Location Prediction of Rogue Access Point Based on Deep Neural Network Approach

Apisak Ketkhaw and Sakchai Thipchaksurat*

Department of Computer Engineering, School of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
E-mail: 57601001@kmitl.ac.th; sakchai.th@kmitl.ac.th
**Corresponding Author*

Received 22 July 2021; Accepted 14 December 2021;
Publication 05 March 2022

Abstract

One of the serious security problems in wireless local networks (WLAN) is the existence of the rogue access points (RAPs). To prevent our network from the RAP attacks, we need to identify the RAPs by using the RAP detection methods. However, the identification of RAP location is also a challenging task. The objective of this paper is to propose the location prediction scheme for the RAP. We call our proposed scheme as the location prediction of rogue access point (LPRAP). The LPRAP scheme consists of two mechanisms, the RAP detection mechanism and the RAP location prediction mechanism. We apply the concept of the fingerprint in the RAP detection mechanism by considering the SSID, time duration of broadcasting beacon frame and MAC address. We show that this mechanism can detect the number of RAP. For the RAP location prediction mechanism, we utilize the deep neuron network (DNN) to predict the location of RAPs and evaluate its effectiveness. We evaluate the performance of LPRAP by comparing with those of other machine learning methods such as Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Naive Bayes, and Multi-layer Perceptron (MLP).

Journal of Mobile Multimedia, Vol. 18_4, 1063–1078.
doi: 10.13052/jmm1550-4646.1845

We also compare with particle swarm optimization algorithm. The results show that LPRAP can accurately predict the location of RAP up to 99.29%.

Keywords: Wireless local area networks, rogue access point, beacon frame, location prediction, deep neural network.

1 Introduction

In recently years, wireless local area networks (WLAN) are widely used in many areas and in several places such as home, offices, schools, department stores, and airports. In WLAN, the access point (AP) is the major device used for creating the wireless network. It provides the wireless link for the wireless users to connect to the wired-network and then to the Internet. One of the serious security problems concerned with the AP in WLAN is the unauthorized AP [1]. The unauthorized AP may be set up by someone who want to connect to the Internet without authorized via the legitimate AP. Another purpose of the unauthorized AP is for malicious intent. Due to broadcast nature of WLAN, it makes the WLAN vulnerable to eavesdropping, unauthorized access, denial of service attack and man-in-the-middle attack. This kind of RAP can do substantial damage [1–3]. The hacker can use RAP to capture the sensitive information of legitimate clients such as usernames and passwords. The RAP normally uses two wireless network interface cards. One card is built-in network interface card is used for association with the legitimate AP. Another card is plug-and-play network interface card which is used for imitating the legitimate AP to tempt the wireless users connect to RAP as the client. It is essential to secure WLAN and detect doubtful APs [4]. To increase the security of networks, we need to identify RAP by implementing the processes or mechanisms to monitor for RAPs. Those processes or mechanisms are called the RAP detection methods. So far, the several proposed papers have been focused only on the RAP detection methods. However, the location of RAPs should be considered also. So, some papers have proposed techniques for identifying the location of RAPs. To complete the methods concerned with the RAP, the methods should compose of both mechanism for RAP detection and RAP location identifying as well. With these reasons, they encourage us to consider the mechanism for predicting the location of RAPs after the RAPs are detected. In this paper, we aim to present the simple mechanism for detection the RAPs by considering the time interval of beacon frames which are sent by the access points and the location prediction of RAPs mechanism. The main contribution of this paper is to apply deep

neuron network (DNN) for predicting the location of RAPs. We call our proposed scheme as the location prediction of RAP (LPRAP). The process of LPRAP can be divided into two mechanisms; the RAP detection mechanism and RAP location prediction mechanism.

The remainder of this paper are organized as follows. Section 2 presents some related works. Our proposed scheme is explained in Section 3. We evaluate the effectiveness of our proposed scheme by conducting the experiment in Section 4. Finally, we conclude our paper in Section 5.

