2023 IEEE 13th International Conference on Consumer Electronics - Berlin (ICCE-Berlin) | 979-8-3503-2415-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCE-BERLIN58801.2023.10375616

# A Client-Side Evil-Twin Attack Detection System with Threshold Considering Traffic Load

‡Tomoyuki Ueda, †Amgad Saif, ‡Sumiko Miyata, ††Masataka Nakahara, ††Ayumu Kubota
‡Shibaura Institute of Technology, Tokyo, Japan
†KTH Royal Institute of Technology, Stockholm, Sweden
††KDDI Research, Inc., Saitama, Japan
‡{ma23025, sumiko}@shibaura-it.ac.jp, †asmsaif@kth.se, ††{ms-nakahara, ay-kubota}@kddi.com

***Abstract*—In recent years, public wireless LANs have been increasingly installed in public places. On the other hand, free Wi-Fi has various security issues. One of these problems is the evil-twin attack. There are some studies that focus on the round-trip time (RTT) as a detection method for evil-twin attacks. However, their detection criteria are insufficient because they do not assume the traffic load to set the criteria. In this paper, we propose a new evil-twin attack detection method with threshold for detection criteria considering traffic load.**

***Index Terms*—Evil-twin, Rogue access point, Round trip time**

## I. Introduction

In recent years, the rapid proliferation of wireless LANs has led to the enhancement of wireless LAN services and Internet of Things (IoT) devices in various public facilities. Furthermore, the global shift to remote work and online classes due to the new coronavirus has amplified the use of these networks. However, this increased usage has brought various security issues to the fore. One such issue is the evil-twin attack [1]. Evil-twin attack is a type of attack where users are tricked into connecting to a malicious AP that impersonates a legal one. This attack aims to steal information or deliver malware to the connected users. Thus, we need to detect theses rough APs.

Existing studies on rogue AP detection can be divided into two main categories; administrator-side [2], [3], [4] and user-side [5], [6], [7]. Most of existing studies for detection of rough AP focus on the administrator side [2], [3] because they can collect traffic data and perform centralized management [2]. However, these detection methods on the administrator side is costly in terms of time and money, thus, there are many public wireless LANs that do not take any countermeasures.

For user-side detection, delay based methods with Round-Trip Time (RTT) are common [5], [6], [7]. Kitisriworapan et al. [7] state that traffic load in the system leads to increase of variation in RTT. However, this conventional method does not assume that traffic load changes. To know the traffic load of a system, the administrator needs to manage it. However, the only research on the administrator's side is costly detection using fingerprinting and other methods.

In this paper, we focus on both user and administrator side for detection and proposes an attack detection method that sets a threshold every traffic load. Moreover, we show the effectiveness of our detection method by using IoT networks.

The paper is structured as follows. Section 2 mentions the proposed method in detail, Section 3 presents the experimental method and results. Section 4 presents the conclusions and the problems and issues in this study.

## II. Proposed method

In this study, we assume that some devices connect to rough AP relayed to legal AP when evil-twin attack. In our proposed method, we consider detecting whether an evil-twin attack is occurring by using thresholds every traffic load.

We define the traffic load as $i$, $i \in \{1, 2, ..., C\} = \mathcal{C}$. Let $C$ be the number of types of traffic load. By collecting RTT data based on the devices and the load generated using iperf, we aim to detect the rogue AP.

In our proposed method, the initial $t$ data points obtained from the legal AP are used as training data. Referring to [7], we use k-means method in order to derive two cluster centroids $\gamma_i^{\mathrm{upper}}$ and $\gamma_i^{\mathrm{lower}}$, and derive cumulative distribution by measuring RTT data. Specifically, for each load class $i$, we set threshold $\theta_i$, where $\theta_i = \frac{\gamma_i^{\mathrm{upper}}}{\gamma_i^{\mathrm{lower}}}$, representing the ratio of y-axis values of the cluster centroids. Similarly, we use the derived threshold $\rho_{i,j}$, where $i \in \mathcal{C}$, obtained through the k-means algorithm for each load class $i$, and $j \in \mathcal{D}$ data set number $j$ to detect the rogue AP. Here, $\mathcal{D} = \{1, 2, ..., D\}$ represents the index of the data set used for evaluation.

