustic information) yielding precision and recall rates exceeding 0.90.**

***Index Terms*—Zero-knowledge proof, CSI, Wi-Fi, acoustic information, blockchain**

## I. Introduction

The smart cities that collaborate with autonomous robots are attracting attention for supporting various social activities in the real world. In facilities that provide such services, various systems coexist including systems for managing the state of the facility and systems for managing the operation of the robots. By enabling the systems to interoperate and share information about the status of the facility and robots, it becomes possible to realize a variety of services that support safety and security within the facility such as detailed monitoring of facility conditions and accident avoidance around robots.

The behavior of the robots is often controlled by AI making it difficult to audit the decision-making processes of the AI that inherently suffers from the black-box problem. To ensure safety in smart cities, a reliable framework is required to verify that the AI observes the conditions within the facility and behaves as intended by the facility's operators without compromising privacy. However, robot operators are reluctant to share detailed trajectory and sensor data, as such information constitutes confidential operational data. To resolve this dilemma, a mechanism is needed that can prove the reliability of important operational conditions of the robots (e.g., proximity to major landmarks) to the facility without disclosing the detailed internal information.

The existing studies propose systems that verify the approximate location of an observation target without knowing its specific position based on environmental information dependent on each area and time within a facility. Existing methods using environmental information such as CSI and acoustic data are vulnerable to replay attacks and data tampering [1] [2] [8] [9] [10]. Furthermore, these methods lack mechanisms to prove processing correctness to third parties. On the other hand, systems utilizing zero-knowledge proofs (ZKP) are proposed as a technology to prove the correctness of processing applied to data [3] [4]. ZKP technology enables proving that data is processed correctly and that it satisfies the specific predefined conditions without disclosing the data itself.

Therefore, this study focuses on the observation of environmental information that accurately reflects the real-world situation for estimating the proximity between the robot and each landmark in a facility. As the environmental information, the proposed system combines CSI with acoustic information, which possesses time and space specific characteristics, to efficiently collect information dependent on the location in the facility. Furthermore, the ZKP technology is utilized for enabling the robot to prove to other operators whether it passed through specific locations without disclosing detailed movement history.

## II. Related Works and Objectives of Our Study

### *A. Research on Device Location Estimation Using Wi-Fi Sensing*

Xie et al. (2019) propose an indoor positioning system using Wi-Fi sensing that analyzes AoA, ToF, AoD, and

Doppler shift [2]. However, this method requires optimal device placement and incurs high computational costs.

On the other hand, Gu et al. (2023) propose a system that recognizes human behavior by utilizing Wi-Fi sensing and machine learning techniques [6]. This system uses time-series data of CSI (Channel State Information) including amplitude and phase of radio waves around the receiver. Specifically, by constructing a machine learning model that takes CSI amplitude data as input, the system enables human position estimation with 98% accuracy. However, this approach requires collecting CSI for each environment and constructing environment-specific models.

### *B. Research on Device Location Estimation Using Acoustic Information*

Karapanos et al. propose a two-factor authentication system that verifies device proximity by comparing ambient sound observations [8] [9].

Furthermore, Liu et al. propose a SoundID, a dynamic acoustic fingerprint-based two-factor authentication system, as a countermeasure of man-in-the-middle (MITM) attacks against location estimation based on acoustic fingerprints, location specific features extracted from acoustic information [10]. However, malicious attackers can potentially bypass authentication by presenting forged acoustic data or analysis results during the similarity verification process. Therefore, it remains a critical challenge for proving correctness of the processing.

### *C. Research on Verification of Sensor Data Processing Utilizing ZKP*

A system utilizing zero-knowledge proofs (ZKP) is proposed to prove the integrity of various types of data without revealing the data itself. Ko et al. (2021) propose a system that uses zero-knowledge proofs to verify that a redacted image, created by blacking out portions of an ID photo, is correctly edited from the authenticated original image [3]. Specifically, by proving the editing process via ZKPs, the method can verify whether the image is correctly edited in a predefined process or not without disclosing the original one.

Additionally, Guo et al. (2024) propose an authentication system enabling privacy protection of fingerprint images by proving the correctness of the hashing process applied to them using ZKP technology [4]. By constructing a ZKP-based function to prove each step of the process, the method becomes possible to address the risks of information leakage and replay attacks inherent in biometric authentication.

