Wi-Alert: WiFi Sensing for Real-time Package Theft Alerts at Residential Doorsteps

Maya McDonough
mcdonoughms@vcu.edu
Department of Computer Science
Virginia Commonwealth University
Richmond, Virginia, USA

Thomas Moomaw*
tmoomaw@uncc.edu
Department of Computer Science
University of North Carolina at Charlotte
Charlotte, North Carolina, USA

Md Touhiduzzaman
touhiduzzaman@vcu.edu
Department of Computer Science
Virginia Commonwealth University
Richmond, Virginia, USA

Eyuphan Bulut
ebulut@vcu.edu
Department of Computer Science
Virginia Commonwealth University
Richmond, Virginia, USA

ABSTRACT

Since the rapid growth of e-commerce, the number of package deliveries to residential doorsteps has significantly increased. However, the convenience of online shopping has also led to a rise in package theft, resulting in frustration and financial loss for both consumers and companies. While various commercial solutions are available to address package theft, they often have considerable drawbacks, such as high ongoing costs and privacy concerns. In response to these issues, we introduce *Wi-Alert*, a budget-friendly WiFi sensing-based package detection system. Our solution analyzes Channel State Information (CSI) acquired from ambient WiFi signals and employs deep learning models trained to identify movements at the front door. The system accurately distinguishes between various actions, such as knocking, lingering visitors, package deliveries, and package theft. These actions trigger real-time alerts, enabling users to monitor their front door activity and swiftly respond to security threats. Through real-world experiments, we demonstrate the versatility and practical application of the system in diverse residential settings, including houses and apartment buildings. Our solution offers a convenient and economical approach to enhancing package security, providing peace of mind to individuals receiving deliveries.

CCS CONCEPTS

• **Human-centered computing** → **Ubiquitous and mobile computing systems and tools**; • **Hardware** → **Wireless integrated network sensors**; • **Computing methodologies** → *Machine learning*.

*The student was a REU participant at Virginia Commonwealth University when this work was performed.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
MobiHoc '23, October 23–26, 2023, Washington, DC, USA
© 2023 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-9926-5/23/10.
https://doi.org/10.1145/3565287.3617615

KEYWORDS

WiFi sensing, device-free, intruder detection.

ACM Reference Format:
Maya McDonough, Thomas Moomaw, Md Touhiduzzaman, and Eyuphan Bulut. 2023. Wi-Alert: WiFi Sensing for Real-time Package Theft Alerts at Residential Doorsteps. In *The Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '23), October 23–26, 2023, Washington, DC, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3565287.3617615

1 INTRODUCTION

In 2022, research revealed that approximately 49 million individuals in the United States had fallen victim to package theft [18]. The convenience of e-commerce has revolutionized how we shop, allowing us to order a wide range of products and deliver them right to our doorsteps. With the increasing frequency of package deliveries, package theft has become a prevalent problem, causing financial losses, frustration, and security concerns for consumers. This issue has become even more significant since the onset of the pandemic, as the reliance on online shopping has surged [1]. Aside from the financial losses incurred due to stolen packages, consumers have also had to deal with the inconvenience and hassle of filing claims, reordering items, and waiting for replacements. This has decreased consumer confidence and made some individuals less likely to order products online, impacting e-commerce and the overall economy [17].

In response to this ongoing, increasing problem, various commercial package surveillance systems have been developed. Traditional surveillance video cameras and the Ring doorbell are among the more well-known options. As an alternative to these existing systems, we propose a WiFi sensing-based package detection system, *Wi-Alert*, for monitoring front door activity. When comparing our solution with these alternatives, several factors stand out. Firstly, our approach is highly cost-effective, priced under $100, making it significantly more affordable than traditional video cameras or the Ring doorbell, which often come with higher upfront and ongoing costs. The initial investment for surveillance cameras can range from hundreds to thousands of dollars, depending on the brand and features [19]. These cameras may also require professional

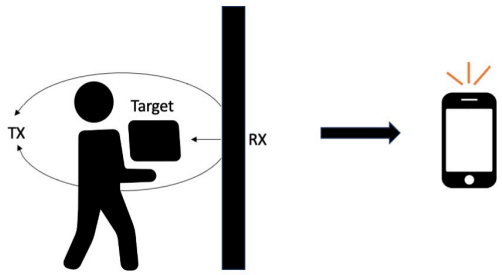

Figure 1: Simplified illustration of our proposed system. WiFi signals propagate the target area to detect the event and trigger a mobile phone alert.

