Data Poisoning Attacks Against RSSI-Based Indoor Localization Systems for Smart Environments

1st Giuseppe Pio La Tosa
Department of Computer Science
University of Pisa
Pisa, Italy
g.latosa@studenti.unipi.it

2nd Michele Girolami
National Council of Research
ISTI-CNR
Pisa, Italy
michele.girolami@isti.cnr.it

3rd Stefano Chessa
Department of Computer Science
University of Pisa and
National Council of Research, ISTI-CNR Pisa, Italy
stefano.chessa@unipi.it

***Abstract*—Indoor localization systems are increasingly adopted in smart environments for asset tracking, access control, emergency management, and people monitoring. RSSI-based localization systems are attractive due to their low cost and compatibility with existing BLE infrastructures, but they are often designed without considering data integrity and security. This work investigates the vulnerability of RSSI-based indoor localization systems to runtime data poisoning attacks. Using a real BLE 5.1 dataset collected in a controlled indoor environment, we implemented a localization pipeline based on RSSI-to-distance estimation, robust multilateration, gating, and temporal filtering. We then analyzed both generic and targeted RSSI manipulation attacks. Experimental results demonstrate that manipulating RSSI measurements from only a subset of anchors is sufficient to steer the reconstructed trajectory toward attacker-defined paths with sub-meter accuracy. The study highlights the importance of integrity protection mechanisms for indoor positioning systems used in smart environments and critical infrastructures.**

***Index Terms*—localization, RSSI, data poisoning, attacks.**

I. Introduction

Indoor localization systems are becoming a fundamental component of smart cities and smart buildings, enabling a wide range of applications such as indoor navigation, healthcare monitoring, emergency management, access control, industrial automation, and asset tracking. In these contexts, location information is often considered reliable and is directly used to support automated decisions and security-sensitive operations. Technologies based on Bluetooth Low Energy (BLE) and Received Signal Strength Indicator (RSSI) measurements are particularly attractive because they can exploit existing wireless infrastructures while maintaining low deployment and maintenance costs. Despite the rapid diffusion of Indoor Positioning Systems (IPS), most research efforts have primarily focused on improving localization accuracy and reducing computational complexity, while security and data integrity aspects are frequently overlooked. However, localization systems are intrinsically vulnerable because position estimation directly depends on wireless measurements collected from the environment. In RSSI-based systems, radio signals are strongly influenced by noise, multipath propagation, attenuation, and environmental dynamics, making malicious manipulations difficult to distinguish from natural signal fluctuations. This issue becomes particularly critical in smart-city and IoT scenarios, where indoor localization systems are increasingly integrated into monitoring and control infrastructures. An attacker capable of altering RSSI measurements can potentially induce the localization system to reconstruct false yet plausible trajectories. Such attacks may compromise access-control systems, monitoring applications, or emergency-management infrastructures by making unauthorized movements appear legitimate. Consequently, localization reliability must be considered not only in terms of accuracy, but also in terms of robustness against adversarial manipulation.

In this work, we investigate runtime data poisoning attacks against RSSI-based indoor localization systems. Starting from a real BLE 5.1 dataset collected in a controlled indoor environment, we implemented a complete localization pipeline based on RSSI-to-distance estimation, robust multilateration, gating mechanisms, and temporal filtering. We then evaluated the impact of several classes of attacks, ranging from simple perturbations to targeted trajectory manipulation attacks formulated as optimization problems.

II. Related Work

Previous research on indoor localization has mainly focused on improving positioning accuracy using RSSI, AoA, CSI, and fingerprinting techniques. RSSI-based systems remain among the most popular approaches because of their simplicity and low deployment cost. At the same time, several studies highlighted the vulnerability of indoor positioning systems to spoofing, replay, relay, and data tampering attacks. Existing literature also demonstrated that manipulated BLE beacons and adversarial perturbations can significantly degrade localization reliability. Nevertheless, few works investigated targeted runtime data poisoning attacks capable of steering trajectory reconstruction toward attacker-defined paths in realistic BLE-based deployments.