2 Related Works

So far, the researchers have proposed several methods related to RAP. Most of the papers have focused on the detection of RAP that can be classified into different groups. One group use the concept of fingerprint by utilizing the packet sniffers to capture one or more characteristics of AP via wireless traffic and analyze these characteristics to detect the RAP [5–7]. These characteristics can be Medium Access Control (MAC) address, Service Set Identifier (SSID), and Received Signal Strength Indicator (RSSI). The example of the approach in this group is [7]. B. Alotaibi and K. Elleithy propose the passive approach by using fingerprint technique to detect the RAP [7, 8]. They use the beacon frame size as the fingerprint. The approach tries to find the threshold value for the appropriate beacon frame size by using training sample and testing process. The threshold value can be derived from the average of deviation between the maximum beacon frame size of the RAP and the minimum beacon frame size of the legitimate AP. Another example is the clock skews technique which is proposed by S. Jana and S. K. Kasera [9]. They propose the fast and accurate detection technique of unauthorized wireless AP. They use the concept of clock skews of the AP for detecting the RAP. The clock skews are calculated from time synchronization function timestamps which are sent out in the beacon frames. These clock skews of AP can be used as the fingerprint for detecting RAP. The other approaches consider in case the RAP is located between the wireless user and the legitimate AP [10–12]. In this case, the information such as the number of wireless hop can be utilized to detect the RAP. In [10], the authors present the timing-based scheme for RAP detection. The scheme is called the user-centric approach by observing the round trip time (RTT) between the wireless user and the DNS server in order to determine the RAP. The scheme can be done without any assistance from the wireless network administrator. Some approaches may use the concept of centralized database to keep the list of authorized APs [13].

R. Shrestha and Y. Nam propose the AP selection mechanism to avoid the RAP. The mechanism uses the centralized server called AP registration center to manage the list of authorized APs. The wireless users can request to server for checking the legitimate APs.

In addition to the detection of RAP in wireless networks, the determination of RAP location is also essential problems. However, the researches related to the problem of RAP location are not many. In [14], the authors propose the RAP detection and localization architecture by implementing the client-server model. The clients work as the monitors which are the laptop computers installed with a modification of inSSIDer software. The localization algorithm is run at centralized server. The information is collected from all monitors by the server. Then, the server runs the localization algorithm in order to identify and locate the RAPs. F. Awad, et al. [15] propose the RAP location approach using particle swarm optimization (PSO). This research use received signal strength to estimate the distance between the access point and the number of known locations around AP by using the set of received signal strength and known location as the input to PSO technique. The authors focus only on determining the location of RAP without considering the RAP detection technique. The machine learning algorithms are also used for considering the location in WLAN. In [16], the authors propose the method for WIFI indoor poisoning by using KNN algorithm. Deep neural networks are proposed by [17] for localization indoor and outdoor environments in WLAN. However, there are not many papers utilize the deep neural networks for predicting the RAP locations. So, these encourage us to consider this paper.

3 The Proposed Scheme

In this section, we present our proposed scheme called Location Prediction of Rogue Access Point (LPRAP) scheme. The LPRAP can be divided into 2 mechanisms as shown in Figure 1.

- The rouge access point detection mechanism: This mechanism is the first step of LPRAP scheme for detecting the RAP in the network by considering the beacon frames which are broadcasted from the legitimate access point (LAP) and may be broadcasted from the rogue access point (RAP) as well. The detail of rouge access point detection mechanism will be explained in the following section.
- The rogue access point location prediction mechanism: In this mechanism, we have applied deep neural network (DNN) for predicting the

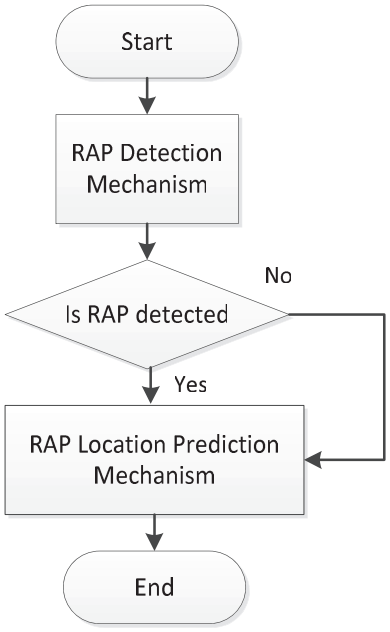

Figure 1 Location Prediction of Rogue Access Point (LPRAP) scheme.

location of RAP. The mechanism will be explained in the following section.