installation, and some require monthly fees for cloud storage. Similarly, the Ring doorbell also involves an upfront purchase cost of around $100, and it comes with an additional monthly or yearly subscription fee for cloud storage and access to certain features, such as person and package alerts [13, 15]. Over time, these ongoing fees can accumulate, making the Ring doorbell a more expensive option in the long run. This cost advantage is crucial for individuals seeking an efficient security solution without incurring excessive expenses.

Privacy is another important aspect when designing a front door alarm system. The continuous recording of activities that camera-based systems require raises significant concerns about unauthorized access to personal information [2]. This leaves users vulnerable to potential breaches from government entities and malicious hackers. However, *Wi-Alert* uses advanced WiFi signal analysis techniques that enable precise alerts without resorting to constant surveillance. This approach enhances security and mitigates potential privacy risks associated with continuous monitoring and data collection. Furthermore, the Ring doorbell's reliance on a stable internet connection for optimal performance introduces an additional factor to consider [14]. Unstable or limited internet service can disrupt video feed and audio quality, potentially leading to gaps in surveillance coverage. This can leave the front door vulnerable, especially during periods of connectivity issues. In contrast, our WiFi sensing system operates seamlessly, unaffected by Internet connectivity limitations, ensuring reliable functionality.

The subsequent sections of this paper are organized as follows. Section 2 provides a background on WiFi sensing technology and discusses relevant research in the field. Section 3 presents the details of our proposed system, highlighting its features, functionality, and live prediction process. The system's performance is evaluated through real-world experiments in Section 4. Finally, in Section 5, we provide our concluding remarks.

2 BACKGROUND

2.1 Channel State Information

WiFi sensing technology harnesses ambient WiFi signals to detect and perceive the physical properties of the surrounding environment [8, 12]. These radio frequency (RF) signals travel through the environment along multiple paths, moving from a transmitter (TX) to a receiver (RX). As these signals interact with various objects in the background, such as walls, furniture, and people, they undergo slight variations.

Channel state information (CSI) is a metric used in frequency-division multiplexing (OFDM). It is employed to characterize the amplitude and phase variations that wireless signals experience across different subcarrier frequencies during transmission between a transmitter and receiver. The following equation models CSI.

$$y^{(i)} = H^{(i)} x^{(i)} + \eta^{(i)} \tag{1}$$

where i is the subcarrier index, x is the transmitted signal, y is the received signal, η is a noise vector, and H is a complex vector containing the CSI denoting the transformation change required from the input x to the output y. The CSI value collected for each subcarrier is a complex number that consists of both a real component ($H_r^{(i)}$) and an imaginary component ($H_{im}^{(i)}$). In the following equations, we can transform this raw CSI into amplitude, $A^{(i)}$, and phase, $\phi^{(i)}$, for subcarrier i.

$$A^{(i)} = \sqrt{(H_{im}^{(i)})^2 + (H_r^{(i)})^2} \tag{2}$$

$$\phi^{(i)} = atan2(H_{im}^{(i)}, H_r^{(i)}) \tag{3}$$

2.2 Related Work

With the advancement of wireless technology, there has been a growing interest in utilizing WiFi sensing for intruder detection, as demonstrated by two recent studies. The first study presented *Wi-Alarm* to monitor and identify when an intruder enters a room [20]. Unlike traditional methods that involve complex data preprocessing, *Wi-Alarm* directly extracts features from the raw amplitude of CSI. This approach enables the system to generate live alerts, ensuring rapid response to potential intrusion.

Similarly, the second study focuses on replicating the monitoring functions of conventional alarm systems [23]. By leveraging commodity WiFi devices, the authors develop a WiFi sensing system capable of detecting human movements and identifying opened/closed doors and windows in various residential settings. While both studies concentrate on replicating alarm systems for intruders entering the home, our system is specifically tailored to address the issue of package theft at residential doorsteps. By concentrating on this particular aspect, we can present a system that requires minimal equipment and installation time while significantly enhancing security.