As described above, the use of ZKP technology enables proving whether the predefined processing is correctly applied to data or not without disclosing the data itself.

### *D. Objectives of Our Research*

Existing research propose location estimation techniques that observe environmental information depending on specific times and locations. However, these techniques are vulnerable as authentication methods due to data falsification by attackers.

Therefore, this research proposes a new system that focuses on environmental information such as CSI and acoustic information and employs zero-knowledge proof technology in the process of analyzing and comparing this environmental information. This enables each operator to prove the reliability of the location information of the robot without disclosing environmental information, which contains privacy-sensitive data, to other operators.

Specifically, in the proposed system, sensor nodes are deployed at various points within the facility and on the autonomous mobile robot itself, and continuously collecting environmental information such as CSI and acoustic data. When an operator attempts to verify the correctness of the moving trajectory of the robot, proximity between the robot and sensor nodes at each location is verified by evaluating similarity between the environmental information observed by the robot with that observed at each location. By applying zero-knowledge Succinct Non-interactive Arguments of Knowledge (zkSNARKs), a type of zero-knowledge proof, to this verification process, the method can prove whether the processing to analyze and compare the environmental information is performed correctly or not while keeping the environmental information confidential.

## III. Proposed Movement Trajectory Verification System Using CSI and Acoustics

### *A. Overview of the Proposed System*

As shown in Fig. 1, the proposed system consists of fixed sensor nodes, robot-mounted sensor nodes, and a data management platform. The fixed sensor nodes are installed at various locations within the facility and continuously collect environmental information such as CSI and acoustic data. Additionally, the robot-mounted sensor node installed on an autonomous mobile robot performing tasks such as security or delivery continuously collect environmental information while moving within the facility.

The fixed sensor nodes continuously monitor the state of specific channels used for Wi-Fi communication and collect CSI data. Simultaneously, the nodes collect acoustic information using their onboard microphones and transmit the collected environmental data to the data management platform. Meanwhile, the robot-mounted sensor nodes acquire environmental data and calculate its similarity to that collected by the fixed sensor nodes at various locations within the facility, which is publicly available on the data management platform. Based on the calculated similarity, the robot-mounted sensor node identifies the fixed sensor node closest to the robot.

When calculating the similarity, the robot-mounted sensor nodes generate a proof corresponding to the processing by using ZKP (Zero-Knowledge Proof) technology and register it to the data management platform. Subsequently, facility operators can verify the accuracy of the process for identifying location of each robot by validating the registered proof. Through this process of verifying the reliability of location, facility operators can confirm that the robots execute tasks such as security and delivery in the appropriate location without checking the detailed moving trajectory.

### *B. Device Configuration of Sensor node*

The sensor node consists of a Raspberry Pi 3 (2017) which is a small computer supporting Wi-Fi communica-

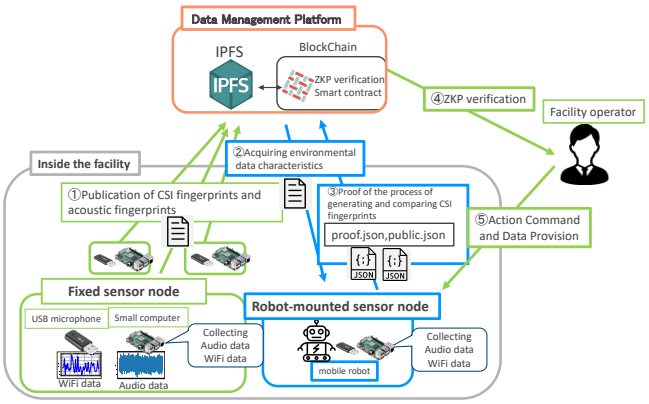


Fig. 1: Overall View of the Proposed System.

