SecuriFi: Highly Robust Person Intrusion Sensing and Localization System Based on Wi-Fi Signals

Daiyang Zhang¹, Zhanjun Hao*, Xiaochao Dang¹ Gaoyuan Liu¹

¹ College of Computer Science and Engineering, Northwest Normal University, Lanzhou, Gansu, 730070, China
*Corresponding author’s e-mail: haozhj@nwnu.edu.cn

Abstract: Home safety has always been a major concern for every family member. How to quickly sense intrusions while keeping costs low and provide users and police with accurate information about the intruder after sensing the intrusion has become an important challenge for every home security system. So we propose SecuriFi, a highly robust indoor person intrusion sensing and localization system based on Wi-Fi signals. SecuriFi uses Channel State Information (CSI) extracted from Wi-Fi signals as a medium for sensing intrusion and locating people, ensuring high system performance while effectively reducing costs. SecuriFi consists of two modules: intrusion sensing and localization. The intrusion sensing module senses the intrusion behavior by judging the change of signal energy. The localization module effectively removes the environmental noise by constructing a combined filter, and then uses an Extreme Learning Machine (ELM) as a classifier to process and form an offline fingerprint database, which maps the CSI data to the human location. In this paper, SecuriFi is verified in two different real-world environments, and the experimental results prove that SecuriFi has stronger sensitivity to intruders and high localization accuracy at the same time.

1. Introduction
Security has always been an important concern, of which home security is one of the most important security issues, so home security has been a popular topic of research. According to statistics from the Ministry of Public Security, China's annual household losses due to burglary are as high as 1,130 billion yuan. These intruders not only cause damage to a home's property, but also pose a threat to the lives of residents, making home security an issue that needs to be addressed by individuals, families, and society. Therefore research into a home security system that can be universal is also an urgent need at this time.

There are currently 2 main types of home security technologies: optical camera-based devices and sensor-based. Optical camera-based security systems rely on high-performance cameras for continuous monitoring in and around the home. This technology can determine whether there is an intruder in the surveillance area by analyzing the video frames captured by the cameras. However, optical cameras have monitoring dead spots and are extremely dependent on good lighting conditions. The infrared camera does not depend on the light source is expensive, not suitable for ordinary home environment.

Although sensors have better concealment as well as monitoring performance, this technology requires a certain number of sensors to be deployed in the environment for effective monitoring.

Since the above 2 home security technologies have certain limitations, there is an urgent need for a technology to solve these problems. With the development of wireless communication as well as passive sensing technology, people sensing technology based on Wi-Fi signals has become an important technology of interest to researchers. Sensing the human body in the environment using the channel
state information extracted from Wi-Fi signals is one of the main research directions. CSI is a channel feature extracted from the physical layer and is a more detailed description of the channel state, which captures multipath variations in the signal propagation path. Based on these outstanding advantages, CSI has also been used in applications such as human activity detection [1], gesture detection [2], and breath detection [3]. In addition, the large coverage of Wi-Fi signals and the low cost of Wi-Fi devices are also conducive to the promotion of this technology. Therefore, CSI-based indoor security system can achieve high performance security effect while ensuring low cost.

In this paper we propose SecuriFi, a device independent home security system based on Wi-Fi CSI. SecuriFi is divided into two modules: the intrusion sensing module and the localization Module. The intrusion module uses the change in energy of the CSI signal to sense the presence of an intruder. The location module is divided into an offline phase and an online phase. In the offline phase, a location fingerprint database is constructed, and in the online phase, after the intrusion sensing module detects an intruder, the localization module collects the intruder's location information in real time and compares it with the location information in the fingerprint database to obtain the intruder's location. The main contributions of this work are as follows:

- This paper presents SecuriFi, a Wi-Fi CSI signal-based home security system. SecuriFi provides powerful intrusion detection and accurate location services, which can greatly protect users' home security.
- In this paper, we construct location datasets for two environments and use combined filters to process location data more effectively, which greatly improves the usability of CSI signals. We improve the accuracy of localization by constructing ELM classifiers to further process location signals and build an offline fingerprint library.
- We tested SecuriFi in two different real-life scenarios, and the experimental results proved that both modules of SecuriFi performed well in the face of various situations.