As illustrated in Algorithm 1, for a specific load class $i \in \mathcal{C}$ and data set number $j \in \mathcal{D}$, if $\rho_{i,j} > \theta_i$, the presence of a rogue AP is detected. Note that, $\theta_i$ is not changed by changing traffic load in reference [7]. After our detection method with k-means, we perform additional detection using the cumulative distribution function (CDF). We calculate the upper confidence interval value denoted as $\theta_i^{\mathrm{CI-upper}}$ from the same data used for the threshold determination. If the average round-trip time $RTT_i^{\mathrm{ave}}$ of the collected data is greater than $\theta_i^{\mathrm{CI-upper}}$, these packets are treated as evil twin attack packets.

## III. Results for our method

### A. Experimental Methods

As shown in Fig.1, the experiment is carried out by applying a load between two connected PCs using iperf and measuring

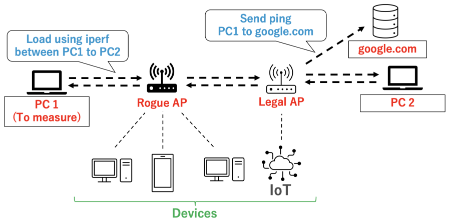
Load using iperf between PC1 to PC2
Send ping PC1 to google.com
google.com
PC 1 (To measure)
Rogue AP
Legal AP
PC 2
IoT
Devices

Fig. 1. Assumed enviorment.

**Algorithm 1** Rogue identification

```
/* gathering RTT */
/* input parameters: $RTT, i, \theta_i, RTT_i^{\mathrm{ave}}, \theta_i^{\mathrm{CI-upper}}$ */
for $RTT$ in $i$ do
    /* Detect with k_means */
    $\gamma \leftarrow$ k_mean($\overline{RTT}$)
    $\gamma_i^{\mathrm{upper}} \leftarrow \max(\gamma)$
    $\gamma_i^{\mathrm{lower}} \leftarrow \min(\gamma)$
    $\rho_{i,j} = \frac{\gamma_i^{\mathrm{upper}}}{\gamma_i^{\mathrm{lower}}}$
    if $\rho_{i,j} > \theta_i$ then
        /* Detect with CDF */
        /* CI = Confidence interval */
        if $RTT_i^{\mathrm{ave}} > \theta_i^{\mathrm{CI-upper}}$ then
            return (rougue-AP is detected)
        end if
    else
        return (No rougue-AP is detected)
    end if
end for =0
```

the time taken for the AP to ping google.com and return as RTT. For IoT connectivity, the frequency band used is 2.4G. For each experiment, 300 packets of 100-byte pings were sent at a rate of 10 times per second. This process is repeated four times. As shown in Fig. 1, both PCs and smartphones are used to mimic natural traffic.

After the removal of outliers, our detection method is performed on the acquired RTT data. The F-score and accuracy are served as evaluation measures. We compare with a conventional method [7] in which the threshold $\theta_i$ is a fixed value ("fixed threshold method"). In our proposed method, thresholds are calculated every load based on the RTT, whereas the fixed threshold method uses only one threshold for detection even if the traffic load is changed.

We set $C = 4$; $i = 1$ represents no load, $i = 2$ represents 3 Mbytes load, $i = 3$ represents 5 Mbytes load, and $i = 4$ represents 7 Mbytes load. It is assumed that a total of 20 devices (16 IoT devices, 3 PCs, and 1 smartphone) are connected to the AP. Also, detection is performed with a measurement data size of $T_j = 300$ for each class $i$ and a detection data size of $D = 24$.

### *B. RTT distribution and detection accuracy*

The resulting RTT graphs from the experiment are illustrated in Figs.2–3. These figures display the RTTs for connections to the legal APs with blue plotslegal and to the rogue APs with red points. Without iperf, both blue and red points overlap. However, when a 7 MB load is applied, there is a significant difference in the variability of RTTs for both the legal and rogue APs.

