Indonesian Journal of Electrical Engineering and Computer Science
Vol. 23, No. 3, September 2021, pp. 1527~1537
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v23.i3.pp1527-1537

The rogue access point identification: a model and classification review

Diki Arisandi[1], Nazrul Muhaimin Ahmad[2], Subarmaniam Kannan[3]
[1]Faculty of Information Science & Technology (FIST) Multimedia University (MMU), Melaka, Malaysia
[1]Department of Informatics Engineering, Universitas Abdurrab, Pekanbaru, Indonesia
[2,3]Thundercloud Research Lab, Faculty of Information Science & Technology (FIST) Multimedia University (MMU), Melaka, Malaysia

Article Info

Article history:

Received Oct 24, 2020
Revised May 21, 2021
Accepted Jul 1, 2021

Keywords:

Hardware-based
Model and classification
Rogue access point
Software-based
Wi-Fi

ABSTRACT

Most people around the world make use of public Wi-Fi hotspots, as their daily routine companion in communication. The access points (APs) of public Wi-Fi are easily deployed by anyone and everywhere, to provide hassle-free Internet connectivity. The availability of Wi-Fi increases the danger of adversaries, taking advantages of sniffing the sensitive data. One of the most serious security issues encountered by Wi-Fi users, is the presence of rogue access points (RAP). Several studies have been published regarding how to identify the RAP. Using systematic literature review, this research aims to explore the various methods on how to distinguish the AP, as a rogue or legitimate, based on the hardware and software approach model. In conclusion, all the classifications were summarized, and produced an alternative solution using beacon frame manipulation technique. Therefore, further research is needed to identify the RAP.

Corresponding Author:

Diki Arisandi
Faculty of Information Science & Technology (FIST)
Multimedia University (MMU)
75450 Melaka, Malaysia
Email: 1181402373@student.mmu.edu.my, diki@univrab.ac.id

1. INTRODUCTION

The institute of Electrical and Electronics Engineers (IEEE) 802.11 standards are well known as wireless local area network (WLAN) or Wi-Fi, which enables low price deployment, and used to reach the areas where cables are unable to cover [1]. IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) protocols, which specifies the medium access control (MAC) and physical layer protocol in the implementation of WLAN, on Wi-Fi computer communication in various frequencies, such as 2.4 GHz, 5 GHz, and 60 GHz. Presently, Wi-Fi has become the most common choice for local area networking, as it offers low cost and quick wireless connectivity. The places where users simply connect easily and efficiently to exchange or sharing data [2], includes small office and home settings, business and ad-hoc environments [3]. Also, it is the world's most used wireless networking standards, for allowing devices to easily access the Internet [4].

Furthermore, WLAN highly raise productivity and flexibility by providing a high-speed internet access anytime and anywhere. The optical connection through fiber optic link is capable of delivering a bandwidth with a large capacity, through long-haul distance, which results into a low-noise signal [5]. The low cost of equipment and user-friendly installation steps, also allow everyone to deploy their own Wi-Fi [6]. The ability to access a network with various encryption and authentication method [7], as well as using

captive portal while in the public area, have become significant advantages [8]. However, WLAN or Wi-Fi has lots of security issues [9], due to the broadcasting habit of its wireless medium [10]. Cracker device found wireless networks, which are relatively easy to break, and also used to crack into wired networks [10]. Information is generally exchanged across authorized users on wireless networks, however, prior to the issues mentioned above, this process is susceptible to various malicious threats [11].

One of the most challenging security issues for network administrators, is the presence of rogue access points (RAP) [12]. This is a wireless access point (AP) that has either been deployed on a secure network, without clear authorization from a network administrator [13], initiate the denial-of-service (DoS) attack [14], or has been created to allow a cracker to establish a man-in-the-middle attack [15], and also, to intercept the communication between active devices on the network [16]. By using a unique identifier, the traditional RAP identification techniques are chosen. This procedure is used to monitor the activity of a device, allowing any suspicious operation to be verified, and suspended by the network administrator. This procedure, however, does not guarantee the true identity of a network-connected device. RAPs are classified into four categories, namely evil twin AP [16], improperly configured AP [17], unauthorized AP [18], and compromised AP [19].

Based on the description above, the RAP identification was summarized based on various strategies, approaches, and tools. Therefore, the main contributions of this article are:

- first, to deliver a brief study on the previous approaches, based on software and hardware model, according to the implementation, and also indicates which strategies or methods are much more effective,
- second, to propose a beacon frame-based manipulation development, as an alternative solution in identifying the presence of RAP.

2. RESEARCH METHOD

Systematic literature review was used to analyses the recent studies, findings, and comparing the results obtained. The systematic literature review aims to eliminate bias and incompleteness through a systematic mechanism [20]. Therefore, article selection is needed after obtaining some literature from reliable sources, sorting the papers based on criteria, followed by generalization and characterization phase. At this stage, the literatures were separated based on an approach to identify hardware or software RAPs. Classification and generalization approaches are also needed for deducing similarities between the literature that have been explored to provide interpretation and summary. To achieve the objective, the following research questions (Rs) were composed on Table 1. The references from various and reliable sources were explored, 45 journal articles and 30 conference papers which were relevant to RAP identification models and classifications were found. There was a period when the research based on RAP identification from 2008 to 2020 were published as illustrated in Figure 1.

Table 1. Research questions

Code	Research Question	Definition
R1	What are the tools for identifying RAP?	Aims at the tools in identifying RAP, whether using hardware or software as a basic tool
R2	What type of topology detect RAP?	Focuses on which side of the user's position, when probing RAP in the network
R3	How does the client expose the presence of RAP?	Describes how the client exposes the presence of RAP, whether passive or active probing.
R4	How to classify RAP detection?	How to classify RAP identification, based on the detection approach
R5	What are the features of RAP?	Describes the basic features used in identifying RAP

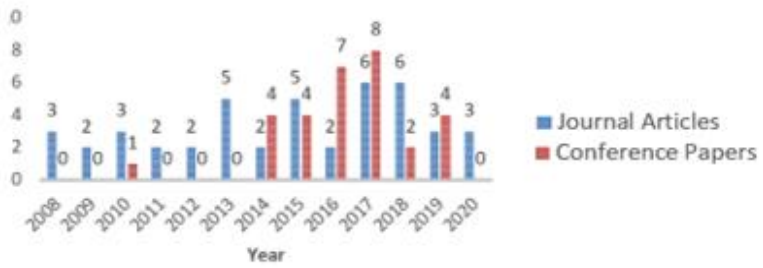

Figure 1. Number of publications based on RAP identification

The typical development of RAP surveillance using hardware or software in Figure 2, referring to the collected sources on how the RAP tricks network users, while the surveillance performs their monitoring on the available APs. A group of network users were connected to the AP, and one of the APs was rogue. RAP usually takes the advantage of several aspects compared to legitimate APs, such as closer distance to the client, stronger signal, and the ignorance of users. RAP leverage the same internet connection as a legitimate AP or being connected using a private connection such as 3G or 4G modem. Some RAPs also frequently de-auth the authorized link, to disconnect a client and legitimate AP, for the client to be associated with RAP. The difference between the development of a software and hardware-based model lies in the devices used. As the instrument to identify RAP, software-based methods tend to use tailored-software tools or using their own existing network devices, such as the internal wireless interface. However, Hardware-based uses dedicated sensors, special-purpose UAVs, and additional hardware to identify the presence of RAP.

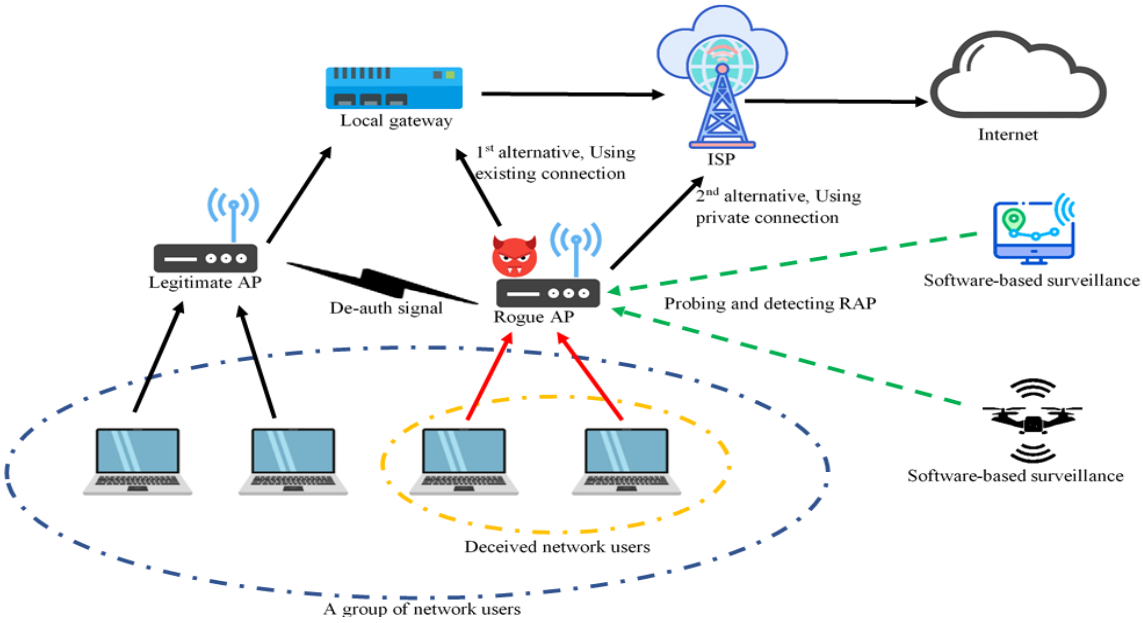

Figure 2. The software and hardware developments for RAP surveillance

3. DISCUSSION

In this section, RAP identification approaches are being discussed. And are mainly classified into two perspectives, software and hardware-based approach, with their individual advantages and limitations.

3.1. Software-based RAP identification

RAP identification using a software-based, is the most common used approach, some of the reasons are the cost efficiency and involving other fields of knowledge. This approach simply uses existing hardware and some additional software, such as open-source operating system, Wireshark, Aircrack-ng suite, Scapy, etc. Some of the literature, detected by software-based approach are more at the data-link level, with the physical layer features. However, the others also describe the upper-layer network detection.

3.1.1. AP profiling

A software-based was identified using AP profiling. This technique exploits the beacon frame obtained from the legitimate AP and becomes a profile or whitelist that is used to detect other APs. When the scanning result profile is different from the whitelist in the database, this indicated that the AP is Rogue. Corbett *et al*. [21] suggested a statistical approach via spectral analysis in identifying the presence of any wireless interface on the network. Panch and Singh [22] provided an authentication to the server based on hash digest, sent by client as RAP mitigation. Pang *et al.* [23]employed the collaboration technique among wireless users to determine the Legitimate AP called Wi-Fi-Reports, based on the fundamental aspect of network. Vanjale *et al.* [24] exploited the sniffing technique of the frames from the AP, then comparing with the existing data to determine the AP profile. Yang *et al.* [25] presented a spatial association in calculating inbound received signal strength indication (RSSI) number, from AP in identifying a RAP. Gopalakrishnan *et al.* [26] used a dedicated monitoring software tool to secure the airport from malicious wireless activities. Yang *et al.* [27] combined the RSSI and channel state information (CSI) as novel AP

localization technique to identify the RAP. Kim *et al.* [28] leveraged on the measurement and classification of the round-trip-time from the mobile RAP. Another study from Milliken *et al.* [29] was prone to verify the suspected AP by exploiting the management frame information. Agrawal *et al.* [6] reinforced the current intrusion detection system (IDS) with machine learning approach to identify the presence of RAP. While Reising *et al.* [30] utilized the radio-frequency certificate as a part of physical information, and analyzing the data using dimensional reduction analysis and machine learning approach to generate the RAP profile.

In 2016, Alotaibi and Elleithy [31] proposed to develop spoofing detector based on RSS Value and classifier method to identify the adversary on the network. Cox *et al.* [32] proposed RAP detection, based on software-defined network approach and exploiting WebRTC platform. Vanjale and Mane [33] invented a server-based RAP profiling, based on threshold estimate from clustering analysis. Wu *et al.* [34] proposed the calculating the forwarding behaviour of AP method using statistical methods to distinguish RAP. Nakhila *et al.* [35] created a multi-virtual gateway for the internet provider on the server side, to compare the device fingerprinting as RAP detection. Another study by Vanjale and Mane *et al.* [36] proposed to create whitelist AP database, setting the parameter for detection, then comparing the beacon new inbound AP. Mustafa and Wu [37] built the detection system, based on the AP profiling parameters to distinguish Legitimate and Rogue AP. While Ketkhaw and Thipchaksurat [38] also invented a RAP detection system, using the inbound sequence number. They [39] also built a system for discovering the hidden RAP from the current network by using the beacon frame anomaly. Another AP profiling research conducted by Li and Li [40], proposed a novel approach by capturing and processing the frame to acquire the fingerprint, then determining the AP status, based on Gaussian and Naive Bayes algorithm. A study from Alotaibi and Elleithy [41] explained how to capture, extract, and store the features from the beacon frames, as a fundamental detection characteristics of RAP profiling algorithm.

Some of the studies offered solution to avoid the adversary before they launch an attack. Baharudin *et al.* [42] proposed a personal IDS which is able to notify users, when RAP is attempting to impersonate. Selvarathinam *et al.* [43] enhanced the current IDS, with discrete event system (DES) as anti-failure of RAP detection, while Kumar and Paul [44] were prone to leveraging the previous AP information value, as the identifier in determining the RAP surrounding the area. Another preventing solution from Xu *et al.* [45] was by collecting and processing the RSSI data and distance measurement, to gain an optimal reference point of RAP. Chatfield and Haddad [46] proposed a novel RAP identification technique using phase error detection in CSI feature. Hua *et al.* [47] invented the carrier-frequency offset device, also a fingerprinting mechanism framework, for identifying RAP in the network. Vansickle tested the effectiveness of the three open-source software, for detecting the presence of RAP [48], while Ahmad *et al.* [49] conducted RAP detection by collecting RSSI value from the APs, and determining the RAP based on unsupervised machine learning algorithm.

3.1.2. Packet behaviour analysis

This method is almost closely the same with AP profiling, which relies on the beacon frame as the main information source. However, the fundamental difference is the packet behavior approach, which focused more on detecting anomaly on the beacon frame. Mano *et al.* [50] presented a novel packet slicer method, combined with local round trip time, for analysing the frames and any RAP on the network, while Jana and Kasera [51] calculated the clock skew on the time synchronization function from any AP beacon frame, including RAP, as a device fingerprinting. The RAP identification method was invented from Kao e*t al.* by comparing the sliding window size from the existing AP, with the whitelisted profile to match the criteria of RAP [52]. A study from Wei *et al*. [53] proposed a lightweight and online-wireless traffic identification of RAP, based on inter-ACK time flow. A research from Han *et al*. [54] focused on calculating the round trip time and hops between a user and a domain server to determine the RAP. Another study of packet behaviour analysis from Yang *et al*. [55] focused on developing new statistical and probability method from the combination of trained mean matching and hop differentiating technique for analysing inter-arrival time of any AP. An approach from Jadhav and Vanjale [56] recorded the timestamp field, and calculated the threshold value, then created a RAP detection algorithm using timestamp interval difference, based on Least Square fitting method. Hsu *et al*. [57] proposed a novel RAP method using reverse-traceroute called RAF to identify the RAP. Xu *et al*. [58] presented a new method for identifying RAP using a device fingerprinting from the beacon frame, emitted by the AP.

A recent study from Lu *et al.* [59] proposed a novel approach for detecting ETA, and identify the arrival time of the special frames with the same length, to determine the forwarding behaviour of RAP, while Hsu *et al*. [60] invented a novel reverse-traceroute algorithm for indicating the RAP. The novel framework using SYN reflection, TCP handshake, and NAT gateway behaviour were also proposed by Lu *et al.* [61]. Using the non-unique terms are still the normal method of some research, however, the goal remains the same. Lanze *et al*. [62] was passively estimating AP clock skew from the information contained in the

management frames as RAP feature. Lu *et al*. [63] utilized a data frame filtering and statistic technique to identify RAP on the network, while Nakhila and Zou [64] proposed a real-time client-side ETA detection, using single internet provider to determine the presence of RAP.

3.1.3. Agent deployment

Agent deployment is generally used by network administrator. This approach allows an administrator to deploy and spread slave agents to all the networks as an information collector. Wang *et al*. [65] deployed the agents, to mitigate the network user from the DDoS Attack by adversary AP, using DaMask, based on cloud and software-defined networking (SDN). Agrawal and Tapaswi [66] proposed a novel method by combining a Honeypot and IDS, for detecting the presence of RAP, based on the captured data frame. Another research of RAP using agents was proposed by Agarwal *et al*. [67], who were developing the served-based agent to sniff, filter, and analyses the beacon frame, as an evil twin/RAP detection approach. Jain *et al*. [68] presented a mitigation scheme by preventing a device assault of RAP, via the fingerprinting scanning by using IDS. A similar research was conducted by developing multi-agent-IDS as the guardian, to combat RAP on the existing network by Sriram *et al.* [69] and Kharat [70]. Some other studies of RAP using the agent, were conducted by Chatfield and Haddad [71], with cosine similarity and data sectoring of RSSI, for identifying the presence of RAP. Li *et al*. [72] proposed a framework to Protect the users from the sensitive keystrokes that reflected by CSI, while Sharma and Gupta [73] developing the three-layered IDS security system, to encounter the RAP and also protecting the user.

As a summary of the RAP identification based on software approach, a brief tabular view was shown in Table 2. Based on Table 2, the client-based approach is the mostly used for software-based RAP detection. Many previous studies assumed that clients associate directly with the AP and require to be more aware to encounter the RAP. Both AP profiling techniques and packet behaviour analysis rely on beacon frames, however, the trend for AP profiling is only based on previous AP profiles that have been stored in the database. Most of the AP profiling technique are using MAC and network and upper layer (NUL), as a RAP detection features. A more comprehensive process is actually obtained from the packet behaviour analysis technique, which emphasizes on analysing the anomalies of beacon frame for detecting the presence of RAP, not only exploiting the MAC and NUL, and also physical (PHY) feature, which requires further process than AP profiling. While agent deployment, which is an admin-side approach, has good prospects for the industrial application, as it allows automation in detecting RAP without a significant role from the client, as implemented by several network companies.

Table 2. Software-based approach summary

Tool (R1)	Topology (R2)	Probing (R3)	Classification (R4)	Features (R5)	References
Software-based	Admin-side	Active	Agent deployment	MAC, NUL	[65], [66], [67], [69], [70]
			AP Profiling	MAC, NUL	[26], [35]
			Packet behaviour	MAC, NUL, PHY	[52], [55]
		Passive	Agent deployment	PHY	[71]
			AP Profiling	MAC, PHY	[33], [34], [74]
			Packet behaviour	MAC	[50]
	Client-side	Active	Agent deployment	MAC, PHY, NUL	[72], [73]
			AP Profiling	MAC, NUL	[23], [28], [37], [44]
			Packet behaviour	MAC, NUL	[54], [60], [61], [64]
		Passive	Agent deployment	MAC	[68]
			AP Profiling	MAC, PHY	[6], [21], [24], [25], [27], [29], [30], [75], [36], [38], [39], [40], [41], [42], [43], [45], [46], [47], [48], [49], [31]
			Packet behaviour	MAC, NUL, PHY	[51], [53], [56], [57], [58], [59], [62], [63]
	Both sides (admin and client)	Active	AP Profiling	MAC, NUL	[22], [32]
		Passive	-	-	-

3.2. Hardware-based RAP identification

The hardware-based method in the RAP detection method is not very commonly used. This approach requires more hardware as additional equipment, such as censors or dedicated network hardware. An extra budget has to be spent on research to buy the particular equipment, and also requires additional mastery to run the hardware. However, the finding claimed to only detect the presence of rogue AP by their physical features, not only the data-link level or network upper layer.

3.2.1. AP profiling

Normally, this process is the same as software-based AP profiling. This process exploits the beacon frame from the legitimate AP and becomes a profile or whitelist for detecting other APs. Schweitzer *et al.*

developed a hardware-based tool to visualize and locate the presence of RAP or legitimate AP, surrounding the area using specific sensors. Shah *et al.* [76] exploited a RF Signal processed by directional beacon-based algorithm, to spot the wireless object. Du *et al*. [77] drawn the eavesdropper Wi-Fi, by exploiting the RSS movement as the information basis for the RAP identifier. Wang *et al*. [78] proposed the RAP detection by utilizing CSI, based on the device antenna. Zegzhda *et al*. [79] utilized a dedicated and automated RAP detector machine to protect user on the network, while Awad *et al*. [80] developed an autonomous robot, equipped with sensors and localization algorithm, to detect the RSS value from the fraud AP. Zuo *et al*. [81] developed an AP fingerprinting detection, using bright beacon device and kriging interpolation as RSSI measurement approach, while Jang *et al*. [82] built a hardware-based practical RAP using intentional channel interference engine. Pradeepkumar *et al*. [83] proposed a predicting rogue AP algorithm, by using RF signal strength and distance threshold. A study from Qu *et al*. [84] proposed a RAP detection, based on ranging device and global positioning system (GPS) location.

3.2.2. Agent deployment

This approach allows the administrator to deploy and send the hardware-based sniffer to all the network, to detect rogue AP. Shrivastava *et al*. [85] proposed a SDN-based RAP identification and mitigation system. Wang *et al*. [86] invented a solution by deploying a special unmanned-aerial vehicle (UAV) to extract the packet characteristics, and analyse the features with IDS. Hooper [87] presented a novel method in securing RAP, using UAV by intercepting their advertising signal. However, the research by Jang [88] evolved a dedicated and practical hardware-based-Hunter, as the agent to search RAP on the network. In 2017, Zhou [89] employed the crowd sensing detection, from the surrounding devices to identify RAP. While in the same year, Awad *et al*. [90] utilized the WiMAP algorithm as a basis in autonomous robot, for identifying the presence of RAP.

3.2.3. Packet behaviour analysis

This method relies on the beacon frame as the main information source, by observing the detecting anomaly on the beacon frame, such as packet forwarding behaviour, timestamp interval, or clock skew intervals. Kao *et al*. [91] proposed the algorithm, based on deviation of the beacon time interval using dedicated sensors. As a summary of the RAP identification based on hardware approach, a brief tabular view was shown in Table 3. Based on Table 3, a few research on RAP identification employs a hardware based. This is an unusual technique, because hardware-based requires additional costs and equipment, such as dedicated sensors and drones. Besides the common issues of the additional materials, most of the previous studies leverage on the PHY, which is from the lowest level of a beacon frame to uncover the presence of RAP, since the information obtained is hard to be falsified. The tool selection, whether by hardware or software approach, is considered a subjective option for identifying the presence of RAP on the network. However, the advantages' comparison and the deficiencies were shown in Table 4.

Table 3. Hardware-based approach summary

Tool (R1)	Topology (R2)	Probing (R3)	Type of Classes (R4)	Features (R5)	References
Hardware-based	Admin-side	Active	Agent deployment	PHY, MAC	[82], [87]
			AP Profiling	PHY	[92]
		Passive	-	-	-
	Client-side	Active	Agent deployment	PHY	[89]
			AP Profiling	NUL, PHY	[79], [84]
		Passive	Agent deployment	MAC, PHY	[85], [86], [88], [90]
			AP Profiling	PHY, MAC	[76], [77], [78], [80], [81], [83]
			Packet behaviour	MAC	[91]
	Both sides (Admin and client)	Active	-	-	-
		Passive	-	-	-

Table 4. The advantages and deficiencies of hardware and software-based approach

Approach	Advantages	Deficiencies
Software-based	- The most-commonly used approach - Detecting the RAP by only using the existing devices - Easy to develop with various software or method	- The use of existing devices did not show significant results in several studies - Sometimes cause overburden on the performance of an existing device, and increasing the false rate detection
Hardware-based	- More open to various tools (hardware or software) collaboration - Better detection result, since it uses dedicated equipment	- Require more expertise, since it uses various tools - spending extra cost and time to develop the RAP detector

4. CRITICAL ANALYSIS OF RAP IDENTIFICATION APPROACHES

Both approaches used for identifying RAP, AP profiling, and packet behaviour are regular classification model, due to their nature to exploit the beacon frame, as a mechanism for covering the presence of users when avoiding the RAP before attempting to impersonate. The beacon frame manipulation is a rare solution in identifying RAP. One of the reasons was that, due to a risk when performing the beacon frame modification. Particularly by embedding the unstandardized materials to identify the RAP, while the results were successful [93]. Because once the change is failed, the beacon frame is no longer useful. A fresh sample is required to modify a beacon frame, and injecting a piece of additional information, as well as sending the beacon into the air to detect the presence of RAP [94]. Previous study conducted by Nyathi and Ndlovu [95], proposed RAP detection, by manipulating the timestamp field in updating the local clock for synchronization. Gupta and Rohil. [96] also investigated a RAP detection by manipulating the frame, and embedding the permutation key using 4 unused bits of the timestamp field.

However, the manipulation method, whether software or hardware-based, is predicted to be a challenge in the future. The other solution, such as using an agent deployment, appears to be another potential response in the future. The trend of the agent deployment literature appears to be a more relevant topic in the recent year, while many network vendors develop an autonomous agent in the form of software or hardware to secure the network.

5. CONCLUSION

The detection of RAP from the client and administrator aspects has been increasingly published. However, this review discusses the use of hardware and software model in identifying the RAP. Both approaches have advantages and disadvantages. Some of the classifications are recommended for further research, in order to identify RAP, such as beacon frame modification or agent deployment. This is carried out using existing hardware or to develop the dedicated tools, and also based on different features.

ACKNOWLEDGEMENTS

The authors acknowledge the support granted by the Faculty of Information Science and Technology (FIST), Multimedia University, especially all the CICC/Thundercloud lab members.

REFERENCES

[1] B. Bellalta, L. Bononi, R. Bruno, and A. Kassler, "Next generation IEEE 802.11 Wireless Local Area Networks: Current status, future directions and open challenges," *Computer Communications*, vol. 75, pp. 1-25, 2016, doi: 10.1016/j.comcom.2015.10.007.

[2] I. Ahmed, "A brief review: Security issues in cloud computing and their solutions," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 17, no. 6, pp. 2812-2817, 2019, doi: 10.12928/TELKOMNIKA.v17i6.12490.

[3] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184-208, 2016, doi: 10.1109/COMST.2015.2402161.

[4] Q.-D. Ho, D. Tweed, and T. Le-Ngoc, "Ieee 802.11/wi-fi medium access control: An overview," in *Long Term Evolution in Unlicensed Bands*, Springer, 2017, pp. 31-41.

[5] A. Willner, *Optical fiber telecommunications*, vol. 11, Cambridge, USA: Academic Press, 2019.

[6] M. Agarwal, D. Pasumarthi, S. Biswas, and S. Nandi, "Machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization," *International Journal of Machine Learning and Cybernetics*, vol. 7, no. 6, pp. 1035-1051, 2014.

[7] J. Noh, J. Kim, and S. Cho, "Secure Authentication and Four-Way Handshake Scheme for Protected Individual Communication in Public Wi-Fi Networks," *IEEE Access*, vol. 6, pp. 16539-16548, 2018, doi: 10.1109/ACCESS.2018.2809614.

[8] A. Dabrowski, G. Merzdovnik, N. Kommenda, and E. Weippl, "Browser History Stealing with Captive Wi-Fi Portals," *IEEE Security and Privacy Workshops (SPW)*, 2016, pp. 234-240, doi: 10.1109/SPW.2016.42.

[9] A. Holt and C.-Y. Huang, *802.11 wireless networks: security and analysis*, USA: Springer Science & Business Media, 2010.

[10] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727-1765, Sept. 2016, doi: 10.1109/JPROC.2016.2558521.

[11] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027-2051, thirdquarter 2016, doi: 10.1109/COMST.2016.2548426.

[12] M. M. Noor and W. H. Hassan, "Wireless Networks : Developments , Threats and Countermeasures," International *Journal of Digital Information and Wireless Communications*, vol. 3, no. 1, pp. 119-134, 2013.

[13] A. Bartoli, E. Medvet, and F. Onesti, "Evil twins and WPA2 Enterprise: A coming security disaster?," *Computers & Security*, vol. 74, pp. 1-11, 2018, doi: 10.1016/j.cose.2017.12.011.
[14] T. A. Assegie and P. S. Nair, "A review on software defined network security risks and challenges," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 17, no. 6, pp. 3168-3174, 2019, doi: 10.12928/telkomnika.v17i6.13119.
[15] A. Javier, P. Bernal, O. José, S. Parra, R. Albeiro, and P. Díaz, "Man in the Middle Attack : Prevention in Wireless LAN," *International Journal of Applied Engineering Research*, vol. 13, no. 7, pp. 4672-4674, 2018.
[16] K. Brenski, M. Choluj, and M. Luckner, "Evil-AP - Mobile Man-in-the-Middle Threat," *IFIP International Conference on Computer Information Systems and Industrial Management*, pp. 617-627, 2017.
[17] O. Delgado, L. Kechtban, S. Lugan, and B. Macq, "Passive and active wireless device secure identification," *IEEE Access*, vol. 8, pp. 83312-83320, 2020, doi: 10.1109/ACCESS.2020.2991649.
[18] R. Gonçalves, M. E. Correia, and P. Brandão, "A flexible framework for rogue access point detection," *ICETE 2018 - Proc. 15th Int. Jt. Conf. E-bus. Telecommun.*, vol. 2, pp. 466-471, 2018, doi: 10.5220/0006832904660471.
[19] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, "The Human Factor of Information Security: Unintentional Damage Perspective," *Procedia - Social and Behavioral Sciences*, vol. 147, pp. 424-428, 2014, doi: 10.1016/j.sbspro.2014.07.133.
[20] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *Journal of Business Research*, vol. 104, pp. 333-339, 2019, doi: 10.1016/j.jbusres.2019.07.039.
[21] C. L. Corbett, R. A. Beyah, and J. A. Copeland, "Passive classification of wireless NICs during active scanning," *International Journal of Information Security*, vol. 7, no. 5, pp. 335-348, 2008.
[22] A. Panch and S. K. Singh, "A Novel approach for Evil Twin or Rogue AP mitigation in wireless environment," *International Journal of Security and Its Applications*, vol. 4, no. 4, pp. 33-38, 2010.
[23] J. Pang, B. Greenstein, M. Kaminsky, D. McCoy, and S. Seshan, "Wifi-reports: Improving wireless network selection with collaboration," *IEEE Transactions on Mobile Computing*, vol. 9, no. 12, pp. 1713-1731, Dec. 2010, doi: 10.1109/TMC.2010.151.
[24] S. B. Vanjale, A. K. Kadam, and P. A. Jadhav, "DETECTING AND ELIMINATING ROGUE ACCESS POINT IN IEEE 802.11 WLAN," *Journal of Engineering Research and Studies*, vol. II, no. III, pp. 105-108, 2011.
[25] J. Yang, Y. J. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 44-58, Jan. 2013, doi: 10.1109/TPDS.2012.104.
[26] K. Gopalakrishnan, M. Govindarasu, D. W. Jacobson, and B. M. Phares, "Cyber Security for Airports," *International Journal for Traffic and Transport Engineering*, vol. 3, no. 4, pp. 365-376, 2013, doi: 10.7708/ijtte.2013.3(4).02.
[27] Z. Yang, Z. Zhou, and Y. Liu, "From RSSI to CSI: Indoor Localization via Channel Response," *ACM Computing Surveys*, vol. 46, no. 2, pp. 1-32, 2013, doi: 10.1145/2543581.2543592.
[28] I. Kim, J. Seo, T. Shon, and J. Moon, "A novel approach to detection of mobile rogue access points," *Secur. Commun. Networks*, vol. 7, no. 10, pp. 1510-1516, 2013.
[29] J. Milliken, V. Selis, and A. Marshall, "Detection and analysis of the Chameleon WiFi access point virus," *EURASIP Journal on Information Security*, vol. 2013, pp. 1-14, 2013, doi: 10.1186/1687-417X-2013-2.
[30] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1180-1192, June 2015, doi: 10.1109/TIFS.2015.2400426.
[31] B. Alotaibi and K. Elleithy, "A new MAC address spoofing detection technique based on random forests," *Sensors (Switzerland)*, vol. 16, no. 3, 2016, doi: 10.3390/s16030281.
[32] J. H. Cox, R. Clark, and H. Owen, "Leveraging SDN and WebRTC for Rogue Access Point Security," *IEEE Transactions on Network and Service Management*, vol. 14, no. 3, pp. 756-770, Sept. 2017, doi: 10.1109/TNSM.2017.2710623.
[33] S. B. Vanjale and P. B. Mane, "Multi Parameter Based Robust and Efficient Rogue AP," *Wirel. Pers. Commun.*, 2017.
[34] W. Wu, X. Gu, K. Dong, X. Shi, and M. Yang, "PRAPD : A novel received signal strength – based approach for practical rogue access point detection," *International Jpurnal of Distributed Sensor Network*, vol. 14, no. 8, 2018, doi: 10.1177/1550147718795838.
[35] O. Nakhila, M. F. Amjad, E. Dondyk, and C. Zou, "Gateway independent user-side wi-fi Evil Twin Attack detection using virtual wireless clients," *Computers & Security*, vol. 74, pp. 41–54, 2018, doi: 10.1016/j.cose.2017.12.009.
[36] S. Vanjale and P. B. Mane, "A novel approach for elimination of rogue access point in wireless network," in *11th IEEE India Conference: Emerging Trends and Innovation in Technology, INDICON 2014*, 2015, pp. 1-4, doi: 10.1109/INDICON.2014.7030418.
[37] H. Mustafa and W. Xu, "CETAD: Detecting evil twin access point attacks in wireless hotspots," *2014 IEEE Conf. Commun. Netw. Secur. CNS 2014*, pp. 238-246, 2014, doi: 10.1109/CNS.2014.6997491.
[38] A. Ketkhaw and S. Thipchaksurat, "Rogue Access Point Detection Mechanism Considering Sequence Number Of Beacon Frame For Wireless Local Area Networks," in *14th International Conference on Electrical Engineering / Electronics, Computer, Telecomunications and Information Technology (ECTI-CON)*, 2017, pp. 509-512, doi: 10.1109/ECTICon.2017.8096286.
[39] A. Ketkhaw and S. Thipchaksurat, "Hidden Rogue Access Point Detection Technique for Wireless Local Area Networks," in *21st International Computer Science and Engineering Conference (ICSEC)*, 2017, vol. 6, pp. 1-5, doi: 10.1109/ICSEC.2017.8443803.

[40] X. Li and X. Li, "Rogue Access Points Detection Based on Theory of Semi-Supervised Learning," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS 2016)*, 2016, pp. 155-167.
[41] B. Alotaibi and K. Elleithy, "A passive fingerprint technique to detect fake access points," in *Wireless telecommunications symposium (WTS), IEEE*, 2015, pp. 1-8.
[42] N. Baharudin, F. H. M. Ali, M. Y. Darus, and N. Awang, "Wireless intruder detection system (WIDS) in detecting de-authentication and disassociation attacks in IEEE 802.11," *5th International Conference on IT Convergence and Security (ICITCS)*, 2015, pp. 1-5, doi: 10.1109/ICITCS.2015.7293037.
[43] N. S. Selvarathinam, A. K. Dhar, and S. Biswas, "Evil twin attack detection using discrete event systems in IEEE 802.11 Wi-Fi networks," in *27th Mediterranean Conference on Control and Automation, MED 2019 - Proceedings*, 2019, pp. 316-321, doi: 10.1109/MED.2019.8798568.
[44] A. Kumar and P. Paul, "Security analysis and implementation of a simple method for prevention and detection against Evil Twin attack in IEEE 802.11 wireless LAN," in *2016 International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016 - Proceedings*, 2016, pp. 176-181, doi: 10.1109/ICCTICT.2016.7514574.
[45] B. Xu, M. Peng, Q. F. Zhou, and X. Cheng, "Fake access point localization based on optimal reference points," in *2018 IEEE 4th International Conference on Computer and Communications, ICCC 2018*, 2018, pp. 784-788, doi: 10.1109/CompComm.2018.8780768.
[46] P. Liu, P. Yang, W. Z. Song, Y. Yan, and X. Y. Li, "Real-time Identification of Rogue WiFi Connections Using Environment-Independent Physical Features," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pp. 190-198, 2019, doi: 10.1109/INFOCOM.2019.8737455.
[47] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, "Accurate and Efficient Wireless Device Fingerprinting Using Channel State Information," in *Proceedings - IEEE INFOCOM*, 2018, pp. 1700-1708, doi: 10.1109/INFOCOM.2018.8485917.
[48] R. Vansickle, T. Abegaz, and B. Payne, "Effectiveness of Tools in Identifying Rogue Access Points on a Wireless Network," in *2019 KSU Conference on Cybersecurity Education, Research and Practice*, 2019.
[49] N. M. Ahmad, A. H. M. Amin, S. Kannan, M. F. Abdollah, and R. Yusof, "A RSSI-based rogue access point detection framework for Wi-Fi hotspots," in *ISTT 2014 - 2014 IEEE 2nd International Symposium on Telecommunication Technologies*, 2015, pp. 104-109, doi: 10.1109/ISTT.2014.7238186.
[50] C. D. Mano *et al.*, "RIPPS: Rogue Identifying Packet Payload Slicer detecting unauthorized wireless hosts through network traffic conditioning," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 2, pp. 1-23, 2008, doi: 10.1145/1330332.1330334.
[51] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Trans. Mob. Comput.*, vol. 9, no. 3, pp. 449-462, 2008, doi: 10.1109/TMC.2009.145.
[52] K. F. Kao, I. E. Liao, and Y. C. Li, "Detecting rogue access points using client-side bottleneck bandwidth analysis," *Computers & Security*, vol. 28, no. 3-4, pp. 144-152, 2009, doi: 10.1016/j.cose.2008.11.005.
[53] W. Wei *et al.*, "Passive online detection of 802.11 traffic using sequential hypothesis testing with TCP ACK-pairs," *IEEE Trans. Mob. Comput.*, vol. 8, no. 3, pp. 398–412, 2009, doi: 10.1109/TMC.2008.126.
[54] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," *IEEE Trans. parallel Distrib. Syst.*, vol. 22, no. 11, pp. 1912-1925, 2011, doi: 10.1109/TPDS.2011.125.
[55] C. Yang, Y. Song, and G. Gu, "Active user-side evil twin access point detection using statistical techniques," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 5, pp. 1638-1651, 2012, doi: 10.1109/TIFS.2012.2207383.
[56] S. Jadhav and S. Vanjale, "Wireless Rogue Access Point Detection Using Clock Skew Method," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 2, no. 3, pp. 1344-1349, 2013.
[57] F. H. Hsu, C. S. Wang, Y. L. Hsu, Y. P. Cheng, and Y. H. Hsneh, "A client-side detection mechanism for evil twins," *Comput. Electr. Eng.*, vol. 59, pp. 76-85, 2015, doi: 10.1016/j.compeleceng.2015.10.010.
[58] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 94-104, 2015, doi: 10.1109/COMST.2015.2476338.
[59] Q. Lu, H. Qu, Y. Ouyang, and J. Zhang, "SLFAT: Client-Side Evil Twin Detection Approach Based on Arrival Time of Special Length Frames," *Secur. Commun. Networks*, vol. 2019, doi: 10.1155/2019/2718741.
[60] F. H. Hsu, Y. L. Hsu, and C. S. Wang, "A solution to detect the existence of a malicious rogue AP," *Comput. Commun.*, vol. 142–143, pp. 62-68, 2019, doi: 10.1016/j.comcom.2019.03.013.
[61] Q. Lu, R. Jiang, Y. Ouyang, H. Qu, and J. Zhang, "BiRe: A client-side Bi-directional SYN reflection mechanism against multi-model evil twin attacks," *Comput. Secur.*, vol. 88, p. 101618, 2020, doi: 10.1016/j.cose.2019.101618.
[62] F. Lanze, A. Panchenko, B. Braatz, and T. Engel, "Letting the Puss in Boots Sweat: Detecting Fake Access Points using Dependency of Clock Skews on Temperature," in *ASIA CCS '14: Proceedings of the 9th ACM symposium on Information, computer and communications security*, 2014, pp. 3-14, doi: 10.1145/2590296.2590333.
[63] Q. Lu, H. Qu, Y. Zhuang, X. J. Lin, Y. Zhu, and Y. Liu, "A passive client-based approach to detect evil twin attacks," in *Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems*, 2017, pp. 233-239, doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.242.
[64] O. Nakhila and C. Zou, "User-side Wi-Fi evil twin attack detection using random wireless channel monitoring," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, pp. 1243-1248, 2016, doi: 10.1109/CCNC.2015.7157983.
[65] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking," *Comput. Networks*, vol. 81, pp. 308-319, 2015, doi: 10.1016/j.comnet.2015.02.026.

[66] N. Agrawal and S. Tapaswi, "The Performance Analysis of Honeypot Based Intrusion Detection System for Wireless Network," *Int. J. Wirel. Inf. Networks*, vol. 24, no. 1, pp. 14-26, 2017.
[67] M. Agarwal, S. Biswas, and S. Nandi, "An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802 . 11 Wi - Fi Networks," *Int. J. Wirel. Inf. Networks*, no. 0123456789, 2018.
[68] V. Jain, V. Laxmi, M. S. Gaur, and M. Mosbah, "ETGuard: Detecting D2D attacks using wireless Evil Twins," *Comput. Secur.*, vol. 83, pp. 389-405, 2019, doi: 10.1016/j.cose.2019.02.014.
[69] V. S. S. Sriram, G. Sahoo, and K. K. Agrawal, "Detecting and eliminating rogue access points in IEEE-802.11 WLAN - A multi-agent sourcing methodology," in *2010 IEEE 2nd International Advance Computing Conference, IACC 2010*, 2010, pp. 256-260, doi: 10.1109/IADCC.2010.5422999.
[70] P. M. Kharat and N. D. Kale, "Fake Access Point and Invalid Client Detection and Elimination using Agent Multi Sourcing," in *IJCA Proceedings on National Conference on Advancements in Computer & Information Technology*, 2016, pp. 2-6.
[71] B. Chatfield and R. J. Haddad, "RSSI-based spoofing detection in smart grid IEEE 802.11 home area networks," *2017 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2017*, 2017, doi: 10.1109/ISGT.2017.8086064.
[72] M. Li, *et al.*, "When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals," in *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 1068-1079, 2016, doi: 10.1145/2976749.2978397.
[73] K. Sharma and B. B. Gupta, "Multi-layer Defense Against Malware Attacks on Smartphone Wi-Fi Access Channel," *Phys. Procedia*, vol. 78, pp. 19-25, 2016, doi: 10.1016/j.procs.2016.02.005.
[74] N. Agrawal and S. Tapaswi, "Wireless Rogue Access Point Detection Using Shadow Honeynet," *Wirel. Pers. Commun.*, vol. 83, no. 1, pp. 551-570, 2015.
[75] Q. Lu, H. Qu, Y. Zhuang, X. J. Lin, and Y. Ouyang, "Client-side evil twin attacks detection using statistical characteristics of 802.11 data frames," *IEICE Trans. Inf. Syst.*, vol. E101D, no. 10, pp. 2465-2473, 2018, doi: 10.1587/transinf.2018EDP7030.
[76] S. F. A. Shah, S. Srirangarajan, and A. Tewfik, "Implementation of a directional beacon-based position location algorithm in a signal processing framework," *IEEE Trans. Wirel. Commun.*, vol. 9, no. 3, pp. 1044-1053, 2010, doi: doi: 10.1109/TWC.2010.03.081204.
[77] S. Du, J. Hua, Y. Gao, and S. Zhong, "EV-Linker: Mapping eavesdropped Wi-Fi packets to individuals via electronic and visual signal matching," *J. Comput. Syst. Sci.*, vol. 82, no. 1, pp. 156-172, 2016, doi: 10.1016/j.jcss.2015.06.005.
[78] C. Wang, X. Zheng, Y. J. Chen, and J. Yang, "Locating Rogue Access Point Using Fine-Grained Channel Information," *IEEE Trans. Mob. Comput.*, vol. 16, no. 9, pp. 2560-2573, 2017, doi: 10.1109/TMC.2016.2629473.
[79] D. P. Zegzhda, D. A. Moskvin, and A. D. Dakhnovich, "Protection of Wi-Fi network users against rogue access points," *Autom. Control Comput. Sci.*, vol. 51, no. 8, pp. 978-984, 2017.
[80] F. Awad, M. Naserllah, A. Omar, A. Abu-Hantash, and A. Al-Taj, "Collaborative indoor access point localization using autonomous mobile robot swarm," *Sensors (Switzerland)*, vol. 18, no. 2, 2018, doi: 10.3390/s18020407.
[81] J. Zuo, S. Liu, H. Xia, and Y. Qiao, "Multi-phase fingerprint map based on interpolation for indoor localization using iBeacons," *IEEE Sensors Journal*, vol. 18, no. 8, pp. 3351-3359, 2018, doi: 10.1109/JSEN.2018.2789431.
[82] R. Jang, J. Kang, A. Mohaisen, and D. Nyang, "Catch me if you can: Rogue access point detection using intentional channel interference," *IEEE Transactions on Mobile Computing*, vol. 19, no. 5, pp. 1056-1071, 2020, doi: 10.1109/TMC.2019.2903052.
[83] B. Pradeepkumar, K. Talukdar, B. Choudhury, and P. K. Singh, "Predicting external rogue access point in IEEE 802.11 b/g WLAN using RF signal strength," in *2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017*, 2017, vol. 2017, pp. 1981-1986, doi: 10.1109/ICACCI.2017.8126135.
[84] H. Qu, L. Guo, W. Zhang, J. Li, M. Ren, "Rogue access point detection in vehicular environments," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9204, pp. 446-456, 2015.
[85] P. Shrivastava, M. S. Jamal, and K. Kataoka, "EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 89-102, 2020, doi: 10.1109/TNSM.2020.2972774.
[86] J. Wang, N. Juarez, E. Kohm, Y. Liu, J. Yuan, and H. Song, "Integration of SDR and UAS for Malicious Wi-Fi Hotspots Detection," in *Integr. Commun. Navig. Surveill. Conf. ICNS*, pp. 1-8, 2019, doi: 10.1109/ICNSURV.2019.8735296.
[87] M. Hooper *et al.*, "Securing commercial WiFi-based UAVs from common security attacks," in *Proceedings - IEEE Military Communications Conference MILCOM*, 2016, pp. 1213-1218, doi: 10.1109/MILCOM.2016.7795496.
[88] R. Jang, J. Kang, A. Mohaisen, and D. Nyang, "Rogue Access Point Detector Using Characteristics of Channel Overlapping in 802.11n," *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp. 2515-2520, 2017, doi: 10.1109/ICDCS.2017.153.
[89] T. Zhou, Z. Cai, B. Xiao, Y. Chen, and M. Xu, "Detecting Rogue AP with the Crowd Wisdom," in *Proceedings - International Conference on Distributed Computing Systems*, 2017, pp. 2327-2332, doi: 10.1109/ICDCS.2017.31.
[90] F. Awad, A. Omar, M. Naserllah, A. Abu-Hantash, and A. Al-Taj, "Access point localization using autonomous mobile robot," in *2017 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies, AEECT 2017*, 2017, pp. 1-5, doi: 10.1109/AEECT.2017.8257754.
[91] K. F. Kao, W. C. Chen, J. C. Chang, and H. Te Chu, "An accurate fake access point detection method based on deviation of beacon time interval," in *Proceedings - 8th International Conference on Software Security and Reliability - Companion, SERE-C 2014*, 2014, pp. 1-2, doi: 10.1109/SERE-C.2014.13.
[92] D. Schweitzer, W. Brown, and J. Boleng, "Using visualization to locate rogue access points," *J. Comput. Sci. Coll.*, vol. 23, no. 1, pp. 134-140, 2007.

[93] M. Vanhoef, P. Adhikari, and C. Pöpper, "Protecting wi-fi beacons from outsider forgeries," *WiSec 2020 - Proc. 13th ACM Conf. Secur. Priv. Wirel. Mob. Networks*, pp. 155-160, 2020, doi: 10.1145/3395351.3399442.
[94] T. Nyathi and S. Ndlovu, "Beacon Frame Manipulation to Mitigate Rogue Access Points : Case of Smartphone Rogue Access Points Beacon Frame Manipulation to Mitigate Rogue Access Points : Case of Smartphone Rogue Access Points," *COMPUSOFT, An Int. J. Adv. Comput. Technol*, vol. 3, no. 2, pp. 576-581, 2014.
[95] P. K. Somase, A. R. Shelke, A. S. Bhise, R. R. Balpande, and S. D. Bhusari, "Introduction to IEEE 802 . 11 Rogue Access Point Detection Mechanism Using Covert Channel," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 5, no. V, pp. 1980-1985, 2017.
[96] V. Gupta and M. K. Rohil, "Bit-Stuffing in 802.11 Beacon Frame: Embedding Non- Standard Custom Information," *Int. J. Comput. Appl.*, vol. 63, no. 2, pp. 6-12, 2013.

BIOGRAPHIES OF AUTHORS

Diki Arisandi is a Ph.D. student at Multimedia University, Melaka Campus, Malaysia. He is also a lecturer in the Department of Informatics Engineering, Universitas Abdurrab. His research interests include networking and security, big data analytics, and IT in education.

Nazrul Muhaimin bin Ahmad is a lecturer in the Faculty of Information Science and Technology (FIST) at the Multimedia University (MMU), Malaysia. His research interests include wireless communication and security, cloud computing, Internet of things (IoT), and blockchain.

Subarmaniam A/L Kannan is a lecturer in Faculty of Information Science and Technology, Multimedia University (MMU), Malaysia. His research area includes semantic web technology and knowledge management, automatic speech recognition for Bahasa Malaysia, information system audit, and wireless communication.