2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI) | 978-1-7281-7734-2/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICATMRI51801.2020.9398377

Overview On Public Wi-Fi Security Threat Evil Twin Attack Detection

Said Abdul Ahad Ahadi
Department of Computer Science and Engineering
Sharda University
UP, India
saidahad7@gmail.com

Nitin rakesh
Department of Computer Science and Engineering
Sharda University
UP, India
nitin.rakesh@gmail.com

Sudeep varshney
Department of Computer Science and Engineering
Sharda University
UP, India
sudeep.varshney@sharda.ac.in

***Abstract*—Wi-Fi is widely used internet source which use to provide internet access in many areas such as Stores, Cafes, University campuses, Restaurants and so on. Due to transmission of data over the air which makes network vulnerable so it becomes prone to various threats such as Evil Twin and etc. The Evil Twin is a kind of adversary which impersonates a legitimate access point (LAP) as it can happen by spoofing the name (SSID) and MAC address (BSSID) of a legitimate access point (LAP). And this attack can cause many threats such as MITM, Service Interruption, Access point service blocking. In this paper we review various Evil Twin Attack Detection Techniques and proposed methods with their comparisons.**

Keywords: Evil Twin, LAP, SSID, Wi-Fi Security, RTT, External IP address, ETAD, IDS, ML.

I. INTRODUCTION

Wireless network widely used internet source service around the world, because of amazing and extensive improvement in wireless network evolution in current years. People are able to use Internet all around at any time by using their wireless devices connecting to Wi-Fi. Wi-Fi provides internet access in many more public areas such as Stores, Hotels, Coffee Shops, University campuses and so on.

Norton Report shows that 68% of users in public Wi-Fi Network are victims to different cybercrimes, that can be mistreat to rob private information like passwords, bank credit-card numbers, conversation messages, E-mails and etc [1]. Due to transmission of data over the air this makes network prone to various threats such as Evil Twin and etc. The Evil Twin is a kind of adversary impersonates a legitimate access point (LAP) as it can happen by spoofing the name (SSID) and MAC address (BSSID) of a legitimate access point (LAP). Users might unexpectedly get connected to the adversary's access point, thinking that access point is belongs the real network. As the connection is initiated, the adversary can set up Man-In-Middle, Service Interruption, and Access point service blocking attacks [2].

Public places where network is using open Wi-Fi is not hard for attacker to set up an evil twin attack successfully [4]. In first step attackers configures evil twin AP using a device like a computer or raspberry Pi in the Wi-Fi network by installing some types of software. by configuring the device with the same Wi-Fi name (SSID) and MAC address (BSSID) like legitimate AP impersonates as a legitimate AP and redirect clients get connected to it, attacker. In next step, malicious adversaries to increase its signal lunge use a directional antenna or improve the Received-Signal-Strength-Indicator (RSSI) of evil twin AP by placing them near to clients than a legitimate AP [2][3]. Accordingly, clients might evade to establish connection with evil twin AP when they want to use the Internet using an authorized LAP. At the end, adversary can trace all the clients' network traffic using evil twin AP [3].

In this paper we have discussed various Evil Twin Attack Detection Techniques whether the technique is Client side or Network administrator side, some techniques are active or passive, and some requires protocol revising or it needs some types of hardware. The paper is consisting of 7 parts introduction part, Evil twin attack concept, classification of existing Evil twin detection techniques, Intrusion Detection System (IDS) Based approaches, Machine learning based approaches, comparison of different techniques and conclusions.

II. EVIL TWIN ATTACK

An Evil Twin Attack is one of well-known attack since two decades, the attacker by impersonating as Legitimate AP cheats user to get connection with fake access point while he/she is not aware of that and he/she is getting connected to the hacker's AP. Evil Twin Attack some time use to capture clients information which is a kind of phishing, mostly Evil Twin acts as rouge access point which indicates to Clients as Legitimate AP while it is a fraud AP configured by an attacker to spoof on the connection between clients and AP. As soon as client established a connection with this fraud AP his/her all private information is lost or modified. Like when a client wants to establish a connection with a special network that is visible in his/her network preferred list of wireless network connection window, the user sends a probe message to its demanded network in wireless network connection list. This probe message is interrupt by an adversary and set up an

978-1-7281-7734-2/20/$31.00 ©2020 IEEE

ET attack [4] [6]. Then attacker can steal client's private information like passwords, credit card information and so on as shown in Fig 1.