Limited research has been conducted on package theft detection; however, one approach involves utilizing security cameras to develop a computer vision system for automatic package theft detection [10]. This approach aims to differentiate between normal and intruder behavior by extracting patterns within specific periods of recorded package pickups. The authors propose a novel package detection framework incorporating weakly labeled training videos, allowing the system to adapt to different environments without retraining. While this approach is promising, it relies on visual input and may face challenges in scenarios with limited camera coverage.

Wi-Alert's strength lies in its minimal equipment and its ability to effectively penetrate through and around the target area. This feature makes it particularly suitable for scenarios where visual

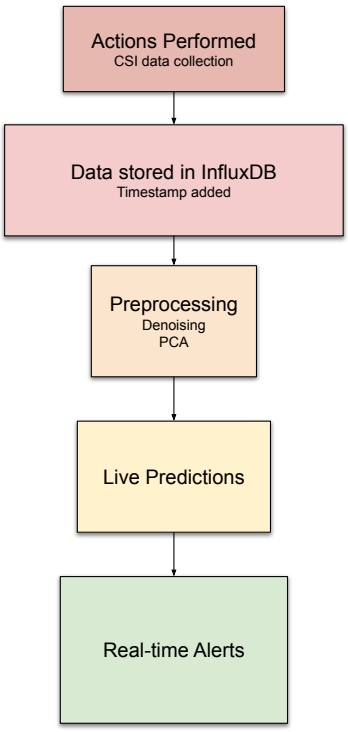

Figure 2: Flowchart depicting the live prediction process.

obstructions could hinder traditional systems relying on video input. By providing a cost-effective and easily deployable solution for package theft detection, *Wi-Alert* offers a practical and efficient alternative for enhancing residential security.

3 OVERVIEW OF *WI-ALERT*

3.1 CSI Data Collection

During the experiments, we collect CSI data using WiFi-enabled ESP32 microcontrollers and the ESP32-CSI Toolkit [4]. Unlike other data collection methods that require a host laptop with an updated Network Interface Card (NIC), these microcontrollers offer a compact, cost-effective, and independent solution. The portability and versatility of the ESP32s facilitate easy deployment. In order to run the proposed solution in resource limited edge devices efficiently, we integrate solutions like online sampling of collected CSI data [7]. In our system, one ESP32 serves as the receiver (RX), capturing the data at 100Hz. Depending on the environment, one or multiple transmitters (TX) may send data frames to the receiver. The stored CSI data from the ESP32 is retrieved and exported to a data file by connecting the receiver to a Raspberry Pi 4B.

3.2 Preprocessing and Machine Learning Model Development

The CSI data undergoes preprocessing steps before being fed into the machine learning model for training. Initially, we denoise the collected CSI data by independently applying a moving average to each subcarrier using a window of size w. Next, we use Principal Component Analysis (PCA) to further denoise and reduce the dimensionality of the collected data.

Once the preprocessing steps are finished, we use the data to train a classifier model, denoted as $\mathcal{M}$. The classifier uses a Dense Neural Network (DNN) architecture with two dense layers. To prevent overfitting, a dropout layer is added between each dense layer. We use a hyperparameter optimization tool designed with the Optuna framework to determine the most effective model configuration. The optimization of the loss function is performed using the Adam optimizer.

Table 1: Details of the experiment data sets collected for the front door alarm.

Environment	Actions	Reps.
Apartment	• Package Placed • Package Taken • Knocking • Standing • Walking By	30
House	• Package Placed • Package Taken • Knocking • Standing • Doorbell	30

3.3 Live Prediction

During the live prediction phase, our system uses the trained classifier model, $\mathcal{M}$, to make real-time predictions on incoming CSI data. This process involves five steps (Fig. 2). Firstly, we collect CSI data using the ESP32 microcontrollers. We then store the incoming data as a string consisting of 28 data fields. Next, we transmit the string to InfluxDB, a time series database, where a timestamp is assigned. InfluxDB enables us to extract specific time windows to analyze the past t seconds of data. Once we group data based on our sliding window size, we run it through the preprocessing steps. The data is subsequently tested against our model $\mathcal{M}$ in batches of t seconds to generate live predictions. In the case of *Wi-Alert*, our model predicts activity every 1 second to detect events at the front door promptly. After completing the live prediction process, the results are transmitted to users through a mobile app.

