From Signals to Trajectories: Passive Tracking Across Wi-Fi Zones

Sheida Nozari
University of Genoa
Genoa, Italy
sheida.nozari@edu.unige.it

Chiara Garibotto
University of Genoa
Genoa, Italy
chiara.garibotto@unige.it

Andrea Sciarrone
University of Genoa
Genoa, Italy
andrea.sciarrone@unige.it

Igor Bisio
University of Genoa
Genoa, Italy
igor.bisio@unige.it

Aldo Grattarola
University of Genoa
Genoa, Italy
aldo.grattarola@unige.it

Fabio Lavagetto
University of Genoa
Genoa, Italy
fabio.lavagetto@unige.it

GLOBECOM 2025 - 2025 IEEE Global Communications Conference | 979-8-3315-7781-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/GLOBECOM59602.2025.11432780

***Abstract*—The Widespread adoption of randomization in modern operating systems has introduced significant challenges for passive monitoring and user tracking in wireless environments. These challenges are further increased in large-scale environments covered by multiple access points, where associating transmission across zones becomes more complicated. This paper presents a frame association-based approach that enables cross-zone tracking and trajectory reconstruction using Wi-Fi probe request frames. The proposed method correlates transmissions across multiple access points by analyzing a combination of fingerprints. Results show that our approach effectively associates frames transmitted from the same origin, tracks devices across multiple zones, and provides insights into user movement and behavior, such as the type of transitions between zones and the reconstructed trajectory, all while preserving user privacy.**

***Index Terms*—crowd monitoring, Wi-Fi tracking, MAC randomization, indoor mobility, trajectory reconstruction**

I. Introduction

In the last decade, the concept of smart buildings has become popular, leading to a growing demand for easy interaction between humans and their surroundings. In this context, wireless communication has played a crucial role, driven by the rapid increase in mobile device usage. These systems leverage the ubiquitous presence of Wi-Fi-enabled devices to gather information about the environment [1], [2]. By analyzing signals transmitted by mobile devices, it becomes possible to monitor crowd behavior [3], understand movement patterns [4], ensuring safety and efficient crowd management [5], [6], and optimize resource utilization in smart environments [7]–[9].

Wi-Fi technology serves as a cornerstone for such applications due to its widespread adoption, and the continuous communication between devices and access points (APs), without requiring additional hardware. One critical aspect of this communication is the transmission of probe request (PRs) frames, which mobile devices send to discover available networks. These PRs contain various information elements that can be analyzed to infer the presence and movement of devices within a given area.

However, the implementation of randomization policies in modern operating systems presents a significant challenge [10]–[12]. This privacy-preserving method generates virtual MAC addresses during PR transmissions, which change randomly in each burst (*i.e.,* a group of frames). It prevents the identification and tracking of mobile devices over time, as traditional methods relying on static MAC addresses are no longer effective.

Previous research has explored various techniques to address these issues [13], [14]. For instance, some studies have proposed identification based on information elements (IEs) [15]–[17] and signal characteristics to group transmissions from the same device despite MAC randomization [18]–[20]. Another metric involves the use of captured RSSI by the AP, while this fingerprint may be useful for the association of virtual addresses [14], [21], [22], they are inconsistent in terms of time and position [23]. Therefore, an RSSI-based association approach is not reliable.

Alternatively, some studies analyze the temporal characteristics of transmitted PR frames, such as inter-frame times, to identify devices with randomized MAC addresses [24]–[26]. However, implementing randomization not only for MAC addresses but also for associated sequence numbers, which had previously increased linearly [14], [27], [28], along with the lack of specific patterns in frame transmission time or burst numbers [11], [29], [30], makes device identification even more challenging. In addition to randomization policies and broadcasting behavior, identifying and tracking mobile devices in a large-scale environment equipped with multiple APs is another critical difficulty that needs to be addressed.