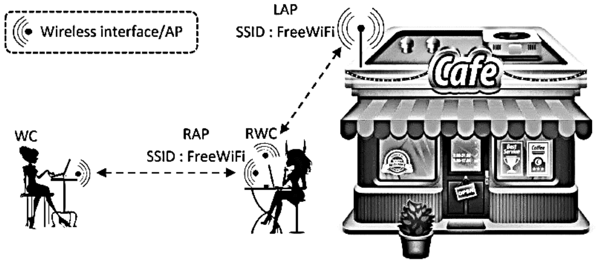


Fig. 1: Evil Twin Attack. [3]

A. Evil twin attacks executions methods [2]:

Passive evil twin attack method: the adversary makes signal strength of the evil twin's hotspot stronger to launches the evil twin attack. Therefore, when any client wants to associate with AP, it gets connected to evil twin access point (ETAP).

Active evil twin attack method: attacker intends to disconnect the users which are connected before with AP by launching a Deauthentication attack over LAP. By this way, the user disassociates with legitimate AP and associates with the evil twin's AP.

B. Attack launching strategies [5] [6]:

1. Coexistence-: the authorized AP and the ETAP exist at the same time in the same location. The ETAP spoofs the SSID and MAC address of the authorized AP by making its signal strength stronger to obligate clients to select ETAP to access an internet connection. Then by using legitimate AP's internet connection relays packets. To perform Attack ET uses two cards, built-in wireless card (for association with LAP) and plug-and-play wireless card (for impersonation as LAP).

2. Replacement-: The Attacker close the legitimate AP and replaces it and runs its own private Internet connection as shown in Fig 2.

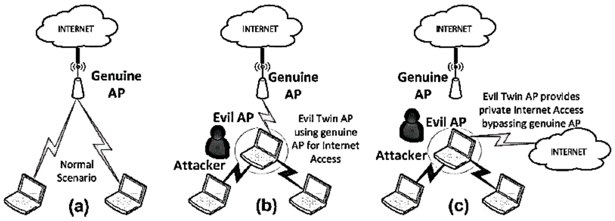


Fig. 2: Normal and of Evil Twin Setup. [23]

C. Evil Twin Attack Background:

The evil twin attack described in a timeline (Fig. 3). The presumption is an open Wireless network scenario. G is an authorized and legitimate access point, and E is a fake access point (ETAP) in a wireless network area. The adversary is following the scenario as showed in Fig. 3 to perform ET attack. All time-slots showing in Fig. 3 is explained as follows:

1. [1st Timeslot (T1) first Handshake]: User asks for authentication frame to G, E listens silently and trace all the frames are exchanging in the network.
2. [2nd Timeslot (T2) second Handshake]: in this stage G replies with an authentication frame. Open Wireless networks do not need for key exchange to authenticate users, but need a frame exchange between User and AP. E passively provides a record of Users and their different parameters which are authenticated to G without exposing its appearance to any user. It runs in passive mode getting ready for association.
3. [3rd Timeslot (T3) third Handshake]: The User asks for association frame to Y.
4. [4th Timeslot (T4) fourth Handshake]: E sends an association response frame to the User before G.
5. [5th Timeslot (T5)]: G also traces an association request frame which sent by the User in time-slot (T3).
Thus G, sends an association response frame.
6. [6th Timeslot (T6)]: From this phase to further the User is associated with E in place of G for network connection, as E's reply was received first. The User ignores the G's association response frame.

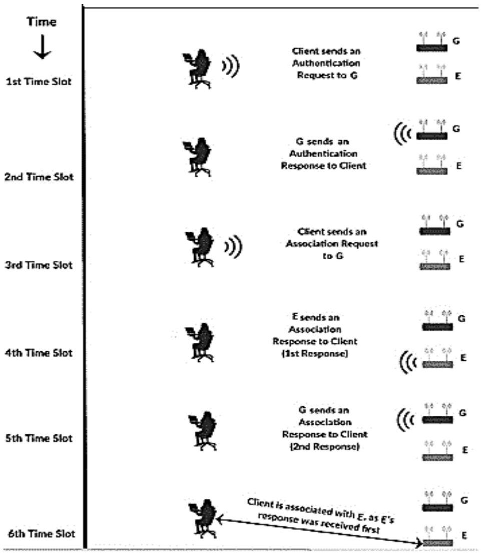

Time
1st Time Slot
Client sends an Authentication Request to G
G
E
2nd Time Slot
G sends an Authentication Response to Client
G
E
3rd Time Slot
Client sends an Association Request to G
G
E
4th Time Slot
E sends an Association Response to Client (1st Response)
G
E
5th Time Slot
G sends an Association Response to Client (2nd Response)
G
E
6th Time Slot
Client is associated with E, as E's response was received first
G
E

