Taxonomy and Future Threat of Rogue Access Point for Wireless Network

Kashyap C. Patel
Department of Computer Science
Ganpat University
Gujarat, India
kcp03@ganpatuniversity.ac.in

Ajaykumar Patel
A. M. Patel Institute of Computer Studies
Ganpat University
Gujarat, India
ajaykumar.patel@ganpatuniversity.ac.in

***Abstract*— Wireless network communication is an enormous and vast area of research. Many companies and organizations, related to wireless security have struggled due to the narrow, limited, and restricted access to the legitimate network. In a simplistic sense and most common manner, radio frequency (RF) is used for data communication on a network without wires. By its nature and methodology, wireless communication uses an air interface, and hence, it is vulnerable to attackers or hackers who can leverage these things and will compromise the legitimate network, devices, servers, applications, databases, and connected users. Wireless network attacks can be categorised into various types named Distributed Denial of Service (DDoS), Evil-twin, Man-in-the-Middle (MITM), Wireless Fidelity (Wi-Fi) Deauthentication, and Internet of Things (IoT)-based attacks. These types of attacks can compromise and infect the operational technology of large-scale public and private sector organizations' Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA). A wireless rogue access point has already done harmful things to businesses of all sizes, not just coffee shops, airport terminals, tube stations, or public gardens. This paper classifies rogue access points (RAPs) in wireless communication as a serious threat to the Wireless Local Area Network (WLAN) 802.11 protocol. The aim is to classify various types of wireless attacks and their various techniques, which are especially performed through RAP successfully. This paper also presents the statistical data and literature survey based on demand of next generation Wi-Fi enabled technologies and related cyber threats, which show that RAP is a serious threat to legitimate networks for wireless network and communication.**

Keywords*— *Rogue Access Point, WLAN, Wireless, 802.11, Distributed Denial of Service, Security, Threat.

I. INTRODUCTION

Coronavirus Disease of 2019 (COVID-19) forced most people to work from home [1], which commenced to increase demand for internet usability and access, and in particular, people set up Wi-Fi zones at home. Usage of publicly available and free Wi-Fi also increased during this time. But the Internet, or Wi-Fi connection, which is available in public places for free, lacks security to a large extent. A Wi-Fi connection at home and freely available Wi-Fi connectivity in public places have very weak security parameters so that cybercriminals can take advantage of them and perform various kinds of wireless attacks that can compromise your system and gain access to your machine, tools, and data. Peer-to-Peer attacks, eavesdropping, man in the middle attacks, password theft, Wi-Fi jamming, wardriving, DDoS, Media Access Control (MAC) spoofing, encryption cracking, RAP attacks are the most commonly performed attack types over a wireless network by attackers or malicious users to compromise users' systems (networks, servers, mail-servers, IoT-based devices, wired and wireless devices, etc.), tools, and data [2]. Antennas, routers, access points (APs), Wi-Fi cards, etc. are necessary components to run WLAN successfully, which follow the 802.11 regulation and technological guidelines. Data traversal, encoding, and decoding follow the 802.11 standards-compliant WLAN components[3]. So, unlike wired networks, anyone can interact with your communication media and interface, leading to major security issues in WLAN communication. We are examining increasing reports of wireless attacks. Annual pen-testing of wireless for acquiescence will become redundant especially for unrestricted public Wi-Fi. Nowadays, if you have a computer or laptop with a chipset that includes a Wi-Fi network adapter and internet connectivity, you can compromise any public Wi-Fi.

II. ACCESS POINT VS. ROGUE ACCESS POINT

Mobility is the common apparent benefit of wireless networking. Whether it is an airport or a coffee shop, a super mall or a retail shop, a garden or a railway station, a library or a hotel, the use of public Wi-Fi is increasing day by day as it is available for free or without cost [2]. According to the characteristics of Wi-Fi, the air interface is used for data communication, data transmission, and data relay. WLAN is a cluster of physical layer and MAC for the purpose of communication, technological rules, and standards defined by the Institute of Electrical and Electronics Engineers (IEEE) 802.11.In wireless communication, data is communicated loosely and readily in the air at 2.4 GigaHertz (GHz) and 5 GigaHertz (GHz), proper protection and assurance are needed to assure data privacy, so robust encryption is essential.

An access point (AP) is devised to collect, forward, and manage the wireless signals of the network. However, it cannot route data traffic of wireless networks also not usually organized for security. Commonly, the range of a wireless network is extended through an AP. The range of the wireless network can be extended by establishing and configuring an AP at the outer surface of that distance. Using WLAN AP connection is possible between the wireless segments of a network and the wired ethernet part of the network. So, an AP is like an Ethernet hub, but instead of transmitting Local Area Network (LAN) frames only to

978-93-80544-44-1/22/$31.00 ©2022 IEEE

other 802.3 stations, an AP transmits 802.11 frames to all other 802.3 or 802.11 stations. Built-in antennas, transmitters, adapters, Service Set Identifier (SSID) - IP address, Basic Service Set Identifier (BSSID) – physical address, and Extended Service Set Identifier (ESSID) are the core components of Wireless Application Protocol (WAP). So, if this kind of AP is placed and configured in the local or secure network without restrictions and without permission of an administrator by any organizational or non-organizational employee or malicious activist, known as a RAP [2]-[5]. RAPs broadcast their behaviour over the air. This type of rogue AP creates a major risk, and the main reason is its default configuration mode. Generally, in this default configuration mode, encryption methodology and authentication mode are disabled. These WLAN signals can traverse building walls and high-density objects, an open ap connected to any organisational network the absolute target for wardriving [3]-[6]. Many of the employees deployed RAPs for unrestricted network connections, and these kinds of access points are known as "soft access points." Through active and passive methodologies of data intercepting, attackers can intercept data from any network through RAP. A rogue AP can read the data, but data manipulation is not possible in the passive methodology of interception. For example, intercepting the data (like username, password etc.) traversing over web applications is possible but it cannot be altered or modified. User's data records of online activities are known as "internet footprinting" is intercepted by RAP is called "active intercepting." In, active intercepting methodology, the attacker can read the incoming user data, alter it however they want, and send it to the target endpoint. For example, in active intercepting methodology, a RAP can redirect and deposit the money into the hacker's account instead of a legitimate user account [3]. Figure 1 [2]-[6] demonstrates the basic architecture of rogue AP connections in WLAN.