4 EXPERIMENTS

4.1 Experiment Data

To evaluate the effectiveness of *Wi-Alert*, we collected CSI data for two residential environments. Table 1 presents an overview of the data sets for each scenario, detailing the types of actions and the number of repetitions. To simulate real-world scenarios, each action began with the volunteer walking to the door instead of merely recording the action in isolation. Moreover, we use packages of

Figure 3: (a) Apartment setup (b) House setup (c) Packages used

varying sizes to ensure the system's detection capabilities encompass different types, including parcels and small boxes (Fig. 3c).

4.1.1 Apartment environment. The first data set collected was for the apartment environment. As depicted in Fig. 3a, one TX/RX pair was positioned from the door to the hallway to ensure a direct line of sight (LOS) at the apartment entrance.

The actions performed in this scenario include placing a package, taking a package, knocking, standing, and walking by. The volunteer performed each action for a specific duration: 4 seconds for placing and taking a package, 3 seconds for knocking and standing, and 2 seconds for walking by. The actions were executed in a round-robin manner (i.e., after each action was performed once, the second repetitions were then performed) for thirty repetitions. A 5-second rest period was introduced between each action while ensuring the volunteer was out of the line of sight (NLOS). The round-robin fashion was used to consider the temporal changes in user behavior and enhance the robustness of the machine learning model to such variations.

4.1.2 House environment. The next data set focused on the house environment, specifically setting up a system to cover the front porch area, a typical setup in suburban properties. As shown in Fig. 3b, we positioned the receiver inside the front door, with two transmitters placed outside on the porch posts, diagonally facing the door. Both transmitters emitted signals to the single receiver using the same channel.

The actions performed in this environment included placing a package, taking a package, knocking, standing, and ringing the doorbell. During the data collection for the house environment, we deliberately excluded the walking by action. Individuals within the line of sight of the TX/RX could only be approaching the house. This is in contrast to the apartment environment, where a neighbor or someone passing by in the hallway might walk by the front door, potentially triggering a false alarm. The volunteer performed each action for a specified duration: 5 seconds for placing and taking a package, and 4 seconds for knocking, standing, and ringing the doorbell. We increased the time for each action in this environment due to the additional time required to walk up the steps to the front porch. The actions were again executed in a round-robin manner for thirty repetitions, with a 7 second rest between each.

4.2 Experiment Results

After collecting CSI data for the specified actions in each environment, we developed corresponding deep learning models using the steps outlined in Section 3.2. Half of the collected data for each environment was used as training data, while the other half was reserved for testing.

4.2.1 Apartment results. Using the optimized deep neural network, we achieved an overall accuracy of 78.2% in classifying the actions from our first data set. As illustrated in Fig. 4, the actions of knocking (97.5%) and walking by (94.6%) demonstrated the highest accuracy rates. The accuracy of the walking by action holds particular significance within the apartment environment, as it demonstrates the system's effectiveness in detecting instances of individuals passing through the TX/RX signal path. By achieving a high level of detection for walking by, it substantially reduces the occurrence of false alarms, thereby enhancing the system's overall reliability.

Conversely, the action with the highest misclassification rate is package placed, achieving an accuracy of only 52.76%. The lower accuracy of the package placed action can be attributed to the near-identical nature of package placed and package taken actions, differing only in the presence of an object at the doorstep. The placement of the TX/RX pair in the middle of the front door may lead to weakened signals reaching the bottom of the door where the package is positioned. However, since both actions fall under the category of package events, the higher misclassification rate of package placed as package taken does not compromise the system's fundamental ability to trigger real-time alerts for package-related events.

