IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 1, 2021, accepted April 19, 2021, date of publication April 28, 2021, date of current version May 7, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3076176

Secure Region Detection Using Wi-Fi CSI and One-Class Classification

YONGJAE YOO[1], (Graduate Student Member, IEEE), JIHWAN SUH[1], (Graduate Student Member, IEEE), JEONGYEUP PAEK[2], (Senior Member, IEEE), AND SAEWOONG BAHK[1], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering and INMC, Seoul National University, Seoul 08826, Republic of Korea
[2]School of Computer Science and Engineering, Chung-Ang University, Seoul 06974, Republic of Korea

Corresponding author: Saewoong Bahk (sbahk@snu.ac.kr)

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1A2C2101815).

ABSTRACT Location-based authentication for Internet of Things (IoT) devices can be used to permit activation and participation only to those devices that are in their predefined areas. It secures the devices from being used elsewhere (e.g. misplacement or theft), and also secures the system by preventing non-authorized devices from joining the network. However, absolute location is not required for such purposes; only whether the device is within the designated 'secure' region or not matters, which we define as the *secure region detection* problem. In this work, we propose *SWORD*, the first *secure region detection* scheme based on channel state information (CSI) of Wi-Fi and deep *one-class classification (OCC)* technique. OCC can be trained using data only from the inside of a secure region and no negative reference point is required, a critical advantage considering that outside of a secure region is practically unbounded. Our real-world experiment results show that *SWORD* can achieve 99.14% true-negative rate (TN, successfully rejecting devices not in secure region) and an acceptable true-positive (TP) of 76.90% for practical usage. Furthermore, there is an user-adjustable trade-off between TN and TP based on application requirement, and TP can be improved to 97.92% without a big loss of TN using simple automatic repeat mechanism.

INDEX TERMS Secure region detection (SRD), one-class classification (OCC), Wi-Fi, channel state information (CSI), the IoT authentication.

I. INTRODUCTION

Imagination of Internet of Things (IoT) devices being used ubiquitously in daily life has become a reality. The number and diversity of IoT applications, devices, and users have experienced enormous increase in recent years [1]. Consequently, security of IoT devices in terms of both the physical hardware and access to them has emerged as an important issue [2]. However, the sheer diversity of IoT devices makes generally-applicable and user-convenient security solutions challenging.

Location-based authentication (LBA) is a compelling technique for IoT security that allows a device to be activated or accessed only at a predefined location. It prevents devices from being used elsewhere (e.g. theft, misplacement, manipulation), and allows legitimate devices to access the system only from the correct location. However, absolute location is not required for such purposes; only whether the device is within the designated 'secure' region or not matters, which we define as the *secure region detection (SRD)* problem.

Secure region detection would be an obvious task if precise absolute location is given. However, practical and precise indoor localization is challenging and expensive (Section II-A). Existing approaches have various limitations such as privacy concerns, complexity, number of devices required to provide the desired coverage, accuracy, and most importantly, the *"amount of training process and data needed"*. For example, camera-based localization [3], [4] has gained spotlight recently thanks to its high accuracy with the development of computer vision and machine learning techniques. However, considering the large number of IoT devices, cost, scale, and privacy issues hinder their wide practical use.

The associate editor coordinating the review of this manuscript and approving it for publication was Vicente Alarcon-Aquino.

Wi-Fi-based localization has been studied extensively during the past two decades (e.g. pioneering work in [5]) with acceptable accuracy in testbed settings. However, trilateration based techniques suffer low accuracy in practice due to complexity of indoor wireless environments. Fingerprinting-based methods can be accurate, but the biggest drawback is that they require enormous learning data which is labor intensive [6], [7]. It is not only a tedious task to collect data from reference points 'within' the target region, but is practically infeasible to collect corresponding negative data since 'outside' of a target space is practically unbounded.

Our intuition is that *secure region detection* is a problem that can be solved by knowing only whether the device is inside the target area, and therefore, we can achieve both practicality and accuracy with far less data collection effort. With this insight, we propose *SWORD*, a **S**ecure, **W**i-Fi and **O***ne-class classification* (OCC) based, **R**egion **D**etection scheme. *SWORD* achieves accuracy by extracting spatial features from Wi-Fi CSI (which has 56 subchannel [1] amplitude values as opposed to a single channel RSS), and solves the problem of unbounded learning data collection effort through OCC (Section III).

We implement *SWORD* on commercial Wi-Fi NICs, and evaluate its performance through real experiments to show that *SWORD* achieves an excellent true-negative (TN) ratio of 99.14%, which means non-authorized devices outside the secure region are correctly rejected. This comes with an acceptable true-positive (TP) of 76.9%, which can be augmented with a few automatic retries to achieve 97.92% for practical use. Furthermore, there is a fundamental trade-off between TN and TP depending on user policy, and the parameter can be tuned based on application requirement.

The contributions of this paper are as follows;

- We define the new *"secure region detection"* problem, and discuss how it can overcome the challenges of existing RF-based localization work by taking advantage of its characteristics.
- We propose *SWORD*, a novel secure region detection scheme. To the best of our knowledge, this is the first work that uses *one-class classification* on Wi-Fi CSI to solve the region detection problem using data *only* from the target region without any *negative reference data*.
- We implement *SWORD* on a commercial Wi-Fi chip and evaluate its accuracy through real world experiments.

