J Inf Process Syst, Vol.16, No.3, pp.541~556, June 2020
https://doi.org/10.3745/JIPS.03.0137

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Enhancing the Reliability of Wi-Fi Network Using Evil Twin AP Detection Method Based on Machine Learning

Jeonghoon Seo*, Chaeho Cho*, and Yoojae Won*

Abstract

Wireless networks have become integral to society as they provide mobility and scalability advantages. However, their disadvantage is that they cannot control the media, which makes them vulnerable to various types of attacks. One example of such attacks is the evil twin access point (AP) attack, in which an authorized AP is impersonated by mimicking its service set identifier (SSID) and media access control (MAC) address. Evil twin APs are a major source of deception in wireless networks, facilitating message forgery and eavesdropping. Hence, it is necessary to detect them rapidly. To this end, numerous methods using clock skew have been proposed for evil twin AP detection. However, clock skew is difficult to calculate precisely because wireless networks are vulnerable to noise. This paper proposes an evil twin AP detection method that uses a multiple-feature-based machine learning classification algorithm. The features used in the proposed method are clock skew, channel, received signal strength, and duration. The results of experiments conducted indicate that the proposed method has an evil twin AP detection accuracy of 100% using the random forest algorithm.

Keywords

Access Point, Classification Algorithm, Clock Skew, Evil Twin AP, Rogue AP, Wireless Network

1. Introduction

Developed by the University of Hawaii in 1971, the Additive Links On-line Hawaii Area network (ALOHAnet) ushered in the era of wireless networks. Since then, wireless network technology has evolved and become virtually ubiquitous owing to advantages such as better mobility and scalability compared to wired networks. With the development of wireless network technology and the proliferation of smartphones and Internet of Things (IoT) devices, the demand for Wi-Fi to provide wireless networks to wireless terminals has increased. Currently, Wi-Fi has become essential in homes and public places such as libraries, schools, restaurants, airports, and hotels [1,2]. Wi-Fi is based on the IEEE 802.11 standard, and it provides a network to wireless terminals through communication with a wireless access point (AP) connected to a wired network [3,4].

Wi-Fi also provides advantages such as low cost and simple implementation. However, it also has the disadvantage of being vulnerable to attacks such as traffic analysis, sniffing, authentication, denial of service, response attacks, session hijacking, and rogue APs [5-7]. A rogue AP is a wireless AP installed

Manuscript received October 11, 2019; first revision January 15, 2020; accepted March 12, 2020.
Corresponding Author: Yoojae Won (yjwon@cnu.ac.kr)
* Dept. of Computer Science Engineering, Chungnam National University, Daejeon, Korea (sjh9309@cnu.ac.kr, greatopen@cnu.ac.kr, yjwon@cnu.ac.kr)

without the network administrator's permission. Rogue APs are classified into evil twin APs, improperly configured APs, unauthorized APs, and compromised APs [8]. An evil twin AP is an AP that is disguised as an authorized AP by duplicating the service set identifier (SSID) or media access control (MAC) address of an authorized AP. Attackers can carry out man-in-the-middle attacks using evil twin APs to bypass users who connect to phishing sites or send forged packets. Additionally, open source tools have been developed to easily create evil twin APs that can be used to attack wireless networks.

Because an evil twin AP copies and disguises the SSID and MAC address of the authorized AP, it is difficult to detect without checking its physical location. Therefore, to detect evil twin APs, various methods for distinguishing a new identifier based on physical characteristics rather than conventional identifiers such as clock skew, Received Signal Strength (RSS), Round Trip Time (RTT), and radio frequency have been proposed. However, because of the characteristics of wireless networks, which are more unstable than wired networks, errors due to small environmental changes can occur, making it difficult to accurately measure characteristic values, and therefore necessitating additional expensive wireless signal collection equipment for accurate measurement.

This paper proposes a method for extracting various features of wireless APs and detecting evil twin APs using machine learning. As the proposed method collects wireless signals using wireless network interface cards (NICs), it does not require expensive wireless signal acquisition equipment and is not significantly affected by various environmental changes as it uses machine learning algorithms. The main features used for detection are as follows: the clock skew generated owing to the minute differences in the manufacturing process of wireless communication devices; RSS, which is the signal strength of the target AP; the channel used by the AP; duration, which is the transmission time of a frame. To improve the evil twin AP detection accuracy, these four features were applied to several machine learning classification algorithms to compare their performance; specifically, logistic regression, naïve Bayes, k-nearest neighbors (k-NN), support vector machine (SVM), and random forest.

The remainder of this paper is organized as follows: Section 2 provides the background for the study. Section 3 discusses related work. Section 4 describes the evil twin AP detection technique based on multiple features. Section 5 analyzes the experiments and the results of detecting evil twin APs using the proposed technique. Finally, Section 6 concludes the paper and outlines the direction of future work.

2. Background

This section gives an overview of passive AP scanning, evil twin APs, and the classification algorithms used in machine learning.

2.1 Passive AP Scan

A station must connect with a surrounding AP to connect to a wireless network. The AP is connected to a wired network, and it communicates with the station via a wireless signal. Hence, a user cannot physically check whether the AP exists in the vicinity. Therefore, the user must scan and identify the surrounding AP through the station. The station scans for the surrounding AP via either passive scanning or active scanning. Fig. 1 shows the passive AP scanning process.