The most critical accuracy is package taken, in which the apartment model correctly classified and triggered real-time alerts 78.4%

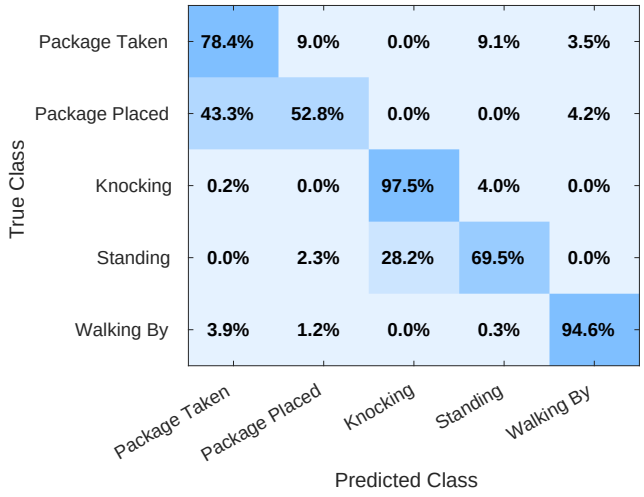

Figure 4: Confusion matrix for the apartment environment (Accuracy: 78.2%)

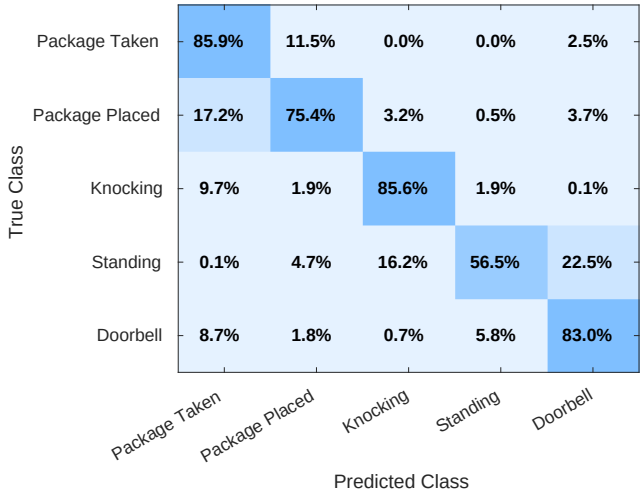

Figure 5: Confusion matrix for the house environment (Accuracy: 77.4%)

of the time. Since package theft events are the primary concern, this level of accuracy significantly contributes to enhancing security by effectively detecting and notifying homeowners of potential theft incidents.

4.2.2 House results. The optimized model for the house environment data set had an overall accuracy of 77.4%. Fig. 5 illustrates that, out of the five actions, the system displayed high accuracy in detecting package taken events (85.9%). Conversely, the standing action demonstrated the lowest accuracy, with a detection rate of only 56.55%. The standing action was mainly confused with the knocking and doorbell actions.

In contrast, both the knocking (85.6%) and doorbell (82.3%) actions exhibited significantly higher accuracies than the standing

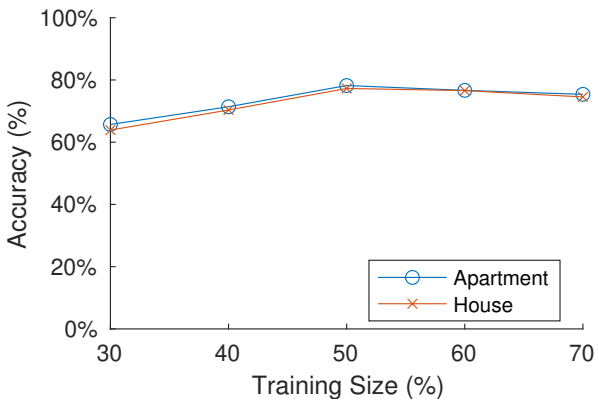

Figure 6: The impact of training data percentage on the accuracy in both environments.

action and were infrequently mistaken for one another. This could be attributed to their distinct characteristics. Knocking typically follows a rhythmic impact pattern, whereas the doorbell action generates a consistent signal. These unique attributes likely generate discernible patterns in the gathered CSI data, facilitating accurate differentiation by the model. The standing action may often be mistaken for the other two since all three actions involve moments of stationary posture, particularly during the approach to the door before initiating the action. This resemblance in the early stages might lead to similar WiFi signal patterns.

A notable difference in accuracy was observed for the package placed action between the house and apartment environments. In the apartment setting, the accuracy was 52.8%, while it increased to 75.4% in the house environment. The difference in accuracy could be attributed to the positioning of the TX/RX pairs in the house environment. Additionally, the presence of walls, corners, and other obstacles in the apartment hallway could cause reflections and multi-path effects, making it more challenging for the system to accurately detect the package placed action.