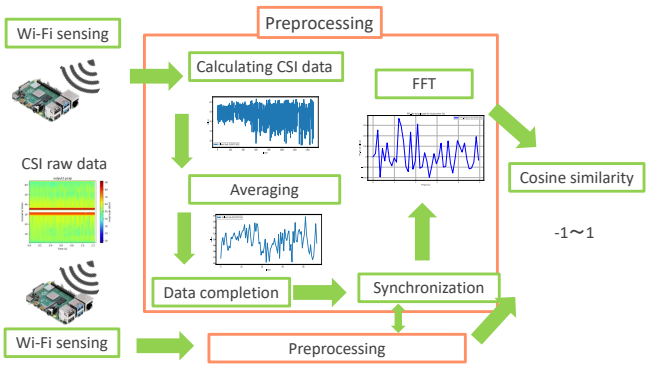


Fig. 2: Overview of Feature Extraction Process Based on CSI.

tion, connected to a USB microphone (DUNGZDUZ) for acquiring acoustic information. Furthermore, Nexmon and CSIkit are installed on the computer for CSI collection [7]. In this study, a 44-channel Wi-Fi frequency band (5.21-5.23GHz) is selected for observation to collect CSI, and 10-second measurements are continuously performed at one-minute intervals.

### C. Device Configuration of Data Management Platform

The data management platform consists mainly of an IPFS (InterPlanetary File System) and a blockchain platform, Hyperledger Fabric. Features extracted from the environmental data such as CSI and acoustic information collected by sensor nodes installed within the facility are stored in the IPFS in conjunction with timestamp. On the robot-mounted sensor node, proximity determination processing based on features is executed within a mathematical circuit corresponding with the processing for the zero-knowledge proof, and the proof and the processing results are stored on the blockchain. This allows verifiers (e.g., facility operators) to confirm that the robot passes by near the sensor node at a specific location in a trustworthy manner.

## IV. Proposed Proximity Determination Method and Zero-Knowledge Proof Design

### A. Proximity Determination Method Utilizing CSI Data

Wi-Fi-based proximity determination methods are primarily classified into two phases. Phase 1 involves preprocessing to generate CSI features from the original CSI collected by sensor nodes. Phase 2 executes proximity determination processing using the CSI features. Section IV-A1 details the Phase 1, and Section IV-A2 details the Phase 2.

*1) Extraction of CSI Features:* In this study, we adopt deterministic mathematical approaches (FFT and Cross-correlation) to validate the physical distinctiveness of the environmental features.

Figure 2 illustrates the overview of a feature extraction process based on CSI. In the proposed method, the average amplitude is calculated at 50 ms intervals within the 10-second CSI data observed by each sensor node. If there are intervals in which CSI data is not observed, the average amplitude from the preceding and following intervals is interpolated as the amplitude for that interval. Subsequently, a Fast Fourier Transform (FFT) is applied to the time-series of CSI data for each of 64 subcarriers on the 44 channel of Wi-Fi frequency band. With respect to the frequency components of the output CSI data, the average amplitude is then calculated at 0.1 Hz intervals across the frequency range from 0 to 12.5 Hz. The positive components of the calculated frequency spectrum are defined as the CSI features for that specific time. In this study, the Fourier transform is performed using the FFT function from NumPy, a numerical computation library for Python, to calculate the frequency components of the CSI data.

*2) Proximity Determination Processing via CSI Feature Comparison:* The robot-mounted sensor node calculates a similarity metric of the CSI features between each fixed sensor node within the facility and itself. This method adopts the cosine similarity between the feature vectors as the similarity metric. The robot-mounted sensor node calculates the cosine similarity for the CSI features corresponding to each fixed sensor node for each subcarrier. Specifically, the method selects the specific number of the subcarriers with the highest similarity and calculates their average value of the similarity on the selected ones. The appropriate number of subcarriers should be determined by balancing computational efficiency and classification accuracy. The appropriate values are investigated through experiments in Section V-A.

The robot identifies its own location to be the site where the sensor node with the highest similarity is installed. As a specific processing step, the similarity is calculated for each deployed sensor node, and the location indicating the highest value is selected as a candidate. After executing this process multiple times, the nearest sensor node is determined by majority vote across the iterations. The number of iterations in similarity comparison is defined as the window size. The cosine similarity comparison using CSI features is performed within the mathematical circuit of ZKP, enabling the robot to perform the comparison while keeping the information about the measured data confidential.