We introduce a frame association framework to address the challenges of tracking mobile devices under modern randomization techniques and environmental complexities. We measure correlations between detected mobile devices across several APs by analyzing multiple fingerprints. It enables tracking through different zones and provides insight into transition behaviors within indoor environments. The main

contributions of this work are summarized as follows.

- We propose a multi-zone tracking framework to identify mobile devices in a large-scale indoor environment equipped with multiple APs, enabling tracking despite randomization techniques while preserving user privacy.
- The presented approach enables reconstruction of movement trajectories as individuals transition between different zones.
- We replicate real-world movement dynamics in a controlled simulated environment, enabling the evaluation of Wi-Fi-based crowd tracking methods before practical deployment.
- The introduced approach adapts to diverse indoor environments, ensuring scalability across different spatial configurations.
- We conduct comprehensive experiments to validate the effectiveness of our approach, demonstrating its capability in crowd monitoring, including transition behaviors and zone preferences.

II. Proposed Methodology

As Fig. 1 illustrates, this section introduces a framework to identify and track individuals in multi-zone environments. In the following, there is a detailed description of the proposed approach steps.

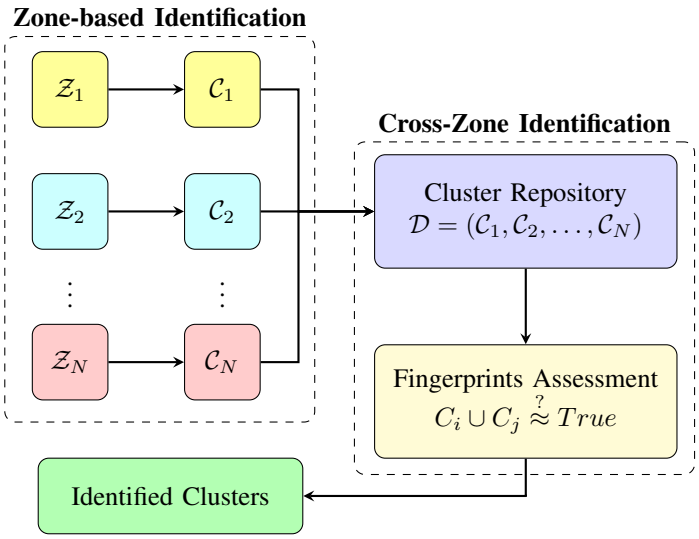

Fig. 1: An overview of the multi-zone identification framework.

A. Environment Observation

The first step is to observe the environment using the Wi-Fi frames transmitted by mobile devices. To address this, we consider the PR frames captured from multiple APs deployed in different zones, denoted as $\mathscr{Z} = \{\mathcal{Z}_1, \mathcal{Z}_2, \ldots, \mathcal{Z}_N\}$, where N is the total number of covered zones in the environment. Given a set of received PR frames $(\mathcal{P})$ from each AP as:

$$\mathcal{Z}_n = \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_M, \tag{1}$$

where $\mathcal{Z}_n \in \mathscr{Z}$ and M represents the total number of PRs collected at $\mathcal{Z}_n$.

B. Zone-based Identification

In this step we consider each zone separately to identify unique mobile devices. To overcome the randomization implementation, we consider common shared characteristics to group PR frames. The association procedure builds upon our previous work, CrowdWatch [31], which utilizes multiple fingerprints to assess the correlation between PR frames. In particular, for each zone the system applies a frame association function $\mathcal{A}(.)$ to group PR frames into sets that correspond to individual devices. It results in a set of clusters $(\mathcal{C})$ that likely each cluster (C) originates from the same device:

$$\mathcal{C}_n = \mathcal{A}(\mathcal{Z}_n), \tag{2}$$

where $\mathcal{C}_n = \{C_1, C_2, \ldots, C_I\}$ is the set of clusters $(C_i \in \mathcal{C}_n)$ formed in zone $\mathcal{Z}_n$.