4.3 Challenges

One of the key challenges we are currently tackling is ensuring our system's adaptability across diverse environments. We are exploring many options for achieving this objective, including analyzing how training data quantity affects accuracy. To this end, we conducted experiments using varying percentages of training data. The trends observed as training data proportions ranged from 30% to 70% are depicted in Fig. 6. The highest accuracy is consistently attained at the 50% training data mark, aligning with the testing size hyperparameter employed by both our optimized models. The graph reveals a general trend across the models, providing strong evidence that the model effectively learns and recognizes the underlying patterns associated with each action, regardless of the specific conditions of those environments. This discovery suggests that the model can generalize, indicating the potential for an environment-independent model—a concept we intend to investigate during our future research [11].

Another approach we are considering to address the system's limited adaptability involves conducting further experiments and data collection across various residential settings. We plan to engage more volunteers and find TX/RX placement alternatives suitable for multiple environments. For instance, one idea involves discreetly positioning the transmitters closer to the ground, integrating them into structures such as rocks or even beneath the soil. This setup could apply to various settings while also enhancing the system's inconspicuous nature.

Furthermore, we are actively working to improve the model's ability to distinguish between closely related actions, such as package placed and package taken. To enhance our model's performance, we are researching various strategies. Firstly, we are exploring potential environmental improvements, such as experimenting with different TX/RX positions, as research has shown that placement adjustments can substantially enhance accuracy [21]. Moreover, we are considering integrating an additional TX/RX pair along the bottom width of the door, aimed at generating a more direct Line of Sight (LOS) for package events. Simultaneously, we also want to explore more advanced techniques for model optimization, such as federated learning [6] and transfer learning [3] to enhance our model's development process.

Note that while WiFi sensing mitigates privacy risks, research has demonstrated that unauthorized entities can still exploit ambient WiFi signals to extract certain information [5, 22, 24]. Recent efforts have introduced potential remedies [9, 16]. We will study how *Wi-Alert* could benefit from incorporating these solutions to protect against such privacy breaches.

5 CONCLUSION

In this research, we introduce *Wi-Alert*, an innovative and cost-effective WiFi sensing package detection system designed for residential doorsteps. Since the rise of online shopping, package deliveries to homes have significantly increased, making front door security a pressing concern. Compared to existing commercial solutions, our system offers a low-cost, privacy-preserving, and versatile approach to monitor for potential security threats. As demonstrated through comprehensive evaluations in various environments, our system can detect multiple actions using optimized deep neural networks.

With its real-time alert capabilities, *Wi-Alert* is an efficient tool in addressing the growing challenge of package theft, offering a proactive and practical approach to safeguarding deliveries and ensuring a sense of security. As we continue refining and expanding *Wi-Alert*'s features, its significance in curbing package theft will likely play an increasingly vital role.

ACKNOWLEDGMENTS

This work is supported in part by National Science Foundation (NSF) Award# 2050958: REU Site: End-User Programming of Cyber-Physical Systems, and by Commonwealth Cyber Initiative (CCI) Award# VV-1Q23-015. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the funding agencies.

REFERENCES

[1] Anam Bhatti, Hamza Akram, Hafiz Muhammad Basit, Ahmed Usman Khan, Syeda Mahwish Raza, Muhammad Bilal Naqvi, et al. 2020. E-commerce trends during COVID-19 Pandemic. *International Journal of Future Generation Communication and Networking* 13, 2 (2020), 1449–1452.

[2] Joey F George, Rui Chen, and Lingyao Yuan. 2021. Intent to purchase IoT home security devices: Fear vs privacy. *PLoS one* 16, 9 (2021), e0257601.

[3] Jingtao Guo, Ivan Wang-Hei Ho, Yun Hou, and Zijian Li. 2023. FedPos: A federated transfer learning framework for CSI-based Wi-Fi indoor positioning. *IEEE Systems Journal* (2023).

[4] Steven M Hernandez and Eyuphan Bulut. 2020. Lightweight and standalone IoT based WiFi sensing for active repositioning and mobility. In *2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 277–286.

[5] Steven M Hernandez and Eyuphan Bulut. 2021. Adversarial occupancy monitoring using one-sided through-wall WiFi sensing. In *ICC 2021-IEEE International Conference on Communications*. IEEE, 1–6.