The remainder of this paper is organized as follows. Section II motivates this work by providing background and related work. Then, Section III presents the design of our proposed scheme *SWORD*. Section IV evaluates the SRD performance of *SWORD* through real implementation and experiments. Finally, we conclude the paper in Section V.

[1]The IEEE 802.11 standard defines 64 subcarriers with 20MHz bandwidth: 48 for data, 4 pilot, and 12 virtual. However, commercial Atheros chip provides measurement from only 56 subcarriers. Intel allows 30.

II. BACKGROUND AND RELATED WORK

In this section, we first introduce the existing wireless signal-based indoor localization research, and point out their limitations. Then, the reason for using CSI data to characterize Wi-Fi signal for spatial information will be described. We present a preliminary study which shows how Wi-Fi CSI performs with binary classification technique, and motivate our work on one-class classification and why it should be used.

A. WIRELESS SIGNAL-BASED INDOOR LOCALIZATION

Indoor localization has been an interesting research topic especially since the emergence of IoT and smart mobile devices [5], [8], [9]. Approaches based on wireless/RF signals have gained the most popularity among them because they do not require additional sensors such as IMU or camera, and most IoT devices are already equipped with wireless interfaces. Most RF-based localization techniques can be categorized into trilateration /triangulation [10]–[12] and fingerprinting [5], [13] methods, and latter has been regarded relatively more accurate due to complex nature of indoor wireless environments. However, several papers point out that obtaining data for fingerprinting is labor-intensive [6], [7]. Thus, there have been many studies that attempt to improve the accuracy of localization while reducing the effort required to obtain training data.

In order to improve accuracy, Luo and Hsiao [14] augmented Bluetooth low energy (BLE) beacons to a Wi-Fi-based localization system at places where it is difficult to distinguish Wi-Fi signals between two different reference points. Then, received signal strength (RSS) of both the Wi-Fi and BLE are used for fingerprinting to improve accuracy. Similarly, Tong *et al.* [15] also proposed to use BLE to improve the accuracy of Wi-Fi-based system, but with crowd-sourced BLE data instead of controlled fingerprinting. Sun *et al.* [16] pointed out that constructing a sophisticated wireless map using Wi-Fi is time-consuming, and proposed a Gaussian process regression model to predict the spatial distribution in uncorrected domains. Although this reduces the fingerprinting effort, accuracy was sacrificed.

Machine learning techniques have been popular for indoor localization as well. DeepFi [17] is a deep-learning-based indoor fingerprinting system using Wi-Fi CSI, which uses a four-layer neural network and a greedy learning algorithm for training the model. ConFi [18] maps Wi-Fi CSI amplitude data from 3 antennas as RGB image, and uses a convolutional neural network (CNN) on that image for indoor localization. More recently, Xun *et al.* [19] have also devised a method using Wi-Fi CSI and a CNN, and divided a room into several smaller subareas while training their CNN to overcome the complexity problem.

Although the aforementioned papers either improve accuracy or reduce the effort in obtaining reference point (RP) training data with the aid of prediction, machine learning, or other sensors, a common problem with these methods in

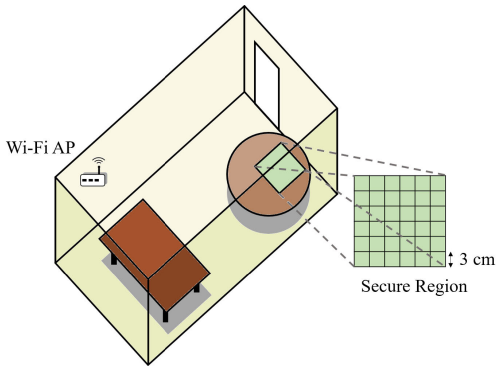


FIGURE 1. Example: secure region on a table (green grid area). An user device can be unlocked only when in that region.

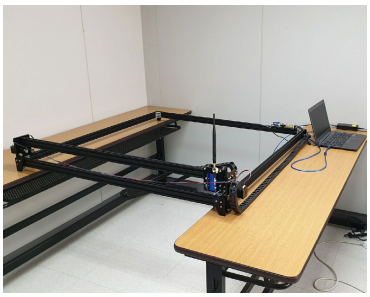


FIGURE 2. Equipment for accurate and fine-grained CSI measurements.

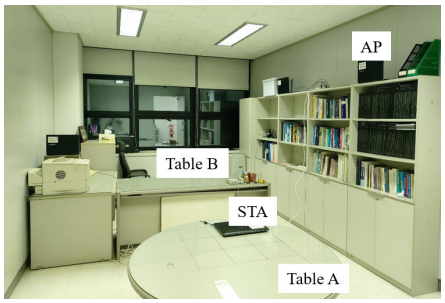


FIGURE 3. Experimental setup for binary classification of two tables.

the context of *secure region detection* is that RP information outside the target area is still required for fingerprinting. Obtaining radio signal information from RP outside the target area is not impossible, but would be very labor intensive and ambiguous in many cases since 'outside' is practically unbounded. We fundamentally solve this problem by devising a method using one-class classification that does not require information outside the target area for *secure region detection*.

B. Wi-Fi CSI

RSS is one of the most widely used measure in wireless systems for various purposes such as ranging, localization, link quality measurement, and routing due to its fundamental relation with physical distance [20]. For example, Heo *et al.* [21] classified users as in- and outside of a room using RSS of Wi-Fi. However, it fluctuates significantly due to multipath, fading, and occupants in the environment, and its granularity is insufficient to capture delicate spatial information. Furthermore, it provides only a single feature (per AP) to accomplish the classification task.