In the passive scanning method, each neighboring AP is recognized by scanning the signal transmitted

by the AP to inform itself about the station without any other action [9]. In this case, the signal broadcast by the AP is referred to as a beacon frame. The owner of the AP can determine the period in which the AP broadcasts the beacon frame through the beacon interval setting.

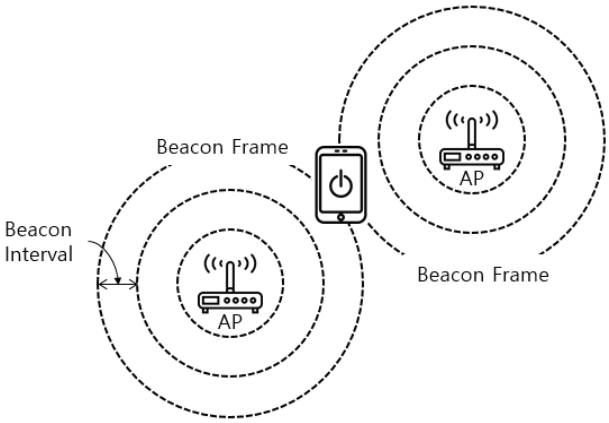

Fig. 1. Passive AP scanning.

2.2 Evil Twin AP

An evil twin AP is a rogue AP that impersonates an authorized AP by assuming its SSID or MAC address. The SSID or MAC address can be easily identified through the probe response and beacon frame. An attacker installs an evil twin AP and sets its signal to be stronger than that of the authorized AP or executes a distributed denial of service (DDoS) attack against the authorized AP to connect a station and the evil twin AP [10-12].

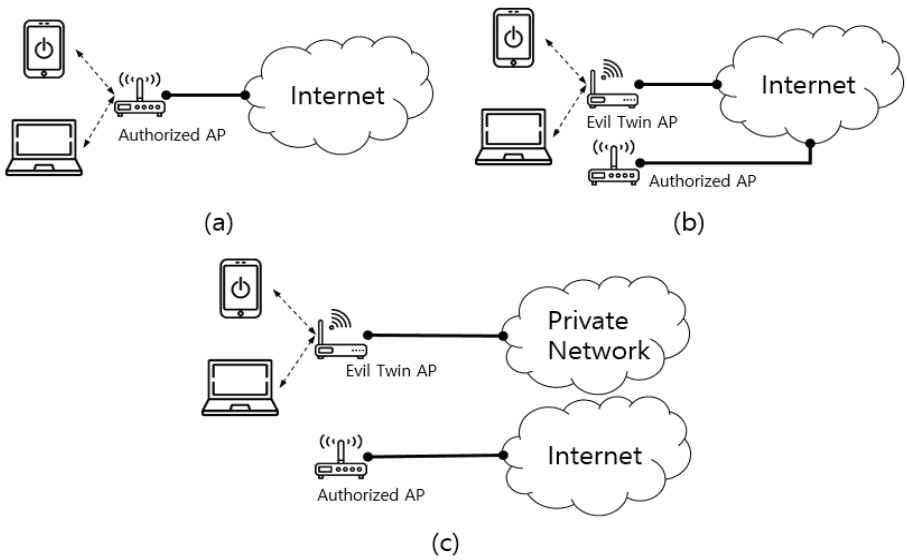

Fig. 2. Authorized AP and evil twin AP connection scenarios. (a) The connection between an authorized AP and a station. (b) An evil twin AP attack scenario. (c) Another evil twin AP attack scenario.

Fig. 2(a) shows the connection between an authorized AP and a station. The authorized AP is connected to a wired network, and it provides wireless Internet access to the connected station. Fig. 2(b) shows an evil twin AP attack scenario. The evil twin AP is wired to the Internet, similar to the authorized APs, to provide wireless Internet access to connected stations. The evil twin AP can intercept packets from and to the station. Fig. 2(c) shows another evil twin AP attack scenario, in which an evil twin AP is connected to an attacker's private network. The station connected to the evil twin AP appears to be accessing the wireless Internet. However, private information and important data can be leaked because it is connected to the attacker's private network [13].

3. Related Work

This section reviews studies that have used single and multiple features to detect evil twin APs.

3.1 Evil Twin AP Detection Using a Single Feature

Jana and Kasera [14] proposed a method of using clock skew to detect an evil twin AP. Clock skew is calculated from the IEEE 802.11 Time Synchronization Function timestamp of the beacon frame broadcast from the target AP. They defined clock offset o_i, which is the difference between transmission time and reception time when the transmission and reception times of the ith frame are T_i and t_i, respectively, as follows:

$$o_i = (T_i - T_1) - (t_i - t_1) \tag{1}$$

They defined the rate of change of the calculated o_i as clock skew and calculated it using linear programming and least squares fitting. They state that the calculated clock skew could be used as an identifier to distinguish between an evil twin AP and a normal AP. Furthermore, they proposed a threshold-based algorithm that could separate each beacon frame set from the entire set containing the beacon frames of an evil twin AP and a normal AP. They demonstrated that clock skew could identify APs within an error range of 0.2 ppm.

Arackaparambil et al. [15] pointed out problems with the reliability of the beacon frame reception time required to calculate clock skew. The reception time of a beacon frame is determined by the internal clock of the wireless NIC that receives it. They indicated that the internal clock of the wireless NIC changes in synchronization with the clock of the most recently connected AP. They also conducted experiments to measure the AP's clock skew using a wireless NIC to prove their claim. Their experimental results show that the AP's clock skew is measured differently depending on how recently the AP is connected to the wireless NIC.