3.1 Rogue Access Point Detection Mechanism

We have considered the network configuration as shown in Figure 2. The legitimate Access Point (LAP) connects to the Internet via switch and router, respectively. The RAP can be connected to Internet using wireless LAN (WLAN) or connected to the cell tower using cellular networks such as 4G or 5G as shown in Figure 2. The beacon frames are broadcasted from both the LAP and RAP. The time duration of broadcasting beacon frame normally for every 102.4 ms or 1024 μs as shown in Figure 3.

This time duration of beacon frame has encouraged us in considering the detection mechanism of RAP. The basic idea is that since we know the time duration of beacon frame in any duration of time from starting time to ending time. The number of beacon frame can be obtained exactly by monitoring and counting the broadcasted beacon frame. So if the RAP does not exist in the network, the calculated number of beacon frame and the number of

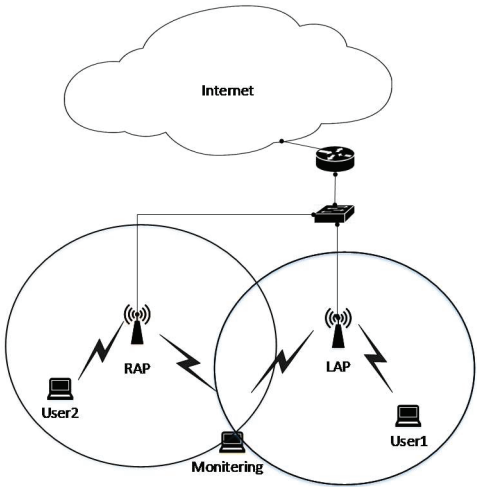

Figure 2 Network configuration.

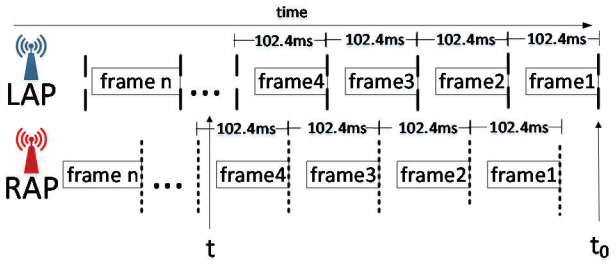

Figure 3 Broadcasting beacon frame.

beacon frame counted by the monitor node should be equal. The number of calculated beacon frame (n_c) can be given by,

$$n_c = \frac{t - t_0}{t_b} \tag{1}$$

Where t_0 is the starting time for first capturing the starting of the first beacon frame, t is the ending time for monitoring broadcasting beacon frame, and t_b is time duration of broadcasting beacon frame which is usually set to 102.4 ms. The number of RAP (n_r) is given by,

$$n_r = \left\lceil \frac{n_m}{n_c} \right\rceil - 1 \tag{2}$$

Where n_m is the number of beacon frame derived by monitoring and counting the broadcasting beacon frame. The process of RAP detection mechanism can be demonstrated as shown in Figure 4.

3.2 Rogue Access Point Location Prediction Mechanism

In this mechanism, we apply the Deep Neural Network (DNN). DNN algorithm is one of the powerful machine learning model. We exploit the DNN for classifying the location to predict the location of the RAP. The structure of DNN can be shown in Figure 5. The DNN structure show an input layer, 5 hidden layers and output layer. The hidden layers have different number of units such as 256, 128, 64, 128, and 256 units, respectively and use ReLU as the activation function. For the output layer, we use Softmax function. The learning process is done by capturing the beacon frames to get the information such as time stamp, RSSI, SSID, and MAC address.

To obtain the dataset for training and testing, we introduce the network area by dividing into NxN subareas as shown in Figure 6. Where N is the position odd number and N is greater than or equal to 3. The Legitimate AP (LAP) is located in the center of NxN subareas which has the location coordinate of ((N+1)/2, (N+1)/2). We introduce the mechanism of location prediction for RAP by learning the information of received signal strength indicator (RSSI) which are received by the user.

The process of dataset preparation can be described as the following steps.

Step 1: We measure the RSSI in case the RAP does not exist by setting the location of LAP at the center of network area. Then we measure the RSSI by the user at every subarea.

Step 2: We measure the RSSI incase the RAP exist by setting the location of LAP at the center of network area. We first locate the RAP at subarea (1,1) and measure the RSSI by the user from subarea (1,1) to subarea (N,N). Then we move to location of RAP to subarea (1,2) and repeat the same process by the user until the RAP move to subarea (N,N).