III. Dataset and Implemented Localization System

The proposed localization system was developed and evaluated using a real Bluetooth Low Energy (BLE) 5.1 dataset collected by ISTI-CNR within a controlled indoor environment specifically designed for indoor localization experiments [1]. The measurement campaign was conducted in an open indoor area of approximately 110 m^2 (13.8 × 8 m, height 3.1 m), chosen to reproduce realistic propagation conditions while

maintaining a controlled experimental setup. The sensing infrastructure is based on the u-blox XPLR-AOA-1 platform and consists of four BLE anchors positioned along the room perimeter at a height of approximately 2.3 m. The anchors receive BLE advertising packets transmitted by a mobile BLE tag worn by a user during the experiments. Each received packet includes timestamp information, BLE channel, anchor identifier, and two RSS measurements corresponding to different antenna polarizations. Ground-truth positions were manually annotated through a synchronized Android application and associated with known coordinates within the environment reference grid. The dataset includes multiple experimental scenarios designed to reproduce different operating conditions. In the calibration scenario, the BLE tag was positioned at 119 known locations uniformly distributed over the environment. These measurements were used to estimate anchor-specific path-loss models capable of converting RSSI measurements into distance estimates. The static scenario evaluates the effect of body orientation and human attenuation by collecting measurements while a user remains stationary at predefined positions. The mobility scenario, which represents the main reference for this work, contains multiple trajectories acquired while a user walks through the environment at approximately 0.5 m/s. Finally, a proximity scenario includes interactions among multiple users and points of interest to emulate realistic smart-environment applications. The implemented localization pipeline is divided into two main phases. During the calibration phase, RSSI measurements are aggregated and used to estimate empirical polynomial regression models for each anchor independently. These models capture the nonlinear relationship between RSSI and distance under realistic indoor propagation conditions. In the mobility phase, RSSI measurements are aggregated over temporal windows, converted into distance estimates through the calibrated path-loss models, and combined through robust multilateration to estimate the target position. To improve robustness against multipath and noisy measurements, the system integrates several stabilization mechanisms. A robust gating procedure based on residual analysis and Median Absolute Deviation (MAD) identifies inconsistent anchors and removes outlier measurements. Furthermore, a two-dimensional alpha-beta temporal filter smooths the estimated trajectory and reduces high-frequency jitter typically affecting RSSI-based localization systems.

IV. Data Poisoning Attacks

This work investigates both simple and targeted data poisoning attacks against the RSSI-based localization pipeline. Simple attacks include additive Gaussian noise, constant bias, scaling, and packet-drop perturbations applied directly to RSSI measurements. These attacks significantly increase localization errors and distort the reconstructed trajectory. More advanced targeted attacks are formulated as optimization problems. The attacker controls a subset of BLE anchors and injects additive RSSI offsets in order to force the localization system toward reconstructing a predefined target trajectory. The optimization objective minimizes the Euclidean distance between the estimated position and the attacker-selected target path. Since the objective function is non-convex, deterministic coarse-to-fine optimization and Simulated Annealing are adopted to estimate the optimal offsets.

V. Experimental Results

The experimental evaluation demonstrates that RSSI-based indoor localization systems are highly vulnerable to runtime data poisoning attacks. In the baseline configuration, the implemented localization pipeline achieves meter-scale accuracy, with a mean localization error below one meter during mobility experiments. However, even simple perturbations significantly degrade localization performance. Among the analyzed simple attacks, scaling perturbations produced the strongest impact, increasing trajectory reconstruction errors up to approximately 2.18 meters MAE, while Gaussian noise, constant bias, and packet-drop attacks also generated significant distortions in the reconstructed trajectories. These results show that small RSSI manipulations can propagate nonlinearly through the localization pipeline and strongly affect multilateration stability. More importantly, the proposed targeted attacks proved capable of steering the reconstructed trajectory toward attacker-defined paths. Experimental results show that controlling only one BLE anchor allows partial trajectory manipulation, while controlling two or three anchors dramatically improves attack effectiveness. In the most favorable configurations, the manipulated trajectory follows the attacker-defined target path with sub-meter accuracy, reaching errors as low as 20–30 cm with respect to the target trajectory.

The experiments also reveal that the attack objective function is highly non-convex, motivating the use of optimization strategies such as deterministic coarse-to-fine search and Simulated Annealing. Results indicate that increasing the number of compromised anchors is more effective than simply enlarging the admissible RSSI perturbation range.

Overall, the results highlight the practical security implications of data poisoning attacks against indoor localization systems used in smart environments and critical infrastructures. The study emphasizes the need for integrity-aware localization algorithms, anchor authentication mechanisms, and anomaly-detection techniques capable of identifying malicious RSSI manipulations in real deployments.

Acknowledgment

AI tools were used to assist with minor language editing. No generative AI tools were used to create or modify from scratch any figures, images, text contents, or artworks.

References

[1] M. Girolami, F. Furfari, P. Barsocchi, and F. Mavilia, "A bluetooth 5.1 dataset based on angle of arrival and rss for indoor localization," *IEEE Access*, vol. 11, pp. 81 763–81 776, 2023.