Kim et al. [16] proposed an evil twin AP detection scheme using RSS. Their scheme assumes that an attacker broadcasts signals from multiple authorized APs on one NIC. Their method collects radio signals from neighboring APs, sorts them in the order of collection to generate an RSS sequence, and normalizes the sequence to fill noise or empty values to improve detection accuracy. Then, the RSS sequences are compared for similarities. If two RSS sequences are found to be similar, they are classified as fake signals from one device. They performed several experiments by changing the value of the threshold and found

that the accuracy of the method is 97.1% when the threshold is one, with true positive and false positive rates of 30.1% and 0.9%, respectively. Moreover, when the threshold is two, it has a 96.5% accuracy, with 100% true positive rate and 3.6% false positive rate.

Lee et al. [17] argued that in the past, it was necessary to build a separate network to install an evil twin AP, but recently, the hotspot function of mobile devices such as smartphones and tablets makes it easy to build evil twin APs connected to cellular networks such as 3G and LTE. They point out that it is possible to conduct man-in-the-middle attacks and state that an evil twin AP connected to a cellular network will increase communication latency more than an AP connected to a wired network owing to the presence of the eNodeB base station in the communication process. They subsequently proposed an evil twin AP detection technique. Through experiments, they measured the RTT of the AP connected to the wired network and the evil twin AP connected to the cellular network and generated a learning model using the k-SVM algorithm. We also conducted an evil twin AP detection experiment using the trained model to achieve maximum evil twin AP detection accuracy of 93.4%.

3.2 Evil Twin AP Detection Using Multiple Features

Vanjale and Mane [18] proposed an evil twin AP detection method using multiple features. They pointed out the limitation of single-feature-based evil twin AP detection and designed a system to detect evil twin APs using MAC address, SSID, RSS, channel, frequency, authentication type, timestamp, sequence count, and clock skew. Their proposed method is divided into a learning mode and a detection mode. In the learning mode, a detection policy is created using multiple features. In the detection mode, the created policy is used to classify authorized APs, unauthorized APs, and evil twin APs. They confirmed the capabilities of the proposed system for the detection of rogue APs, evil twin APs, and MAC spoofing attacks.

Kang et al. [19] proposed an evil twin AP detection method using an SVM and two features. They pointed out that the detection of evil twin APs using RTT is less accurate in crowded channels and added packet inter-arrival time (PIAT) to compensate for this. Their RTT measurement method is based on the existing RTT measurement method. PIAT is a measure of the interval of response packets returned when a packet is transmitted at regular intervals for RTT measurement. It is used for checking whether there is a change in the packet reception interval depending on channel congestion or the workload of an AP. They measured RTT and PIAT and conducted an evil twin AP detection experiment using an SVM. Evil twin APs were detected with a maximum accuracy of 96.5% and a minimum accuracy of 89.75% in congested channels.

4. Proposed Method

The studies described in Section 3 used clock skew, which is a unique feature that an attacker cannot forge to identify an AP. However, clock skew is measured through packets that are broadcast in the air, and thus depends on several factors, including the measurement environment, measurement time, and the state of packet collectors. Therefore, we propose a method that uses multiple features, including clock skew, to detect evil twin APs. Fig. 3 shows the flowchart of the proposed method.

The proposed method is composed of the following components: a feature extractor for extracting

features from an authorized AP in advance, a learning phase for generating an evil twin AP detection model through machine learning with extracted features, a detection phase for detecting evil twin APs using the trained model.

4.1 Feature Extractor

Feature extractors are used to generate data for machine learning in the learning and detection phases. A feature extractor extracts the feature of each AP from a collected beacon frame. Assuming that there are N APs, the input of the feature extractor is the beacon frame set collected from the N APs. The output of the feature extractor is a 1 × 5 vector that includes four features extracted using the elements of the input set and a label matching the SSIDs from zero to N. The features extracted by the feature extractor are clock skew, channel, RSS, and duration.

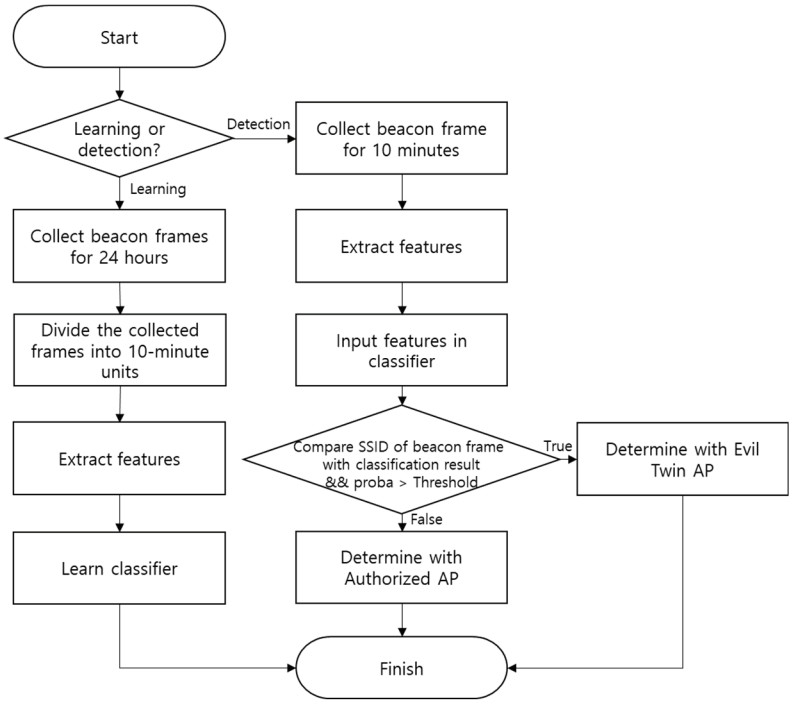

Fig. 3. Flowchart of the proposed method.