The dataset preparation process can be demonstrated as shown in Figure 7.

4 Experiment and Results

In this section, we evaluate the performance of our proposed scheme by means of the experiment. We set up the experimental model as shown in

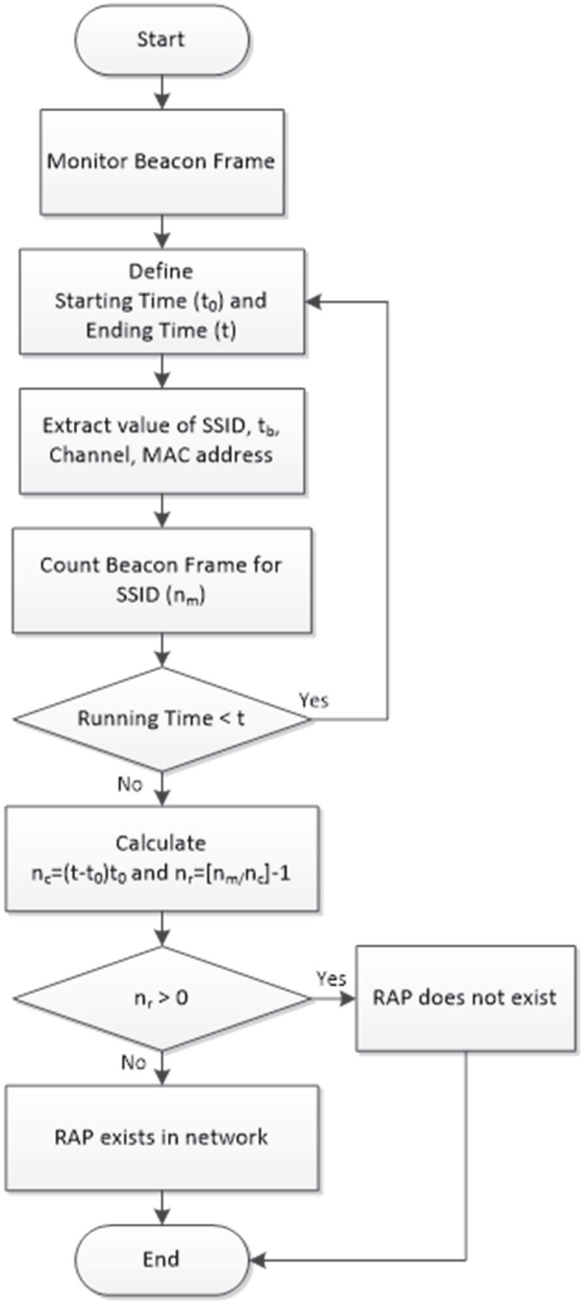

Figure 4 Rogue access point detection mechanism.

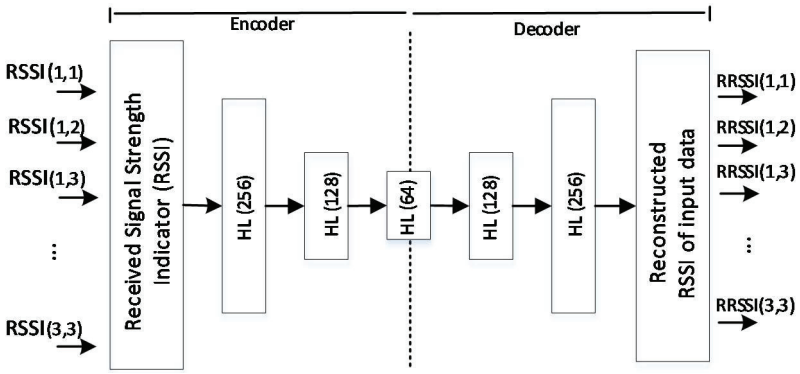

Figure 5 Structure of deep neural network.

