Smart Shielding: Using ML and AirTag RSSI Data for Better Privacy

Katharina O.E. Müller[1], Samuel Frank[1], Dario Monopoli [1], Daria Schumm[1], Bruno Rodrigues[2], Burkhard Stiller[1]
[1]Communication Systems Group CSG, Department of Informatics IfI, University of Zurich UZH, Switzerland
[2]Embedded Sensing Group ESG, School of Computer Science SCS, University of St. Gallen HSG, Switzerland
E-mail: [mueller|schumm|stiller]@ifi.uzh.ch, [samuelandreas.frank|darioalberto.monopoli]@uzh.ch, bruno.rodrigues@unisg.ch

***Abstract*—Bluetooth Low Energy (BLE)-based trackers have become increasingly widespread due to their affordability, energy efficiency, and integration into Crowd-Sourced Finding Networks (CFNs). CFNs, such as Apple's Find My system, leverage vast user bases to enable device location even without direct Internet connectivity. However, the expansion of such technologies has raised concerns about security and potential misuse, particularly for unauthorized tracking.**

This paper investigates whether Received Signal Strength Indication (RSSI) data, when combined with Machine Learning (ML) techniques, can enhance the detection and protection mechanisms for individuals targeted by such misuse. A dataset comprising 13,353 labeled entries was collected using Apple AirTags to simulate various tracking scenarios and used to train and evaluate multiple classification models. Among these, a Decision Tree classifier demonstrated a strong balance between accuracy, F1-score, and overfitting resilience, achieving an accuracy of 85.35%. The model was subsequently integrated into HomeScout, marking a promising step toward proactive misuse mitigation in BLE-tracking ecosystems.

***Index Terms*—Internet-of-Things, Personal Trackers, Offline Finding Network, BLE**

I. Introduction

In recent years, Bluetooth Low Energy (BLE) has seen explosive adoption: in 2023 alone, 5.4 billion Bluetooth devices were shipped globally, up from 4.9 billion in 2022, with projections estimating 7.6 billion annual shipments by 2027 [1]. Among BLE devices, personal trackers such as Apple's AirTag, have gained widespread popularity due to their compact design, long battery life, and affordability. These trackers broadcast a unique identifier, and nearby devices can calculate an approximate distance using Received Signal Strength Indicator (RSSI) values. However, RSSI is inherently noisy due to environmental factors such as signal absorption and interference [2]. Despite this, RSSI remains a critical component for proximity estimation and localization tasks, and several studies have evaluated its reliability in indoor environments [3], [4], [5], [6], [7].

AirTag, launched in 2021, leverages BLE and is integrated into its vast Find My network, a crowdsourced finding network (CFN) composed of hundreds of millions of Apple devices. While similar trackers exist from companies like Tile, Samsung, and Chipolo, Apple's dominant ecosystem offers significant location tracking precision and device density. However, this has raised privacy concerns. The ability of trackers to silently piggyback on surrounding devices has resulted in high-profile misuse cases, including stalking incidents and a class action lawsuit [8].

The motivation for this paper lies in addressing the gap in BLE tracker protections for users, particularly in scenarios where multiple trackers are present, such as crowded airports, making it difficult to determine device ownership. Thus, this paper investigates whether proximity estimation of BLE trackers can be used to enhance threat detection in systems like HomeScout [9]. Specifically, it explores the use of Machine Learning (ML) models to estimate the physical distance of AirTags based on RSSI data, thus enabling the detection of potentially malicious trackers based on proximity behavior. The contributions of this paper are as follows:

- Dataset of 13,353 labeled entries and analysis of the correlation between RSSI values and physical distance[1]
- Multiple ML models are evaluated for proximity estimation, with a Decision Tree (DT) being most effective
- Integration into *HomeScout* to improve the detection of potentially malicious BLE-based trackers

The paper is organized as follows: Sections II and III review key concepts and related work. Section IV describes the system design, while Section V covers dataset generation. Section VI presents results and discussion. Section VII concludes with future directions.

II. Background

RSSI metadata reflects the power level of a received signal and is used to assess signal quality in radio frequency systems such as Bluetooth. It is typically expressed in decibels relative to one milliwatt (dBm). Higher RSSI values indicate stronger, more stable connections, while lower values suggest weaker signals prone to interference or attenuation [23].

A. RSSI and Distance

RSSI typically decreases with greater distance due to signal attenuation and propagation loss. While not precise, it provides an approximate indication of proximity between devices [23]. [24] proposed a formula to estimate RSSI based on distance:

$$RSSI[dBm] = -\left(10n \log_{10} d - Tx\right) \tag{1}$$

[1]www.kaggle.com/datasets/katharinaoemller/ble-rssi-to-distance-data

TABLE I: Related Work on ML for RSSI-Based Localization and Proximity Estimation

Paper	Proximity Estimation	Localization	Indoor	Outdoor	Samples	Protocol	RSSI Processing Technique	KNN	SVM	FFNN	RF	GBM	DT
[10]	○	●	●	○	15,000	BLE	n/a	○	○	○	○	○	○
[11]	○	●	○	●	1,500	LoRaWAN	n/a	○	○	○	○	○	○
[12], [13]	○	●	●	○	1,420 (LD), 5,191 (UD)	BLE	n/a	○	○	○	○	○	○
[14]	○	●	●	○	n/a	BLE	MA Filter, RSSI linearization (WLS)	●	●	●	○	○	○
[15]	○	●	●	○	n/a	BLE	Pseudo-Linear Solution (PSL)	○	○	○	○	○	○
[16], [17], [18]	○	●	●	○	n/a	BLE	Kalman filter	○	○	○	○	○	○
[19]	○	●	●	○	n/a	BLE	Mean and median filter	○	○	○	○	○	○
[20]	●	○	●	●	n/a	BLE / UWB	n/a	○	○	○	●	○	○
[21]	●	○	○	●	n/a	n/a	n/a	○	○	○	○	●	○
[22]	○	●	●	○	n/a	n/a	n/a	○	●	○	○	○	○
This paper	●	○	●	●	13,353 (LD)	BLE	MA Filter	●	●	○	●	○	●

where d is the distance between the transmitter and receiver, n is the path loss exponent, and Tx is the transmitted signal strength measured at 1 meter. Rearranging Equation 1, d can be isolated as follows:

$$d[m] = 10^{\frac{RSSI - Tx}{-10n}} \tag{2}$$

B. Significance of RSSI Value Levels

TABLE II: RSSI Signal Strength Interpretation [25]

Signal Strength	Signal Quality
-50 dBm	Excellent
-60 dBm	Very Good
-70 dBm	Good
-80 dBm	Poor
-90 dBm	Very Poor
-100 dBm	No Signal

Table II summarizes how RSSI values relate to signal strength and quality. Strong connections are typically indicated by values near -50 dBm, while signal quality progressively declines as RSSI decreases. Values around -80 dBm or lower indicate poor or unusable connections, with -100 dBm representing no detectable signal.

III. Related Work

As summarized in Table I, this section explores RSSI dataset collection and processing, as well as ML-based localization and proximity estimation across wireless technologies.

Several works have focused on collecting labeled RSSI datasets to support localization research. [10] created a dataset with 15,000 entries using 150 testing points, 15 fixed BLE anchors, and 11 mobile devices in a school building. The inclusion of anchor node coordinates allows for both fingerprint- and model-based localization approaches. [11] gathered RSSI data in a challenging harbor environment using a Low Power Wide Area Network (LPWAN), emphasizing conditions such as high humidity and industrial interference. Similarly, [12] collected a BLE RSSI dataset using 13 ceiling-mounted iBeacons and an iPhone 6s in a university library. The space was divided into a grid, producing 820 labeled and 600 testing samples [13].

[14] builds on the dataset from [13], aiming to enhance RSSI-based indoor localization accuracy, applying a moving average filter and the weighted least squares to address RSSI non-linearity and improve precision. Similarly, [15] emphasizes the importance of applying filtering and linearization techniques prior to training ML models, given the inherent variability in RSSI signals. Aligning with other studies, which highlight that preprocessing RSSI data using methods such as the Kalman filter [16], [17], [18] or mean and median filters [19] is essential for achieving high localization accuracy.

[26] highlights that ML methods such as k-nearest Neighbour (KNN), Support Vector Machine (SVM), DTs, and Neural Networks can improve the accuracy of RSSI-based tracking, though they require substantial data and computational resources. Following preprocessing, [14] trained KNN, SVM, and Feed-Forward Neural Network (FFNN) models on an adapted RSSI dataset, with KNN achieving 85% accuracy. [20] used Random Forest (RF) for improved BLE-based proximity estimation, augmented through precise UWB ranges to achieve centimeter-level precision.

In [21], Gradient Boosted Machines (GBM) were applied to BLE RSSI data for social distancing classification, achieving 92.85% accuracy. [22] applied an SVM model with BLE beacons to localize goods in warehouse settings. Based on this review, combining RSSI filtering with models such as KNN, RF, DTs, or SVM appears most suitable for proximity prediction of BLE-emitting devices like AirTags.

Compared to GPS, RSSI-based localization offers better indoor accuracy and lower deployment and energy costs [27], [28]. [29] developed an indoor tracking system for hospital corridors using two reference nodes and a mobile target. By applying a log-distance path-loss model with an exponentially weighted moving average filter, they achieved accurate position estimates. [30] addressed RSSI-based tracking in underground mines, where signal fluctuations are severe but localization is critical. Their hybrid fingerprinting approach, combining reference nodes, dead reckoning, and statistical averaging, achieved 3.13 m accuracy. [31] explored outdoor BLE-based localization to assist visually impaired individuals at intersections. Using a moving average filter and a KNN model, the system achieved 99.8% classification accuracy.

Following the 2021 launch of Apple's BLE-based AirTags, concerns were raised about inadequate protection for Android users, who lacked passive tracking alerts [32]. In response, Apple released the Tracker Detect app, though it required users to manually scan for threats [9], [33]. To address this, several alternative Android solutions have emerged. AirGuard, developed in [34], reverse-engineers Apple's iOS tracking protection to enable passive detection of potential threats. BLE-Doubt [35] scans for BLE trackers, including non-Apple ones, using time, distance, and a hybrid topological classifier to reduce false positives. HomeScout [9] uses similar parameters but extends detection beyond trackers to all BLE-based devices, such as smartphones and laptops, to identify potential misuse.