4.1.1 Clock skew

Clock skew is the distortion of the relative clock between two APs caused by a slight difference in the clock oscillator of each AP in the manufacturing process. This distortion can be used as a unique fingerprint of an AP because it is different even for APs manufactured by the same vendor. In this study, the beacon frame broadcasted by the AP is used to estimate clock skew. As the beacon frame contains a field that indicates the timestamp of a transmitting AP, the transmission time of the transmitting AP can be determined. The time at which the beacon frame is received is measured by the driver of a receiving AP, and the offset of the clock between the target AP and receiving AP can be calculated using the transmission and reception times. As explained in Section 3, clock skew is the rate of change of clock

offset. Hence, estimating clock skew is the same as estimating the slope of the time–clock offset graph. In this study, machine learning linear regression is applied for accurate slope estimation.

When the clock offset for the *i*th frame of the collected AP is $\hat{y}_i$, the receiving time of the *i*th frame is x_i, clock skew is *W*, and bias is *b*, a straight line is calculated by linear regression as follows:

$$\hat{y}_i = W * x_i + b, \tag{2}$$

At this time, *W* and *b* are initialized to a random value between zero and one and adjusted based on the gradient descent algorithm to minimize the cost, *c*, of least squares fitting, as follows:

$$c = \frac{1}{n}\sum_{i=0}^{n}(\hat{y}_i - y_i)^2 \tag{3}$$

The gradient descent algorithm is an optimization algorithm that is mainly used to minimize cost in machine learning. It changes *W* and *b* to reduce the cost during the learning period. When learning is over and the cost reaches its minimum, *W* is the slope of the straight line representing given data, which is estimated based on clock skew.

4.1.2 Channel

The Wi-Fi network used in this study employed a 2.4-GHz frequency band and a 5-GHz frequency band. Channels are units into which a frequency band is divided to reduce crosstalk and interference in wireless communications. Fig. 4 shows the center frequency of each channel in the 2.4 GHz frequency band.

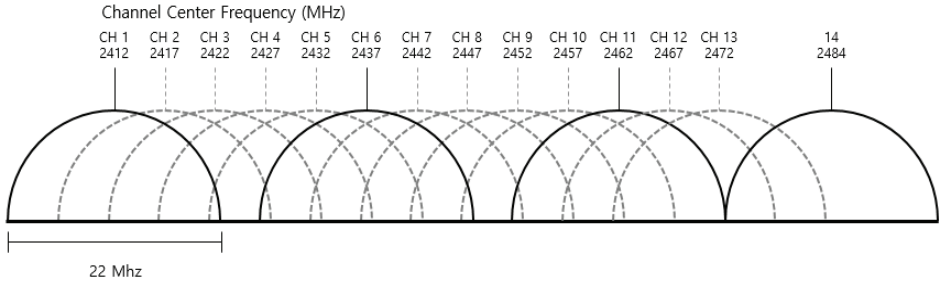

Fig. 4. Center frequency of 2.4 GHz band channel.

The center frequency of wireless communication channels is divided into 2,412 MHz and 5 MHz units, and the number of channels used varies by country. IEEE 802.11n uses a bandwidth of 20 MHz; hence, one channel can affect four neighboring channels.

The owner of an AP can set the channel to be used between the AP and a station for communication. The channel used by the AP is constant until the owner of the AP changes the AP configuration. Therefore, the channel used by the AP may be suspected as an evil twin AP (This does not consider the automatic channel setting function used by APs to find and change the optimal channel). Therefore, we used the channel as an identifier for detecting the evil twin AP. There is a field representing the channel used by the AP in the body frame of the beacon frame transmitted by the AP, and the feature extractor extracts this field value and uses it as the feature.

4.1.3 RSS

RSS refers to the strength of the wireless signal received by a sensor. The unit of RSS is dBm, a log-scale unit based on 1 mW. In other words, when the power of a received signal is 1 mW, RSS is 0 dBm, and a difference of 1 dBm implies a power difference of 10 times. As the power levels of APs are low, RSS is mostly negative. The factors that significantly influence RSS are the transmission power of the transmitting side, the distance between the transmitting side and the receiving side, and the noise caused by the surrounding environment. However, transmission power does not change abruptly in the case of an AP, and the distance between the transmitting AP and receiving AP is constant because an AP is not mobile. Therefore, the rapid change of RSS may be due to noise, but it may be that it is installed as evil twin AP. Therefore, RSS is used as an additional identifier for detecting evil twin APs. A feature extractor extracts the RSS average value of the beacon frame collected during the unit time.