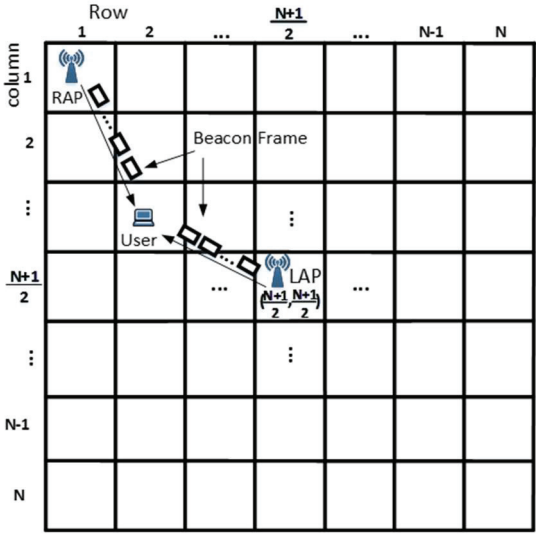

Figure 6 Network area.

Figure 8. The linksys wrt54gl devices are used for the LAP and RAP by setting the same SSID and channel but the MAC addresses are different. The ASUS K450l notebook computer with the Kali Linux operating system is used for monitoring the beacon frame by running in monitor mode. We make the following assumptions. The network area is divided into 9 subareas. We assume that the location of LAP is at the center of network area or subarea (2,2). We collect the information of RSSI totally 90 subareas. There are 9 subareas for non-RAP cases that uses for reference and 81 subareas in case

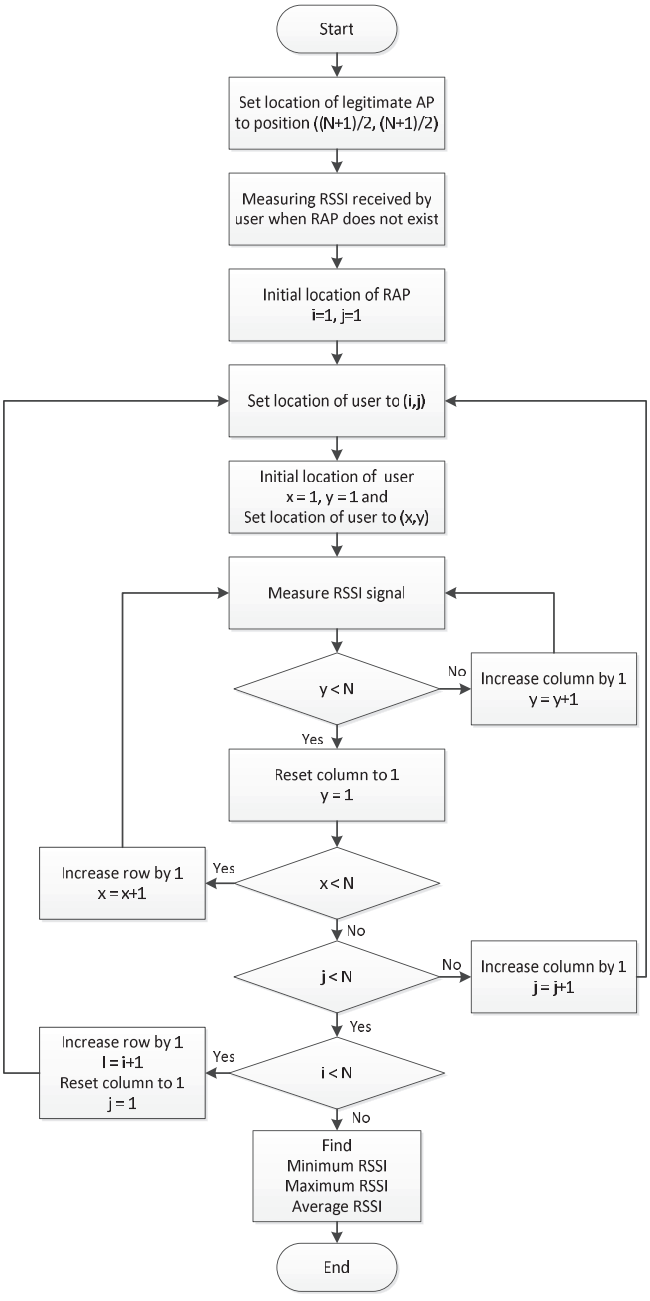

Figure 7 Dataset preparation process.