Fig. 3: Evil Twin Attack Timeline

III. CLASSIFICATION OF EXISTING SOLUTIONS

Existing countermeasures and proposed solutions are classified based on side of detection as the technique is Client side or Network administrator side, and also the techniques are classified in passive or active, and may require protocol revising or it needs extra hardware.

A. Network Administrative Side ET detection techniques

The network administrator side of wireless network can give any information about wireless network and can provide record of fingerprints of all devices which are already joined to the network. Every AP has its own identification parameters which could differentiate one to another, it can be the AP MAC address or its context these identification parameters (fingerprint) and authorized list helps network admin to identify whether the AP is illegitimate or not [7][3].

The network operator side ETA detection is costly to the Wi-Fi network maintenance, it may need to equipped wireless sensors in order to gather information in router to compare with current available identification parameters authorized list and the network administrator is responsible to assist the wireless client to detect Evil Twin Attack [3].

Pragati Shrivastava et al [2]. Introduced “EvilScout” an evil twin attack detection framework and has analyzed evil twin attack in an authentic test-bed with various Wi-Fi setups and discovered that it can cause many different attacks, as demonstrated in Table1.

TABLE I. EVIL TWIN ATTACK’S GENERATED THREATS IN VARIOUS WI-FI SETUPS USING SAME CHANNEL.

Scenario	*Legitimate AP*	*Evil-Twin*	*Observed Attack*
Public-Wi-Fi	Open	Open	MITM
Mixed-Wi-Fi	WPA	Open	Service Interruption
Protected-Wi-Fi	WPA	WPA	AP service blocking

The “Duplicate Association” event of the client during 4-way handshake discovered in between client and AP and ET, with monitoring of the communication and utilizing data extracted from IP-prefix distribution by legitimate AP, this event grant a precise network side ET attack detection technique. Duplicate Association event occurs whenever a fake AP is impersonating as a legitimate AP by spoofing its BSSID on the similar channels, and Wi-Fi user is associated with each legitimate AP and ET AP in the wireless area. By utilizing the existing information in the Wi-Fi network Pragati Shrivastava et al [2] employed, tested and implemented ET in a Software Defined Network (SDN) enabled Wi-Fi network. EvilScout takes advantage of the SDN capability for detection/mitigation of an ET with no any extra hardware or modifications at the AP or user side. SDN enabled Wi-Fi provide extendable security capabilities for detection Rogue AP and Evil Twin [2] [8]. The data that are present at the SDN controller make simple and precise ET detection. EvilScout is installed on head of the SDN controller and uses OpenFlow facilities, and the severe point is execution of EvilScout which utilizes the AP programmability, and require high level knowledge of WLAN controller.

Next administer side Evil Twin Attack detection approach is the clock-skew technique. Jana et al. [9] introduced clock-skews fingerprint in Wi-Fi Network, times-tamps available in beacon frames, presents special physical fingerprint. According to proposed technique the clock skew of each Access Point can be take out from Timing Synchronization Function (TSF), the clock-skew fingerprint is produce by tiny observable speed variance of the crystal oscillator-based clocks. So the Evil Twin AP distinguishes from legitimate AP by comparing the calculation of target AP’s clock-skew and other available APs’ clock-skew.

B. Client-side detection approaches

In the following approaches Additional Hop Count, Timing based, Traffic and channel monitoring using Same ISP gateway and different ISP gateway solutions are mentioned.

Qian Lu et al [10] proposed passive client-side detection approach in this approach clients can identify and detect evil twin AP with no intervention of a wireless network administrator. The important point is forwarding pattern of evil twin APs, in this method all wireless network data frames (sent by target APs to user) are compare to identify ET attacks. ET-spotter is the tool implemented to recognize and detect the evil twin and the algorithm used in this tool can achieve 96% accuracy in distinguishing ETA from AP. The strength point of Evil Twin attack is playing with Wireless Clients connection behavior in wireless LAN [10] [11]. There are two types of networks existing in an operating system [11].

a) Preferred Network list: clients previously connected list.
b) Available Network list: first time clients connecting list.