Accuracy and F-score are used as evaluation metrics. TABLE I presents the results of calculating accuracy and F-score based on the detection outcomes. As observed from TABLE I, the accuracy for the fixed threshold method is 0.74, while the proposed method achieves an accuracy of 0.92. Regarding the F1 score, the baseline method achieves 0.79, while the proposed method achieves 0.92, indicating different values. Thus, our proposed method clearly shows the effectiveness of traffic load-aware detection, as both accuracy and F-score outperform the fixed-threshold method.

TABLE I
DETECTION RESULT

| | Fixed threshold method [7] | Proposed Method |
|---|---|---|
| Accuracy | 0.74 | 0.92 |
| F-score | 0.79 | 0.92 |

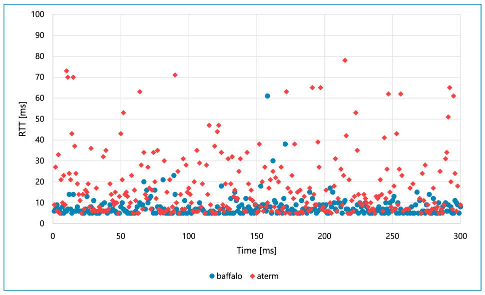

Fig. 2. RTT without iperf.

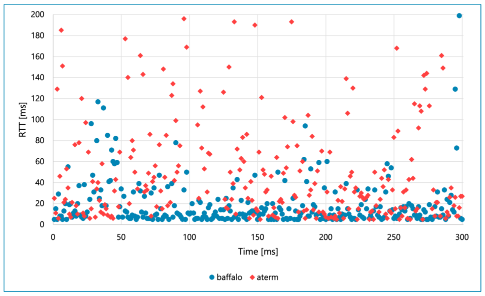

Fig. 3. RTT for 7MB load with iperf.

## IV. Conclusion

In this paper, we proposed a novel evil-twin attack detection method that takes into account the traffic load by using both user and administrator measurements. Our experiments show that our proposed method is effective with F-score exceeding 0.9. In the future work, we plan to extend this detection method by taking into account the characteristics of both traffic load.

## ACKNOWLEDGMENT

These research results were obtained from the commissioned research(No.05201) by National Institute of Information and Communications Technology (NICT) , Japan.

## References

[1] Muthalagu, Raja and Sanjay, Sachin, "Evil Twin Attack Mitigation Techniques in 802.11 Networks", *International Journal of Advanced Computer Science and Applications*, vol.12(6), 2021.

[2] Pu, Qiaolin and Ng, Joseph Kee-Yin and Zhou, Mu and Wang, "Jie A Joint Rogue Access Point Localization and Outlier Detection Scheme Leveraging Sparse Recovery Technique", *IEEE Transactions on Vehicular Technology*, vol.70(2), pp.1866-1877, 2021.

[3] Asaduzzaman, Md. and Majib, Mohammad Shahjahan and Rahman, Md. Mahbubur, "Wi-Fi Frame Classification and Feature Selection Analysis in Detecting Evil Twin Attack", *2020 IEEE Region 10 Symposium (TENSYMP)*, pp.1704-1707, 2020.

[4] Lovinger, Norbert and Gerlich, Tomas and Martinasek, Zdenek and Malina, Lukas, "Detection of wireless fake access points", *2020 12th ICUMT*, pp.113-118, 2020.

[5] Han, H. and Sheng, B. and Tan, C. C. and Li, Q. and Lu, S., "A Measurement Based Rogue AP Detection Scheme", *IEEE INFOCOM 2009*, pp.1593-1601, 2009.

[6] Kitisriworapan, Songrit and Jansang, Aphirak and Phonphoem, Anan, "evil-twin Detection on Client-side", *2019 16th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pp.697-700, 2019.

[7] Kitisriworapan, S., Jansang, A. and Phonphoem, "A. Client-side rogue access-point detection using a simple walking strategy and round-trip time analysis", *J Wireless Com Network 2020*, pp.1-24, 2020.