IV. Design and Implementation

This section details the creation of a labeled AirTag RSSI dataset, covering data collection, design choices, a custom sniffing app, and its use in training ML models and integrating the best one into HomeScout.

A. Data Collection

The setup used a Tile, Chipolo, 11 AirTags, and an nRF52840 DK for passive BLE sniffing in a controlled lab. All trackers were in "lost mode" to simulate misuse scenarios. Only RSSI values and MAC addresses were recorded. Data collection began with passive scanning to evaluate RSSI behavior across vendors. Due to AirTag's dominance and high variability, later tests focused solely on AirTags. A MAC filter isolated their signals, and scanning could be paused to adjust distances manually.

B. Data Filtering

The AirTag filtering logic follows the approach proposed in [9], based on the method and source code from [34]. AirTag packets are initially identified by checking for manufacturer-specific data containing Apple's Company ID (bytes 8 and 9) and the Offline Finding type (byte 10), implemented through a simple conditional check. As these fields are shared by all Apple Find My devices, further filtering is required. Byte 12 (the status byte) is processed using a bitwise AND with 0x30 to isolate the third and fourth bits from the left, which serve as flags to distinguish AirTags from other Apple devices. A theoretical lookup example is shown in Figure 1.

Given the following example status byte:

$$\texttt{status\_byte} = \texttt{0b00010011}$$
$$\texttt{mask} = \texttt{0x30} = \texttt{0b00110000}$$
$$\texttt{status\_byte} \,\&\, \texttt{mask} = \texttt{0b00010011} \,\&\, \texttt{0b00110000} = \texttt{0b00010000}$$

Isolating the 3rd and 4th bits from the left yields the flag bits:

$$\texttt{flag\_bits} = \texttt{0b01}$$

Fig. 1: Sample Classification of a Status Byte

C. Methodology

Data collection was designed for control and repeatability. AirTags were placed at fixed distances from the DK, from 0 to 2 meters in 10 cm increments, to enable accurate labeling. This range was chosen due to the steep initial RSSI decay. A custom battery tester was used to control battery-related signal variation, with its effect on RSSI analyzed in Section V. All measurements were taken at a single indoor location to reduce environmental variability. The setup ensured consistency through fixed distances, controlled conditions, battery monitoring, and data smoothing to reduce interference. Although distance prediction is inherently a regression task, this work frames it as a classification problem by grouping distances into discrete proximity buckets.

D. Model Selection

Initial testing included DT, RF, Naive Bayes, and Multilayer Perceptron (MLP) to evaluate baselines and the modeling of complex relationships. Consequently, four models were selected for implementation and comparison: DT, RF, SVM, and KNN. DT served as a baseline for RF, which was chosen for its strong performance in prior work, [20], achieved centimeter-level proximity estimation using 100 trees. SVM was included for its reported 84% accuracy in indoor localization, while KNN, noted for its simplicity, achieved the highest reported accuracy (85%) [14].

V. Dataset

This section gives an overview of the dataset, an analysis of the effect of the environments and the battery voltage on the RSSI values. A sample of the dataset and structure can be seen in Table III below.