4.1.4 Duration

Duration is calculated based on various types of radio and IEEE 802.11 information, and the total frame duration is measured in microseconds. In this study, the duration is calculated using the following formula:

$$Duration = \frac{Frame\ length}{Data\ rate} \tag{4}$$

Duration is determined by the length of the beacon frame and the speed at which data are transmitted. The length of the beacon frame varies depending on the optional field of the frame, as shown in Fig. 5. The optional field of the beacon frame includes information such as SSID, supported rates, encryption method, and vendor. The same AP does not change the duration because the value of the optional field does not change. That is, two different APs may accidentally have the same duration value, but one AP cannot have two duration values. Therefore, because the change of duration of one AP may be suspected as an evil twin AP, the duration is used as an additional identifier for detecting an evil twin AP. The feature extractor extracts the duration values in the radio information field and uses them as features. In this study, we adjust the units to harmonize the duration with other features.

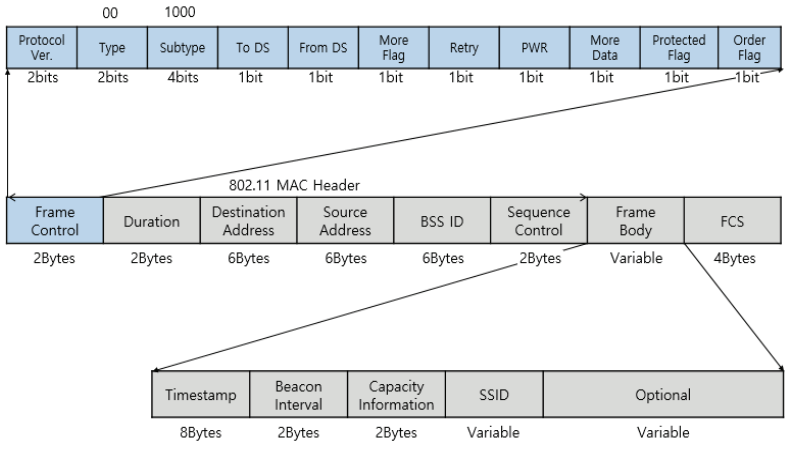

Fig. 5. Beacon frame structure of 802.11.

4.2 Learning Phase

The learning phase refers to the process of generating a training set by collecting and processing a beacon frame and learning an evil twin AP detection model using the training set.

A previously collected beacon frame set must be processed to create a training set. In this study, pre-collection time was set as 24 hours, and it was assumed that an evil twin AP is not installed during this time. The beacon frame set collected for 24 hours from N neighbor APs is processed as follows:

First, beacon frame sets for each AP are generated using the SSIDs of the beacon frames collected over 24 hours. The beacon frames collected for each AP are divided into 10-minute intervals to generate N × 144 subsets. Then, each subset is input to the feature extractor to create a matrix of size (N × 144) × 5 that is then used as the training set.

The performance of several classification algorithms in generating an evil twin AP detection model using the four features and labels was compared. The random forest algorithm was subsequently selected based on the results of the comparison. The details of the comparison are provided in Section 5.

4.3 Detection Phase

In the detection phase, a long pre-collection time is not necessary because the model has already been trained. In the learning phase, the evil twin AP detection prediction model divides the data collected over 24 hours into 10-minute intervals and then learns it. Therefore, the beacon frame of a neighboring AP should be collected for at least 10 minutes to detect an evil twin AP in the detect phase. According to our experimental statistics, approximately 300–500 beacon frames are collected over 10 minutes. After collecting the beacon frames for 10 minutes, the feature extractor is called to extract the feature for each AP. As a result of the extraction, a vector with a size of 1 × 5 is obtained. This vector is input into the learned classifier to check the classification result. The classifier then outputs the classification result and the probability of the input data. If the classification result and the SSID of the beacon frame broadcast by the corresponding AP are the same, and the probability is higher than the threshold, the AP is considered to be an authorized AP. If either condition is not satisfied, it is considered an evil twin AP.

5. Experimental Evaluation

In this section, we outline the experiment conducted to detect the actual evil twin AP using the evil twin AP detection method proposed in Section 4 and compare and measure the performance for various machine learning classification algorithms and experimental environments.

5.1 Experimental Environment and Procedure

Fig. 6 shows the experimental environment. The experiment was conducted on 10 APs on a university campus. A wireless NIC using Ralink's chipset was used to collect the wireless signal. The wireless NIC was connected to a computer running Kali Linux and the wireless signal collection was carried out via Wireshark.

In the experiment, beacon frames were collected over a period of 9 hours for nine authenticated APs, and a training set was created using the feature extractor. Then, the AP most similar to AP 0 was

designated the evil twin AP of AP 0, and beacon frames were collected again over a period of 24 hours for accurate measurement. We created a test set using the feature extractor and measured the performance of the classification algorithms using the training set and the test set.

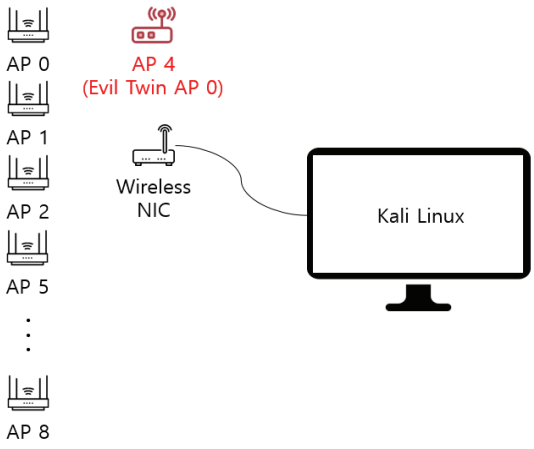

Fig. 6. Experimental environment.