This zone-based frame association enables cross-zone tracking, which is described in the following section.

C. Cross-Zone Tracking

This step determines whether the detected clusters in different zones correspond to the same mobile device, particularly in cases where an individual crosses multiple zones. Due to randomization policies, direct matching is not feasible. Therefore, we evaluate multiple criteria to establish cross-zone associations, as shown in Algorithm 1.

One of the primary indicators of a shared origin between clusters is the presence of a common MAC address. Each mobile device broadcasts a unique virtual MAC address in each burst (*i.e.,* a group of PRs) [29]. During zone transition, there is a possibility that two APs capture PRs from the same burst. The presence of an identical MAC address in multiple clusters indicates that they originate from the same mobile device.

$$C_i \cup C_j \quad \text{if} \quad \exists MAC \in C_i \cap C_j. \tag{3}$$

This process ensures that clusters detected during the same burst transmission across different zones are associated and identified as a single mobile device.

To evaluate the association between clusters where no identical MAC address is recognized, the method analyzes time overlap. Due to the nature of Wi-Fi broadcasting, two different MAC addresses can not overlap in time for the same device [31]. Therefore, in this step, we analyze timestamp overlaps to determine whether the clusters qualify for further evaluation. To summarize, if there is no time overlap between clusters $(C_i^t \cap C_j^t = \emptyset)$, further measurements are required to verify the association between clusters.

In the next step, if the time constraint does not rule out a potential match, we analyze the extracted IEs such as IE vector, SSID and frame length. It is required to measure the similarity between the IEs vector of clusters. If the computed similarity exceeds a predefined threshold $(\text{Sim}(C_i^{\vec{IE}}, C_j^{\vec{IE}}) > \alpha)$, the

clusters are considered potential matches, and additional measurements are performed.

During broadcasting, mobile devices target previously associated SSIDs to assess connection possibilities. As the final step, among the remaining clusters, if two clusters share a common SSID ($C_i^{SSID} = C_j^{SSID}$) and have the same frame length ($C_i^L = C_j^L$) for that SSID, they are highly likely to originate from the same device. This final verification step refines the association process, ensuring that only clusters with strong evidence of a shared origin are merged.

Therefore, when no identical MAC address is detected, clusters that satisfy both the time overlap and IE evaluation can be associated, as follows:

$$C_i \cup C_j \quad \text{if} \quad \left(C_i^t \cap C_j^t = \emptyset\right) \wedge \left(C_i^{IE} \approx C_j^{IE}\right). \tag{4}$$

Algorithm 1 Cross-Zone Cluster Association

Input: Cluster Repository $\mathcal{D} = \{C_1, C_2, ..., C_N\}$
Output: Identified mobile devices

while there exist unprocessed cluster pairs $(C_i, C_j) \in \mathcal{D}$ **do**
  if $\exists MAC \in C_i \cap C_j$ **then**
    Association: $C^* \leftarrow C_i \cup C_j$
    Update $\mathcal{D} \leftarrow C^*$
    Continue
  if $C_i^{MAC} \neq C_j^{MAC}$ **then**
    if $C_i^t \cap C_j^t \neq \emptyset$ **then**
      Reject association
      Continue
    Evaluate IEs:
    if $\text{Sim}(C_i^{\vec{IE}}, C_j^{\vec{IE}}) > \alpha$ **then**
      if $C_i^{SSID} = C_j^{SSID}$ **and** $C_i^L = C_j^L$ **then**
        Association: $C^* \leftarrow C_i \cup C_j$
        Update $\mathcal{D} \leftarrow C^*$
        Continue
return Updated Cluster Repository $\mathcal{D}$

III. Evaluation and Results

A. Data Collection

To evaluate the proposed approach, we designed a realistic simulation emulating Wi-Fi PRs across multiple locations.

a) Multi-Zone Setup: The simulated environment consists of four zones. Each one is equipped with an AP, strategically to capture PR frames broadcast by nearby mobile devices. The transition between the zones are possible via both stairs and an elevator. The layout supports realistic modeling of movement behaviors such as ascending or descending via stairs or elevator, or pausing in a certain zone.

b) Simulation of Movement: The simulator generates PR frames based on real-world user behavior patterns, simulating a total of 150 mobile devices. It runs for a single working day from 8 : 00 to 17 : 30, including different types of users (*i.e.,* long stay or short visit). Each user is assigned a dynamic trajectory through the environment based on probabilistic movement models, reflecting arrival, zone transitions, and departure times. Movements between zones are annotated by a realistic time delay. Additionally, the simulation incorporates silences to reflect inactive periods when mobile devices do not emit PR frames, such as when the device is in flight mode or turned off.

c) Randomization Implementation: To emulate privacy-preserving behavior, MAC address randomization is implemented in the simulation. Each mobile device periodically changes its MAC address, with a new virtual address used at each burst. In addition, the sequence number is randomly assigned to each frame. The generation of other fingerprints, such as IEs, follows our latest analysis presented in [29]. The APs generate detection logs capturing each PR frame's timestamp, virtual MAC address, and AP identifier (zone label). These logs serve as the foundation for subsequent analysis and cross-zone tracking.

d) Labeling Data: Each simulated mobile device is associated with a user ID, providing a ground truth for assessment. This labeling enables an evaluation of the proposed approach by comparing the findings with the actual behavior of the mobile devices.

B. Experimental Results

In this section, we present the results in terms of identification accuracy and user movement analysis across multiple zones.

a) Accuracy: After applying the proposed frame association approach, 117 mobile devices are correctly identified out of 150 simulated ones, achieving an overall accuracy of 78.31%. This indicates that the proposed approach can effectively associate PR frames and detect transitions across different zones in a dynamic environment.

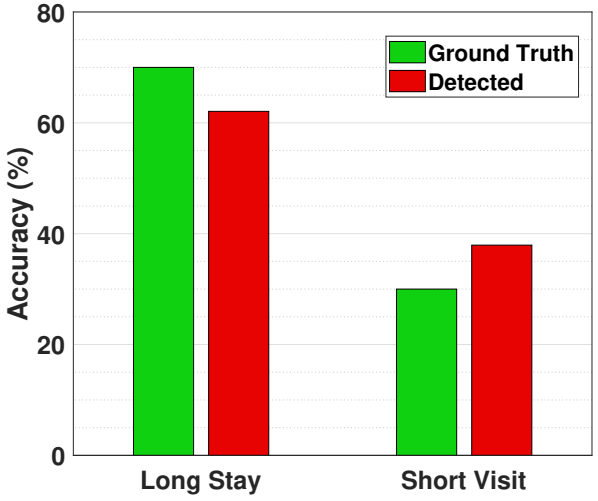

Fig. 2: Distribution of identified user types compared to ground truth.

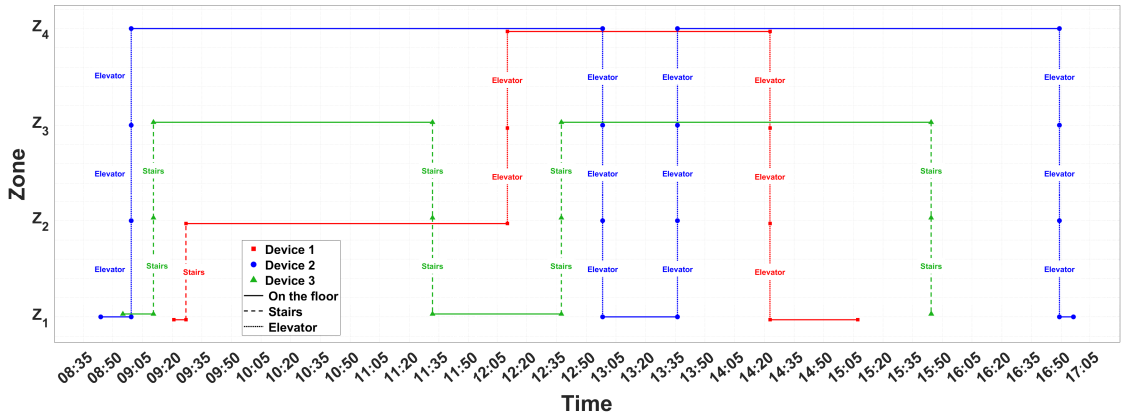

Fig. 3: Detected transitions and zone movements.

Moreover, we analyze the distribution of detected user types compared to the ground truth. In the simulation, the population is composed of 70% long-stay users and 30% short-visitors, as illustrated by the green bars in Fig. 2. Based on the association results, 62.07% of the users are identified as long-stay and 37.93% as short-visit, shown by the red bars. This demonstrates a shift in the classification outcome, reflecting the system's sensitivity to behavioral patterns and duration of presence.

b) Cross-Zone Tracking: After identifying the presence of mobile devices, their movement can be tracked using the APs detection across multiple zones (Z_1 to Z_4). Fig. 3 demonstrates the movement trajectories of three devices as they navigate between zones. Each horizontal segment represents the duration a mobile device remains on a given zone, while vertical transitions indicates movement to other zones. By aligning these detections over time, we can present not only the sequence of zones visited by each device but also how long each one stays in a certain zone. This tracking allows us to analyze a detailed trajectory for each mobile device throughout the day.

As shown in Fig. 3, the transitions are categorized into three types, remaining on the same zone, moving between zones via stair, or using the elevator. To distinguish between these types, we consider the temporal gap and the detection sequence. Remaining on the same zone is identified when a mobile device is continuously detected by the same AP over an extended period without being observed by APs in other zones. For example, in Fig. 3 $Device1$ is continuously captured in Z_2 between $9:26$ and $12:10$.

When a user takes stairs to move between zones, the mobile device is detected consecutively by APs in each intermediate zones, with a short time interval between the last detection in the previous zone and the first capture in the current one. Based on empirical observations, taking stairs between two zones takes $t <= 18$ depending on the pace. Therefore, if APs see a mobile device in successive zones and the time difference between detections is less than the defined threshold, it is classified as a stairs movement. On the other hand, if the time difference is larger and intermediate zones are skipped, it indicates the use of the elevator. Fig. 3 shows three sample trajectories that demonstrate how users may transition between multiple zones. $Device1$ shows a mixed transition pattern, where the user utilizes both stairs and the elevator. In contrast, $Device2$'s trajectory indicates exclusive use of the elevator, and $Device3$ represents a user who moves only via stairs.

TABLE I: Initial detected transition of mobile devices.

Mobile device	Detected by	Transition	Zones
Device 1	$\{AP_1, AP_2\}$	Stairs	$Z_1 \rightarrow Z_2$
Device 2	$\{AP_1, AP_4\}$	Elevator	$Z_1 \rightarrow Z_4$
Device 3	$\{AP_1, AP_2, AP_3\}$	Stairs	$Z_1 \rightarrow Z_2 \rightarrow Z_3$

Moreover, Table I presents the initial detected trajectory of each mobile device after arrival in Z_1. These samples highlight how transition types are inferred based on the sequence and timing of APs detections. $Device1$ is first detected by AP_1 and then consecutively by AP_2, indicating a stairs movement from Z_1 to Z_2, as the time difference between detections falls within the expected threshold. On the other hand, $Device2$ is detected only by AP_1 and AP_4, avoiding Z_2 and Z_3. The longer time gap and the absence of detections in intermediate zones suggest the use of the elevator. Lastly, $Device3$ is sequentially detected by AP_1, AP_2, and AP_3, confirming a stairs-based movement through zones Z_1, Z_2, and Z_3, as indicated by consecutive detections in all intermediate zones with short time intervals between them.

c) Trajectory Analysis: We consider trajectory analysis to understand how detecting the presence of mobile devices over time enables us to reconstruct user trajectories. By identifying when and where each device was detected, we can infer how long it stayed in specific zones and track its movement throughout the environment. Based on this information, we can distinguish between different user roles. For instance, identifying a long-stay user and determining the primary zone of activity, or recognizing a short-visit user based on limited

and brief presence in a certain zone.