[6] Steven M Hernandez and Eyuphan Bulut. 2021. WiFederated: Scalable WiFi sensing using edge-based federated learning. *IEEE Internet of Things Journal* 9, 14 (2021), 12628–12640.

[7] Steven M Hernandez and Eyuphan Bulut. 2022. Online stream sampling for low-memory on-device edge training for WiFi sensing. In *Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning*. 9–14.

[8] Steven M Hernandez and Eyuphan Bulut. 2022. WiFi Sensing on the Edge: Signal Processing Techniques and Challenges for Real-World Systems. *IEEE Communications Surveys & Tutorials* (2022).

[9] Steven M Hernandez and Eyuphan Bulut. 2023. Scheduled Spatial Sensing against Adversarial WiFi Sensing. In *2023 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 91–100.

[10] Hung-Min Hsu, Xinyu Yuan, Baohua Zhu, Zhongwei Cheng, and Lin Chen. 2022. Package Theft Detection from Smart Home Security Cameras. In *2022 IEEE International Conference on Multimedia and Expo Workshops (ICMEW)*. IEEE, 1–4.

[11] Wenjun Jiang, Chenglin Miao, Fenglong Ma, Shuochao Yao, Yaqing Wang, Ye Yuan, Hongfei Xue, Chen Song, Xin Ma, Dimitrios Koutsonikolas, et al. 2018. Towards environment independent device free human activity recognition. In *Proceedings of the 24th annual international conference on mobile computing and networking*. 289–304.

[12] Yongsen Ma, Gang Zhou, and Shuangquan Wang. 2019. WiFi sensing with channel state information: A survey. *ACM Computing Surveys (CSUR)* 52, 3 (2019), 1–36.

[13] Ring. [n. d.]. *Doorbell Cameras*. https://ring.com/collections/doorbell-cameras

[14] Ring. [n. d.]. *Improving your Ring Device Connectivity*. https://support.ring.com/hc/en-us/articles/360030391371-Improving-your-Ring-Device-Connectivity-

[15] Ring. [n. d.]. *Ring Protect Plans*. https://ring.com/protect-plans

[16] Paul Staat, Simon Mulzer, Stefan Roth, Veelasha Moonsamy, Markus Heinrichs, Rainer Kronberger, Aydin Sezgin, and Christof Paar. 2022. IRShield: A countermeasure against adversarial physical-layer wireless sensing. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1705–1721.

[17] Ben Stickle, Melody Hicks, Amy Stickle, and Zachary Hutchinson. 2022. Porch pirates: Examining unattended package theft through crime script analysis. In *Field Studies in Environmental Criminology*. Routledge, 106–122.

[18] Security.org Team. 2023. *2022 Package Theft Annual Report*. https://www.security.org/package-theft/annual-report/#:~:text=Nationally%2C%2049%20million%20Americans%20have,)%20to%20%2480%20(Alaska).

[19] Aliza Vigderman and Gabe Turner. [n. d.]. *How Much Are Security Cameras?* https://www.security.org/security-cameras/cost/

[20] Tao Wang, Dandan Yang, Shunqing Zhang, Yating Wu, and Shugong Xu. 2019. Wi-Alarm: Low-cost passive intrusion detection using WiFi. *Sensors* 19, 10 (2019), 2335.

[21] Xuanzhi Wang, Kai Niu, Jie Xiong, Bochong Qian, Zhiyun Yao, Tairong Lou, and Daqing Zhang. 2022. Placement matters: Understanding the effects of device placement for WiFi sensing. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 1 (2022), 1–25.

[22] Leiyang Xu, Xiaolong Zheng, Xiangyuan Li, Yucheng Zhang, Liang Liu, and Huadong Ma. 2022. WiCAM: Imperceptible Adversarial Attack on Deep Learning based WiFi Sensing. In *2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 10–18.

[23] Shaohu Zhang, Raghav H Venkatnarayan, and Muhammad Shahzad. 2020. A wifi-based home security system. In *IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. 129–137.

[24] Siwang Zhou, Wei Zhang, Dan Peng, Yonghe Liu, Xingwei Liao, and Hongbo Jiang. 2019. Adversarial WiFi sensing for privacy preservation of human behaviors. *IEEE Communications Letters* 24, 2 (2019), 259–263.