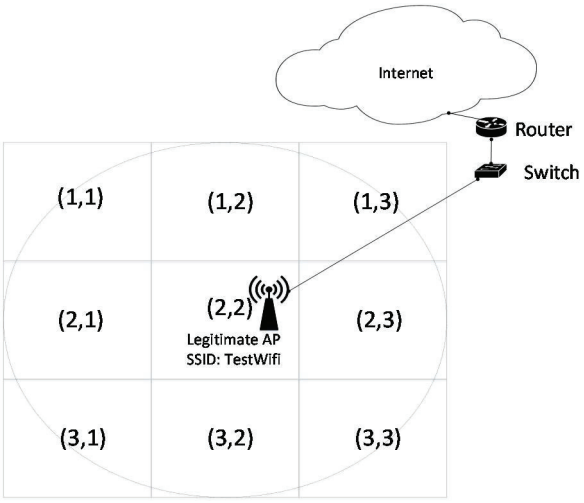

Figure 8 Experimental model.

the RAPs exist. DNN tries to classify set of RSSI to determine the location of RAP. Each location corresponds to one of 9 subareas. Each location is 9×9 (=81) RSSIs in size. We consider that each RSSI is one feature, then DNN uses 81 feature-dimentional feature space to classify the location of RAP. At each subarea, we capture 10,000 beacon frames per subarea to get the RSSI. Totally, we have information of 900,000 beacon frames for learning and testing processes. The number of RAPs is 1 to 4 RAPs. We evaluate the performance of our proposed scheme by means of the accuracy of location prediction. Those results are compared with other 4 machine learning algorithm such as support vector machine (SVM), K-nearest neighbor (KNN), naïve bayes, and multi-layer perceptron (MLP).

Figure 9 shows the number of frames for detecting RAP with the various number of detected RAPs. The results show that our proposed scheme, LPRAP, is applicable to detect in case the several RAPs exist in the network. We can see that the number of captured frames increases as the number of RAPs increases.

Figure 10 shows the accuracy of RAP location prediction versus the various number of subareas for SVM, Naïve Bayes, KNN, MLP, and LPRAP. The results show that our proposed scheme, LPRAP, provides the highest accuracy of prediction comparing with those of other machine learning algorithms. The accuracy of prediction increases as the increasing of the number

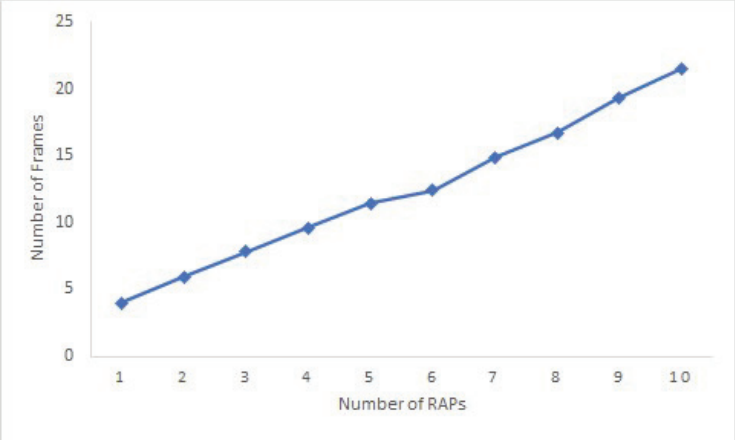

Figure 9 The number of frames with the different number of RAPs.

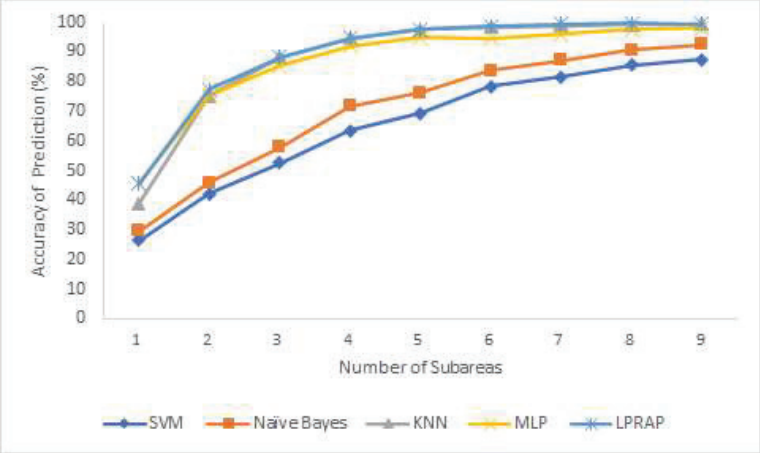

Figure 10 The accuracy of prediction versus the various number of subareas.

of subareas which is used for prediction. For 3 subareas, LPRAP has the accuracy of prediction of 88.31 percentage. The accuracy of prediction is greater than 90 percentage can.