2. Related Work

In this section we present the current work related to intrusion awareness and localization from both device-based and device-independent aspects.

2.1. Device based intrusion localization method

There are 2 main types of device-based intrusion location methods: optical camera-based and sensor-based. The intrusion location method based on optical camera equipment mainly relies on high-resolution optical cameras to shoot in the scene, followed by intrusion detection and location through the analysis of the captured video frames. For example, the literature [4] proposed the Watch Net++ system, which uses a deep sequential network to process the human body information extracted from the video frames captured by the camera into thus performing intrusion detection of people. In the literature [5], a new image localization approach is proposed, which uses a neural network approach for 3D geometric inference of a single image with an initial Six Degree of Freedom (6DOF) pose for the localization of an indoor person. Sensor-based intrusion localization methods require deploying a certain number of sensors in the scene or having the user wear relevant sensor devices, such as in the literature [6] using the detection of human footsteps by deploying acoustic sensors thus enabling the detection of human intrusion. The literature [7] enables the localization of indoor and outdoor people by deploying multiple sensors and capturing the signal change patterns of temporal information using Long and Short Term Memory networks (LSTM). However, both of these methods have their own drawbacks, such as the existence of optical cameras with perceptual dead spots and the high cost required for mass deployment of sensors, which limit the popularity of these two technologies.

2.2. Device-Free intrusion localization method

Wi-Fi signal-based intrusion localization as a device-independent technique effectively overcomes the shortcomings of the above two techniques. In previous studies, researchers have mainly used the Received Signal Strength (RSS) extracted from Wi-Fi signals for intrusion detection and localization of
human bodies. The literature [8] proposed the RASID system, which uses RSS signals combined with different anomaly detection modules to sense the intrusion of people and has good environmental adaptability. The literature [9] proposes an adaptive Access Point (AP) selection method that uses a learning algorithm to obtain the best solution for the adaptive AP selection algorithm, and experimental results prove that the method has high performance as well as positioning accuracy. Although the intrusion localization method based on RSS signals can also achieve better results, since RSS is a superposition of all channels, this leads to the fact that the noise contained in RSS signals is also a superposition of all channels, and removing this noise requires more processing work and increases the system overhead. The CSI signal is based on Orthogonal Frequency Division Multiplexing (OFDM) technology, which decomposes the original signal in the channel into multiple non-interfering subcarriers, so CSI can not only provide subcarrier-level channel carving but also effectively resist interference from environmental noise. Therefore, intrusion localization methods based on CSI signals are also being increasingly studied. The literature [10] proposed the AR-Alarm system, which uses the collected ground CSI signals to perform person intrusion detection through an adaptive learning mechanism and achieves robustness to different environments and disturbances. The literature [11] proposed the PetFree system, which can effectively distinguish whether the intruder is a person or a pet by determining the difference in Effective Interference Height (EIH) of CSI signals between a person and a pet. In the literature [12], a density-based spatial clustering algorithm for indoor localization was proposed to classify the human CSI location data using EC-SVM algorithm to obtain the final location results. The literature [13] used the constructed Wavelet Domain Denoising (WDD) method to process the CSI amplitudes and phases, and used the processed data as location fingerprints to construct an offline fingerprint library for human body localization. Therefore, the use of CSI for personnel intrusion sensing and location can effectively improve system performance while reducing costs, and is highly pervasive.

3. SecuriFi System Design
SecuriFi is divided into three parts: data collection and pre-processing, building an offline fingerprint database and online recognition. The specific process of SecuriFi shows in Figure 1.

Figure 1. SecuriFi system flow chart.

SecuriFi is divided into two phases: offline and online. The offline phase collects a large amount of CSI data for each location, filters and smoothes the original data using a moving average filter as well as sym8 wavelets. After that, the best data is selected using PCA algorithm and the root mean square of the best data of each channel is extracted as the feature value of the action. All the processed location
features form a sample set, and ELM is constructed and trained as a classifier. The ELM-processed data are used as fingerprints to construct an offline location fingerprint library.

In the online phase, the CSI data in the environment is first collected in real time, and the intrusion sensing module performs Fast Fourier Transformation (FFT) on the collected CSI data to extract the signal energy, and determines that there is an intrusion when the energy exceeds the threshold value, at which time the localization module collects the current CSI location information of the intruder and matches it with the fingerprints in the offline fingerprint database after the same processing as in the offline phase, and finally derives the matching. The result will be matched with the fingerprints in the offline fingerprint database, and the real-time location of the intruder will be obtained.