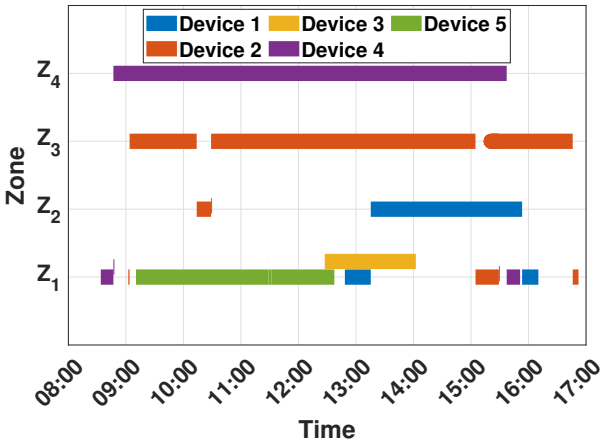

Fig. 4: Zone-level detected trajectories.

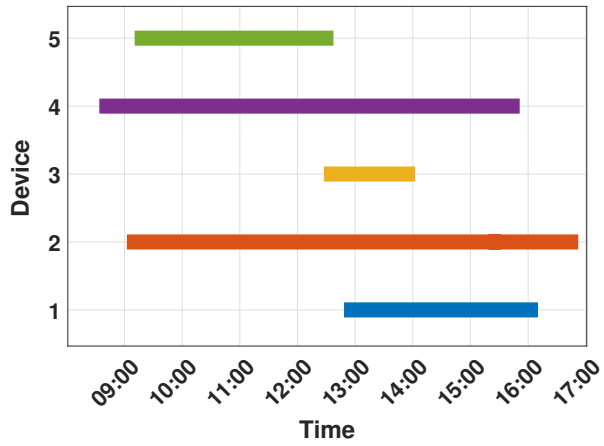

Fig. 5: Full timeline of mobile device presence.

Fig. 4 and Fig. 5 visualize five examples of reconstructed mobile devices trajectories. Fig. 4 displays how each mobile device moves across different zones over time, highlighting the sequence and duration of presence in each zone. This allows us to follow the user's path throughout the environment and observe transitions between areas. Fig. 5 provides a complete view of each device's activity timeline, enabling us to distinguish between short visits (*e.g.,* $Device1, Device3, Device5$) and long stays (*e.g.,* $Device2, Device4$). These visualizations support our earlier claim that analyzing presence patterns makes it possible to infer not only user trajectories but also their likely roles in a certain environment. For instance, long-stay users who spend extended time in higher zones (such as $Device2$ in Z_3 or $Device4$ in Z_4) may correspond to regular occupants, while short visits limited to lower zones may indicate occasional visitors.

IV. Conclusion

We introduced a novel framework for tracking mobile devices and reconstructing user trajectories in multi-zone indoor environments, under realistic conditions involving MAC address randomization. By leveraging multiple fingerprints extracted from PR frames, the proposed approach associates frames broadcast from the same origin and identifies cross-zone transitions.

One of the key contributions of this work is the integration of frame association techniques with movement pattern analysis, enabling not only the reconstruction of user trajectories but also the consideration of user roles based on presence duration and zone activity. This ability to extract behavioral insights from low-level network data represents a significant advancement in privacy-preserving indoor tracking.