### B. Proximity Determination Method Utilizing Acoustic Information

Figure 3 shows the procedure of a proximity determination process using acoustic information. The USB mi-

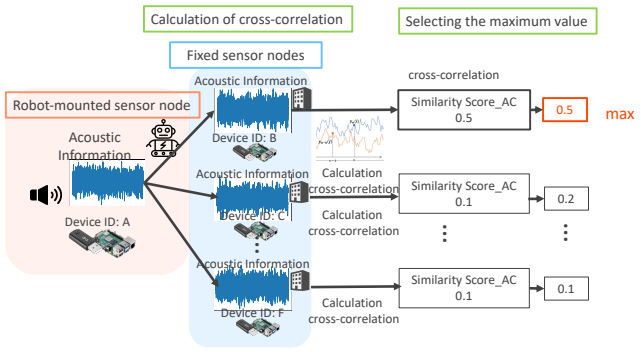


Fig. 3: Overview of Proximity Determination Processing Using Acoustic Information.

crophone of the sensor node collects acoustic information 10 times per minute, each for 3 seconds. The acoustic information is collected at a sampling rate of 44.1 kHz and represented as a vector with 132,300 elements.

In this proposed system, the cross-correlation shown in Eq. (1) is adopted as the similarity metric for comparing acoustic information.

$$R_{xy}(m) = \sum_{n=0}^{N-1} x(n) \cdot y(n+m) \tag{1}$$

The cross-correlation is calculated as the sum of element-wise products and serves as a quantitative metric for assessing similarity between acoustic signals. For two arrays $x$ and $y$ indicating the acoustic information measured by different sensor nodes, the product of each corresponding element is computed, and their sum is determined as the correlation value. The correlation value is calculated while progressively shifting the first element of the array one by one, and the highest value is adopted as the similarity measure.

The cross-correlation is calculated between the robot-mounted sensor node and each fixed sensor node installed within the facility. The sensor node that the cross-correlation is the highest is considered a candidate for the location of the robot. Similar to the method in Section IV-A2, the closest sensor node is determined by majority vote in the predefined window size and the optimal value of the window size is experimentally verified in Section V-B.

### *C. Verification of Similarity Calculation Using Zero-Knowledge Proof Circuits*

The robot-mounted sensor node proves the validity of the CSI similarity and acoustic similarity calculation processes using ZKPs. This system employs zkSNARKs, a ZKP technology capable of proving arbitrary mathematical processing, to generate proofs corresponding to the process of calculating the similarity of environmental information including CSI data and acoustic information between each fixed sensor node and the robot-mounted sensor node.

The zkSNARKs enables the generation of a mathematical circuit corresponding to the similarity calculation process, and the generation of proof information to verify its validity. A circuit consists of numerous constraints,

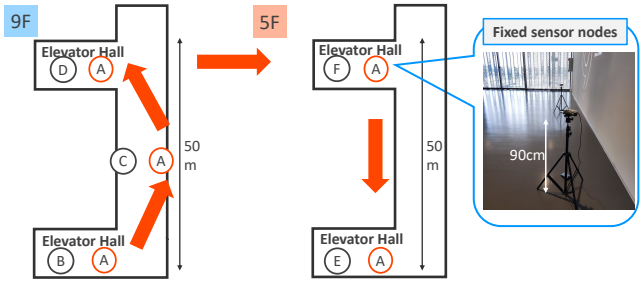


Fig. 4: Placement of Fixed Sensor Node for CSI Experiments.

where the constraints refer to conditional expressions that mathematically express the validity of computations in zero-knowledge proofs. Each step of arithmetic operations and logical processing is incorporated into the circuit as a constraint, hence the more computations a process involves, the greater the number of constraints becomes.

This proposed system employs snarkjs, a ZKP development and execution support tool, and Circom, a circuit description language [11] [12]. The zkSNARK algorithm employs Groth16 and PLONK, and Section V-C compares and evaluates the performance of both algorithms. The robot-mounted sensor node registers the generated proof to the blockchain, and operators (e.g., facility operators) execute verification scripts based on this proof to reliably confirm that the similarity calculation is properly performed on the autonomous mobile robot.

## V. Evaluation

### *A. Proximity Determination Accuracy Based on CSI*

This section describes the accuracy evaluation experiments for the CSI-based proximity determination method described in Section IV-A. The fixed sensor nodes are deployed at five locations within the Ritsumeikan University campus. A robot-mounted sensor node is then deployed to traverse these locations and collect CSI. The method described in Section IV-A is applied to the collected data to verify the proximity determination accuracy.