In this experiment, the performance of LPRAP is compared with those of particle swarm optimization (PSO) under the same environment. Based on experimental results, LPRAP may provide the higher accuracy of prediction than those of PSO.

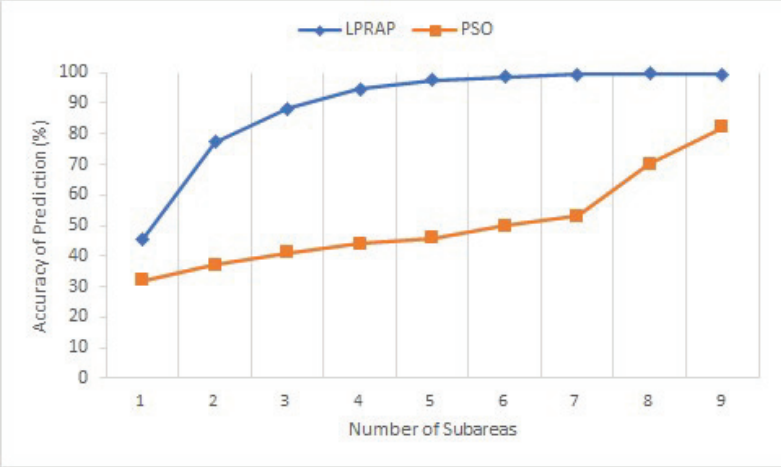

Figure 11 The accuracy of prediction versus the various number of subareas for LPRAP and PSO.

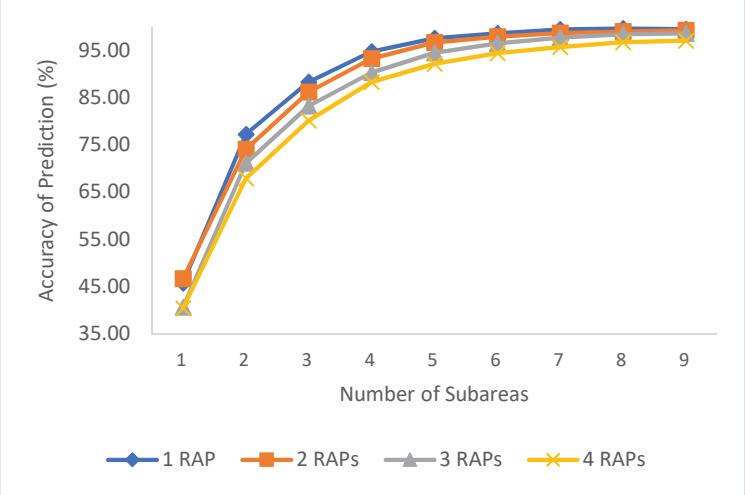

Figure 12 The accuracy of prediction versus the various number of subareas for location prediction of 1 RAP to 4 RAPs.

Figure 12 shows the accuracy of prediction versus the number of subareas for various the number of RAPs. The objective of this figure is to show the effect of the number of RAPs on the accuracy of prediction of the number of RAPs of 1, 2, 3, and 4 RAPs, respectively. The results show that the accuracy

of prediction increase as the increasing of the number of subareas for all the number of RAPs. For the number of RAPs, the accuracy of prediction decreases as the increasing of RAPs. It is clear that the accuracy of prediction can be improved if we increase the number of subareas.

5 Conclusion

We have proposed the location prediction of rogue access point (LPRAP) scheme. LPRAP is divided into two mechanisms, the RAP detection mechanism and the RAP location prediction mechanism. The RAP detection mechanism considers the beacon frames which are broadcasted from the legitimate access point (LAP) and may be from the RAP. For the RAP location prediction mechanism, we utilize the deep neural network (DNN) for predicting the location of the RAP by learning the received signal strength indicator (RSSI) which are received by the wireless user. We evaluate the performance of LPRAP by means of the experiment in order to show the effectiveness of LPRAP. The result show that, for RAP detection mechanism, the LPRAP can effectively detect the number the RAPs. For RAP location prediction mechanism, the experimental results are compared with four machine learning approach – Support Vector Machine (SVM) algorithm, K-Nearest Neighbor (KNN) algorithm, Naïve Bayes algorithm, and Multilayer Perceptron (MLP) algorithm. We also compare with the particle swarm optimization algorithm. The results show that the LPRAP is able to predict the location of RAPs effectively. The LPRAP has up to 99.29% accuracy in location prediction of RAPs.