5.2 Generation of Training Set

A total of 850,886 beacon frames were collected over 24 hours around the 10 APs to generate a training set. The distribution of the beacon frames collected for different APs is shown in Fig. 7.

In the case of AP 0, more beacon frames were collected compared to the other APs owing to its location advantage. Approximately 50,000 to 100,000 beacon frames are collected for all APs except AP 0. After separating the beacon frames collected over 24 hours according to APs and dividing them into 10-minute intervals, we generated 144 learning datasets for each AP using the feature extractor. Table 1 shows the training set used for feature extraction. The analysis of the training set shows that the error in clock skew was approximately 7 ppm. Additionally, AP 0 and AP 4 had extremely similar ranges, channels, and durations of clock skew but different RSS.

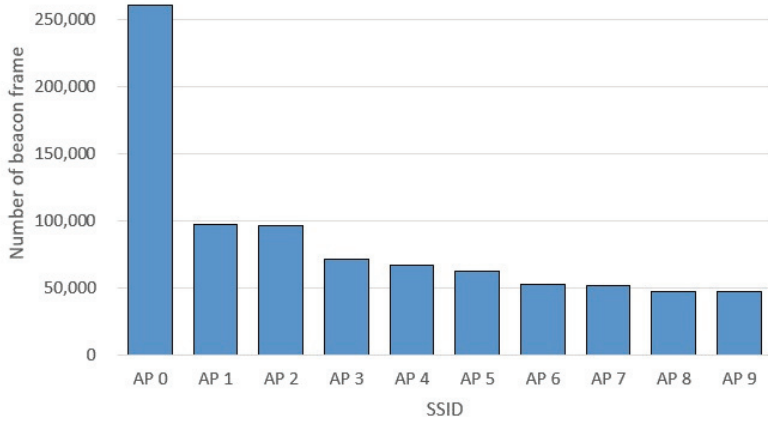

Fig. 7. Distribution of beacon frames per AP.

Table 1. Average of the features of the training set

SSID	Clock skew (ppm)	Channel	RSS (dBm)	Duration (10^{-4}s)
AP 0	–16.72	8	–22.81	22.88
AP 1	–08.95	1	–40.31	26.40
AP 2	–13.45	11	–62.55	18.08
AP 3	–04.03	11	–38.40	17.52
AP 4	–12.43	7	–53.00	23.20
AP 5	–14.02	9	–60.95	23.84
AP 6	–07.43	2	–47.51	25.92
AP 7	–03.54	11	–56.86	3.80
AP 8	–03.07	10	–74.93	22.96

5.3 Generation of Test Set

The proposed method requires data collected over a period of 10 minutes to detect evil twin APs, but this test required a large amount of test data because it aims to measure the evil twin AP detection accuracy of the algorithm. Therefore, we created a test set by collecting beacon frames for 24 hours, and each test set was divided into 10-minute intervals and used as a test set. Table 2 shows the average of the test set features.

Through the collected test set, the clock skew and RSS sensitive to the surrounding environment had a little error that occurred between the training set and the test set. The beacon frame of AP 0 and evil twin AP 0 could be separated using the threshold-based algorithm of [14].

Table 2. Average of the features of the test set

SSID	Clock skew (ppm)	Channel	RSS (dBm)	Duration (10^{-4}s)
AP 0	–16.96	8	–23.93	22.88
AP 1	–09.27	1	–39.47	26.40
AP 2	–13.39	11	–62.72	18.08
AP 3	–04.01	11	–38.48	17.52
AP 4	–12.38	7	–53.00	23.20
AP 5	–14.12	9	–61.40	23.84
AP 6	–07.49	2	–47.45	25.92
AP 7	–03.43	11	–57.54	3.80
AP 8	–03.18	10	–74.88	22.96
Evil twin AP 0	–16.96	8	–39.45	24.72

5.4 Evil Twin AP Detection Results

We compared the output results by inputting 1,440 test data collected in addition to the random forest model generated by 1,440 training data. Table 3 shows the experimental results. The random forest model correctly classified all 144 data from AP 0 to AP 8. Evil twin AP data was classified as AP 0 because it was never trained but was classified as an evil twin AP because the probability did not exceed the threshold.

Table 3. Evil twin AP detection results

SSID	AP 0	AP 1	AP 2	AP 3	AP 4	AP 5	AP 6	AP 7	AP 8	Evil twin AP 0
AP 0	144	-	-	-	-	-	-	-	-	-
AP 1	-	144	-	-	-	-	-	-	-	-
AP 2	-	-	144	-	-	-	-	-	-	-
AP 3	-	-	-	144	-	-	-	-	-	-
AP 4	-	-	-	-	144	-	-	-	-	-
AP 5	-	-	-	-	-	144	-	-	-	-
AP 6	-	-	-	-	-	-	144	-	-	-
AP 7	-	-	-	-	-	-	-	144	-	-
AP 8	-	-	-	-	-	-	-	-	144	-
Evil twin AP 0	-	-	-	-	-	-	-	-	-	144

5.5 Performance Analysis of Classification Algorithms

To obtain more objective results, two beacon frames were collected every 2 hours for 2 days, and then two additional test sets were generated. We compared the performance of classification algorithms for evil twin AP detection using a total of three test sets. The features used were clock skew, RSS, channel, and duration; the comparison algorithms were logistic regression, naïve Bayes, k-NN, SVM, and random forest. The threshold of each algorithm was set to the highest accuracy through several experiments. Table 4 shows the detection accuracy of each algorithm according to the test set.

Table 4. Accuracy (%) of evil twin AP Detection for each algorithm according to test set

Test set no.	Logistic regression (T=0.45)	Naïve Bayes (T=0.5)	k-NN (k=3, T=0.5)	SVM (T=0.5)	Random Forest (T=0.5)
No. 1	78.12	89.93	89.93	92.15	100
No. 2	72.22	88.75	88.75	93.47	99.51
No. 3	76.18	89.44	89.44	90.48	99.86

Although there is a difference between algorithms, the superiority of accuracy did not change, and in the No. 1 test set, each algorithm showed high accuracy. Therefore, we measured the change in accuracy according to the number of features of each algorithm using the first test set. Table 5 shows the accuracy of each algorithm according to the number of features.

Table 5. Evil twin AP detection accuracy (%) of each algorithm according to number of features

Used features	Logistic regression (T=0.45)	Naïve Bayes (T=0.5)	k-NN (k=3, T=0.5)	SVM (T=0.5)	Random forest (T=0.5)
Clock skew	10.06	41.94	55.27	25.97	59.09
Clock skew, channel	30.06	84.30	84.30	83.95	82.36
Clock skew, RSS	36.59	85.41	85.48	75.34	85.83
Clock skew, channel, RSS	95.06	89.23	89.23	86.80	89.93
All	78.12	89.93	89.93	92.15	99.93

The random forest algorithm showed the highest accuracy when all four features were used. In the last experiment, we fixed four features and changed the number of classes of the learning data to two, four, and nine. Further, the test data class was changed to three, five, and 10 by adding a rogue AP 0 to the

class of the training data. Table 6 shows the accuracy of each algorithm according to the number of classes. The experimental results show that the smaller the class, the higher the accuracy of the random forest. When the class is three or five, the maximum detection accuracy of the evil twin AP is 100%.

Table 6. Accuracy (%) of evil twin AP detection for each algorithm according to the number of classes

Number of classes	Logistic regression (T=0.7)	Naïve Bayes (T=0.5)	k-NN (k=3, T=0.5)	SVM (T=0.5)	Random forest (T=0.65)
3 (AP 0, Rogue AP 0)	66.66	66.66	66.66	66.66	100
5 (AP 0–3, Rogue AP 0)	76.94	80.00	80.00	79.00	100
10 (All)	78.12 (T=0.45)	89.93	89.93	92.15	100

5.6 Comparison with Previous Methods

Table 7 compares the method proposed in this paper to previous methods. Because the proposed method uses multiple factors, [18] and [19] were selected for comparison as they are similar. In the case of [18], a total of eight features are extracted from the beacon frame to generate a white list and similarity detection for the evil twin AP with 100% accuracy, whereas the proposed method uses four features. The proposed method also uses clock skew, RSS, and channel, but adds a new feature called duration, which makes it less susceptible to errors caused by the machine learning, rather than similarity comparison. On the other hand, [19] differs from the proposed method, in that two features, RTT and PIAT, are obtained using ICMP packets, and the number of packets required for detection is similar to those of the proposed method. The evil twin AP detection is performed using SVM, a machine learning classification algorithm. In terms of performance, [19] showed 93.4% accuracy and the proposed method achieved 100% accuracy in an environment with 10 APs by changing various variables.

Table 7. Comparison of previous methods and the proposed method

	Vanjale and Mane [18]	Kang et al. [19]	Proposed method
Used feature	MAC address, SSID, RSS, channel, Auth type, Seq no, timestamp, clock skew	RTT, PIAT	Clock skew, RSS, channel, duration
Collected packet	Beacon frame	ICMP	Beacon frame
Number of packets needed for detection	500	300	300
Method	Whitelist-based similarity comparison	Machine learning (support vector machine)	Machine learning (linear regression, random forest)
Accuracy (%)	100	93.4	100

6. Conclusion

This paper proposed an evil twin AP detection method using machine learning for accurate evil twin AP detection and compared the performance of classification algorithms for the evil twin AP detection process. The proposed method estimates sensitive clock skew using linear regression and adds channel, RSS, and duration as features to improve accuracy. Moreover, we analyzed the performance of the

classification algorithms using four features, and obtained 100% evil twin AP detection accuracy via the random forest algorithm. The Evil Twin AP 0 used in the experiment had a clock skew difference of only 1–2 ppm because AP 0 and the clock were synchronized. However, repetitive experiments did not show perfect classification accuracy in various environmental changes, and there was a false positive rate of about 1%. While the existing evil twin AP detection methods use features such as clock skew, RSS, RTT, and channel only, in this study, we added a feature called duration. Furthermore, the experiments confirmed that it is more effective to use a combination of these features than to use these features independently, and in particular, in the case of duration, an accuracy increase of approximately 10% was observed compared to the unused model. Additionally, through the experiment to verify the correlation between the number of APs and the accuracy allowed by the administrator, it was found that the number of APs authorized can achieve at least the same level of accuracy. However, the accuracy was not confirmed in the environment where more than 10 APs are operated. In the future, experiments will be conducted in an environment that can operate more than 10 APs.

Finally, the proposed method can detect evil twin APs by collecting radio signals for a short time. Therefore, when an AP is installed in the enterprise or institution that is not authorized by the network administrator, it can be used to quickly detect such an AP. This study is expected to contribute to providing a secure wireless network environment by integrating with the existing security solutions.

In the future, research will be conducted on an evil twin AP detection system with real-time enhancement through wireless signal collection libraries such as Scapy and Pyshark, with blocking and location tracking technology on the detected evil twin AP.

Acknowledgement

This work was supported by the research fund of Chungnam National University.

References

[1] J. Kim and I. Lee, “802.11 WLAN: history and new enabling MIMO techniques for next generation standards,” *IEEE Communications Magazine*, vol. 53, no. 3, pp. 134-140, 2015.

[2] F. H. Hsu, Y. L. Hsu, and C. S. Wang, “A solution to detect the existence of a malicious rogue AP,” *Computer Communications*, vol. 142-143, pp. 62-68, 2019.

[3] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the Internet of Things: perspectives and challenges,” *Wireless Networks*, vol. 20, no. 8, pp. 2481-2501, 2014.

[4] P. Feng, “Wireless LAN security issues and solutions,” in *Proceedings of 2012 IEEE Symposium on Robotics and Applications*, Kuala Lumpur, Malaysia, 2012, pp. 921-924.

[5] M. Waliullah and D. Gan, “Wireless LAN security threats and vulnerabilities,” *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 1, pp. 176-183, 2014.

[6] K. Gafurov and T. M. Chung, “Comprehensive survey on Internet of Things, architecture, security aspects, applications, related technologies, economic perspective, and future directions,” *Journal of Information Processing Systems*, vol. 15, no. 4, pp. 797-819, 2019.

[7] N. Y. Kim, S. Rathore, J. H. Ryu, J. H. Park, and J. H. Park, “A survey on cyber physical system security for IoT: Issues, challenges, threats, solutions,” *Journal of Information Processing Systems*, vol. 14, no. 6, pp. 1361-1384, 2018.

[8] B. Alotaibi and K. Elleithy, "Rogue access point detection: taxonomy, challenges, and future directions," *Wireless Personal Communications*, vol. 90, no. 3, pp. 1261-1290, 2016.

[9] V. Gupta and M. K. Rohil, "Information embedding in IEEE 802.11 beacon frame," *IJCA Proceedings of National Conference on Communication Technologies & Its Impact on Next Generation Computing*, vol. 2012, no. 3 pp. 12-16, 2012.

[10] H. Siadati, "Prevention, detection, and reaction to cyber impersonation attacks," PhD dissertation, New York University, NY, 2019.

[11] A. Srinivasan and J. Wu, "VOUCH-AP: privacy preserving open-access 802.11 public hotspot AP authentication mechanism with co-located evil-twins," *International Journal of Security and Networks*, vol. 13, no. 3, pp. 153-168, 2018.

[12] Z. Tang, Y. Zhao, L. Yang, S. Qi, D. Fang, X. Chen, X. Gong, and Z. Wang, "Exploiting wireless received signal strength indicators to detect evil-twin attacks in smart homes," *Mobile Information Systems*, vol. 2017, article no. 1248578, 2017.

[13] M. Agarwal, S. Biswas, and S. Nandi, "An efficient scheme to detect evil twin rogue access point attack in 802.11 Wi-Fi networks," *International Journal of Wireless Information Networks*, vol. 25, no. 2, pp. 130-145, 2018.

[14] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 449-462, 2009.

[15] C. Arackaparambil, S. Bratus, A. Shubina, and D. Kotz, "On the reliability of wireless fingerprinting using clock skews," in *Proceedings of the 3rd ACM Conference on Wireless Network Security*, Hoboken, NJ, 2010, pp. 169-174.

[16] T. Kim, H. Park, H. Jung, and H. Lee, "Online detection of fake access points using received signal strengths," in *Proceedings of 2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, Yokohama, Japan, 2012, pp. 1-5.

[17] J. W. Lee, S. Y. Lee, and J. S. Moon, "Detecting rogue AP using k-SVM method," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 24, no. 1, pp. 87-95, 2014.

[18] S. B. Vanjale and P. B. Mane, "Multi parameter based robust and efficient rogue AP detection approach," *Wireless Personal Communications*, vol. 98, no. 1, pp. 139-156, 2018.

[19] S. Kang, D. Nyang, and K. Lee, "Evil-twin detection scheme using SVM with multi-factors," *Journal of the Korean Institute of Communications and Information Sciences*, vol. 40, no. 2, pp. 334-348, 2015.

Jeonghoon Seo **https://orcid.org/0000-0001-8059-4993**

He received his bachelor's degree in Computer Engineering from Chungnam National University in 2018. Currently, he is pursuing his master's degree in Computer Engineering from Chungnam National University.

Chaeho Cho **https://orcid.org/0000-0003-2285-8553**

He is a PhD candidate in the Department of Computer Science and Engineering at Chungnam University, Korea. His main research interests are network security using machine learning and digital forensics.

Yoojae Won **https://orcid.org/0000-0002-7706-5983**

He received B.S. and M.S. from the Department of Computational Statistics, Chungnam National University, Korea, in 1985 and 1987, respectively. He received a Ph.D. from the Department of Computer Science and Engineering, Chungnam National University, Korea, in 1998. He worked on wireless Internet information security at Electronics and Telecommunications Research Institute from February 1987 to February 2001, mobile security at AhnLab from March 2001 to August 2004, and incident handling and management planning at Korea Internet & Security Agency from September 2004 to February 2014. Currently, he is a professor in the Department of Computer Science and Engineering, Chungnam National University.