In preferred network the list is saved in OS to enable automatic connection to AP whenever clients are available within the range of the preferred network they can get automatically connected. So this technique tricks a client into associating with the fake AP. A methodology proposed using operating system potential in this method there is two sections which can solve the above discussed problem, section I is executed on Access Point side and section II is implemented on Operating System. Section II is responsible for the detection of Evil Twin attack [11].

Diogo Mónica et al [12] introduced Wi-FiHop a client side scheme ET attack detection using common ISP gateway, whenever the client wants to connect with legitimate AP if there are extra Wireless hop existed in wireless channel it recognizes the existence of an ETAP. The method used in Wi-FiHop employ a ‘watermarked packet (random bit stream) sends by user to the requested server, through the currently associated AP and only client is aware of the watermark signature, after sending the watermarked packet in the AP associated channel the client keeps listening to other distinct channel, and make an effort to find the presence of the watermarked packet in the communication happening in that channel. If attack is existed, the watermark definitely become visible on the wireless link between the ETAP and the LAP, it indicates that there is an attack [12].

Omar Nakhila et al [3]. Introduced client side real-time multiple Wi-Fi channel monitoring scheme for ET detection. In this approach to detect ETA client monitors the channels only when the fake AP use LAP to give internet access to the client. The client detects this fake AP by monitoring all Wi-Fi channels randomly seeking for a special data packets (watermarked packet) sending by a dedicated sever through the Internet. After detecting the attack, the system categorizes the AP whether it is LAP or a RAP [3].

Qian LU & Haipeng QU et al [4] proposed client side detection passive scheme that allow clients to recognize and locate ETAs with no aid from network administrator. To decide whether client is connected to ETAP or LAP, this technique analyzes the forwarding frames, the forwarding behavior of evil twin which can state the technique to compare wireless data frames sending by target AP to clients. This technique implemented in a Python tool by the name of ET-Spotter [4].

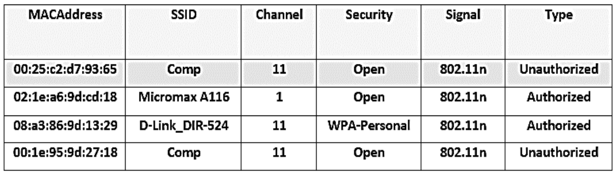
En-Chun KUO et al [7]. Proposed User Side Evil Twin Attack Detection Using Time-Delay (TD) Statistics of server and user TCP termination. This proposed TD prototype is evaluated from different termination time intervals: Initial Termination, Termination Response, and Confirmed Termination. The mean idea in this approach is the monitoring of TCP packets passing through the Server and User when webpage is opening and closing [7].

Qian Lu & Haipeng Qu et al [13] proposed a novel passive client-side approach, this technique monitors Special Length Frames Arrival Time (SLFAT), to identify the evil twin attack, it work on which same gateway connection used as the LAP. SLFAT extracts some parameters such as, the entry time of special frames and by comparing the entry time of the frame's length it determines the evil twin's forwarding behavior which can detect ETA. This approach implemented in a prototype named as ETD-SLFAT.

Hao Han & Bo Sheng et al [14] introduced Timing-Based Schemed technique for ETAP Detection This timing technique utilizes the round trip time values. The client explores a server to measures the RTT from the server's response. The client keeps exploring this process for a several times and keeps recording the RTTs until connection termination. Then the mean value of RTTs calculate if it statistically bigger than the specified threshold, then associated AP marks as an Evil Twin AP.

Songrit Kitisriworapan, Aphirak Jansang and Anan Phonphoem et al [15] proposed an Evil-Twin detection technique on client-side, the clients themselves can identify the Evil Twin. The Idea is to identify the single-hop and double-hop WiFi connection in order to calculate and analyses RTT and it MCS values which are collecting from clients' device. So to take decision the variance of frames' RTT (round trip time) will identify the Evil Twin.

An Operating System based detection system introduced [16]. The main module of system which sort packets according to different traffic characteristics parameters from beacon frames and a probing function takes decision by executing the algorithm whether the AP is legitimate AP or Evil Twin AP.