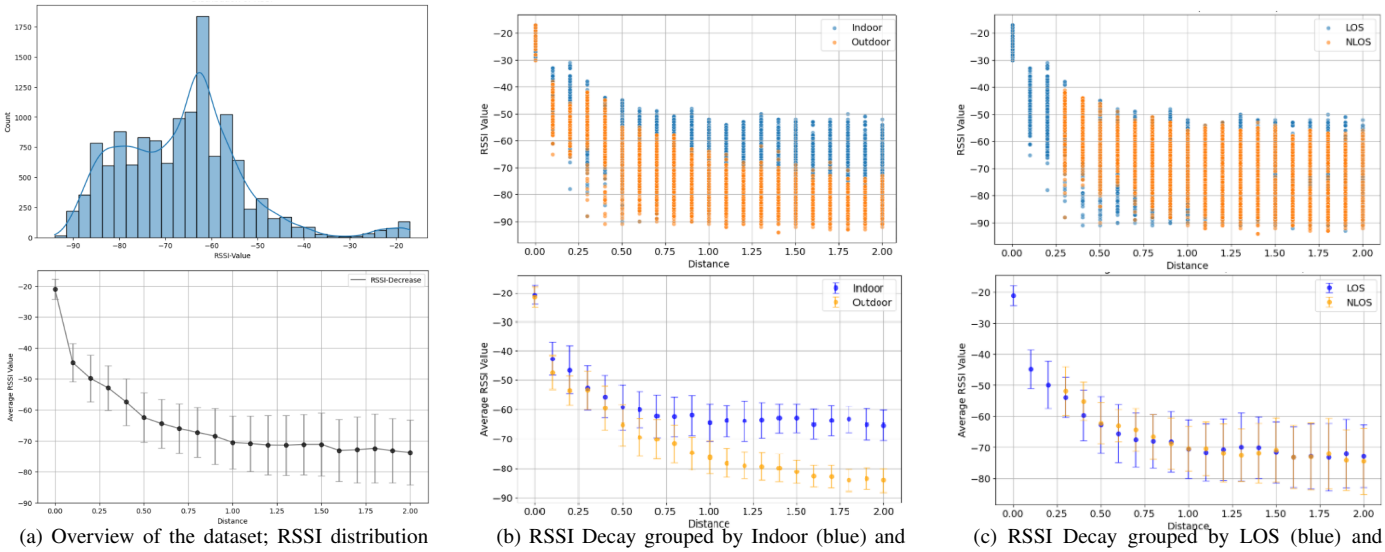
TABLE III: Final Dataset Structure

Index	RSSI-Value	MAC-Address	Timestamp	LOS	Indoor	Distance
0	-19	F0:79:C0:40:FB:93	2024-09-12 09:45:00	1	1	0.0
1	-18	EA:25:00:4F:3C:4D	2024-09-12 09:45:00	1	1	0.0
2	-21	EF:0D:1E:F2:0C:B2	2024-09-12 09:45:01	1	1	0.0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
13352	-82	E8:9B:11:7B:D7:0F	2024-11-30 15:56:26	0	0	2.0

The final dataset includes 13,353 samples labeled by distance taken from 11 AirTags over a period of 37 minutes. Data was collected under all combinations of indoor and outdoor (*c.f.* Figure 2b), as well as Line of Sight (LOS) and Non-Line of Sight (NLOS) (*c.f.* Figure 2c) conditions. Figure 2a shows the RSSI distribution, which clusters around -60 dBm and decreases with distance before leveling off. Increasing error bars suggest that signal noise grows with distance.

A. Environmental Effects

To assess environmental effects, data was grouped by indoor and outdoor settings. As shown in Figure 2b, indoor RSSI values are consistently higher than outdoor ones. In contrast, Figure 2c shows no clear correlation between LOS/NLOS conditions and RSSI values.



(a) Overview of the dataset; RSSI distribution and decay

(b) RSSI Decay grouped by Indoor (blue) and Outdoor (orange) data

(c) RSSI Decay grouped by LOS (blue) and NLOS (orange) data

Fig. 2: Dataset Overview and RSSI Decay Comparisons

B. Battery Insights

To assess battery impact on RSSI, AirTags A7 (3V) and A8 (lowest voltage) were tested at increasing distances from the DK. As shown in Figure 3, A7 unexpectedly showed lower RSSI values than A8, suggesting battery level does not significantly affect RSSI. The baseline was formed by averaging the measurements of all 11 tested AirTag.

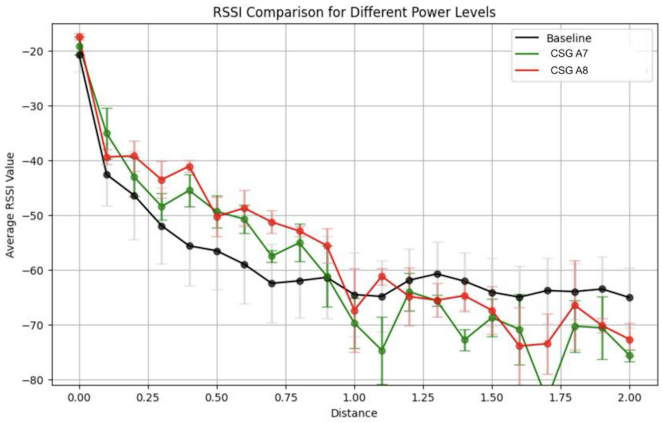


Fig. 3: Battery Effect on RSSI A7 (green) and A8 (red)

VI. Results and Evaluation

This section contains the RSSI behaviour analysis, model comparison, feature analysis, and performance evaluation.

A. Vendor-Specific RSSI Behaviour

Based on the average RSSI values from 10 repeated experiments for AirTag, Chipolo, SmartTag, and Tile across 0 to 10 m (Table IV), the expected RSSI decay over distance is observed. However, significant fluctuations can be observed across all trackers, with a peak Standard Deviation (SD) of ± 15.78 dB for AirTag and an average SD of ± 11.92 dB around the 1.5 m mark, indicating significant mid-range variability. Finally, stabilizing again at longer distances (10 m).

TABLE IV: Mean RSSI Values (dBm ± SD) for Each Device and Distance, Averaged Over 10 Measurements

Device	0 m	0.3 m	0.5 m	1.5 m	4 m	10 m
AirTag	-40.7 (±1.70)	-59.3 (±1.64)	-65.8 (±4.05)	-76.1 (±15.78)	-77.7 (±0.95)	-89.9 (±2.47)
Chipolo	-45.9 (±4.75)	-62.2 (±3.65)	-61.0 (±7.26)	-72.0 (±2.75)	-82.0 (±4.47)	-93.9 (±3.45)
SmartTag	-40.0 (±5.35)	-49.3 (±5.29)	-51.5 (±8.77)	-58.3 (±9.46)	-73.0 (±4.19)	-89.2 (±3.61)
Tile	-31.1 (±3.18)	-50.2 (±9.91)	-54.0 (±5.93)	-60.2 (±3.82)	-64.6 (±3.81)	-86.6 (±3.44)
Mean	**-39.42 (±6.62)**	**-55.25 (±8.06)**	**-58.08 (±8.64)**	**-66.65 (±11.92)**	**-74.33 (±7.41)**	**-89.90 (±4.11)**

This indicates that it is necessary to further investigate each tracker to asses whether these results are vendor-specific divergences, especially considering the massive variability observed in AirTag, the most widely used tracker. Therefore, this paper focuses on investigating AirTag and whether it can be utilized as a general baseline for all further research.