Figure 4 shows the setting of sensor node placement for this experiment. As shown in this figure, five fixed sensor nodes B-F are placed on the 5th and 9th floors of the facility. In this experiment, we verify whether it is possible to correctly identify a proximate fixed sensor node when the robot-mounted sensor node passes within 5 meters of each fixed sensor node, with the window size fixed at 1.

Figure 5 shows the relationship between the number of subcarriers and each performance metric (i.e., precision, recall, F1-score). As shown in this figure, for all cases of the number of subcarriers, all metrics consistently show high values above 0.9. Based on the experimental results, considering computational efficiency and classification accuracy comprehensively, we adopt only the highest similarity for all subcarriers in subsequent experiments.

### *B. Proximity Determination Accuracy Based on Acoustic Information*

This section describes the experimental evaluation conducted to assess the accuracy of the proximity detection method using acoustic information described in Section

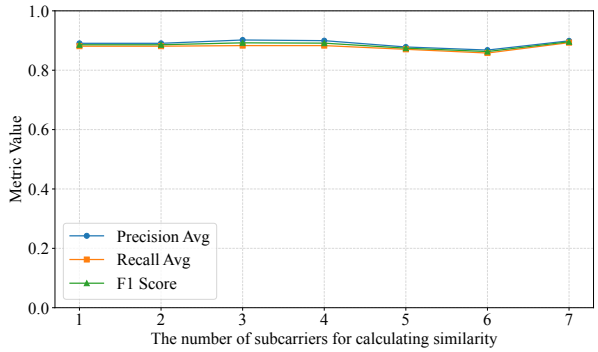


Fig. 5: Proximity Determination Accuracy for in Case of CSI Each Number of Subcarriers.

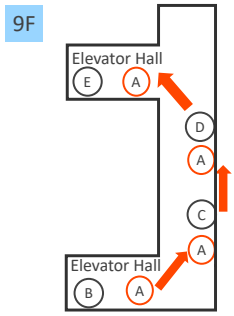


Fig. 6: Placement of Fixed Sensor Nodes for Acoustic Experiments.

IV-B. In this experiment, four fixed sensor nodes are installed at predetermined intervals within the Ritsumeikan University campus, and proximity detection is performed using the method described in Section IV-B. Figure 6 shows the setting of the placement of the fixed sensor nodes environment for this experiment. The fixed sensor nodes B-E are placed on the 9th floor at approximately 20 meters intervals. In this experiment, we verify whether the robot-mounted sensor node A can correctly identify nearby fixed sensor nodes when passing within 5 meters of each sensor node.

Figure 7 shows the relationship between the window size and each performance metric. As shown in this figure, setting the window size to 3 or more achieves precision and recall values of approximately 0.90. Based on these experimental results, considering both computational efficiency and detection accuracy, we adopt a window size of 3 for subsequent experiments. These results demonstrate that the proposed acoustic-based method can effectively identify proximate sensor nodes with high accuracy.

### *C. Performance Evaluation of Zero-Knowledge Proofs*

This section describes experimental evaluations measuring the execution time of proof generation and verification processes in a proximity determination method utilizing zero-knowledge proofs. The experiments were conducted on a MacBook Pro running macOS, equipped with an Apple M4 (10-core) processor and 24GB of memory. The objective of this experiment is to verify whether the

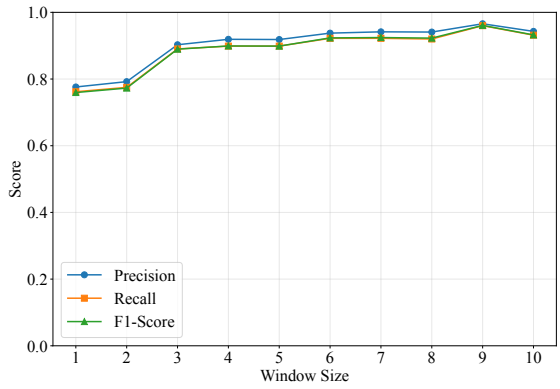


Fig. 7: Proximity Determination Accuracy in Case of Acoustic Information for Each Window Size.

processing for identifying the closest sensor nodes can be executed within a practical time.