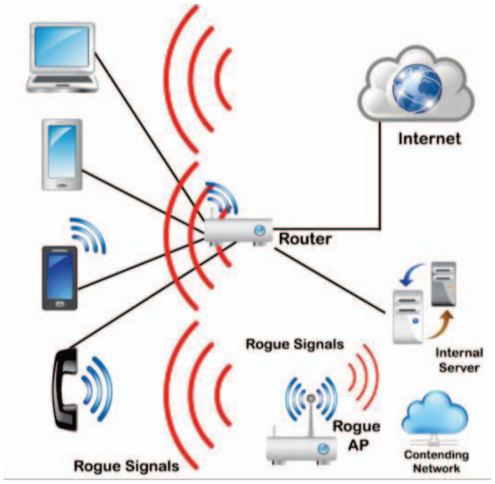

Fig. 1. Basic architecture of Rogue AP

III. Harmfulness of Rogue AP for Public Wi-Fi.

Geekdom doesn’t think much before connecting to public Wi-Fi or free Wi-Fi available at various public places and even at places like corporate and government offices, classrooms, computer labs, libraries, etc. With growing numbers of RAPs that are easily deployed in any public place or any organization, it’s becoming more critical to monitor users and connectivity. There are plenty of ways that intruders could place, install, and configure a rogue wireless access point on your network without your knowledge. At some point, students, intruders, and corporate employees all work as hackers. RAP could be hiddenly connected to any network or computer system, or it could be linked directly to network devices like switches or routers or any network port [3]-[8]. This is how it works:A rogue AP could be a cell phone [3] [9] connected via USB that creates a wireless AP and works as a malicious device or any WLAN card that could be placed on the server. A RAP could be a small-sized wireless AP that connects with a network firewall or network switch on any existing network and can be mounted on any unused cabinets, deployed on walls, put into pots of plants, etc. RAPs are installed and configured behind the firewall of any organisational network, which can be more harmful to WLAN security [3] [4] [10]. It is very tough to monitor and manage the RAPs and rogue clients at the initial level who get authenticated and granted access to the network by the administrator (by mistake or intentionally) of a legitimate network, and these kinds of RAPs do not support and obey the legitimate network security procedure [10]. Some of the employees may not have harmful or malicious purposes. The APs installed, configured, and utilized without the consent and approval of the network administrator are supposed to be rogue [3].

There are numerous ways to configure RAP and perform various RAP based attacks on wireless networks. Network admin could misconfigure a wireless network or some of the employees could bring their own devices (Bring Your Own Device - BYOD) like AP to connect wireless devices more easily, are the possibilities and scenarios of installed Rogue AP and performs various attacks based on RAP at corporate WLAN. This indicates that the network administrator is unsure about the WLAN's security [3]. Moreover, employees don't have to set security parameters on their personal APs, so it's, even easier for attackers to utilise that AP to intercept traffic from WLAN [8] [10]. RAP is a great way for hackers to get into business ecosystems and steal, intercept, and change data and wireless communication.

IV. Rogue AP and Possible Attacks

Hacktivist dogma, business grudges, monotony, blackmailing and extortion, government authorised cyber warfare and cyber vandalism, etc. are core elements or situations or states of mind where hackers are motivated. Hackers can perform Evil-Twin [3] [11] [12] [13] [27] [28] [61], MITM [3] [14]-[22] [24] [25] [26], DDoS [20] [27] [29] [30] [48] [51] [54], Vehicular Rogue AP [17] [28] [31], Internet of Things (IoT) - based Rogue AP [15] [17] [32]-[35], Wi-Fi Deauther [36] [37], Wi-Fi jamming [27] [28] [36] [37], Rogue (Wi-Fi) hotspot [37], MAC address duplication [3] [38] [39], and WLAN spoofing [25] [27] [29] types of attack through a RAP in public or corporate Wi-Fi networks.

A. Evil-Twin

An evil twin is a fraudulent Wi-Fi network set up by an attacker masquerading as a legitimate AP, but it is used for eavesdropping on wireless communications. The hackers inspect and scan the field for the targeted AP information. The attacker uses SSID, BSSID (MAC address), and channel info to create a fake AP. The hackers repeatedly de-authenticated and tried to break the clients linked to the authentic or legitimate AP, forcing them to join with the fake AP. With the rise of wireless networking devices and the usage of WLAN technology in public, it is considerably easier to set up and configure evil twins. Honeypots or base station clones are also known as Evil-Twin [3] [11]-[13] [27] [28] [61] [62].

B. Man-in-the-Middle

In the MITM, the attacker has injected themselves between the two communication systems in the WLAN, which think they are directly connected and communicating, but the attacker transfers and alters the data communication (of legitimate two systems) silently. It is easy for MITM attackers to intercept data between the systems because the data transfer is based on American Standard Code for Information Interchange (ASCII) and Hypertext Transfer Protocol (HTTP). Spoofing, hijacking, intercepting, and eavesdropping are the most common procedures that hackers use to be man-in-the-middle [3] [15] [16] [19] [24] [26] [40]–[45] [47]. Cyber assaulters can perform MITM attacks to accumulate control of machines or systems in different ways, which are mentioned in Table I [14] [16] [18]-[22] [24]-[26] [38]-[40] [44]-[47].

TABLE I. MITM ATTACK VECTORS

MITIM Attack Vectors	Parameters
ARP (Address Resolution Protocol) Poisoning	MAC Address, ARP Protocol, IPv4
NDP Poisoning	IPv6 Address
ICMP (Internet Control Message Protocol) Redirection	IP Packets, Half-Duplex, Domain Name System (DNS), DNS Traffic
SSL(Secure Socket Layer) Hijacking / Stripping	SSL, HTTPS
Port Stealing	Fragmented Packet Attack Packet InterNet Groper (Ping) of Death, Smurf DDoS
Stealing Browser Cookies	Session, Cookies
DHCP Spoofing	Gateway, Dynamic Host Configuration Protocol (DHCP), DNS Server
IP Spoofing	IP Address, Network Packets
DNS Spoofing / Multi DNS Spoofing	DNS, DNS Cache Information, IP Address
HTTPS Spoofing	Domain name, non-ASCII characters,
Email Hijacking	Email Accounts
Wi-Fi Eavesdropping	Wi-Fi Hotspot
Session Hijacking	Session Tokens, Session ID, Session Cookie

C. Distributed Denial of Service (DDoS) Attack

Instead of being attacked from one location, the target being attacked from many different locations at once is a core characteristic of a DDoS attack. As a result of the attackers' DDoS attacks on the hosting server, the services related to hosting servers are temporarily suspended and interrupted. A DDoS attack happens when multiple systems organise a synchronised DoS attack on a particular individual or single victim. In DDoS attacks, fake or dummy traffic is generated by the attackers in WLAN and trying to down the systems (like sending ICMP Ping requests or Ping Flood) whether it is server systems or workstations [3] [19] [30] [49] [50]. Botnet attacks are accountable for the biggest DDoS attacks on comprehensive record. A botnet is a combination of machines or computers that have been affected by malicious parameters or harmful malware and have been controlled by an attacker. Botnets [51] can be devised to perform unlawful or malicious activities like sending false and inappropriate data or messages, spam, advertisements, ransomware-type threats, or DDoS attacks. In many cases of DDoS attacks, attackers can use botnets that are already infected with malware or any threatening code used to send malicious traffic to a legitimate system [20] [48] [51] [54]. Nowadays, DDoS attacks are a lethal weapon in cyber warfare. As per the characteristics, parameters, and functionalities of DDoS attacks, Table II represents DDoS threat vectors and possible attack types. [30] [35] [48]-[50] [55].