B. Classification Analysis

Initial tests in two different cities revealed a strong environmental influence on RSSI-based distance estimates. Contrary to the vendor-specific analysis, differences are most pronounced at short ranges rather than mid-range, for instance, a ±13.89 dB gap at 0.3 m with a SD of ±9.79 dB, as shown in Table V. Nevertheless, these differences decrease with distance, stabilizing again at longer distances (10 m). Thus, underscoring the need for context-aware models, as those trained in a single environment may generalize poorly.

To address this, the two-city evaluation combined data from both locations, utilizing it to train and evaluate an RF, DT, Naive Bayes, and MLP classifier, to predict distance from RSSI, achieving the results in Table VI.

Overall, Naive Bayes achieved the highest accuracy at 70.30% and showed the smallest difference between training and cross-validated R^2, indicating strong generalization.

TABLE V: Average RSSI Value per Distance Comparison

Distance (m)	Location 1 RSSI (dBm)	Location 2 RSSI (dBm)	Diff (dB)	SD (dB)
0.0	-28.63	-19.99	-8.64	6.10
0.3	-44.83	-58.72	13.89	9.79
0.5	-51.21	-61.28	10.07	7.12
1.0	-64.61	-64.85	0.24	0.17
2.0	-67.35	-73.26	5.91	4.18
4.0	-77.09	-76.36	-0.73	0.52
10.0	-79.62	-82.88	3.26	2.30

TABLE VI: Initial Model Performance Comparison

Model	Training R^2	Cross-validated R^2	Diff	Test Accuracy
RF	0.7219	0.7210	0.0009	0.6432
DT	0.7219	0.7211	0.0008	0.6432
Naive Bayes	0.5644	0.5657	-0.0013	0.7030
MLP	0.7077	0.7086	-0.0009	0.6322

However, all models exhibited minimal overfitting, suggesting a need for more detailed data, such as finer distance increments (e.g., every 10 cm). Additionally, all test results were 10–20% lower than reported in the literature, highlighting the need for further investigation.

C. Categorization

Initially, the data was categorized into multiple discrete classes using the following binning strategy:

[0,1), [1,2), [2,4), [4,10) and [10,∞)

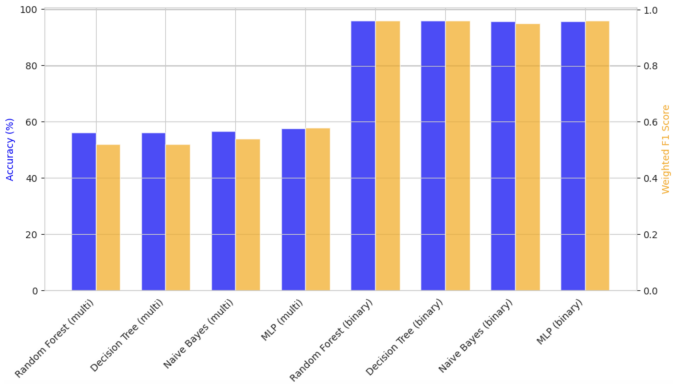


Fig. 4: Classification Performance Using Initial Models on New 13,352 Packet Dataset

As shown in Figure 4, multi-class classification yielded accuracy and F1 scores below 60%, while simplifying to binary consistently raised performance above 80%. Given this improvement and alignment with application needs, subsequent training used the binary approach, treating trackers within 0.5 m as likely malicious.

D. RSSI Smoothening

Following prior work [14], [15], [16], [17], [18], a moving average filter (window size 5) was applied to reduce RSSI noise. The smoothed values, shown in Figure 5, were added as input features for subsequent feature importance analysis.

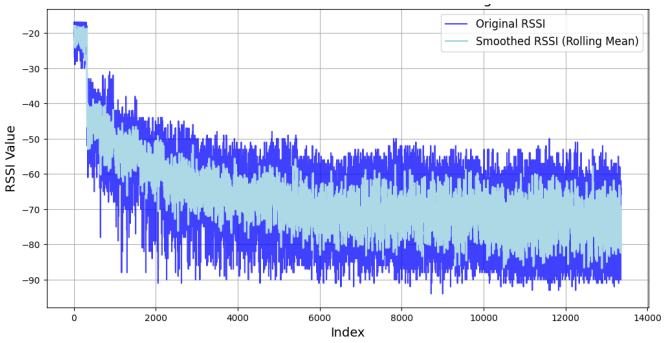


Fig. 5: Visualized Results of the MA Filter

E. Feature Selection

Table III lists the available input features, including RSSI, environment (indoor/outdoor), and visibility (LOS/NLOS). To assess their impact, feature importance was analyzed using DT and RF classifiers, and permutation importance was applied to KNN and SVM.