In this evaluation, two representative zkSNARKs protocols, Groth16 and PLONK, are adopted. Groth16 features fast proof generation and small proof sizes, but requires setup on the relevant computers for each mathematical circuit. Conversely, PLONK allows a single generic setup for different circuits, but tends to have longer proof generation times. Performance evaluation is conducted by applying each protocol to the two proximity determination algorithms described in the Section IV, which utilize CSI and acoustic information.

The experimental results are shown in Fig. 8. Regarding CSI, both Groth16 and PLONK achieve fast proof generation at approximately 0.18 seconds. In contrast, for acoustic information, proof generation takes 21.9 seconds for Groth16 and 526.8 seconds for PLONK. This difference arises because processing of similarity based on acoustic information involves the comparison of numerous elements, leading to an enormous number of constraints in the circuit. Conversely, processing of CSI involves the comparison of fewer features than the acoustic information, resulting in fewer constraints in the circuit. Calculating the cross-correlation for acoustic information generates approximately 1.06 million constraints, whereas calculating the cosine similarity for CSI features requires only about 90,000 constraints. This significantly lower number of constraints results in a substantial difference in processing time.

As mentioned above, Groth16 can process the proof generation 24 times faster than PLONK for acoustic information, confirming its computational efficiency in large-scale circuits. Conversely, PLONK's generic setup allows flexible switching between different proximity detection methods, making it effective for systems combining multiple sensing techniques. On the other hand, verification time is approximately 0.18-0.20 seconds across all conditions, demonstrating practical performance for proof verification in both approaches.

The result indicates that when processing high-dimensional acoustic data (132,300 elements), the ZKP circuit incurs a heavy computational cost (526.8s). This explicitly demonstrates the difficulty of processing the raw data in the ZKP, and an AI-based approach is expected

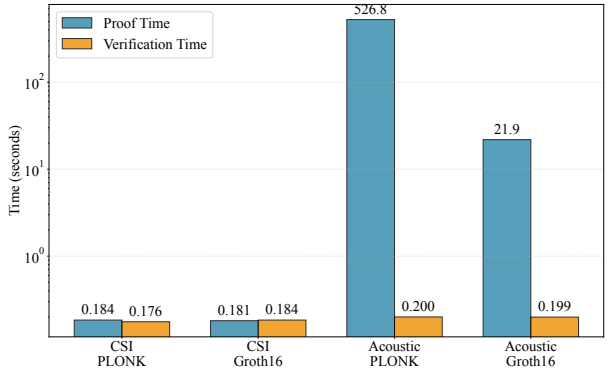


Fig. 8: Real-time Property of Proximity Detection Method Using Zero-Knowledge Proof.

to extract the important features from the raw data. By compressing the raw data into a low-dimensional feature vector using AI, the number of constraints can be reduced by orders of the number of dimensions.

### *D. Security Discussion against Attack Scenarios*

To evaluate the robustness of the proposed system, we discuss its security against three typical attack scenarios: Replay Attacks, Data Tampering, and Privacy Leakage.

*1) Resistance to Replay Attacks:* An attacker may attempt to impersonate a legitimate robot at a specific location by replaying previously recorded CSI or acoustic data. However, the proposed system calculates the similarity between the data sensed by the robot and the data sensed by the fixed sensor nodes at the same timestamp. Since environmental information such as CSI and ambient sound is highly time-variant and location-specific, previously recorded data results in low similarity scores when compared to the current environmental data collected by the facility. Therefore, the replay attack fails to generate a valid proof of proximity.

*2) Prevention of Data Tampering:* A malicious robot might attempt to falsify its location by manipulating the similarity calculation process. In the proposed system, the entire process from feature extraction to similarity calculation is executed within a zkSNARK circuit. The verification on the blockchain ensures that the proof is generated only if the computation is performed correctly according to the predefined circuit. Consequently, it is mathematically impossible for an attacker to generate a valid proof using falsified intermediate values or incorrect algorithms.