MACAddress	SSID	Channel	Security	Signal	Type
00:25:c2:d7:93:65	Comp	11	Open	802.11n	Unauthorized
02:1e:a6:9d:cd:18	Micromax A116	1	Open	802.11n	Authorized
08:a3:86:9d:13:29	D-Link_DIR-524	11	WPA-Personal	802.11n	Authorized
00:1e:95:9d:27:18	Comp	11	Open	802.11n	Unauthorized

Fig. 4: Access point system decision list view. [16]

Hossen Mustafa & Wenyuan Xu et al [17] are proposed CETAD mechanism using public server in order to detect evil twin attack. CETAD can be install as an app at user's device and no need to change the hotspot Aps. This mechanism uses three statistics measure in its detection system, such as the differences of RTT values, the standard deviation of RTT values and similarity of ISP information. Using these measurements, although CETAD is created for user side devices, it can be expanding to a network side as well to detect ETAPs.

Harold Gonzales et al [18] introduced a context-leashing approach to detect evil twin by checking AP trust by location. The procedure is to record all visible APs to a user when that user associates for first time to an AP. The recorded APs depicts as wireless prominent features so that user can identify the correct location of that network. Then during next time associations, the user automatically associates to the AP only if the location matches with previously recorded locations [18] [19].

A-Burns, L. Wu, X. Du and L. Zhu et al [20] developed a novel detection system using network diagnostic tool trace-route. The system is a bi-directional remote detection a remote detector server is employed to trace route the client-to-server and server-to-client then compare the result, so the incompatibility among these two trace-route results exposes the evil twin attack.

Y. Song, C. Yang, and G. Gu et al [21] introduced a novel user-side evil twin detection approach, a statistical and anomaly detection algorithms designed. These algorithms are applyed in a system called ETSniffer system. So the system activates when the clients are connecting to a new Access Point to detect and identify the Evil Twin Attack. The algorithms are exploited communication structure of EVT attack [21] [22].

IV. INTRUSION IDETECTION SYSTEM (IDS) BASED TECHNIQUES

Mayank et al [23], proposed a technique an algorithm that Check whether evil twin AP is presence in network or not in this technique some key parameters in authentication frames and some association frame parameters are analyzed and designed an algorithm to differentiate the parameters generated by fake AP and legitimate AP.

Nirmal Selvarathinam [24] designed a Discrete Event System (DES) technique for IDS to identify ETAs in wireless network. The basic idea is to employ association-ID, retry-bit and sequence-number parameters of association response frame sending from access point to the user. The presence of ETAP in network can be detect by analyzing mentioned key parameters [23] [24]. This concept introduced using DES models for both LAP and ETAP. In this model a detector plays vital role which is a state estimator that monitors the network and warn if the network is under attack state.

Vishwa Modi & Asst. Prof. Chandresh Parekh et al [25] proposed a technique to detect Evil Twin Attack relying on different and same MAC address and different and same external IP addresses of APs. This approach detects and the ETA and give warning to user to disconnect from it. In this technique the external IP address and internal IP address can shows that the attacker is using different ISP or Same ISP [25] [6].

V. MACHIN LEARNING BASED DETECTION APPROACHES

A machine learning approach introduced by Constantinos Kolias [26], which used AWID public data set to categorize most popular attacks on 802.11. This approach is client side which analyze M-in-M attack with its impersonation characteristics to deploy machine learning technique to recognize whether the AP is normal or ET.

Machine learning algorithms applied on the values of RTT (Round Trip Time) features, these machine learning algorithms are Support Vector Machine K-nearest neighbors and Multilayer Perceptron to detect unauthorized fake AP and as the results shows that C-4.5 and K-NN algorithm are has high accuracy in TP (True Positive) and SVM has high accuracy in FP (False Positive) [27] [30].

Jeonghoon Seo, Chaeho Cho, and Yoojae Won et al [28] proposed a multiple-feature-based machine learning evil twin AP detection technique, the machine learning classification algorithms applied on duration (transmission time of a frame), clock skew and channel RSS features. And also by using machine learning a technique for extracting different features of wireless APs and detecting evil twin APs discussed. The interface cards (NICs) used to collects wireless signals and doesn't required any other additional devices. In this technique several machine learning classification algorithms like logistic regression, naïve Bayes, K-nearest neighbors (k-NN), support vector machine (SVM), and random forest applied on extracted features among all these classification algorithms the random forest algorithm perform highest accuracy.