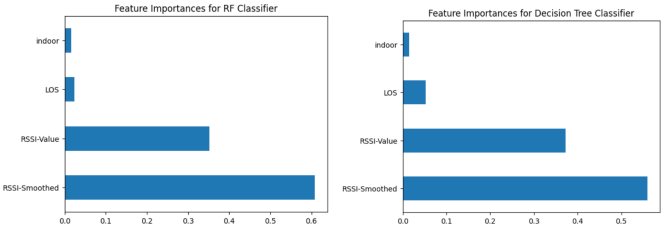


Fig. 6: Feature Importance Analysis: RF and DT

According to the feature importance analysis in Figure 6, Smoothed RSSI is the most influential feature, contributing most to model performance. This aligns with the permutation importance results in Figure 7.

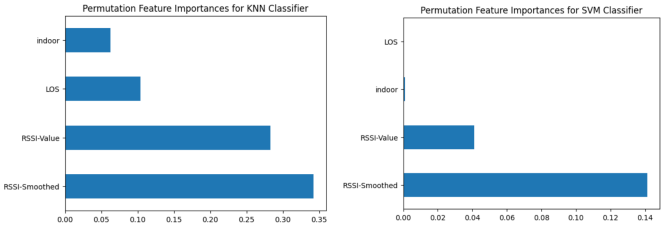


Fig. 7: Permutation Importance Analysis: RF and DT

Smoothed RSSI, the top-performing feature across all models, was included as a classifier input. Indoor and LOS features showed limited overall impact but were retained due to their benefit to KNN performance.

F. Performance Evaluation

This section provides insight into how the selected models performed in the context of the outlined structure. The initial step is to conduct an overview of all models. Subsequently,

the model that has been identified as the most promising in terms of the defined performance score will be the subject of closer examination.

1) Model Overview: A summary of ML performance scores can be found in Table VII. It is noteworthy that the KNN classifier demonstrated satisfactory accuracy with a high weighted F1 score. However, due to the relatively high discrepancy between the test and training accuracy, as well as the inherent risk of overfitting, KNN did not exhibit a good overall performance.

TABLE VII: Comparison of Classifier Performance Metrics

Model	Cross-Validated Accuracy	Weighted F1 Score	Normalized Overfitting Penalty
DT	0.8535	0.8882	0.0297
RF	0.8531	0.8882	0.0297
SVM	0.8411	0.8980	0.0626
KNN	0.8187	0.9064	0.0870

To connect to Sections III and IV, Table VIII compares model performance reported in the literature with the results achieved in this paper.

TABLE VIII: Comparison: Accuracy Results vs Literature

Model	Reference	Reported Accuracy	This Paper (Initial)	This Paper (Final)
DT	N/A	N/A	0.6432	0.8535
RF	[20]	Centimeter-level	0.6432	0.8531
SVM	[14]	0.84	N/A	0.8411
KNN	[14]	0.85	N/A	0.8187
Naive Bayes	N/A	N/A	0.7030	N/A
MLP	N/A	N/A	0.6322	N/A

2) Best Performing Model: As seen in Table IX, the DT achieves a high test accuracy of about 88.6 % and a strong weighted F1 score of about 0.89, which indicates a balanced performance across all classes. The accuracy difference of 0.0297 is relatively small, indicating that the model does not exhibit drastic overfitting. Overall, the model's performance emphasizes its robust effectiveness in this classification task.

TABLE IX: Key Metrics for the DT Classifier

Metric	Value
Training Accuracy	0.8595
Test Accuracy	0.8858
F1 Score (Test)	0.8882
Mean Cross-Validation Accuracy	0.8535 ($\pm$ 0.0103)
Normalized Accuracy Difference	0.0297

The high and consistent accuracy score across different folds further underlines the robustness of the classifier and its ability to generalize to unseen data.

TABLE X: Confusion Matrix for DT on Test Data

True Label	Predicted 0	Predicted 1
0	1901	190
1	115	465

However, since SMOTE was applied only to the training data, the original class imbalance remains in the test set, as shown in the confusion matrix (Table X). Here, label 0 indicates distances over 0.5 m, while label 1 (malicious) indicates distances under 0.5 m.

3) Insights: The strong performance of the DT classifier was not initially anticipated. This result is likely influenced by the simplification of the task into a binary classification problem, which inherently reduces model complexity. Furthermore, the limited number of input features contributes to a lower-dimensional feature space, making it feasible for simpler models to perform well. A key advantage of this outcome is that it enables efficient and lightweight integration into the HomeScout application, while also enhancing model interpretability and maintainability.

G. Resource Consumptions Considerations

In the test case, the classification process took just 26 ms, indicating efficient per-scan handling. To assess battery impact, a fully charged phone with RSSI shielding enabled carried multiple AirTags. Over 40 minutes of tracking protection, battery usage was minimal, with only a 1% drop.