*3) Privacy Preservation:* Facility operators might attempt to infer the robot's raw sensor data from the submitted proofs. Thanks to the Zero-Knowledge property of zkSNARKs, the verifier (facility operator) can confirm only the verification result (i.e., whether the similarity score is valid) without gaining access to the private inputs (raw CSI/acoustic waveforms). This ensures that the robot's internal operational data remains confidential.

## VI. Conclusion

In this study, we proposed a system for verifying the reliability of movement trajectories of autonomous mobile robots by measuring environmental information (i.e., CSI and acoustic information) and adopting zero-knowledge proofs to verify the correctness of the processing. The proposed system enables verification of the processing without disclosing the data, thereby achieving both privacy protection and transparency. Through experimental evaluation, we demonstrated the effectiveness of the proposed method for estimating the proximity between two devices. By employing deterministic algorithms, we established a reliable accuracy benchmark, which is essential before transitioning to probabilistic Deep Learning models (e.g., 1D-CNN) for improved computational efficiency in future implementations. Additionally, we confirmed that practical real-time performance can be achieved in proof generation utilizing zero-knowledge proofs.

In future work, we will address the computational overhead identified in the evaluation by integrating Deep Learning models, such as Autoencoders or 1D-CNNs, into the sensor nodes. These models will extract low-dimensional feature vectors from raw environmental data, significantly accelerating ZKP processing. Furthermore, we aim to utilize the verified trajectory data to train anomaly detection models, thereby constructing a comprehensive security system that audits the behavior of autonomous robots.

## Acknowledgement

This work is supported by Japan Society for the Promotion of Science (JSPS) KAKENHI Grant Number JP24K20774, JP24K02916, and JP23K28078.

## References

[1] Ramsey Faragher and Robert Harle, "Location Fingerprinting With Bluetooth Low Energy Beacons," IEEE Journal On Selected Areas In Communications, Vol 33, No 11, pp2418–2428, November 2015.

[2] Yaxiong Xie and Jie Xiong and Mo Li and Kyle Jamieson, "mD-Track: Leveraging Multi-Dimensionality for Passive Indoor Wi-Fi Tracking," MOBICOM'19, October, 2019.

[3] Hankyung Ko, Inguen Lee, Seunghwa Lee, Jihye Kim, and Hyunok Oh, "Efficient Verifiable Image Redacting based on zk-SNARKs," ASIA CCS '21, pp213–226, June 2021.

[4] Chunjie Guo, Lin You, Xigyu Li, Gengran Hu, Shengguo Wang, and Chengtang Cao, "A novel biometric authentication scheme with privacy protection based on SVM and ZKP," Computers & Security, July 2024.

[5] Petros Spachos and Konstations N. Platanitis, "BLE Beacons for Indoor Positioning at an Interactive IoT-Based Smart Museum," IEEE Systems Journal, Vol 14, No 3, pp3483–3493, September 2020.

[6] Hao Gu, Jun Yang, and Haris Gacanin, "TripletMatchNet Based Indoor Position Method Using CSI Fingerprint Similarity Comparison," IEEE Transaction On Vehicular Technology, Vol 72, No 12, pp16905–16910, December 2023.

[7] Gi-z, "CSIKit," https://github.com/Gi-z/CSIKit, Accessed: October 2025.

[8] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Čapkun, "Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound," in Proceedings of the 24th USENIX Security Symposium, pp. 483-496, August 2015.

[9] Jiliang Zhang, Xiao Tan, Xiangqi Wang, Aibin Yan, and Zheng Qin, "T2FA: Transparent Two-Factor Authentication," IEEE Access, Vol 6, pp. 32677-32686, June 2018.

[10] Dan Liu, Qian Wang, Man Zhou, Peipei Jiang, Qi Li, Chao Shen, and Cong Wang, "SoundID: Securing Mobile Two-Factor Authentication via Acoustic Signals," IEEE Transactions on Dependable and Secure Computing, Vol 20, No 2, pp. 1687-1701, March/April 2023.

[11] iden3, "circom: A Circuit Compiler for Zero-Knowledge Proofs," https://docs.circom.io/, Accessed: October 2025.

[12] iden3, "snarkjs: zkSNARK JavaScript Library," https://iden3-docs.readthedocs.io/en/latest/iden3_repos/snarkjs/README.html, Accessed: October 2025.