3.1. Data Pre-processing

This paper is based on the Intel 5300 NIC for the experimental study, so the CSI information of the 3 channels can be obtained. The specific parameters of the experimental equipment are described in this paper in Section 4.1. Figure 2(a) shows the raw CSI data of three channels at one location for the experimenter, and it can be seen that the raw data contains a large amount of ambient noise, so a combined filter is designed in this paper to process the raw location data using the moving-mean filter as well as the sym8 wavelet function. It can be seen from Figure 2(b) that the processed signal becomes significantly smoother.

![Raw CSI data for three channels](image1)
![Processed CSI data for three channels](image2)

Figure 2. Raw data for three channels at one location and processed data.

After that, the PCA algorithm is used to extract the one data with the highest contribution from each channel as the optimal data for that channel. Figure 3 shows the data of location 1 and location 2 after the selection by PCA algorithm.

![Location 1 data](image3)
![Location 2 data](image4)

Figure 3. After processing by PCA algorithm to extract the best data for each channel.
In the processing of digital signals, the mean square value of the signal can indicate the strength of the signal, so the mean square value is selected as the feature of this position in this paper. The mean square value is calculated as follows.

\[ K = \frac{K_1^2 + K_2^2 + \cdots + K_n^2}{n} \]

where \( K_n \) denotes the data in the \( n \)th bit of the signal to be calculated and \( n \) is the data length of the signal. The eigenvalue of each channel can be calculated by Equation 1.

3.2. Intrusion Sensing

The movement of the human body affects the CSI signal, causing a change in the CSI signal. The figure shows the change in the CSI signal when no one is present and the CSI signal when someone enters.

As can be seen in Figure 4(a), when there is no person in the scene, the CSI signal has remained stable and only the ambient noise has slightly disturbed it. When there is a person intrusion, the CSI signal starts to fluctuate drastically, and it can be clearly seen from Figure 4(b) that the intrusion occurs around 3s again, and the intruder leaves the sensing area after 6s. Therefore, it can be seen from Figure 4 that the intrusion of people can be effectively sensed by using the CSI signal.

Personnel entering into the sensing area will not only interfere with the CSI signal, but also affect the CSI energy in the area. The energy change of the CSI signal can be obtained by performing fast Fourier transform on the CSI signal. In order to make a more effective judgment of the intrusion behavior, this paper uses the energy change of the CSI signal as the judgment criterion of the intrusion behavior. Figure 5 shows the change of FFT energy curve when no one is in the scene as well as when someone is in the scene.

As can be seen in Fig. 5(a), the change in the FFT energy curve is not obvious when the scene is unoccupied, and only a slight change is caused by the ambient noise. Figure 5(b) then shows the change
in the FFT energy curve caused when an experimenter enters the testing area. From the figure, it can be seen that the entry of the testers causes a significant change in the FFT curve. Therefore, in this paper, we set the threshold to detect the change of FFT energy to sense whether there is an intrusion of personnel in the area.

3.3. Building an offline fingerprint library

As shown in Figure 6, ELM is divided into three layers, namely, input layer, hidden layer and output layer, and the input layer mainly consists of the training set \( \{x_i, d_i | x_i \in H^F, d_i \in H^T, i = 1, 2, \ldots, n\} \) of location features, where \( x_i \) is the \( i \)th location feature data and \( d_i \) is the token of the \( i \)th location feature. all three layers are fully connected.