The findings show that the approach can accurately identify the mobile devices under randomized conditions and differentiate between user types, enabling a deeper understanding of crowd dynamics. The proposed framework provides a foundation for future applications in smart buildings, monitoring, and public safety, where user movement analysis is critical yet constrained by privacy requirements.

Acknowledgment

This work has been partially funded by the European Union - NextGenerationEU. However, the views and opinions expressed are those of the authors alone and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them. It was carried out within the framework of the project "RAISE – Robotics and AI for Socioeconomic Empowerment" and has been supported by European Union - NextGenerationEU. This work has also been partially funded by the Italian Ministry of Enterprises and Made in Italy (MIMIT) - in the framework the "Development and Cohesion Fund 2014-2020" as per CIPESS Resolution No. 9/2021" - through the House of Emerging Technologies of Genoa (CTE Genova): research, experimentation, and technology transfer center that pursue projects aimed at the use of emerging technologies to support next-generation networks. [CUP B37F23000000008].

References

[1] M. Salman, Y.-D. Soe, and Y. Noh, "Wifi-enabled occupancy monitoring in smart buildings with a self-adaptive mechanism," in *Proceedings of the 38th ACM/SIGAPP symposium on applied computing*, 2023, pp. 759–762.

[2] M. Zakarya, L. Gillam, A. A. Khan, O. Rana, and R. Buyya, "Apmove: A service migration technique for connected and autonomous vehicles," *IEEE Internet of Things Journal*, 2024.

[3] M. Kato, T. K. Rodrigues, T. Abe, and T. Suganuma, "Exploiting radio frequency characteristics with a support unmanned aerial vehicle to improve wireless sensor location estimation accuracy," *IEEE Internet of Things Journal*, 2024.

[4] Y. Zhang, G. Wang, H. Liu, W. Gong, and F. Gao, "Wifi-based indoor human activity sensing: A selective sensing strategy and a multi-level feature fusion approach," *IEEE Internet of Things Journal*, 2024.

[5] A. Basalamah, "Crowd mobility analysis using wifi sniffers," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 12, 2016.

[6] J. R. Santana, L. Sánchez, P. Sotres, J. Lanza, T. Llorente, and L. Munoz, "A privacy-aware crowd management system for smart cities and smart buildings," *IEEE Access*, vol. 8, pp. 135 394–135 405, 2020.

[7] N. Alishahi, M. Nik-Bakht, and M. M. Ouf, "A framework to identify key occupancy indicators for optimizing building operation using wifi connection count data," *Building and Environment*, vol. 200, p. 107936, 2021.

[8] W. Li, M. J. Bocus, C. Tang, R. J. Piechocki, K. Woodbridge, and K. Chetty, "On csi and passive wi-fi radar for opportunistic physical activity recognition," *IEEE Transactions on Wireless Communications*, vol. 21, no. 1, pp. 607–620, 2021.

[9] K. C. J. Simma, A. Mammoli, and S. M. Bogus, "Real-time occupancy estimation using wifi network to optimize hvac operation," *Procedia Computer Science*, vol. 155, pp. 495–502, 2019.

[10] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis," in *Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, 2003, pp. 46–55.

[11] E. Fenske, D. Brown, J. Martin, T. Mayberry, P. Ryan, and E. C. Rye, "Three years later: A study of mac address randomization in mobile devices and when it succeeds." *Proc. Priv. Enhancing Technol.*, vol. 2021, no. 3, pp. 164–181, 2021.

[12] Z. Zhu, S. Chen, and L. Lu, "Research on real mac address acquisition technology for wifi connection," in *2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*. IEEE, 2021, pp. 561–564.

[13] M. Vanhoef, C. Matte, M. Cunche, L. S. Cardoso, and F. Piessens, "Why mac address randomization is not enough: An analysis of wi-fi network discovery mechanisms," in *Proceedings of the 11th ACM on Asia conference on computer and communications security*, 2016, pp. 413–424.