VII. Summary and Future Work

This paper investigated using RSSI data to estimate BLE tracker proximity for detecting potentially malicious devices. Data collected in varied environments confirmed the expected RSSI decay with distance, though with high variance, especially outdoors and in NLOS conditions. Indoor RSSI values were consistently stronger than outdoor ones.

Proximity prediction was framed as a binary classification task: trackers within 0.5 m were labeled malicious; those beyond, benign. Among all models tested, the DT achieved the highest accuracy (85.35%), likely due to the task's simplicity and minimal features, making it ideal for resource-constrained devices and mobile apps. This approach enables threat detection based on actual proximity rather than distance moved, which is especially useful in crowded spaces like train stations. By improving alert precision, the system reduces false positives and data collection, enhancing user privacy.

Future work includes validating the outdoor–RSSI relationship in varied conditions and extending the labeled dataset to other BLE use cases or models. For HomeScout, automating context features such as inferring indoor status via the Google Places API could improve accuracy, but raises privacy and resource concerns. LOS detection remains unresolved; a practical fallback may assume hidden trackers are typically NLOS, such as when concealed in bags or vehicles.

VIII. Ethical Statment

The data collected in this study consists solely of BLE advertisement data, which is freely broadcast and publicly accessible metadata. It does not contain any personally identifiable information, thus anonymous, or patient data, and all payload is removed. Following UZH's ethical policy, such work does not require explicit ethical approval.

REFERENCES

[1] Bluetooth SIG, "2023 bluetooth market update," https://img.anfulai.cn/bbs/118741/2023%20Market%20Update%20_%20Bluetooth%20Technology%20Website.pdf, 2023, visited: 20.02.2024.

[2] Wikipedia, "Bluetooth low energy beacon," https://en.wikipedia.org/wiki/Bluetooth_Low_Energy_beacon, visited: 21.02.2024.

[3] Q. Dong and W. Dargie, "Evaluation of the reliability of rssi for indoor localization," *2012 International Conference on Wireless Communications in Underground and Confined Areas*, pp. 1–6, 2012.

[4] A. Mussina and S. Aubakirov, "Rssi based bluetooth low energy indoor positioning," in *2018 International Conference on Advances in ICT for Emerging Regions (ICTer)*, October 2018.

[5] Y. Wang, X. Yang, Y. Zhao, and Y. Liu, "Bluetooth positioning using rssi and triangulation methods," in *Consumer Communications and Networking Conference (CCNC), 2013 IEEE*. Las Vegas, NV, USA: IEEE, Jan. 2013.

[6] J. Du, C. Yuan, M. Yue, and T. Ma, "A novel localization algorithm based on rssi and multilateration for indoor environments," *Sensors*, vol. 17, no. 9, 2017.

[7] M. N. Amr, H. M. ELAttar, M. H. A. E. Azeem, and H. E. Badawy, "An enhanced indoor positioning technique based on a novel received signal strength indicator distance prediction and correction model," *Sensors*, vol. 21, no. 3, p. 719, 2021.

[8] "Class action complaint," Feb. 2025, last visit 21 of Feb, 2025. [Online]. Available: https://www.classaction.org/media/hughes-et-al-v-apple-inc.pdf

[9] K. O. E. Müller, L. Bienz, B. Rodrigues, C. Feng, and B. Stiller, "HomeScout: Anti-Stalking Mobile App for Bluetooth Low Energy Devices," in *2023 IEEE 48th Conference on Local Computer Networks (LCN)*. IEEE, 2023, pp. 1–9.

[10] Y. Assayag, H. Oliveira, M. Lima, J. Junior, M. Preste, L. Guimaraes, and E. Souto, "Indoor Environment Dataset Based on RSSI Collected with Bluetooth Devices," *Data in Brief*, vol. 55, p. 110692, 2024.

[11] A. Moradbeikie, M. Zare, A. Keshavarz, and S. I. Lopes, "RSSI-Based LoRaWAN Dataset Collected in a Dynamic and Harsh Industrial Environment with High Humidity," *Data in Brief*, vol. 53, p. 110120, 2024.

[12] M. Mohammadi, A. Al-Fuqaha, M. Guizani, and J.-S. Oh, "Semisupervised Deep Reinforcement Learning in Support of IoT and Smart City Services," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 624–635, 2018.

[13] M. Mohammadi and A. Al-Fuqaha, "BLE RSSI Dataset for Indoor localization and Navigation," [Online]. Available: https://www.kaggle.com/datasets/mehdimka/ble-rssi-dataset/, 2018, Last visit December 26, 2024.

[14] M. W. P. Maduranga, V. Tilwari, and R. Abeysekera, "Improved RSSI Indoor Localization in IoT Systems with Machine Learning Algorithms," *Signals*, vol. 4, no. 4, pp. 651–668, 2023.

[15] M. W. P. Maduranga, R. Abeysekera, and V. Tilwari, "Improved-RSSI-Based Indoor Localization by Using Pseudo-Linear Solution with Machine Learning Algorithms," *Journal of Electrical Systems and Information Technology*, vol. 11, no. 1, pp. 10–20, 2024.