In this work, we aim to learn the features of a space using Wi-Fi CSI data which has substantially more information than RSS [22]. Modern Wi-Fi signals are transmitted through multiple subcarriers (e.g. 56 with 20 Mhz bandwidth) using OFDM modulation. Thus, CSI data (amplitude and phase[2]) can be obtained from the channels experienced by each of these 56 subcarriers, which can provide a multitude of more temporally fine-grained information about the characteristics of each location.

Regarding the spatial granularity of information, it is well known that two channels measured at a distance greater than half-wavelength are uncorrelated [23]. At Wi-Fi's 2.4 GHz band, half-wavelength is about 12 cm long. Therefore, to distinguish a target area from elsewhere with only the training data obtained from the target area, the spatial granularity of reference points must be at most 6 cm or less. To this end, information about the target area is obtained at intervals of 3 cm in our proof-of-concept implementation. This makes it possible to learn a target space larger than half a wavelength through the surrounding reference points.

C. PRELIM: BINARY CLASSIFICATION ON Wi-Fi CSI

Before investigating the feasibility of *one-class classification* for *secure region detection*, we first need to confirm whether Wi-Fi CSI captures sufficient information about the region of interest to distinguish different regions. For this purpose, we perform a preliminary region identification experiment using a traditional binary classification technique. Note that this is 'not' our proposal; our goal is to detect a secure region using data only from the target region, without any negative data, using one class classification, not binary classification.

First, we select two tables in an office room to obtain Wi-Fi CSI data. On each table, we create an 18×18 cm^2 secure region, and divide the region into a 6×6 grid of 3×3 cm^2 units. We actually draw a 6×6 grid on each table and measure the Wi-Fi CSI at the vertices (reference points) of each 49 grid crossings (FIGURE 1). Then, we collect 500 Wi-Fi CSI data samples per RP (each sample consists of 56 subcarrier amplitude values), which totals 49,000 samples (500 samples * 49 grid points * 2 tables). The data collected from table A and table B are labeled 1 and 0, respectively, where table A is regarded as the 'secure region'. Illustration of the experiment setup can be found in FIGUREs 1 and 3.

Using this dataset, we train a fully connected neural network that classifies the two tables. We set up a total of two hidden layers and one output layer. Each hidden layer has 16 and 8 nodes, and the activation function is leaky ReLU. Then, we generate another test dataset of 1,000 samples by

[2]In this work, we have used only the amplitude because phase had more variability. We plan to investigate the use of phase info in our future work.

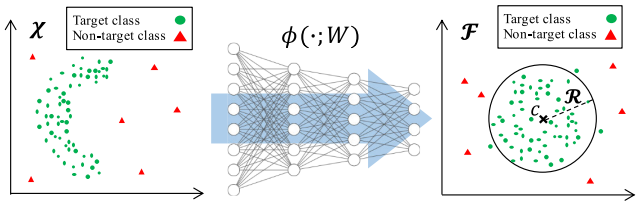


FIGURE 4. Deep one-class classification overview [26].

obtaining Wi-Fi CSI data from several internal points of the secure region other than the vertices of the grid. Finally, we use this test dataset as the input to classify tables.

The result turns out to be straight forward: it is possible to distinguish the two tables with 100% accuracy (100% TP and TN). This means that Wi-Fi CSI data contains enough information to identify regions of interest. However, *secure region detection* is not a balanced binary classification problem like the previous table A vs. table B example. In a practical and general SRD scenario, it is infeasible to get all data outside the secure region; 'all' is undefined. This leads us to consider one-class classification, which we explain next.

III. DESIGN OF *SWORD*

This section presents the design of *SWORD* including one-class classification and why it should be used, the structure of *SWORD*'s neural network, and how it removes outliers using *density-based spatial clustering of applications with noise* (DBSCAN) [24].

A. ONE-CLASS CLASSIFICATION (OCC)

OCC is a machine learning classification technique that conducts learning with only the data of the target class [25], [26]. Then, when a test input data is given, it is determined whether the input corresponds to the target class or not. This method of learning is very effective and convenient when there are vast amount or types of *outside* classes available, or when the information from outside classes cannot be fully covered. It is widely used for *abnormality detection* because it can detect various unknown or unpredictable classes.

To achieve this goal, each data sample $\mathcal{X}$ is transformed and mapped into a feature vector space $\mathcal{F}$ using a kernel function ϕ, and OCC aims to find the smallest hypersphere in the feature vector space $\mathcal{F}$ that contains all of the training data. This hypersphere is centered at point c with a radius $\mathcal{R}$ (which is found through the learning process), and OCC expects that training data will be gathered in a somewhat small hypersphere if they are similar enough to be grouped into a single class. The process of obtaining the kernel function ϕ through a deep neural network is well documented in the paper by Ruff et.al [26], and FIGURE 4 illustrates how it works. We inherit this concept in our design in Section III-B. After that, OCC classifies the new test data by determining whether it is inside or outside the hypersphere.