TABLE II. DDOS ATTACK VECTORS

DDoS Attack Vectors	Types of Attacks
Voluminous	ICMP Flood (Ping Flooding), IP/ICMP Fission, IPSec Flooding, User Datagram Protocol (UDP) Flooding, Reflection Amplification
State Weariness Attacks	SYN Flood, SSL / TLS (Transport Layer Security) Weariness [24] [40] [46] (Exhaustion), NXDOMAIN Flooding / DNS Query
Application Layer DDoS Attack	BGP plunderage, Slowloris, Slow Post, Slow Read, HTTP/ HTTPS Flood, Low and Slow Attack, POST Request (Large Payload), Mimicked User Browsing), Reflection Amplification DDoS Attack, DNS Amplification / Reflection DDoS Attack
Protocol Attacks	Fragmented Packet Attack, Ping of Death, Smurf DDoS

D. Internet of Things based Rogue Access Point

IoT stands for "Internet of Things", defined as the network of physical devices and logical objects, including various technological sensors, applications, and tools that can generate and transmit data over the other networks and systems that are connected to the Internet. Every day, millions of new devices are linked to the internet, so a notable volume and amount of data roams loosely across the different networks, different remote networks, cloud [56] [57] networks, and hundreds of connected devices with irrelevant visibility, making it challenging to secure and trace this data [58] [59]. An attacker can use IoT [15] [17] [32] devices to create a RAP and perform spoofing [3], DDoS [3] [30] [48]-[50], MITM [3] [15]-[17] [24] [41] [42] [43] [57]-[60], and Evil-Twin [2] [3] [11]–[13] [61] [62] in WLAN. Hackers can use Raspberry Pi, Wi-Fi adapters, and Linux [42] [43] [63] variants as operating systems (OS) (Kali [21], Parrot OS, etc.) to create and perform RAP based attacks on WLAN [63]. The Raspberry Pi [21] [37] is a pocket-size, low-cost computer that includes ports to connect and manage associated electronic devices and provides solutions for the IoT.

E. Wi-Fi Deauthor

The cost of hacking Wi-Fi has slipped, and microcontrollers are more frequently being utilised into low-cost yet effective and powerful tools for hacking and malicious activities, and the ESP8266 [37] (SOC-System on Chip) is one of them. The ESP8266 is a modest, economical, and highly integrated Wi-Fi Micro Controller Unit (MCU) [37]. It has a Wi-Fi module, so it is distinct for its consistency, reliability, accuracy, integrity, and powerful performance for RF [36]. Hackers frequently use this device as a Wi-Fi Deauther [37] to generate disassociated data packets and for de-authentication. Any system on WLAN can forward these data packets to anyone and represent them like the packets are forwarded by network routers so in major cases, and scenarios these packets are threatful. When any machine on WLAN gets the data packets, will rapidly disconnect from Wi-Fi and Wi-Fi Deauther [37] [64] does this in a repetitive manner, spamming linked machines with disconnect messages. As a result, devices will not join the network quickly on the network, and a jamming effect occurs in WLAN, probably known as Wi-Fi jamming [37]. An attacker can create multiple RAPs with any SSID and observe the network and channels. [3] [27] [37].

F. Vehicular Rogue Access Point

Setting up RAPs in running vehicles or in moving objects at the roadside is the most dangerous thing for other vehicles and roadside or pedestrian traffic. Due to wireless mobility, a vehicle-based RAP or moving [35] object-based RAP can sustain a long-time connection with users or victims. Thus, the opponent means hackers have sufficient time to perform different kinds of attacks to hack and steal the victim's information. In the current situation, many metropolitan cities are connected by Wi-Fi networks. APs are placed on the roadside for vehicular networks. In many countries, internet-connected vehicles [65] (implemented with wireless abilities known as the connected car) can communicate over the Internet through roadside APs and thus the problem of vehicular RAP is rising for security in wireless networks. These vehicular RAPs [65]-[67] are defined as static rogue AP (configured as a fix) and mobile rogue AP. In mobile rogue AP, it's a challenging task to detect vehicular rogue AP and prevent legitimate users from using them. Even if sniffers are placed at the roadside, the vehicular rogue will have moved to another location before the legal authorities can identify it. So, in the future, drone [68] based RAP attacks will rise, too. Here, Figure 2 demonstrate the possibilities of vehicular and road side rogue AP and related attacks.

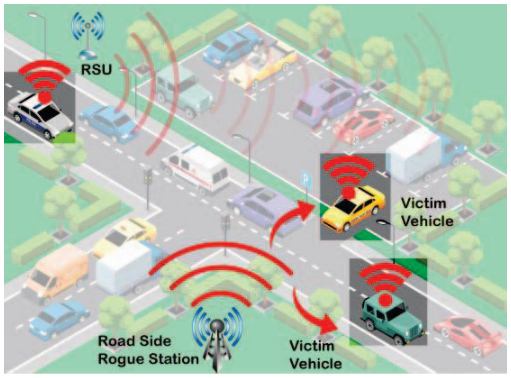

Fig. 2. Road side Rogue AP or Vehicular Rogue AP

G. Rogue Access Point for ICS / SCADA and Industrial Internet of Things:

Wireless connectivity is the future of ICS / SCADA systems [69]. Instruments, controllers, Human Machine Interface (HMI), network connection, and database (cloud) are core components of the SCADA system [26] [27] [49] [51]. It is scalable, and secure which makes the prominent preference moving ahead for oil and gas, energy and power, healthcare, food and beverages, production sector etc. In ICS, multiple attacker groups like Magnallium, Chrysene, Hexane, Xenotime, Dragonfly APT, Dymalloy APT launched various kinds of attacks named Trisis, Triton, Havex malware, etc. against oil and gas enterprises, water management facility providers, and associations in the energy sector [70]. Solo hackers or groups of malicious groups can pick up information on wireless networks or other vulnerabilities and launch MITM [26] and DDoS [27] [30] through RAPs, so the communication needs to be safer and more accurate in the SCADA system. About 1+ million SCADA/ICS APs are facing vulnerabilities and, they are at high risk of being compromised through cyberattacks and especially from wireless attacks, so the whole technology is like an international challenge and at the emergency level [26] [27] [30] [49]. Based on upcoming security concerns, here we represent a graphical demonstration in Figure 3 of a rogue ap threat to ICS/SCADA.

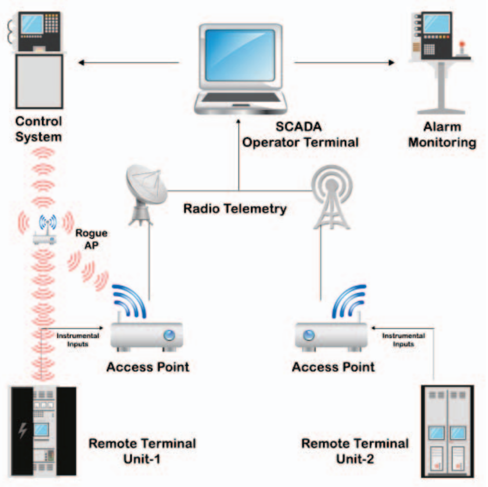

Fig. 3. Rogue AP threat for ICS / SCADA

H. Rogue Access Point for Unmanned Aerial Vehicle and Rogue Unmanned Aerial Vehicle

Airframe, navigation functionality, power system, payload, Ground Control Station (GCS) and communication system are main parts of any aerial vehicle. Nowadays weapons, exploits, and autonomous control systems are also a part of the UAV [37] [71]-[76] [95]. Without Global Positioning System (GPS) [17], navigation is not possible by UAV and, through GPS spoofing, it can be easily compromised. From the external environment, attackers also compromised the on-board sensors of the UAV and infected the flight control system. A UAV can access Wi-Fi APs from ground level, and attackers can compromise those legitimate APs and take control over the UAV by jamming [27] the same. Many of the researchers are working on UAV-based AP and related DDoS detection and prevention for wireless network communications [55] [68] [73] [77]. In the current scenario, most military organizations use UAVs to compromise fake drones [31] [37] [38] [71]-[76] [95].