[16] L. Alsmadi, X. Kong, K. Sandrasegaran, and G. Fang, "An Improved Indoor Positioning Accuracy Using Filtered RSSI and Beacon Weight," *IEEE Sensors Journal*, vol. 21, no. 16, pp. 18 205–18 213, 2021.

[17] D. R. D. Ainul, S. Wibowo and M. Siswanto, "An Improved Indoor RSSI Based Positioning System Using Kalman Filter and MultiQuad Algorithm," in *2021 International Electronics Symposium (IES)*. IEEE, 2021, pp. 558–564.

[18] M. H. Dwiputranto, D. J. Suroso, and N. A. Siddiq, "Kalman filter for RSSI-based indoor positioning system with min-max technique," *AIP Conference Proceedings*, vol. 2968, no. 1, 2023.

[19] V. R, V. Mittal, and H. Tammana, "Indoor Localization in BLE using Mean and Median Filtered RSSI Values," in *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2021, pp. 227–234.

[20] S. Debnath and K. O'Keefe, "Proximity Estimation with BLE RSSI and UWB Range Using Machine Learning Algorithm," in *2023 13th International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. Nuremberg, Germany: IEEE, 2023, pp. 1–6.

[21] Z. Su, K. Pahlavan, E. Agu, and H. Wei, "Proximity Detection During Epidemics: Direct UWB TOA Versus Machine Learning Based RSSI," *International Journal of Wireless Information Networks*, vol. 29, no. 4, pp. 480–490, 2022.

[22] H. Zadgaonkar and M. Chandak, "Locating objects in warehouses using BLE beacons & Machine Learning," *IEEE Access*, vol. 9, pp. 1–1, 2021.

[23] Telecom Trainer, "RSSI (Receive Signal Strength Indicator)," https://www.telecomtrainer.com/rssi-receive-signal-strength-indicator/, visited: 21.02.2024.

[24] J.-H. Huh and K. Seo, "An indoor location-based control system using bluetooth beacons for iot systems," *Sensors*, vol. 17, no. 12, p. 2917, 2017.

[25] NetSpot, "What is rssi and its relation to a wi-fi network," https://www.netspotapp.com/wifi-signal-strength/what-is-rssi-level.html, visited: 21.02.2024.

[26] R. M. M. R. Rathnayake, M. W. P. Maduranga, V. Tilwari, and M. B. Dissanayake, "RSSI and Machine Learning-Based Indoor Localization Systems for Smart Cities," *Eng*, vol. 4, no. 2, pp. 1468–1494, 2023.

[27] K. Filus, S. Nowak, J. Domańska, and J. Duda, "Cost-effective Filtering of Unreliable Proximity Detection Results Based on BLE RSSI and IMU Readings Using Smartphones," *Scientific Reports*, vol. 12, no. 1, p. 3263, 2022.

[28] D. Biswas, S. Barai, and B. Sau, "New RSSI-fingerprinting-based Smartphone Localization System for Indoor Environments," *Wireless Networks*, vol. 29, no. 3, pp. 1281–1297, 2023.

[29] A. Booranawong, P. Thammachote, Y. Sasiwat, J. Auysakul, K. Sengchuai, D. Buranapanichkit, S. Tanthanuch, N. Jindapetch, and H. Saito, "Real-time Tracking of a Moving Target in an Indoor Corridor of the Hospital Building Using RSSI Signals Received from Two Reference Nodes," *Medical & Biological Engineering & Computing*, vol. 60, no. 2, pp. 439–458, 2022.

[30] M. Cavur and E. Demir, "RSSI-based hybrid algorithm for real-time tracking in underground mining by using RFID technology," *Physical Communication*, vol. 55, p. 101863, 2022.

[31] K. Shin, R. McConville, O. Metatla, M. Chang, C. Han, J. Lee, and A. Roudaut, "Outdoor Localization Using BLE RSSI and Accessible Pedestrian Signals for the Visually Impaired at Intersections," *Sensors*, vol. 22, no. 1, p. 371, 2022.

[32] T. Mayberry, E. Fenske, D. Brown, J. Martin, C. Fossaceca, E. C. Rye, S. Teplov, and L. Foppe, "Who Tracks the Trackers?: Circumventing Apple's Anti-Tracking Alerts in the Find My Network," in *Proceedings of the 20th Workshop on Privacy in the Electronic Society (WPES)*. New York, NY, USA: ACM, 2021, pp. 181–186.

[33] B. Roston, "Apple's New Tracker Detect App Helps Android Users Find Hidden AirTags," [Online]. Available: https://www.slashgear.com/apples-new-tracker-detect-app-helps-android-users-find-hidden-airtags-14702343/, 2021, Last visit July 23, 2024.

[34] A. Heinrich, N. Bittner, and M. Hollick, "AirGuard - Protecting Android Users from Stalking Attacks by Apple Find My Devices," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*. New York, NY, USA: ACM, 2022, pp. 26–38.

[35] J. Briggs and C. Geeng, "BLE-Doubt: Smartphone-Based Detection of Malicious Bluetooth Trackers," in *2022 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2022, pp. 208–214.