Our idea is to apply this OCC technique on Wi-Fi CSI data for *secure region detection* problem. However, using too

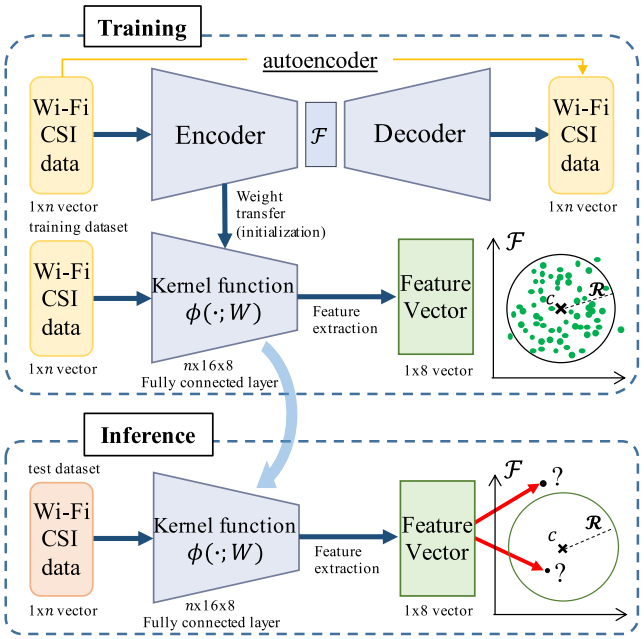


FIGURE 5. *SWORD* system overview.

many dimensions of data can result in not only prolonged training time but also poor learning performance. Therefore, we aim to extract only the core features from CSI data that has sufficient information, and obtain a kernel function ϕ that can transform the data into a new, more distinct vector space. We expect to get an appropriate center point c and a well distinguishing hypersphere radius $\mathcal{R}$ through this process.

B. NEURAL NETWORK STRUCTURE OF SWORD

SWORD uses a deep neural network as the kernel function to classify secure region. FIGURE 5 depicts an overview of the *SWORD* system. Firstly, Wi-Fi CSI data is converted into a vector of 8-dimensional feature space $\mathcal{F}$ in order to obtain a hypersphere with better classification performance. As mentioned in Section III-A, a kernel function ϕ performs this conversion, and the data passing through the kernel are clustered around the center point c. To build this kernel function, we use an autoencoder. The autoencoder is a method of training a neural network whose input and desired output are both training data to extract the key features of that data. The autoencoder is divided into an encoder part and a decoder part, and embeds feature information in a hidden layer between the two parts. We create a hidden layer with 16 nodes between the input layer and the encoded layer, and the encoded layer has 8 nodes which represents the 8-dimensional feature vector. Once the autoencoder is trained, we convert the training data into feature vectors using only the encoder part of the trained autoencoder. (The trained encoder part acts as the kernel function.) Then, we set the center point c as the center-of-mass of the transformed feature vectors.

This process is based on the following intuition and expectation;

- Wi-Fi CSI data measured from the secure region will (most likely) be clustered near the center point c in the feature space $\mathcal{F}$.
- Wi-Fi CSI data measured outside the secure region will (most likely) be beyond a certain distance $\mathcal{R}$ from the center point c in the feature space $\mathcal{F}$.

If our expectation holds with high probability, we can draw a hypersphere with distance $\mathcal{R}$ as the radius to distinguish the inner versus outer points. To meet these expectations, we additionally train the encoder part taken from the autoencoder to be a suitable kernel function. In the training phase of the kernel function, the kernel's initial weight follows that of the learned autoencoder.

SWORD learns the following new objective function,

$$\min_{W} \frac{1}{n} \sum_{i=1}^{n} \|\phi(x_i; W) - c\|^2 + \frac{\lambda}{2} \sum_{l=1}^{L} \left\| W^l \right\|_F^2, \qquad (1)$$

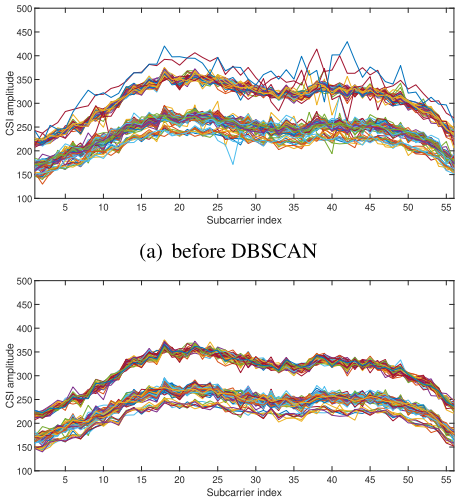
where W is the weight of the neural network, and the added second term is the regularization term. Through the first term, the neural network learns with the goal of getting the x value converted through the kernel function ϕ as close as possible to c in the feature space. Finally, it determines the smallest hypersphere radius $\mathcal{R}$ that can contain *as many data points as possible*.

In the inference phase, *SWORD* converts the newly entered data point into the feature space $\mathcal{F}$ through the learned kernel function ϕ. Then, whether the feature vector is inside the hypersphere or not determines whether the data point belongs to the secure region or not.

The selection of radius $\mathcal{R}$ during the training process can be tuned based on the application requirement and policy; If $\mathcal{R}$ is more relaxed, higher TP rate is expected at the cost of lower TN. On the other hand, if $\mathcal{R}$ is selected more tightly, higher TN is expected at the cost of lower TP. Thus, there is an inevitable trade-off depending on the tightness policy for selecting $\mathcal{R}$. Note that in the SRD scenario, TN is more critical; devices outside the secure region should not be authorized or activated while devices inside the secure region can afford a few retries. Thus, we tune *SWORD* to train $\mathcal{R}$ such that TN is higher than TP.