Dr. Harsha and Dr. Khalid Nazim et al [29] introduced a simple light weight security system for Evil twin prevention, the android API used in prevention system for smart phones. In order of create dataset all known access points are added by default to the training set without consideration of their consequent value. The system algorithm is executed as a program in JAVA for taking decision It classify the access point to "safe" or "unsafe" before the device send data packets through the access point.

VI. COMPARISONS OF DIFFERENT EVIL TWIN ATTACK DETECTION TECHNIQUES

TABLE II. COMPARISONS OF DIFFERENT EVIL TWIN ATTACK DETECTION TECHNIQUES

Technique	***Network / client Side***	***Active / passive***	***Hardware /software modification***	***Accuracy***
Traffic Monitoring	N	p		99%
Duplicate RSSI	C	p		97%
Clock Skew	C	p		90%
Inter packet arrival time	both		both	NA
RTT measurement	both		both	NA
Time Synchronization Function (TSF)	C		H	NA
DNS Server, two hops	N	A		60%
ETSniffer		A		99%
Signal strength		P		97%
Context-leashing	C	A	S	NA

VII. CONCLUSION

In this paper, we have described Evil Twin Attack and reviewed many different papers with proposed techniques by many researchers in order to detect and mitigate the evil twin attack. Most of techniques execute in Network side or in Client side and some techniques require special hardware such as Sensor, IDS and etc. for most accurate classification of APs Machine Learning is used in order to identify the evil twin attack.

VIII. REFERENCES

[1]. Jose Emmanuel Cruz de la Cruz, Christian Augusto Romero Goyzueta, Cristian Delgado Cahuana, "Intrusion Detection and Prevention System for Production Supervision in Small Businesses Based on Raspberry Pi and Snort", Electronics Electrical Engineering and Computing (INTERCON) 2020 IEEE XXVII International Conference on, pp. 1-4, 2020.

[2] P. Shrivastava, M. S. Jamal and K. Kataoka, "EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi," in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 89-102, March 2020, doi: 10.1109/TNSM.2020.2972774.

[3]. O. Nakhila and C. Zou, "User-side Wi-Fi evil twin attack detection using random wireless channel monitoring," MILCOM 2016 - 2016 IEEE Military Communications Conference, Baltimore, MD, 2016, pp. 1243-1248, doi: 10.1109/MILCOM.2016.7795501.

[4]. Qian LU & Haipeng QU, "Client-Side Evil Twin Attacks Detection Using Statistical Characteristics of 802.11 Data Frames" - IEICE TRANS. INF. & SYST., VOL.E101–D, NO.10 OCTOBER 2018.

[5].Bandar Alotaibi and Khaled Elleithy, "Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions", - Article in Wireless Personal Communications · October 2016, DOI: 10.1007/s11277-016-3390-x.

[6]. F. Lanze, A. Panchenko, I. Ponce-Alcaide and T. Engel, "Hacker's toolbox: Detecting software-based 802.11 evil twin access points," 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2015, pp. 225-232, doi: 10.1109/CCNC.2015.7157981.

[7]. En-Chun KUO & Ming-Sang CHANG, "User-Side Evil Twin Attack Detection Using Time-Delay Statistics of TCP Connection Termination" - International Conference on Advanced Communications Technology(ICACT), ISBN 979-11-88428-01-4, ICACT2018 February 11 ~ 14, 2018.

[8]. J. H. Cox, R. Clark, and H. Owen, "Leveraging SDN and WebRTC for rogue access point security," IEEE Trans. Netw. Service Manag, vol. 14, 3, pp. 756–770, Sep. 2017.

[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, vol. 9, no. 3, pp. 449–462, 2010.

[10]. Qian Lu and Haipeng Qu, "A Passive Client-based Approach to Detect Evil Twin Attacks" - 2017 IEEE2 Trustcom/BigDataSE/ICESS.

[11] Anil Kumar , Bibhav Raj and Partha Paul, "DETECTION AND PREVENTION AGAINST EVIL TWIN ATTACK IN WLAN" - International Journal of Computer Engineering and Applications, Special Edition www.ijcea.com ISSN 2321-3469.