Attackers also used Raspberry pi and HackRF One [31] kind of tools to attack on UAV. Nowadays users can manage the UAV through mobile phones and radio controllers too [31]. Here we demonstrate the scenario of a possible rogue AP and rogue UAV attack in Figure 4 how a fake wireless AP compromised a UAV and how a rogue drone jammed the signals of a legitimate UAV.

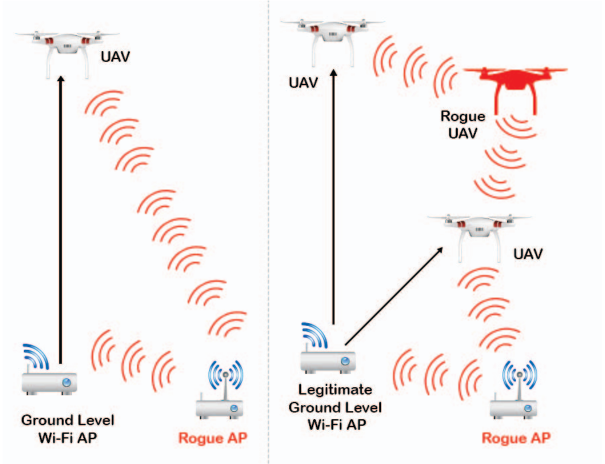

Fig. 4. Rogue AP attack on UAV with Rogue UAV

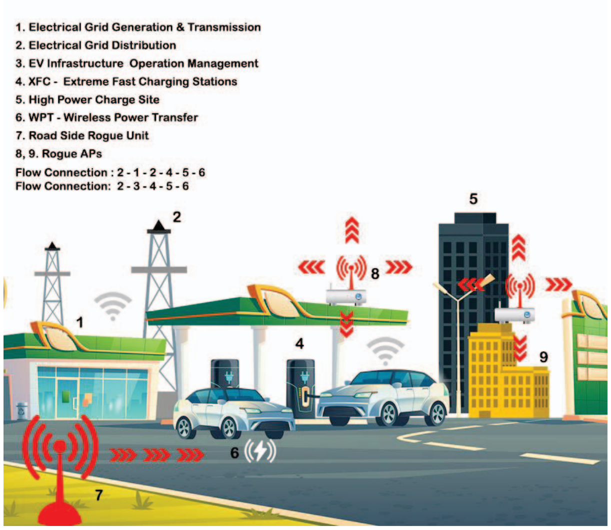
1. Electrical Grid Generation & Transmission
2. Electrical Grid Distribution
3. EV Infrastructure Operation Management
4. XFC - Extreme Fast Charging Stations
5. High Power Charge Site
6. WPT - Wireless Power Transfer
7. Road Side Rogue Unit
8, 9. Rogue APs
Flow Connection : 2 - 1 - 2 - 4 - 5 - 6
Flow Connection: 2 - 3 - 4 - 5 - 6
1
2
4
5
6
7
8
9

Fig. 5. EV Charging Station and RAP Threat

I. *Rogue Access Point for Electric Vehicle and Electric Vehicle Charging Station:*

The transmitter, receiver, coils, compensation network, Alternating Current (AC)–Direct Current (DC) converter, battery management system, and grids are core components of an EV [88] vehicle for charging them. In a static wireless charging station, the transmitter is set up underneath the ground and the signal receiver is set up under the vehicle's surface. Malicious hackers use signal or frequency capturing tools to compromise this kind of setup very easily. Road side deployed fix RAPs can destroy the Internet of Electric Vehicles (IoEV) and EVs [52]-[54] [79]-[82] stations too. Through this RAP, attackers can perform DDoS and MITM attacks very easily. But when we consider threat issues for Electronic Vehicle Charging Station (EVCS) components like Radio Frequency Identification (RFID) and physically deployed APs are much more harmful to cyber-attack. Through these, attackers can perform reverse engineering, DoS, DDoS, and MITM. In Figure 5, we demonstrate a graphical representation of a threat related scenario. In Table III, we present some technology and related threats for IoEV [80]-[82].

TABLE III. IOEV CMMUNICATION TECHNOLOGY AND VARIOUS ATTACKS

IoEV Technology		
Communication	***Communication Interface***	***Possible Attack***
V2S (Vehicle-to-Sensor)	Sensor	DoS, DDoS, Wi-Fi Jamming, Data Injection
V2V (Vehicle-to-Vehicle)	Device to Device	DoS, DDoS, Wi-Fi Jamming, Data Injection, avesdropping, Black Hole, Vehicular Rogue AP
V2R (Vehicle-to-Road)	RSU (Roadside Units)	Vehicular Rogue AP, DDoS, Jamming
V2I or V2N (Vehicle-to-Internet / Network)	RSU, Sensors, Cellular Technologies, Satellite, UAV	Vehicular Rogue AP, DDoS, RSU Spoofing, Jamming, MITM, Eavesdropping
V2H (Vehicle-to-Human)or V2P (Vehicle-to-Pedestrian)	RSU, Sensors, Smart Devices	Eavesdropping, Jamming

V. LITERATURE SURVEY AND STATISTICS

Snooping-based and time-based RAP detection methods are widely used by researchers. Major parameters used in snoop-based RAP detection methodologies include MAC address [83], Received Signal Strength Indicator (RSSI) [84]-[86], SSID, and channel [22] [47], but these parameters are easily spoofable. While the timing-side channel is used in time-based rogue AP detection methodology. In some cases, inter-packet communication delay and round-trip time are common parameters to detect the RAP in time-based terminology, but, in some cases, it's happening through software bridging. The packet delay [87] is a common factor for both of these techniques to detect the RAP. Some of the rogue AP detection methods work on the wired side, and some of them work on wireless, while some of the methods depend on the hardware and software compatibilities with operating systems and infrastructure scenarios. Even though some of the techniques work on the client-side or user-side and admin-side, separately. Some researchers face problems with critical infrastructures, and not all techniques play an efficient role in mitigating attacks. As a result, cyber attackers use a variety of attack methods to carry out various attacks on discrete units and technologies [3]-[8] [16] [32] [36] [38] [47] [72] [86]–[89]. Nowadays, researchers can use various datasets of different kinds of attacks and apply machine learning [23] algorithm-based techniques [84] to detect RAP. As we discussed, there are many scenarios to perform rogue AP based attacks and, for those tools and applications, devices, internet connectivity, topology, scenarios, and victim side situations may differ. So, the results of rogue AP detection based on the pre-defined dataset and ML-based algorithm will diverge.

As per the annual internet report of year 2018-2023, CISCO predicts the following aspects by 2023:

- Apx. 5.3 billion total internet users (means 66% of global population) [90].
- Apx. 29.3 billion IP network based devices [90].
- 14.7 billion M2M (Machine 2 Machine which is also referred to as IoT) connections [90].
- Connected home applications will have nearly half or 48% of M2M share [90].

- Apx. connected car applications will grow at 30% CAGR [90].
- Mobile devices will raise approximately 13.1 billion (1.4 billion of those will be 5G capable) [90].
- Globally, 628 million public Wi-Fi hotspots [90].

From the above statistics, the number of attackers, attacking techniques and scenarios will drastically change. An organization or a person who neglects the seriousness of upcoming time, paying off so much loss. Here, we mentioned some examples related to various kinds of wireless attacks which have been performed in this current year and past years.

Street [28] used different wireless gadgets to perform wireless attacks through evil APs on public streets and on the tube. As compared to 2018, 15.4 million DDoS attacks will be raised by 2023 [91]. The average size of a DDoS attack is 1 Gbps, and 23% of attacks are greater than 1 Gbps. Year over year, 776% of the increase in attacks is between 100 and 400 Gbps [92].

Nowadays, hackers can perform attacks on connected cars using HackRF [31] [82] [88] and other tools. Even IoT based smart doors and smart locks can be cracked with these devices easily. The growth of the industrial infosec and cyber security market is expected to rise at a CAGR of 5.81% from $16.9 billion in 2020 to $22.5 billion in 2025 [93]. A total of 1000 rogue aps were mined from 100 different buildings on Microsoft's campus in October 2019 [1].

Generally, people think that the cellular network is much safer than the WLAN. But 5G [50] deployments induce more security hazards, issues, and a risk-filled environment. According to the prediction of Cisco [94], a 5G connection will provide up to 575mbps by 2023. So, mobile device or IoT-based applications will grow tremendously. A majority of mobile (cellular) data packet users are using public Wi-Fi [40] or free hotspots due to the almost free cost, which means they will be vulnerable to Wi-Fi hacks. 5G network traffic itself has security breaches [50] that will be misused. Torpedo and Piercer, two different attacks that allow amateur attackers to intercept calls and track the device's location without any idea. Even, there is research going on to detect and mitigate RAP in public Wi-Fi [40] or WLAN, it's all about air interface and 802.11, which means attacking WLAN is an endless journey. In the future, vehicular-based RAP attacks will reach high, especially charging station of EV and IoT-based devices play a major role to compromise it. UAV - Drone [31] [95] based RAP is the new possibility for WLAN attack.

The security of IoT-based devices, which are used in smart cities, smart home devices, or smart farming-based devices, sensors, and applications, is a major concern for the next-gen WLAN. Devices that are stored and manipulated by the RF will compromise different kinds of simulators, whether they are used for the corporate sector, government sector, or for the public. So there are possibilities for rogue cloud, rogue vehicles, rogue vehicle charging station, rogue IoT devices, rogue UAVs etc.[31] for next generation threat of WLAN. In EVCS, through the malicious RAP attacker can fetch the data from infrastructure operations and the SCADA [26] system of EVCS by performing DDoS or MITM. Hackers can manipulate the signals of wireless charging systems of stations and vehicles, too. Even roadside units or pedestrian hackers gain access to EVs because they're managed through wireless communications. So, administrators who manage these kinds of EV stations, SCADA, Industrial IoT (IIoT) [35] systems, etc. have to be very conscious about the vulnerability of hardware and software. In today's era of cyberwar, weapons are becoming easier and more deadly with the help of wireless signals. It's all about wireless signals, so, there are a lot more possibilities to compromise these weapons, too. The TrackingPoint TP750 Wi-Fi enabled smart rifle can use laser precision through its smartscope feature to notify the shooter when it is clear and in-line for an immaculate shot. AR Quadcopter was shot down by an analyst of the US armed forces using a Raspberry Pi and a Wi-Fi based rifle [96]. UAV-to-UAV communication is not standardized.

Using ML, researchers can take advantage of making and ameliorating a UAV-based communication system. This would make it vulnerable to jamming and DDoS attacks. Drone-to-ground station communications use single-factor authentication on Wi-Fi 802.11, including 2.4 GHz and 5 GHz, which can be effortlessly compromised, and attackers can assemble them vulnerable to MITM. Moreover, Wi-Fi AP established at ground level can compromise surrounding UAVs too, and even UAVs can perform fake UAVs for legitimated wireless UAV. So rogue aps and rogue drone named as rogue UAV can destroy the legitimate devices [31].

VI. Discussion and Result

For security researchers, rogue AP, their attacks, and vulnerabilities in APs are crucial aspects for research in wireless communications and its security. As a result of the facts and literature surveys we elaborate some serious attack scenarios in this paper. Figure 6 and Figure 7 demonstrate the different scenarios of vehicular-based rogue AP. Figure 8 shows the wireless or Wi-Fi based areas in which rogue AP is harmful threat to next-gen technologies [48]-[59] [64]–[72] [74]-[83] [95]-[97].

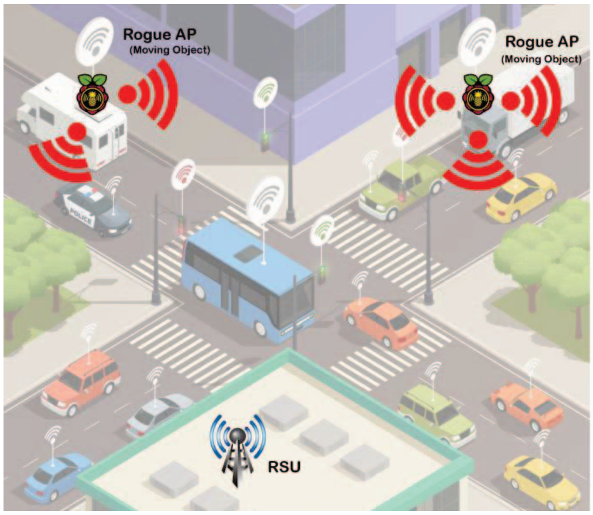

Fig. 6. Moving Rogue AP

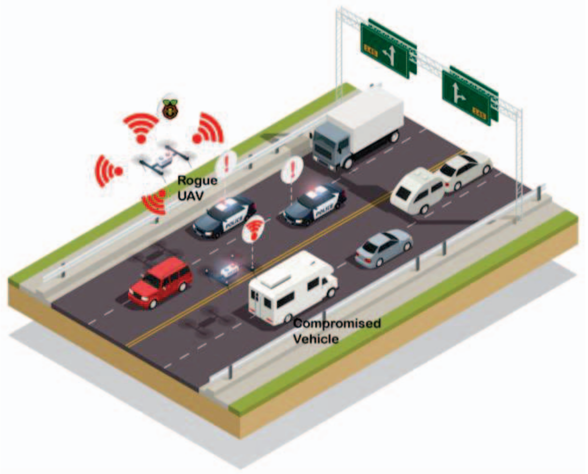

Fig. 7. Moving Rogue AP and Rogue UAV

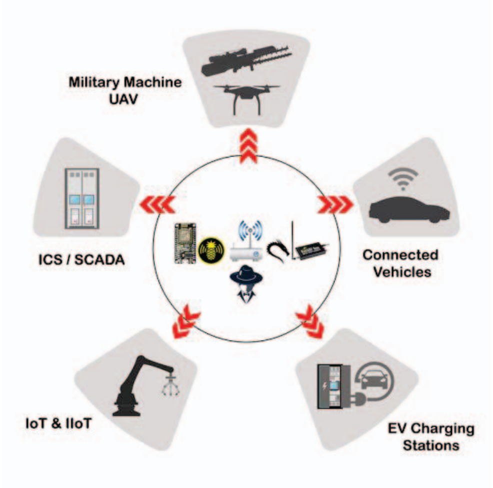

Fig. 8. Rogue AP threat for Future Technologies

VII. Conclusion

The alliances extend their wired network connectivity with wireless APs to deliver more scalability and ease of network communications for their workers, employees, and other users. RAPs and their consumers or users disable the shield of an industry network by potentially allowing unchallenged access to the network by any wireless user or client in its physical environs. This paper has described the concept of the RAP, various types of wireless attacks performed by malicious attackers through RAP on different areas like traditional wireless communication networks, UAV, ICS/SCADA, connected vehicles, EVs, EVCS, IoT, IIoT, military weapons, etc. like technologies and trends with graphical demonstration. This paper also presents the statistical data and literature survey based on demand for next-gen Wi-Fi enabled technologies and related cyber threats, which show that rogue ap is a serious threat to legitimate networks for wireless networks and communication. Although firewalls, IDS, and IPS are available, wireless attacks are continuing to occur and perform successfully in different technical domains, and researchers and technical analysts will try to prevent or eliminate them for betterment.

References

[1] D. Gantenbein, “Finding Rogue Access Points on the Microsoft Corporate Network,” Inside Track Blog, 06-Apr-2021. [Online]. Available: https://www.microsoft.com/insidetrack/blog/finding-rogue-access-points-on-the-microsoft-corporate-network/. [Accessed: 21-Jan-2022].

[2] Wasil, O. Nakhila, S. S. Bacanli, C. Zou and D. Turgut, “Exposing Vulnerabilities in Mobile Networks: A Mobile Data Consumption Attack,” in Proc. of the IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2017

[3] R. Jang, J. Kang, A. Mohaisen, and D. H. 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.

[4] M. Kim, S. Kwon, D. Elmazi, J.-H. Lee, L. Barolli, and K. Yim, “A technical survey on methods for detecting Rogue Access Points,” Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 215–226, 2019.

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

[6] Y. Lin, Y. Gao, B. Li and W. Dong, "Accurate and Robust Rogue Access Point Detection with Client-Agnostic Wireless Fingerprinting," in Proc. of the IEEE International Conference on Pervasive Computing and Communications (PerCom), 2020.

[7] 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 Proc. of the IEEE Conference on Computer Communications, 2019.

[8] R. H. Jang, J. Kang, A. Mohaisen, and D. H. Nyang, “Rogue access point detector using characteristics of channel overlapping in 802.11n,” in Proc. of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017.

[9] L. Qawasmeh and F. Awad, “Tracking a Mobile Rouge Access Point,” in Proc. of the International Conference on Information Technology (ICIT), 2021.

[10] Ketkhaw and S. Thipchaksurar, "Hidden Rogue Access Point Detection Technique for Wireless Local Area Networks," in Proc. of the 21st International Computer Science and Engineering Conference (ICSEC), 2017

[11] M. Asaduzzaman, M. S. Majib and M. M. Rahman, "Wi-Fi Frame Classification and Feature Selection Analysis in Detecting Evil Twin Attack," in Proc. of the 2020 IEEE Region 10 Symposium (TENSYMP), 2020.

[12] A. Burns, L. Wu, X. Du and L. Zhu, “A Novel Traceroute-Based Detection Scheme for Wi-Fi Evil Twin Attacks,” in Proc. of the IEEE Global Communications Conference, 2017.

[13] K. Murugesan, K. K. Thangadorai and V. N. Muralidhara, “PoEx: Proof of Existence for Evil Twin Attack Prevention in Wi-Fi Personal Networks,” in Proc. of the 8th International Conference on Future Internet of Things and Cloud (FiCloud), 2021.

[14] Bhushan, G. Sahoo and A. K. Rai, “Man-in-the-middle attack in wireless and computer networking — A review,” in Proc. of the 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall), 2017.

[15] J. J. Kang, K. Fahd, S. Venkatraman, R. Trujillo-Rasua and P. Haskell-Dowland, “Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks,” in Proc. of the 29th International Telecommunication Networks and Applications Conference (ITNAC), 2019

[16] P. A. W. Putro and R. Rionaldy, “Implementation of the Park Schema on User Authentication Services Using Password-Based Web Codeigniter Library to Overcome Man in the Middle Attack,” in Proc. of the Fourth International Conference on Informatics and Computing (ICIC), 2019.

[17] G. R. Andreica, L. Bozga, D. Zinca and V. Dobrota, “Denial of Service and Man-in-the-Middle Attacks Against IoT Devices in a GPS-Based Monitoring Software for Intelligent Transportation Systems,” in Proc. of the 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), 2020.

[18] Y. Yang, X. Wei, R. Xu, L. Peng, L. Zhang and L. Ge, “Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer

Location Consistency," IEEE Access, vol. 8, pp. 103860-103874, 2020.

[19] Oliva, S. Cioabă and C. N. Hadjicostis, "Distributed Calculation of Edge-Disjoint Spanning Trees for Robustifying Distributed Algorithms Against Man-in-the-Middle Attacks," IEEE Transactions on Control of Network Systems, vol. 5, no. 4, pp. 1646-1656, Dec. 2018.

[20] S. Stricot-Tarboton, S. Chaisiri and R. K. L. Ko, "Taxonomy of Man-in-the-Middle Attacks on HTTPS," in Proc. of the IEEE Trustcom/BigDataSE/ISPA, 2016.

[21] Y. Mirsky, N. Kalbo, Y. Elovici and A. Shabtai, "Vesper: Using Echo Analysis to Detect Man-in-the-Middle Attacks in LANs," IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1638-1653, June 2019.

[22] M. Johnson, P. Lutz and D. Johnson, "Covert Channel Using Man-in-the-Middle over HTTPS," in Proc. of the International Conference on Computational Science and Computational Intelligence (CSCI), 2016.

[23] A. Al-Hababi and S. C. Tokgoz, "Man-in-the-Middle Attacks to Detect and Identify Services in Encrypted Network Flows using Machine Learning," in Proc. of the 3rd International Conference on Advanced Communication Technologies and Networking (CommNet), 2020.

[24] Z. Li, G. Xiong and L. Guo, "Unveiling SSL/TLS MITM Hosts in the Wild," in Proc. of the IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE), 2020

[25] "What is MITM (man in the middle) attack: Imperva," Learning Center, 29-Dec-2019. [Online]. Available: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/. [Accessed: 20-Jan-2022].

[26] D. Deb, S. R. Chakraborty, M. Lagineni, and K. Singh, "Security analysis of MITM attack on SCADA network," Communications in Computer and Information Science, pp. 501–512, 2020.

[27] "ICS/SCADA Wireless attacks," Infosec Resources, 14-Apr-2021. [Online]. Available: https://resources. infosecinstitute.com/topic/ics-scada-wireless-attacks/. [Accessed: 10-Feb-2022].

[28] "Hacker shows how easy it is to hack people while walking around in public," The Hacker News, 24-Feb-2017. [Online]. Available: https://thehackernews.com/2017/02/hacking-in-public.html. [Accessed: 20-Jan-2022].

[29] "What is a distributed denial of service (ddos) attack?," NETSCOUT. [Online]. Available: https://www.netscout.com/what-is-ddos#component--2. [Accessed: 10-Feb-2022].

[30] A. E. M. AL-Dahasi and B. N. A. Saqib, "Attack tree Model for Potential Attacks Against the SCADA System," in Proc. of the 27th Telecommunications Forum (TELFOR), 2019, pp. 1-4, doi: 10.1109/TELFOR48224.2019.8971181.

[31] J. Gordon, V. Kraj, J. H. Hwang and A. Raja, "A Security Assessment for Consumer WiFi Drones," in Proc. of the IEEE International Conference on Industrial Internet (ICII), 2019, pp. 1-5, doi: 10.1109/ICII.2019.00011.

[32] J. Owusu Agyemang, J. John Kponyo, and G. Selorm Klogo, "A lightweight rogue access point detection algorithm for embedded internet of things (IOT) devices," Information Security and Computer Fraud, vol. 7, no. 1, pp. 7–12, 2019.

[33] M. H. Mahalat, S. Saha, A. Mondal and B. Sen, "A PUF based Light Weight Protocol for Secure WiFi Authentication of IoT devices," in Proc. of the 8th International Symposium on Embedded Computing and System Design (ISED), 2018.

[34] T. L. von Sperling, B. de A. França, F. L. de Caldas Filho, L. M. C. e Martins, R. de O. Albuquerque and R. T. de Sousa, "Evaluation of an IoT device designed for transparent traffic analysis," in Proc. of the Workshop on Communication Networks and Power Systems (WCNPS), 2018.

[35] Y. Zhou, G. Cheng, Y. Zhao, Z. Chen and S. Jiang, "Toward Proactive and Efficient DDoS Mitigation in IIoT Systems: A Moving Target Defense Approach," IEEE Transactions on Industrial Informatics, vol. 18, no. 4, pp. 2734-2744, April 2022

[36] 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

[37] K. Kadripathi, L. Y. Ragav, K. Shubha and P. H. Chowdary, "De-Authentication Attacks on Rogue UAVs," in Proc. of the 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020

[38] K. Igarashi, H. Kato and I. Sasase, "Rogue Access Point Detection by Using ARP Failure under the MAC Address Duplication," in Proc. of the IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2021.

[39] A. A. M. M. Amin and M. S. Mahamud, "An Alternative Approach of Mitigating ARP Based Man-in-the-Middle Attack Using Client Site Bash Script," in Proc. of the 6th International Conference on Electrical and Electronics Engineering (ICEEE), 2019

[40] W. Yang, X. Li, Z. Feng and J. Hao, "TLSsem: A TLS Security-Enhanced Mechanism against MITM Attacks in Public WiFis," in Proc. of the 22nd International Conference on Engineering of Complex Computer Systems (ICECCS), 2017

[41] Idiyatullin and P. E. Abdulkin, "A Research of MITM Attacks in Wi-Fi Networks Using Single-board Computer," in Proc. of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2021.

[42] Pingle, A. Mairaj and A. Y. Javaid, "Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use," in Proc. of the IEEE International Conference on Electro/Information Technology (EIT), 2018.

[43] A. R. Chordiya, S. Majumder and A. Y. Javaid, "Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools," in Proc. of the IEEE International Conference on Electro/Information Technology (EIT), 2018.

[44] Bruschi, A. Di Pasquale, S. Ghilardi, A. Lanzi, and E. Pagani, "A formal verification of arpon a tool for avoiding man-in-the-middle attacks in ethernet networks," IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2021.

[45] M. A. Yurdagul and H. T. Sencar, "BLEKeeper: Response Time Behavior Based Man-In-The-Middle Attack Detection," in Proc. of the IEEE Security and Privacy Workshops (SPW), 2021

[46] 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.

[47] S. Gong, H. Ochiai and H. Esaki, "Scan-Based Self Anomaly Detection: Client-Side Mitigation of Channel-Based Man-in-the-Middle Attacks Against Wi-Fi," in Proc. of the IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), 2020.

[48] M. H. Rohit, S. M. Fahim and A. H. A. Khan, "Mitigating and Detecting DdoS attack on IoT Environment," in Proc. of the IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON), 2019.

[49] J. D. Markovic-Petrovic and M. D. Stojanovic, "Analysis of SCADA system vulnerabilities to DDoS attacks," in Proc. of the 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2013

[50] M. A. Javed and S. khan Niazi, "5G Security Artifacts (DoS / DDoS and Authentication)," in Proc. of the International Conference on Communication Technologies (ComTech), 2019

[51] A. Sagala, R. Pardosi, A. Lumbantobing and P. Siagian, "Industrial control system security-malware botnet detection," in Proc. of the International Conference on Computer, Control, Informatics and its Applications (IC3INA), 2016

[52] Y. Fraiji, L. Ben Azzouz, W. Trojet and L. A. Saidane, "Cyber security issues of Internet of electric vehicles," in Proc. of the IEEE Wireless Communications and Networking Conference (WCNC), 2018

[53] S. Saadat, S. Maingot and S. Bahizad, "Electric Vehicle Charging Station Security Enhancement Measures," in Proc. of the 5th IEEE Workshop on the Electronic Grid (eGRID), 2020

[54] O. G. M. Khan, E. El-Saadany, A. Youssef and M. Shaaban, "Impact of Electric Vehicles Botnets on the Power Grid," in Proc. of the IEEE Electrical Power and Energy Conference (EPEC), 2019

[55] A. Mairaj, S. Majumder and A. Y. Javaid, "Game Theoretic Strategies for an Unmanned Aerial Vehicle Network Host Under DDoS Attack," in Proc. of the International Conference on Unmanned Aircraft Systems (ICUAS), 2019

[56] C. -Y. Cheng, E. Colbert and H. Liu, “Experimental Study on the Detectability of Man-in-the-Middle Attacks for Cloud Applications,” in Proc. of the IEEE Cloud Summit, 2019.

[57] P. Patni, K. Iyer, R. Sarode, A. Mali and A. Nimkar, “Man-in-the-middle attack in HTTP/2,” in Proc. of the International Conference on Intelligent Computing and Control (I2C2), 2017.

[58] S. Purwanti, B. Nugraha and M. Alaydrus, “Enhancing security on E-health private data using SHA-512,” in Proc. of the International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP), 2017.

[59] O. Salem, K. Alsubhi, A. Shaafi, M. Gheryani, A. Mehaoua and R. Boutaba, “Man-in-the-Middle Attack Mitigation in Internet of Medical Things,” IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 2053-2062, March 2022.

[60] J. Thomas, S. Cherian, S. Chandran and V. Pavithran, “Man in the Middle Attack Mitigation in LoRaWAN,” in Proc. of the International Conference on Inventive Computation Technologies (ICICT), 2020.

[61] 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 Proc. of the 27th Mediterranean Conference on Control and Automation (MED), 2019.

[62] 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 Proc. of the IEEE Trustcom/BigDataSE/ICESS, 2017.

[63] Al Neyadi, S. Al Shehhi, A. Al Shehhi, N. Al Hashimi, M. Qbea’H and S. Alrabaee, “Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux,” in Proc. of the 12th Annual Undergraduate Research Conference on Applied Computing (URC), 2020

[64] N. Lovinger, T. Gerlich, Z. Martinasek and L. Malina, "Detection of wireless fake access points," in Proc. of the 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2020

[65] Ahmad, F. Kurugollu, A. Adnane, R. Hussain and F. Hussain, “MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles,” IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3310-3322, April 2020.

[66] H. Han, F. Xu, C. C. Tan, Y. Zhang and Q. Li, "Defending against vehicular rogue APs," in Proc. of the Proceedings IEEE INFOCOM, 2011.

[67] H. Han, F. Xu, C. C. Tan, Y. Zhang and Q. Li, "VR-Defender: Self-Defense Against Vehicular Rogue APs for Drive-Thru Internet," IEEE Transactions on Vehicular Technology, vol. 63, no. 8, pp. 3927-3934, Oct. 2014.

[68] D. S. C. Putranto, A. K. Aji and B. Wahyudono, "Design and Implementation of Secure Transmission on Internet of Drones," in Proc. of the IEEE 6th Asian Conference on Defence Technology (ACDT), 2019

[69] Lan, X. Zhu, J. Sun and S. Li, “Traffic Data Classification to Detect Man-in-the-Middle Attacks in Industrial Control System,” in Proc. of the 6th International Conference on Dependable Systems and Their Applications (DSA), 2020.

[70] O. 6, O. 5, J. 28, and F. 2, “ICS/SCADA threats and threat actors,” Infosec Resources, 07-Jun-2021. [Online]. Available: https://resources .infosecinstitute.com/topic/ics-scada-threats-and-threat-actors/. [Accessed: 11-Feb-2022].

[71] G. J. Nunns, Y.-J. Chen, D.-K. Chang, K.-M. Liao, F. P. Tso, and L. Cui, “Autonomous Flying Wifi Access Point,” in Proc. of the IEEE Symposium on Computers and Communications (ISCC), 2019.

[72] N. Chakraborty et al., "On Understanding the Impact of RTT in the Mobile Network for Detecting the Rogue UAVs," IEEE Transactions on Cognitive Communications and Networking, vol. 6, no. 4, pp. 1218-1229, Dec. 2020.

[73] K. Hartmann and K. Giles, "UAV exploitation: A new domain for cyber power," in Proc. of the 8th International Conference on Cyber Conflict (CyCon), 2016

[74] G. Rong-xiao, T. Ji-wei, W. Bu-hong and S. Fu-te, "Cyber-Physical Attack Threats Analysis for UAVs from CPS Perspective," in Proc. of the International Conference on Computer Engineering and Application (ICCEA), 2020

[75] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, “A tutorial on uavs for wireless networks: Applications, challenges, and open problems,” IEEE Communications Surveys &amp; Tutorials, vol. 21, no. 3, pp. 2334–2360, 2019.

[76] X. Tan, Z. Zuo, S. Su, X. Guo, and X. Sun, “Research of Security Routing Protocol for UAV Communication Network based on AODV,” Electronics, vol. 9, no. 8, p. 1185, 2020.

[77] A. M. Patel and H. R. Patel, "Analytical Study of Penetration Testing for Wireless Infrastructure Security," in Proc. of the International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), 2019

[78] S. M. Giray, "Anatomy of unmanned aerial vehicle hijacking with signal spoofing," in Proc. of the 6th International Conference on Recent Advances in Space Technologies (RAST), 2013

[79] Z. Pourmirza and S. Walker, "Electric Vehicle Charging Station: Cyber Security Challenges and Perspective," in Proc. of the IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE), 2021

[80] N. Bhusal, M. Gautam, and M. Benidris, “Cybersecurity of Electric Vehicle Smart Charging Management Systems,” in Proc. of the 52nd North American Power Symposium (NAPS), 2021.

[81] S. Acharya, Y. Dvorkin, H. Pandzic, and R. Karri, “Cybersecurity of Smart Electric Vehicle Charging: A power grid perspective,” IEEE Access, vol. 8, pp. 214434–214453, 2020.

[82] Y. Fraiji, L. Ben Azzouz, W. Trojet and L. A. Saidane, "Cyber security issues of Internet of electric vehicles," in Proc. of the IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1-6, doi: 10.1109/WCNC.2018.8377181.

[83] S. Choi, D. Hwang and Y. Choi, “Wireless intrusion prevention system using dynamic random forest against wireless MAC spoofing attack,” in Proc. of the IEEE Conference on Dependable and Secure Computing, 2017.

[84] R. Liu, Z. Zhang, T. Wang, L. Wang and S. Zhao, "Machine Learning Based Access Point Verification Scheme for the Smart Grid," in Proc. of the 9th International Conference on Power Science and Engineering (ICPSE), 2020.

[85] D. Wu, Y. Guan, K. Liu, T. Zhang, Z. Xu and Y. Liu, “A Robust RSS-Based Rogue AP Localization Algorithm with Unknown Transmit Power,” in Proc. of the 10th International Conference on Communications, Circuits and Systems (ICCCAS), 2018.

[86] 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 Proc. of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017.

[87] Z. Zhang, H. Hasegawa, Y. Yamaguchi and H. Shimada, “Rogue AP Detection using Similarity of Backbone Delay Fluctuation Histogram,” in Proc. of the International Conference on Information Networking (ICOIN), 2020

[88] C. Mercenit, J. C. Rios, Y. Liu, J. Wang, J. Yuan, and H. Song, “Analysis of rogue access points using SDR,” in Proc. of the IEEE International Conference on Industrial Internet (ICII), 2019.

[89] M. Agarwal, "Rogue Twin Attack Detection: A Discrete Event System Paradigm Approach,"in Proc. of the IEEE International Conference on Systems, Man and Cybernetics (SMC), 2019.

[90] “Cisco annual internet Report - Cisco Annual Internet Report (2018–2023) White Paper,” Cisco, 10-Mar-2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspec tives/annual-internet-report/white-paper-c11-741490.html. [Accessed: 20-Jan-2022].

[91] “Data loss protection for the modern cloud,” Snowflake. [Online]. Available: https://www.snowflake.com/guides/data-loss-protection-m odern-cloud. [Accessed: 10-Feb-2022].

[92] “DDoS attack statistics, Facts and Trends for 2018-2022,” Comparitech, 16-May-2021. [Online]. Available: https://www.compa ritech.com/blog/information-security/ddos-statistics-facts/. [Accessed: 10-Feb-2022].

[93] Helga, “Analysts predict the growth of the apcs security market in the next years,” TrustCoyote, 24-Nov-2020. [Online]. Available: https://trustcoyote.com/uncategorized/analysts-predict-the-growth-of-the-ics-security-market-in-the-next-years. [Accessed: 10-Feb-2022].

[94] “New Cisco annual internet report forecasts 5G to support more than 10% of global mobile connections by 2023,” New Cisco Annual Internet Report Forecasts 5G to Support More Than 10% of Global

Mobile Connect | The Network, 18-Feb-2020. [Online]. Available: https://newsroom.cisco.com/press-releasecontent?type=webcontent&amp;articleId=2055169. [Accessed: 10-Feb-2022].

[95] N. Chakraborty, Y. Chao, J. Li, S. Mishra, C. Luo, Y. He, J. Chen, and Y. Pan, “RTT-based rogue UAV detection in Iov Networks,” IEEE Internet of Things Journal, pp. 1–1, 2021.

[96] C. Gorey, “It's pretty easy to hack a smart TrackingPoint sniper rifle, apparently,” Silicon Republic, 30-Jul-2015. [Online]. Available: https://www.siliconrepublic.com/enterprise/hacking-smart-sniper-rifle [Accessed: 22-Jan-2022].

[97] “The Army built a wi-fi ‘gun’ that shoots drones from the Sky,” Army Cyber Institute, 19-Oct-2015. [Online]. Available: https://cyber.army.mil/Library/Media-Coverage/Article/1342615/the-army-built-a-wi-fi-gun-that-shoots-drones-from-the-sky/. [Accessed: 22-Jan-2022].