C. OUTLIER ELIMINATION

To use wireless signal for classification, it is necessary to extract a feature set that can well represent the reference point. However, Wi-Fi signal may have significant fluctuations due to various reasons such as unstable wireless channel, external interference, and user movement. To cope with these fluctuations, several methods have been proposed to remove outliers using clustering [27]. In the case of Wi-Fi CSI data, however, the signal appears in several clusters and the exact number of classes is unknown. To address this challenge, we remove outliers in Wi-Fi CSI data using DBSCAN [24]. DBSCAN is one of the density-based algorithms widely used for clustering which groups data points gathered in high density into one class. DBSCAN has the advantage of finding clusters of geometric shapes, and it is particularly useful when the total number of clusters are unknown. In this work, DBSCAN is effective because the CSI data shows a geometric shape with vectors of multiple subcarriers.



(a) before DBSCAN

(b) after DBSCAN

FIGURE 6. Amplitude of Wi-Fi CSI values before and after outlier elimination using DBSCAN.

DBSCAN uses two parameters, distance threshold ϵ and minimum number of peripheral data points *minPts*, as controllable variables. If a data point has more than *minPts* nearby data points at a distance less than ϵ, these nearby data points are grouped into the same cluster. This process is repeated for all data points after which clustering is complete and outliers have been identified. FIGURE 6 plots the Wi-Fi CSI data before and after eliminating outliers using DBSCAN. Each line represents the amplitude of each subcarrier for one received packet. Even when the measurements were taken at the same location for a short period of time, the figure shows that a non-negligible amount of outliers exist in the Wi-Fi CSI data. These outliers can degrade learning performance. DBSCAN helps in eliminating these outliers.

IV. EVALUATION

This section describes the experiment setup and methodology, the training phase, and the evaluation of *SWORD* on SRD performance.

A. EXPERIMENT SETUP AND METHODOLOGY

We use two laptops with Atheros 9380[3] Wi-Fi NICs to each operate as an AP and a station, and collect CSI data using the Atheros CSI tool[4] [28]. Then, we train *SWORD* on a separate server with a GPU (RTX 2080 Ti) using tensorflow 2.0.[5] The experiment environment is a regular office room, and we installed the AP at a fixed location in the room (FIGURE 3). Details of the setup can be found in TABLE 1.

[3] Supports IEEE 802.11a/b/g/n, 3-stream 11n MIMO, with PCIe interface.
[4] Available at https://wands.sg/research/wifi/AtherosCSI/
[5] Available at https://www.tensorflow.org/

TABLE 1. Experiment settings.

Measurement settings	Value
Wireless chipset	Atheros 9380
Number of {AP, station}	{3, 1}
Wi-Fi PHY	802.11n
Distance interval between RPs	3 cm
Number of RPs	49
Measurement time per RP	1∼2 seconds
Office Size	6.5 x 3.0 m^2
Packet interval	10 ms
Number of inner testing point	8
Number of outer testing point	7

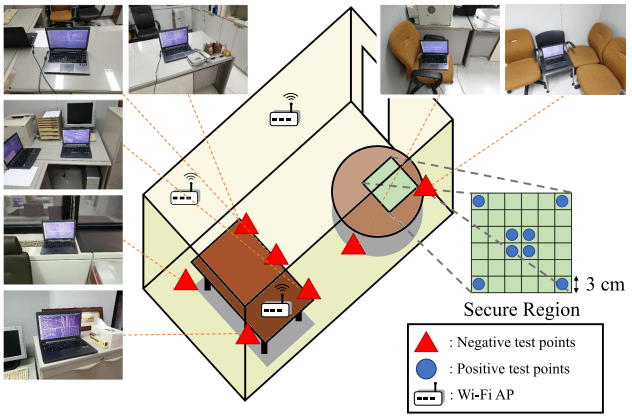


FIGURE 7. Test data points used in the experiment: 8 inner points within secure region, and 7 outer points.

First, we draw a 6 × 6 grid with 3 cm spacing on a table to be defined as a secure region (table A in FIGURE 1). Then, we place the antenna of the station at each vertex (reference point) and measure the Wi-Fi CSI data for 100 received packets which takes approximately 1∼2 seconds. We get the training dataset from a total of 49 vertices (reference points) and train the *SWORD*. To evaluate the classification performance of the trained *SWORD*, we select 8 non-vertex points within the secure region to get positive samples, and 7 random locations in the room as negative samples to create a test dataset. TABLE 7 shows the 8 inner points within the secure region as well as the 7 outer points used for evaluation.

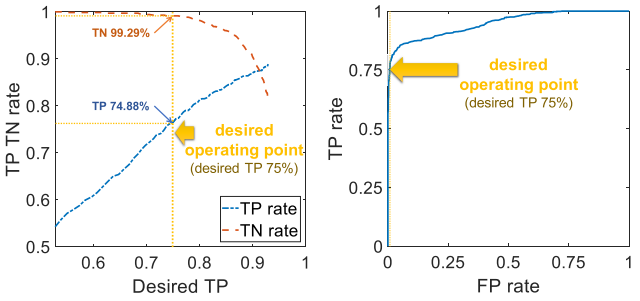
CSI data samples used for this evaluation are from a total of 6,400 Wi-Fi packets. The collected data are organized as follows. A total of 4,900 samples are for 'training', where 100 samples are measured at each of 49 references points within the secure region. For 'testing', 1,500 samples are used; 100 samples each from the 8 internal points within the secure region (positive samples) and 7 external points outside the secure regions (negative samples). The time taken to measure each packet was approximately 10 ms. Data sample from each AP is 56-dimension CSI amplitude vectors. We concatenate the CSI amplitude vectors from three APs and use them as input.