![Figure 6. The structure of the extreme learning machine schematic.](image)

Assuming that the output of the hidden layer is \( F(x) \), it is calculated as follows.

\[
F(x) = [R_1(x), R_2(x), \ldots, R_t(x)]
\]

(2)

where \( F(x) \) is the matrix of the ELM hidden layer output and \( R_t(x) \) is the output of the \( t \)th hidden layer node, which should be obtained by multiplying the input by the corresponding weight plus the deviation, and then processed by a nonlinear function. So usually \( R_t(x) \) is expressed as.

\[
R_t(x) = f(\alpha_t, b_t, x)
\]

(3)

where \( \alpha_t \) and \( b_t \) are the parameters of the hidden layer nodes whose values are randomly generated during the construction of the hidden layer. \( f(\alpha_t, b_t, x) \) is the activation function. In this paper, the Sigmoid function is chosen as the activation function, so the output of the hidden layer after bringing \( f(\alpha_t, b_t, x) \) into the Sigmoid function becomes.

\[
g_t(x) = \sum_{i=1}^{k} \omega_i b_t(x)
\]

(4)

In this equation, \( \omega_i \) is the weight between the hidden layer and the output layer, and \( g_t(x) \) is the result of the output of the hidden layer. However, in the above formula, the weight \( \omega_i \) is an unknown parameter, so it is necessary to solve for \( \omega_i \) using the method of minimizing the approximate squared difference. First, the objective function is constructed as follows,

\[
\min ||\omega F(x) - \delta||
\]

(5)

In the objective function, \( F(x) \) is the output matrix of the hidden layer and \( \delta \) is the objective matrix of the sample data. The optimal solution is obtained after the derivation according to Equation 5 as:
\[ \omega_{\text{best}} = F^\dagger \delta \]  

(6) 

where \( F^\dagger \) is the Moore-Penrose generalized inverse matrix of the hidden layer output matrix \( F(x) \). The ELM classifier can be constructed by the above steps using the sample set of location features. The location data is then processed by the ELM classifier and used as the location fingerprint to build the offline fingerprint library. The pseudo-code for offline fingerprint library construction is shown below.

**Algorithm 1** Construction of an offline Fingerprint Database

**Input:** Sample set of location features \( \{x_i, d_i \mid x_i \in H^x, d_i \in H^y, i = 1, 2, \ldots, n\} \)

**Output:** Offline Fingerprint Library \( F_p \)

1. Determine the number of neurons in the hidden layer // Building ELM classifier
2. Random \( \alpha_i, \beta_i \) // Randomly generate parameters for each hidden layer node
3. \( g(x) = e^x / e^x + 1 \) // Generating the activation function of hidden layer neurons using Sigmoid function
4. \( \omega_{\text{best}} = F^\dagger \delta \) // Calculate output layer weights
5. for \( j = 1, 2, \ldots, n \) do
6. \( x = \{x_i, d_i \mid x_i \in H^x, d_i \in H^y, i = 1, 2, \ldots, n\} \)
7. for \( k = 1, 2, \ldots, i \) do
8. \( g_i(x) = \omega_i b_i(x) + \omega_{i+1} b_{i+1}(x) \) // After processing by ELM classifier to form location fingerprint
9. end for
10. \( F_p = [g_1(x), g_2(x), \ldots, g_n(x)] \) // Building an offline Fingerprint Database
11. end for
12. return

After the above steps, each location feature in the sample set can be turned into a location fingerprint, and an offline fingerprint library can be built by integrating all the location fingerprints.

### 3.4. Online Sensing

The online phase is divided into two parts, firstly, the intrusion sensing module determines whether there is an intrusion, and when an intrusion is sensed the localization module starts to locate the intruder. The complete flow chart of the online phase is shown below.

**Figure 7. Online sensing stage flow chart.**

**Step1:** Real-time collection of CSI data in the environment, after FFT processing to detect whether the energy change exceeds the threshold value to determine whether there is intrusion.

**Step2:** Collect the current location data of the intruder when an intrusion is sensed.

**Step3:** Extract the eigenvalues of the location data as samples after processing with combined filtering.

**Step4:** Input the sample into ELM classifier for processing to get the location fingerprint.

**Step5:** Match the location fingerprint with the fingerprint in the offline fingerprint database to get...
the current location of the intruder.

4. Experimentation and Evaluation

4.1. Experimental setup
In this paper, a total of two experimental scenarios are selected, which are a relatively empty Lobby and a laboratory with a complex environment, as shown in Figure 8(b) and Figure 8(c).

![Experimental equipment](image)

(a) Experimental equipment

![Lobby](image)

(b) Lobby

![Laboratory](image)

(c) Laboratory

Figure 8. Experimental scenarios and experimental equipment.

The transmitter and receiver are arranged in the scenario, and Figure 8(a) shows the transmitter and receiver devices. Two Thinkpad x201i laptops loaded with Intel 5300 NICs are selected as experimental devices, and the CSI-Tool [14] developed by Daniel Halperin et al. can be used to extract CSI data from Intel 5300 NICs. Both computers were equipped with three external antennas with 6Dbi gain, setting up one transmitting antenna and three receiving antennas, for a total of three channels. In addition, five experimenters were set up in this paper, and each experimenter was allowed to collect 30 sets of location data at all locations as a sample set respectively.

4.2. Performance Analysis
In order to verify the overall performance of the SecuriFi system, this paper verifies the intrusion-sensing module and the localization module respectively, and then finally explores the boundaries of the SecuriFi system.

4.2.1. Intrusion sensing module performance testing. In order to verify the sensitivity and interference resistance of the intrusion detection module of SecuriFi system, we tested in two scenarios respectively. Since dropped objects also affect CSI, causing a short-time energy change and thus triggering an intrusion warning, this paper compares human intrusion with dropped objects. Drop items according to the selection of the size in order: pens, water bottles and books. When conducting the fading object experiment, in order to shield the personnel from interference, the experimenter stood still and held the falling object in his hands in advance to ensure that the experimenter made as little movement as possible during the falling of the object. The results of the experiment are shown in Figure 9.
Figure 9. Probability of detecting intrusion for different experimental subjects in two environments.

From the experimental results, we can see that when the experimental object is a person, the probability of detecting intrusion in the hall environment is 98.2%, and the probability of detecting intrusion in the laboratory environment is 97.1%, which is due to the fact that there are more interfering objects in the laboratory, so it has a greater impact on the signal resulting in a lower detection probability. However, the probability of detecting human intrusion in both environments is close to 100%, which proves that the SecuriFi system has extremely high sensitivity to intruders. For different experimental objects, when items are dropped, the probability of triggering intrusion detection increases gradually as the volume of the items increases, but the intrusion detection rate caused by dropping even the largest volume of books in both environments is still below 10%, and the experimental results prove that the SecuriFi system has a strong anti-interference property.

4.2.2. Localization module performance testing. The robustness of the localization module is also an important factor in determining the performance of the SecuriFi system, so this paper verifies the robustness of the SecuriFi system to the environment as well as to the people by analyzing the localization errors of different experimenters in two environments. In this paper, we collect data from multiple sets of different locations for each experimenter separately and calculate the positioning error for each set of data. The experimental results are shown in Figure 10.

Figure 10. Localization error for each experimenter in different environments.

From the results, we can see that when the experimenter is in the hall, the environment is relatively...
empty, so the signal interference is less, and the positioning error is relatively low, and the average positioning error remains at 1.05m, while in the laboratory, due to the complex environment, the signal interference is also amplified, resulting in a higher positioning error, and the average positioning error is 1.28m. The average positioning error was still within 1.3m even in the complex laboratory environment, indicating that the positioning module of the SecuriFi system is highly robust to different environments and people, and has good positioning performance.

4.2.3. SecuriFi system boundedness detection.
The system boundary is also an important indicator to evaluate the system performance, which is the performance of the SecuriFi system in the face of multi-user detection. Therefore, this paper explores the system boundary for two aspects: (1) the influence of other interferers in the environment on the localization results. (2) The accuracy of multi-user localization. The experiments were conducted in two experimental environments, and the results are shown in Figure 11.

![Figure 11](image_url)

(a) Impact of Different Interferers (b) Impact of Multiple Experimenters

Figure 11. Impact of different number of interferers and the impact of multiple users.

Figure 11(a) shows the effect of different number of interferers on the localization error, with a total of up to four interferers, and the localization error when there are no interferers is set as a comparison test. From the experimental results, the localization error gradually increases with the increase of the number of interferers in the scene. The average positioning error remains within 1.5m when the number of interferers is within 2, and remains within 2.5m even when the number of interferers increases to 4. The experimental results prove that the SecuriFi system has satisfactory robustness against interference from people.

Figure 11(b) shows the positioning error of multi-user positioning, and it can be seen that the average positioning error can be kept within 2m when there are 2 experimenters. However, with the increase of the number of experimenters, the average positioning error increases significantly, and reaches about 4m when there are 4 experimenters in the scene. Therefore, for the SecuriFi system, the positioning performance can be maintained well when the number of users is within 2.

5. Conclusion
In this paper we present SecuriFi, a Wi-Fi CSI-based intrusion detection and localization system. SecuriFi consists of two modules: intrusion sensing as well as localization. For the intrusion detection module, SecuriFi determines whether there is an intrusion by monitoring the FFT energy change of CSI data. In the offline phase, SecuriFi constructs a combined filter to process the original data, after which the extracted location features are processed by ELM classifier and used as fingerprints to build a fingerprint database. The online phase compares the real-time location fingerprints after the same processing with the fingerprints in the offline fingerprint library when an intrusion is detected to obtain the final location. The performance of the two modules is verified in two different environments and the
experimental results show that the SecuriFi system performs satisfactorily in various aspects.

Acknowledgments
This work was funded by:
(1) National Natural Science Foundation of China (61762079).
(2) Gansu Province Science and Technology Support Key R&D Program Project (20YF8GA048)
(3) 2019 Chinese Academy of Sciences "Light of the West" Talent Program

References
[1]. J. Huang, B Liu, et al. (2020) Towards Anti-Interference Human Activity Recognition Based on WiFi Subcarrier Correlation Selection. IEEE Transactions on Vehicular Technology. 69:6739-6754.
[2]. Z. Guo, F. Xiao, B. Sheng, H. Fei and S. Yu, (2020) WiReader: Adaptive Air Handwriting Recognition Based on Commercial WiFi Signal. IEEE Internet of Things Journal. 7: 10483-10494.
[3]. A Khamis, B Kusy, C T Chou, W Hu, (2020), WiRelax: Towards real-time respiratory biofeedback during meditation using WiFi, Ad Hoc Networks. 107:1-13.
[4]. Villamizar, M., Martinez-González, A., Canèvet, O. et al (2020) WatchNet++: efficient and accurate depth-based network for detecting people attacks and intrusion. Machine Vision and Applications. 31:1-14.
[5]. Qing L, Jiasong Z, Jun L, et al (2020) 3D map-guided single indoor image localization refinement. ISPRS Journal of Photogrammetry and Remote Sensing. 161:13-26.
[6]. S. G. Iyengar, P. K. Varshney and T. Damarla, (2007) On the Detection of Footsteps Based on Acoustic and Seismic Sensing.In: 2007 Conference Record of the Forty-First Asilomar Conference on Signals, Systems and Computers. Pacific Grove, CA, USA. pp. 2248-2252.
[7]. Y. Zhu, H. Luo, F. Zhao and R. Chen, (2021) Indoor/Outdoor Switching Detection Using Multisensor DenseNet and LSTM. IEEE Internet of Things Journal. 8:1544-1556.
[8]. M. Youssef and A. Kosba, (2012) "RASID demo: A robust WLAN device-free passive motion detection system. In: 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). Lugano. pp. 531-533.
[9]. W. Zhang, K. Yu, W. Wang and X. Li, (2021) A Self-Adaptive AP Selection Algorithm Based on Multiobjective Optimization for Indoor WiFi Positioning. IEEE Internet of Things Journal. 8:1406-1416.
[10].Li S , Li X , Niu K , et al. (2017) AR-Alarm: An Adaptive and Robust Intrusion Detection System Leveraging CSI from Commodity Wi-Fi.In: International Conference on Smart Homes & Health Telematics. Paris France. pp. 211–223.
[11].Y. Lin, Y. Gao, B. Li and W. Dong, (2021) Revisiting Indoor Intrusion Detection With WiFi Signals: Do Not Panic Over a Pet!. IEEE Internet of Things Journal. 7:10437-10449.
[12].Hao Z, Yan Y, Dang X, Shao C. (2019) Endpoints-Clipping CSI Amplitude for SVM-Based Indoor Localization. Sensors. 19:3689-3705.
[13].Dang X, Tang X, Hao Z, Liu Y. (2019) A Device-Free Indoor Localization Method Using CSI with Wi-Fi Signals. Sensors. 19:3233-3250.
[14].Halperin Daniel, et al., (2011) Tool release: Gathering 802.11n traces with channel state information. ACM SIGCOMM Computer Communication Review. 41: 53-53.