References

[1] R. Beyah and A. Venkataraman, "Rogue Access Point Detection," *IEEE Computer and Reliability Societies*, pp. 56–61, 2011.

[2] B. Alotaibi and K. Elleithy, "Rogue access point detection : Taxonomy, challenges, and future direction," *Wireless Personal Communications*, October 2016.

[3] S. Anmulwar, M. Ai-Refai, and A. Al-Qerem, "Rogue access point detection methods : A review," *International Conference on Information Communication and Embedded Systems (ICICES)*, 2014.

[4] K. Sui, Y. Zhao, D. Pei, and L. Zimu, "How bad are the rogue' impact on enterprise 802.11 networks performance?," *IEEE Conference on Computer Communications (INFOCOM)*, pp. 361–369, 2015.

[5] S. Shetty, M. Song, and L. Ma, "Rogue access point detection by analyzing network traffic characteristics," *IEEE Military Communications Conference (MILCOM)*, 2007.

[6] K.-F. Kao, W.-C. Chen, J.-C. Chang, and H.-T. Chu, "An accurate fake access point detection method based on deviation of beacon time interval," *8th International Conference on Software Security and Reliability*, 2014.

[7] B. Alotaibi and K. Elleithy, "A passive fingerprint technique to detect fake access points," *Wireless Telecommunication Symposium (WTS)*, 2015.

[8] B. Alotaibi and K. Elleithy, "An empirical fingerprint framework to detect rouge access points," *Systems, Applications and Technology Conference (LISAT)*, 2015.

[9] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Transactions on Mobile Computing*, March 2010, pp. 449–462.

[10] H. Han, B. Sheng, C. Tan, and S. Lu, "A measurement based rough AP detection scheme," *IEEE International Conference on Computer Communications (INFOCOM)*, 2009.

[11] H. B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rough AP detection," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, Iss. 11, pp. 1912–1925, Nov. 2011.

[12] C. Yang, Y. Song, X. Fang, and J. Tang, "Active user-side evil twin access point detection using statistical techniques," *IEEE Transactions on Information Forensics and Security*, 2012.

[13] R. Shrestha and S. Y. Nam, "Access point selection mechanism to circumvent rogue access point using voting-based query procedure," *IET Communications*, Vol. 8, Iss. 16, pp. 2943–2951, 2014.

[14] T. M. Le, R. P. Liu, and M. Hedley, "Rogue Access point Detection and Localization," *The 23rd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 2489–2493, 2012.

[15] F. Awad, M. Al-Refai, and A. Al-Qerem, "Rogue access point location using particle swarm optimization," *8th International Conference on Information and Communication Systems (ICICS)*, 2017.

[16] X. Ge and Z. Qu, "Optimization wifi indoor positioning KNN algorithm location-based fingerprint," *7th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 2016.

[17] W. Zhang, K. Liu, W. Zhang, Y. Zhang, and J. Gu, "Deep neural networks for wireless localization in indoor and outdoor environments," *Elsevier (Neurocomputing),* Vol. 194, pp. 279–287, June 2016.

Biographies

Apisak Ketkhaw received the B.Eng. degree in Computer Engineering from Naresuan University, Phitsanulok, Thailand, in 2007 and M.Eng. degree in Computer Engineering form Mahanakorn University of Technology, Bangkok, Thailand, in 2010, respectively. He is currently pursuing the D.Eng. degree in Electrical Engineering at King Mongkut's Institute of Technology Ladkrabang. His research interests are in the areas of security of wireless LAN.

Sakchai Thipchaksurat received the B.Sc. degree in Statistics from Srinakarinwirot Prasarnmitr University in 1988, the M.Eng. degree in Electrical Engineering from King Mongkut's Institute of Technology Ladkrabang, Thailand, in 1996, and Ph.D. in Computer Sciences from Gunma University, Japan in 2002. He is now an associate professor in the Department of Computer Engineering, School of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand. His current research interests are in the areas of performance evaluation of communication networks, wireless and mobile communication.