B. TRAINING PHASE

We first train the autoencoder using the data obtained from 49 reference points. Once the autoencoder has saturated, the center point c is calculated. Then, we learn the kernel function to satisfy the objective function (Eq.1) using the weights of the encoder learned earlier as the initial weights. Once the center point and kernel are learned, training data pass through *SWORD* again as an input to make a vector of feature space $\mathcal{F}$. After that, a hypersphere is drawn with a radius $\mathcal{R}$ from the center. Inner points of the hypersphere are determined as positive, and outer points as negative (FIGURE 5).

During the training process, the radius $\mathcal{R}$ of the hypersphere can be adjusted based on user preference/policy with an important trade-off in performance. Larger $\mathcal{R}$ will result in more data points being identified as inside the secure region, and thus TP increases while FP also increases (TN decreases). Smaller $\mathcal{R}$ may falsely recognize points inside the actual secure region as external points, resulting in lower TP but higher TN (lower FP). It is therefore important to set an appropriate radius $\mathcal{R}$ in the feature space based on the application requirement.

Hyperparameter $\mathcal{R}$ can be adjusted based on the '*desired TP*'. The $\mathcal{R}$ value is a distance on the vector space $\mathcal{F}$ and cannot be designated as a specific number because the value has no meaning in the actual physical space. However, we adjust the 'desired TP' according to the desired performance, and accordingly, the *SWORD* model automatically draws a circle including the corresponding training data ratio. Therefore, if only the 'desired TP' is specified in advance, the $\mathcal{R}$ value is automatically determined. In addition, based on application requirement and preference, this 'desired TP' can be adjusted without any additional (re-)training of the *SWORD* model.



(a) TP and TN of *SWORD* while adjusting the 'desired TP'.

(b) Receiver operating characteristic (ROC) curve of *SWORD*

FIGURE 8. Performance of *SWORD*. Note that, since there are only positive samples in the training dataset for OCC, TN/FP cannot be measured during learning; thus, we control the TP.

TABLE 2. Sampled TP & TN of *SWORD*.

	⇐ Higher security			Faster authentication ⇒	
desired TP	70.53%	75.00%	76.90%	80.41%	84.76%
TP	72.25%	76.50%	78.63%	81.50%	84.00%
TN	99.43%	99.14%	99.00%	98.00%	96.00%

C. TEST RESULTS

Performance of *SWORD* is plotted in FIGURE 8. As shown in FIGURE 8(a), TP and TN performance achieved by *SWORD* can be adjusted by changing the 'desired TP' without retraining the model. Furthermore, FIGURE 8(b) plots the receiver operating characteristic (ROC) curve of the entire

TABLE 3. TP & TN with repeated authentication attempts.

	1^{st} trial	2^{nd} trial	3^{rd} trial	4^{th} trial	5^{th} trial
TP	76.90%	93.07%	97.92%	99.38%	99.81%
TN	99.14%	98.44%	97.74%	97.04%	96.35%

SWORD. From these results, an user can select a few 'desired TP' samples and make a choice as shown in TABLE 2. For example, we can focus on higher security by selecting the left side of TABLE 2 for IoT device authentication in industrial plants or at exhibition events where there is a risk of theft. On the contrary, we can obtain higher user convenience by selecting the right side of TABLE 2 when, for example, placing a smartphone on our own desk in the office or automatically authenticating a device when entering our room at home.

In general, low FP (high TN) is considered more important than high TP for *secure region detection* applications. In consideration of this point, *SWORD* will sacrifice TP a little to achieve 99+% TN. To this end, in our proof-of-concept implementation, we select *desired TP ratio* of 75%, which means 75% of the training samples comes into the hypersphere when the learning process has saturated. Thus, our final *SWORD* model shows a TN result of 99.14% and TP of 76.9% when the desired TP is set to 75% (denoted as 'desired operating point' in FIGURE 8). This is the level that was regarded as safe to be actually used by one of our industry partners that motivated this research.

Automatically repeated authentication attempts can increase the user's experience even further. TABLE 3 shows the results of these attempts. If the rate of re-authentication is configured carefully and appropriately (since attackers may also retry indefinitely, or launch denial-of-service attack), allowing repeated authentication attempts can improve the authentication success rate of legitimate devices (TP) sufficiently for practical use in return for very slight increase in probability of wrong judgment (TN). We recommend allowing up to 3 retries, which correctly recognizes a device to be inside a secure region with 97.92% probability while still rejecting outside devices 97.74% of the time.

D. ADDITIONAL EXPERIMENT ON DIFFERENT SETUP

To validate whether the effectiveness of *SWORD* can be generalized in other environments, we have conducted additional experiments using different setups, changing the location of the secure region as well as the Wi-Fi APs. In these experiments, we intentionally placed one AP to be non-line-of-sight (NLOS) from the secure region while the other two APs are in LOS. From these additional experiments with varying locations of secure region and APs, we obtained an average TN of 99.429% and TP of 71.625% when the desired TP was set to 75%. These results are consistent with those in Section IV-C, which confirm that *SWORD* can work in other environments as well.

V. CONCLUSION AND FUTURE WORK

Secure region detection enables practical and convenient location-based authentication for security of IoT devices. This work proposed *SWORD*, the first secure region detection scheme based on Wi-Fi CSI and deep *one-class classification*, which addresses the problem of time-consuming data collection outside the target region. We have shown that spatial information can be inferred through deep learning of Wi-Fi CSI data, and deep one-class classification can effectively classify a secure region without any negative reference points. We have implemented *SWORD* on commercial 802.11n devices. However, our scheme can work with state-of-the-art Wi-Fi standards (e.g. 802.11ax) as well. Our evaluation have shown that *SWORD* can correctly reject devices outside the secure region with 99.14% accuracy while detecting devices inside the secure region with 76.9%. There is an user-adjustable trade-off between TN and TP, and higher TN was the primary target metric for a security scheme while TP can be improved to 97.92% at the cost of slightly higher FP (2.26%).

The contribution of this work is in designing a method that uses Wi-Fi CSI data on one-class classification to detect secure region without requiring any negative data, and this is clearly differentiated from existing research that could only localize the region where reference point data was obtained. We believe that this work will encourage future research on the *secure region detection* problem for preventing loss and intrusion of IoT devices. We plan to further improve accuracy and precision through the use of phase or angle information of Wi-Fi CSI, and also evaluate it on newer Wi-Fi standards such as IEEE 802.11ac and 11ax.

REFERENCES

[1] *The Growing Trend of IoT Devices*. Accessed: Feb. 8, 2021. [Online]. Available: https://cultureofgaming.com/the-growing-trend-of-iot-devices

[2] E. L. C. Macedo, E. A. R. de Oliveira, F. H. Silva, R. R. Mello, F. M. G. Franãa, F. C. Delicato, J. F. de Rezende, and L. F. M. de Moraes, "On the security aspects of Internet of Things: A systematic literature review," *J. Commun. Netw.*, vol. 21, no. 5, pp. 444–457, Oct. 2019.

[3] J. Dong, M. Noreikis, Y. Xiao, and A. Ylä-Jääski, "ViNav: A vision-based indoor navigation system for smartphones," *IEEE Trans. Mobile Comput.*, vol. 18, no. 6, p. 1461–1475, Jun. 2019.

[4] R. Bao, R. Komatsu, R. Miyagusuku, M. Chino, A. Yamashita, and H. Asama, "Cost-effective and robust visual based localization with consumer-level cameras at construction sites," in *Proc. IEEE 8th Global Conf. Consum. Electron. (GCCE)*, Oct. 2019, pp. 983–985.

[5] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proc. Conf. Comput. Commun.*, Feb. 2002, pp. 775–784.

[6] Q. Chen and B. Wang, "FinCCM: Fingerprint crowdsourcing, clustering and matching for indoor subarea localization," *IEEE Wireless Commun. Lett.*, vol. 4, no. 6, pp. 677–680, Dec. 2015.

[7] J. Niu, B. Wang, L. Cheng, and J. J. P. C. Rodrigues, "WicLoc: An indoor localization system based on WiFi fingerprints and crowdsourcing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 3008–3013.

[8] Y. Chen, D. Lymberopoulos, J. Liu, and B. Priyantha, "FM-based indoor localization," in *Proc. 10th Int. Conf. Mobile Syst., Appl., Services*, 2012, p. 169.

[9] V. Otsason, A. Varshavsky, A. LaMarca, and E. de Lara, "Accurate GSM indoor localization," in *Proc. 7th Int. Conf. Ubiquitous Comput. (UbiComp)*. Tokyo, Japan: Springer-Verlag, 2005, pp. 141–158.

[10] X. Yan, Q. Luo, Y. Yang, S. Liu, H. Li, and C. Hu, "ITL-MEPOSA: Improved trilateration localization with minimum uncertainty propagation and optimized selection of anchor nodes for wireless sensor networks," *IEEE Access*, vol. 7, pp. 53136–53146, 2019.

[11] R. C. Luo, O. Chen, and P. Hsien Lin, "Indoor robot/human localization using dynamic triangulation and wireless pyroelectric infrared sensory fusion approaches," in *Proc. IEEE Int. Conf. Robot. Autom.*, May 2012, pp. 1359–1364.
[12] J. Paek, J. Ko, and H. Shin, "A measurement study of BLE iBeacon and geometric adjustment scheme for indoor location-based mobile applications," *Mobile Inf. Syst.*, vol. 2016, pp. 1–13, Oct. 2016.
[13] P. Davidson and R. Piche, "A survey of selected indoor positioning methods for smartphones," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1347–1370, 2nd Quart., 2017.
[14] R. C. Luo and T. Hsiao, "Indoor localization system based on hybrid Wi-Fi/BLE and hierarchical topological fingerprinting approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 10791–10806, Sep. 2019.
[15] X. Tong, K. Liu, X. Tian, L. Fu, and X. Wang, "FineLoc: A fine-grained self-calibrating wireless indoor localization system," *IEEE Trans. Mobile Comput.*, vol. 18, no. 9, pp. 2077–2090, Sep. 2019.
[16] W. Sun, M. Xue, H. Yu, H. Tang, and A. Lin, "Augmentation of fingerprints for indoor WiFi localization based on Gaussian process regression," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10896–10905, Sep. 2018.
[17] X. Wang, L. Gao, S. Mao, and S. Pandey, "CSI-based fingerprinting for indoor localization: A deep learning approach," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 763–776, Jan. 2017.
[18] H. Chen, Y. Zhang, W. Li, X. Tao, and P. Zhang, "ConFi: Convolutional neural networks based indoor Wi-Fi localization using channel state information," *IEEE Access*, vol. 5, pp. 18066–18074, 2017.
[19] W. Xun, L. Sun, C. Han, Z. Lin, and J. Guo, "Depthwise separable convolution based passive indoor localization using CSI fingerprint," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6.
[20] J. Choi, G. Lee, S. Choi, and S. Bahk, "Smartphone based indoor path estimation and localization without human intervention," *IEEE Trans. Mobile Comput.*, early access, Jul. 30, 2020, doi: 10.1109/TMC.2020.3013113.
[21] J. Heo, Y. Yoo, J. Suh, W. Park, J. Paek, and S. Bahk, "FMS-AMS: Secure proximity-based authentication for wireless access in Internet of Things," *J. Commun. Netw.*, vol. 22, no. 4, pp. 338–347, Aug. 2020.
[22] W. Jiang, H. Xue, C. Miao, S. Wang, S. Lin, C. Tian, S. Murali, H. Hu, Z. Sun, and L. Su, "Towards 3D human pose construction using WiFi," in *Proc. 26th Annu. Int. Conf. Mobile Comput. Netw.*, Apr. 2020, pp. 1–7.
[23] A. Goldsmith, *Wireless Communnication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[24] M. Ester, H.-P. Kriegel, J. Sander, and X. Xu, "A density-based algorithm for discovering clusters in large spatial databases with noise," in *Proc. 2nd Int. Conf. Knowl. Discovery Data Mining*, 1996, pp. 226–231.
[25] S. S. Khan and M. G. Madden, "A survey of recent trends in one class classification," in *Artificial Intelligence and Cognitive Science*, L. Coyle and J. Freyne, Eds. Berlin, Germany: Springer, 2010, pp. 188–197.
[26] L. Ruff, R. Vandermeulen, N. Goernitz, L. Deecke, S. A. Siddiqui, A. Binder, E. Müller, and M. Kloft, "Deep one-class classification," in *Proc. Mach. Learn. Res. (PMLR)*, Stockholm, Sweden, vol. 80, Jul. 2018, pp. 4393–4402.
[27] S.-Y. Jiang and Q.-B. An, "Clustering-based outlier detection method," in *Proc. 5th Int. Conf. Fuzzy Syst. Knowl. Discovery*, Oct. 2008, pp. 429–433.
[28] Y. Xie, Z. Li, and M. Li, "Precise power delay profiling with commodity Wi-Fi," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2015, p. 53.

YONGJAE YOO (Graduate Student Member, IEEE) received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, Republic of Korea, in 2019, where he is currently pursuing the Ph.D. degree with the School of Electrical and Computer Engineering. His research interests include the area of security and machine learning in wireless networks, the Internet of Things, and 5G networks.

JIHWAN SUH (Graduate Student Member, IEEE) received the B.E. degree in the field of informatics and mathematical science from Kyoto University, in 2013. He is currently pursuing the Ph.D. degree with the School of Electrical and Computer Engineering, Seoul National University, Seoul, Republic of Korea. His research interests include the area of security, localization, and 5G with AI.

JEONGYEUP PAEK (Senior Member, IEEE) received the B.S. degree in electrical engineering from Seoul National University, in 2003, and the M.S. degree in electrical engineering and the Ph.D. degree in computer science from the University of Southern California (USC), in 2005 and 2010, respectively. He worked as a Research Intern at the R&D Labs, Deutsche Telekom Inc., USA, in 2010, and then joined Cisco Systems Inc., in 2011, where he was the Technical Leader in the Internet of Things Group (IoTG), Connected Energy Networks Business Unit (CENBU, formerly the Smart Grid BU). At Cisco, he was one of the lead engineers for Connected Grid Mesh (CG-Mesh) system and WPAN software. In 2014, he was with the Department of Computer Information Communication, Hongik University, as an Assistant Professor. He is currently an Associate Professor with the School/Department of Computer Science and Engineering, Chung-Ang University, Seoul, Republic of Korea. He is an Editor of the *Journal of Communications and Networks* (JCN), an Editorial Board Member of *Sensors*.

SAEWOONG BAHK (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Seoul National University (SNU), in 1984 and 1986, respectively, and the Ph.D. degree from the University of Pennsylvania, in 1991. He was a member of Technical Staff with AT&T Bell Laboratories, from 1991 to 1994, where he had worked on network management. From 2009 to 2011, he served as the Director of the Institute of New Media and Communications. He is currently a Professor at SNU. He has been leading many industrial projects on 3G/4G/5G and the IoT connectivity supported by Korean Industry. He has published more than 300 technical articles and holds more than 100 patents. He is a member of the National Academy of Engineering of Korea (NAEK). He was a recipient of the KICS Haedong Scholar Award, in 2012. He was the President of the Korean Institute of Communications and Information Sciences (KICS). He has been serving as the Chief Information Officer (CIO) of SNU. He was the General Chair of the IEEE WCNC 2020, IEEE ICCE 2020, and IEEE DySPAN 2018. He was the Director of the Asia–Pacific Region of the IEEE ComSoc. He is an Editor of the *IEEE Network Magazine* and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He was the TPC Chair of the IEEE VTC-Spring 2014, and the General Chair of JCCI 2015, the Co-Editor-in-Chief of the *Journal of Communications and Networks* (JCN), and on the Editorial Board of *Computer Networks* journal and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.