[14] J. Tan and S.-H. G. Chan, "Efficient association of wi-fi probe requests under mac address randomization," in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*. IEEE, 2021, pp. 1–10.

[15] M. Cunche, M.-A. Kaafar, and R. Boreli, "Linking wireless devices using information contained in wi-fi probe requests," *Pervasive and Mobile Computing*, vol. 11, pp. 56–69, 2014.

[16] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "11 user fingerprinting," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, 2007, pp. 99–110.

[17] P. Robyns, B. Bonné, P. Quax, and W. Lamotte, "Noncooperative 802.11 mac layer fingerprinting and tracking of mobile devices," *Security and Communication Networks*, vol. 2017, no. 1, p. 6235484, 2017.

[18] F.-J. Wu, Y. Huang, L. Döring, S. Althoff, K. Bitterschulte, K. Y. Chai, L. Mao, D. Grabarczyk, and E. Kovacs, "Passengerflows: A correlation-based passenger estimator in automated public transport," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2167–2181, 2020.

[19] C. Matte, M. Cunche, F. Rousseau, and M. Vanhoef, "Defeating mac address randomization through timing attacks," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2016, pp. 15–20.

[20] M. Uras, R. Cossu, E. Ferrara, O. Bagdasar, A. Liotta, and L. Atzori, "Wifi probes sniffing: an artificial intelligence based approach for mac addresses de-randomization," in *2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2020, pp. 1–6.

[21] Z. Li, X. Zhao, Z. Zhao, and T. Braun, "Wifi-rita positioning: Enhanced crowdsourcing positioning based on massive noisy user traces," *IEEE transactions on wireless communications*, vol. 20, no. 6, pp. 3785–3799, 2021.

[22] T. He, J. Tan, and S.-H. G. Chan, "Self-supervised association of wi-fi probe requests under mac address randomization," *IEEE Transactions on Mobile Computing*, 2022.

[23] M. Maduraga and R. Abeysekara, "Comparison of supervised learning-based indoor localization techniques for smart building applications," in *2021 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, vol. 4. IEEE, 2021, pp. 145–148.

[24] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 2, pp. 93–108, 2005.

[25] C. Arackaparambil, S. Bratus, A. Shubina, and D. Kotz, "On the reliability of wireless fingerprinting using clock skews," in *Proceedings of the third ACM conference on Wireless network security*, 2010, pp. 169–174.

[26] B. Bezawada, M. Bachani, J. Peterson, H. Shirazi, I. Ray, and I. Ray, "Behavioral fingerprinting of iot devices," in *Proceedings of the 2018 workshop on attacks and solutions in hardware security*, 2018, pp. 41–50.

[27] M. Nitti, F. Pinna, L. Pintor, V. Pilloni, and B. Barabino, "iabacus: A wi-fi-based automatic bus passenger counting system," *Energies*, vol. 13, no. 6, p. 1446, 2020.

[28] G. Chandrasekaran, J.-A. Francisco, V. Ganapathy, M. Gruteser, and W. Trappe, "Detecting identity spoofs in ieee 802.11 e wireless networks," in *GLOBECOM 2009-2009 IEEE Global Telecommunications Conference*. IEEE, 2009, pp. 1–6.

[29] S. Nozari, C. Garibotto, A. Sciarrone, I. Bisio, and F. Lavagetto, "Analyzing broadcast patterns and randomization techniques in wi-fi probe request frames," *IEEE Network*, 2024.

[30] J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, and D. Brown, "A study of mac address randomization in mobile devices and when it fails," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 365–383, 2017.

[31] S. Nozari, H. Haleem, C. Garibotto, A. Sciarrone, I. Bisio, and F. Lavagetto, "Crowdwatch: Privacy-preserving monitoring leveraging wi-fi multiple access information," *IEEE Internet of Things Journal*, 2025.