[12] Diogo Mónica, Carlos Ribeiro , "WiFiHop - Mitigating the Evil Twin Attack through Multi-hop Detection" - Conference Paper · September 2011 DOI: 10.1007/978-3-642-23822-2_2 · Source: DBLP.

[13]. Qian Lu & Haipeng Qu, "SLFAT: Client-Side Evil Twin Detection Approach Based on Arrival Time of Special Length Frames" - Hindawi Security and Communication Networks Volume 2019, Article ID 2718741, 10 pages https://doi.org/10.1155/2019/2718741.

[14]. Hao Han & Bo Sheng, IEEE Member, "A Timing-Based Scheme for Rogue AP Detection -- IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS", VOL. 22, NO. 11, NOVEMBER 2011.

[15]. Songrit Kitisriworapan, Aphirak Jansang and Anan Phonphoem, "Evil-Twin Detection on Client-side" – IEEE 16th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON 2019).

[16]. Abhijit Bodhe , "RAPD Algorithm: Detection of Rogue Access Point in Wireless Network" - International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 6, June 2013).

[17]. H. Mustafa and W. Xu, "CETAD: Detecting evil twin access point attacks in wireless hotspots," 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, 2014, pp. 238-246, doi: 10.1109/CNS.2014.6997491.

[18]. Harold Gonzales, "Practical Defenses for Evil Twin Attacks in 802.11" – 2010 IEEE conference and exhibition on Global Telecommunications.

[19]. Kevin Bauer, Harold Gonzales, and Damon McCoy, "Mitigating Evil Twin Attacks in 802.11" – IEEE International Conference on Performance, Computing and Communications (IPCCC), 2008.

[20]. A. Burns, L. Wu, X. Du and L. Zhu, "A Novel Traceroute-Based Detection Scheme for Wi-Fi Evil Twin Attacks," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8253957.

[21]. Y. Song, C. Yang, and G. Gu, "Who is peeping at your passwords at starbucks?—To catch an evil twin access point," in Proc. IEEE/IFIP Int. Conf. Depend. Syst. Netw. (DSN), 2010, pp. 323–332.

[22].Chao Yang, Yimin Song, and Guofei Gu, "Active User-Side Evil Twin Access Point Detection Using Statistical Techniques", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 5, OCTOBER 2012.

[23]. Mayank Agarwal, "An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks", - Article in International Journal of Wireless Information Networks · March 2018.

[24]. N. S. Selvarathinam, A. K. Dhar and S. Biswas, "Evil Twin Attack Detection using Discrete Event Systems in IEEE 802.11 Wi-Fi Networks," 2019 27th Mediterranean Conference on Control and Automation (MED), Akko, Israel, 2019, pp. 316-321, doi: 10.1109/MED.2019.8798568.

[25]. Vishwa Modi & Asst. Prof. Chandresh Parekh, "Detection of Rogue Access Point to Prevent Evil Twin Attack in Wireless Network", International Journal of Engineering Research & Technology (IJERT) http://www.ijert.org ISSN: 2278-0181 IJERTV6IS040102 Published by : www.ijert.org Vol. 6 Issue 04, April-2017.

[26]. C. Kolias, G. Kambourakis, A. Stavrou and S. Gritzalis, "Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 184-208, Firstquarter 2016, doi: 10.1109/COMST.2015.2402161.

[27]. Doyeon Kim, "Data Set Construction and Performance Comparison of Machine Learning Algorithm for Detection of Unauthorized AP", © Springer Nature Singapore Pte Ltd. 2018 J. J. Park et al. (eds.), Advances in Computer Science and Ubiquitous Computing, Lecture Notes in Electrical Engineering 474.

[28]. Jeonghoon Seo, Chaeho Cho, and Yoojae Won, "Enhancing the Reliability of Wi-Fi Network Using Evil Twin AP Detection Method Based on Machine Learning" – Journal of Information Processing Systems, Vol.16, No.3, pp.541~556, June 2020.

[29]. Dr. Harsha and Dr. Khalid Nazim, "Improving Wi-Fi Security against Evil Twin attack using light weight machine learning application" - COMPUSOFT, An international journal of advanced computer technology, 8(3), March-2019 (Volume-VIII, Issue-III).

[30]. Doyeon Kim & Dongil Shin, "Unauthorized Access Point Detection Using Machine Learning Algorithms for Information Protection", – 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering.