National College of Ireland

A Comparative Analysis of Traditional Rogue AP and Multi-Channel CSA-Spoofing Establishment Against WPA3 Protections in a Simulated Environment.

MSc Research Project
MSc Cybersecurity

Elijah Dyeris
X23367415

School of Computing
National College of Ireland

Supervisor: Eugene Mclaughlin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Elijah Dyeris
Student ID:	X23367415
Programme:	MSc Cybersecurity **Year:** 2024
Module:	Practicum 2
Supervisor:	Eugene Mclaughlin
Submission Due Date:	11th August 2025
Project Title:	A Comparative Analysis of Traditional Rogue AP and Multi-Channel CSA-Spoofing Establishment Against WPA3 Protections In a Simulated Environment.
Word Count:	8697 **PageCount**: 22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: 11th August 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A Comparative Analysis of Traditional Rogue AP and Multi-Channel CSA-Spoofing Establishment Against WPA3 Protections in a Simulated Environment.

Elijah Dyeris
X23367415

Abstract
This study investigates the susceptibility of IoT devices to wireless-based attacks, focusing on Rogue Access Point (Rogue AP) and Channel Switch Announcement Spoofing (CSA-Spoofing) techniques. Using a simulated environment with a dataset of 50 heterogeneous IoT devices, we evaluate the effectiveness of these attacks under probabilistic success rates of 90% and 85%, respectively. The results reveal that CSA-Spoofing consistently bypasses Protected Management Frames (PMF), posing a significant threat to WPA3-enabled networks.
Key limitations of this study include the reliance on simulation rather than real-world testing, the use of synthetic device profiles instead of actual firmware, and the assumption of fixed attack success rates without empirical calibration. A sensitivity analysis demonstrates that even at reduced success probabilities (70–95%), CSA-Spoofing remains a dominant threat. These findings underscore the urgent need for mandatory PMF enforcement, robust firmware update policies, and network segmentation strategies to mitigate IoT vulnerabilities.
This Simulation was done using Python 3 and 50 different IoT devices were modelled and evaluated. The findings indicates that MC-MitM csa-Spoofing exhibits a considerable feasibility with success rates of about 44.20% in WPA3-Only and 44.23% in WPA3-Transition modes While traditional Rogue AP attacks showed lower success rate around 25.22% and 25.21% respectively. PMF effectively neutralizes traditional Rogue AP attacks when enabled (0.00% success), but MC-MitM CSA-Spoofing largely bypasses PMF protection, achieving success rates of 40.94% with PMF enabled and 48.05% with PMF disabled. The research highlights the critical need for user-friendly and effective defense mechanisms for IoT environments, given the ability of MC-MitM attacks to bypass WPA3's advanced features.

Keywords: Wi-Fi, Man-in-the-middle (MitM) attacks, Internet of Things (IoT), Multi-Channel CSA-Spoofing, WPA3.

1. Introduction

1.1. Background:

Wireless Local Area Networks (WLANs) are increasingly used in various applications due to their flexibility, mobility, and wide availability(Bing, 2003). With the rapid growth of the Internet of Things (IoT), Wi-Fi devices are now commonly found everywhere, including smart homes(“State of IoT 2024,” 2024). However, this widespread adoption also makes WLANs vulnerable to many security threats. One significant and common form of security attack targeting wireless networks is the Man-in-the-Middle (MitM) attack. In a MitM attack, the attacker positions themselves between two communicating devices, allowing them to secretly intercept and manipulate the information exchanged(Thankappan, 2022).

An advanced form of this threat is the Multi-Channel Man-in-the-Middle (MC-MitM) attack, first identified in 2014(Thankappan, 2022). What makes MC-MitM particularly dangerous is its ability to manipulate encrypted wireless frames between legitimate devices. Unlike traditional rogue AP MitM attacks, MC-MitM attacks do not need the legitimate Wi-Fi password or to break the existing connection between the client and the real AP. Instead, the attacker uses two different Wi-Fi channels to trick the client and the real AP into communicating through the attacker's setup(Feng et al., 2023). This allows the attacker to reliably block, delay, modify, inject, or replay encrypted wireless frames, making the manipulation appear entirely legitimate to the victims. Notably, MC-MitM attacks can even succeed in environments protected by Protected Management Frames (PMF), a security feature that often prevents traditional rogue AP attacks.

Since their discovery, MC-MitM attacks have been used to exploit various Wi-Fi Protected Access (WPA) protocols, including WPA, WPA2, and WPA3, in both personal and enterprise networks. These attacks encompass a range of exploits such as cipher downgrades, denial of service (DoS), Key Reinstallation Attacks (KRACK) in 2017, and the more recent Frag Attacks in 2021(Thankappan, 2022). KRACK and Frag Attacks have had a widespread impact on millions of Wi-Fi systems, especially those incorporating IoT devices, by exploiting specific programming flaws in the Wi-Fi standard.

Detecting MC-MitM attacks is complex because the attacker operates stealthily. They acquire the MitM position without disconnecting clients or performing noticeable malicious activities like flooding the network with de-authentication frames. The MC-MitM attacker sets up a rogue AP that mimics a legitimate one so perfectly that end devices believe they are communicating directly with their intended partner. This deceptive behavior makes it very difficult to distinguish between normal and malicious network activities, necessitating advanced detection mechanisms(Louca et al., 2021a).

1.2. Motivation:

The increasing deployment of Wi-Fi devices, especially within IoT environments like smart homes, makes them prime targets for sophisticated attacks. MarketsandMarkets reported the global smart home market was expected to grow to US $89.8 billion in 2025 and then US $116.4 billion by 2029, at a CAGR of about 6.6% between 2024–2029("Smart Home Market Research Report, 2024," n.d.). However, effectively preventing MC-MitM attacks is challenging in real-world scenarios, particularly because IoT devices often have limited built-in security features(Fereidouni et al., 2025). Existing defense mechanisms face significant practical limitations: they often require modifications to the Wi-Fi protocol, installation of advanced hardware or software, or updates to proprietary firmware. These requirements frequently impose a substantial technical burden on average users, who typically lack the specialized knowledge needed for complex network setup and maintenance. Moreover, many commercial IoT devices do not support the integration of third-party software, making widespread adoption of these defenses impractical(Thankappan, 2022).

The urgency of this issue is underscored by a surge in recent high-profile IoT security breaches. For instance, Mirai botnet variants continue to exploit newly discovered vulnerabilities in widely deployed devices, such as TBK DVRs and Wazuh servers, compromising tens of thousands of systems globally and leveraging them in powerful DDoS attacks("Mirai Botnets Exploit Flaw in Wazuh Security Platform," n.d.). Similarly, Ring cameras have faced multiple security incidents, including recent reports in July 2025 of suspicious logins across user accounts, prompting fears of unauthorized access despite Ring's claims of a backend issue(Arntz, 2025). These real-world breaches demonstrate that consumer IoT devices, even those from major vendors, remain highly vulnerable to various forms of exploitation including Man-in-the-Middle attacks

A major concern is that MC-MitM attacks can impact WPA3 networks despite their advanced security features, primarily due to their ability to bypass PMF protection(Mathew et al., 2025a). While PMF is designed to protect management frames, it fails to protect pre-authenticated frames such as beacons or probe responses, thereby enabling MitM attacks in both WPA2 and WPA3 devices. Furthermore, insider MC-MitM attacks, where the attacker has authorized access to the network, are particularly dangerous because they can hijack private communications within homes or offices, and current defense mechanisms are often inadequate against them. This situation highlights a critical unresolved research problem concerning the protection of both PMF-capable and PMF-incapable devices from MC-MitM attacks across all WPA standards(Thankappan, 2022).
IoT devices, universally in smart environments, often operate with weak or no encryption, insufficient randomness, or poor key generation mechanisms. This makes them highly susceptible to being tricked or hijacked by MC-MitM attackers, who can then steal sensitive information or carry out other malicious activities(Thankappan, 2022). Consequently, there is an urgent need for the development of user-friendly, affordable, and effective defense mechanisms specifically tailored for IoT environments. Existing literature lacks comprehensive reviews of MC-MitM enabled attacks and their potential impact, as well as analyses of practical challenges preventing the adoption of protective measures, particularly in the IoT context.

Research Question and Objectives: This research aims to evaluate the *Technical Feasibility of Establishing Man-in-the-Middle Positions in Smart Home IoT Environments: A Comparative Analysis of Traditional Rogue AP and Multi-Channel CSA-Spoofing Establishment Against WPA3 Protections in a Simulated environment*.

This paper specifically examines the technical feasibility of establishing the MitM position in smart home IoT environments by comparing the traditional Rogue AP method with the MC-MitM method leveraging CSA-Spoofing. We analyze their effectiveness against WPA3 security, especially considering that PMF is mandatory for new WPA3 certifications. Gaining the MitM position is a necessary precursor for subsequent attacks, such as KRACK or Frag Attacks.
To address this research question, the following specific objectives were established:

- To evaluate the capabilities of Multi-Channel Man-in-the-Middle (MC-MitM) attacks in manipulating protected Wi-Fi communications, specifically against WPA3 networks.
- To compare the characteristics of MC-MitM attacks with traditional rogue AP-based MitM attacks in Wi-Fi networks, analysing their requirements (e.g., Wi-Fi passphrase), ability to manipulate link-layer encrypted traffic, and effectiveness in PMF environments.
- To analyse how MC-MitM attacks impact WPA3 networks, including WPA3-Only and WPA3-Transition modes, considering their ability to circumvent PMF protection.
- To examine the challenges associated with adopting general protection mechanisms, such as security patches and Protected Management Frames (PMF), against MC-MitM attacks, particularly in the context of IoT devices.

1.3. Contribution:

This study helps everyone understand MC-MitM attacks better, showing what they can do and how they work. It also highlights how important it is to protect our Wi-Fi and smart home devices, especially when old devices are mixed with new ones and current protections

don’t work well. Our work aims to show that there’s a big need for new, easy-to-use security systems to fight against these attacks in real smart home setups.
While WPA3 enhances authentication, the connection process, and critically, management frames like beacons and probe responses carrying CSA information, can remain unprotected even when PMF is enabled. This characteristic of the standard allows MC-MitM CSA-spoofing to potentially bypass PMF’s protection against the establishment of an MitM position. The situation is exacerbated in smart home IoT due to device diversity, limited resources, and inconsistent patching against known vulnerabilities, making effective defense implementation challenging.
By comparing these two distinct methods for gaining the MitM position, this paper aims to offer a technical analysis of their practical feasibility against WPA3-protected networks in the context of smart home IoT. We assess the technical requirements and potential success of each method, considering WPA3 features, PMF status, and the unique characteristics of IoT devices.

1.4. Structure:

The structure of this paper examines background information on Wi-Fi security and MitM attacks, details the technical workings of MC-MitM CSA-spoofing compared to traditional rogue AP establishment, evaluates their feasibility in smart home IoT under WPA3, analyses challenges posed by IoT device limitations, and concludes with insights and future research directions.

2. Related Work

This literature review examines the technical feasibility of establishing Man-in-the-Middle (MitM) positions in Smart Home Internet of Things (IoT) environments. The analysis focuses on traditional rogue Access Point (AP) attacks and Multi-Channel Channel Switch Announcement (CSA) spoofing techniques against Wi-Fi Protected Access 3 (WPA3)

The rapid proliferation of Wi-Fi networks and the increasing integration of Internet of Things (IoT) devices, particularly within smart home environments, necessitate robust security measures. Despite advancements in wireless security protocols, Man-in-the-Middle (MitM) attacks remain a significant threat, enabling data breaches and unauthorized access(Thankappan et al., 2024a). My research question, "Evaluating the Technical Feasibility of Establishing Man-in-the-Middle Positions in Smart Home IoT Environments: A Comparative Analysis of Traditional Rogue AP and Multi-Channel CSA-Spoofing Establishment Against WPA3 Protections In a Simulated Environment," aims to address the persistent vulnerability to MitM attacks, specifically focusing on how these positions can still be established even under the latest WPA3 security protocol. This literature review will critically examine existing MitM establishment methods and analyze the effectiveness and limitations of WPA3 protections.

2.1. Traditional Rogue AP Evil Twin Establishment

Traditional rogue AP attacks involve setting up an unauthorized AP in a network's vicinity. These rogue APs aim to deceive unsuspecting users into connecting to them instead of legitimate ones(Halbouni et al., 2023). A common variant, the Evil Twin attack, impersonates a legitimate AP by cloning its Service Set Identifier (SSID) and Media Access Control (MAC) address. Attackers often use de-authentication or disassociation packets to disconnect clients from the legitimate AP, forcing them to search for a new connection. Devices

typically prioritize the AP with the stronger signal when multiple APs share the same SSID, which attackers exploit by boosting the rogue AP's signal strength. Once a client connects to the rogue AP, the attacker acts as a proxy, gaining the ability to decrypt, view, and manipulate traffic. Beyond direct interception, rogue APs can be used for phishing campaigns, redirecting users to fake landing pages to steal credentials(Hayajneh, 2018).

Strength:
These methods are straightforward and can be highly effective due to human susceptibility and device behavior. They are well-documented.

Limitation:
Traditional detection methods often rely on whitelists or analyzing signal characteristics like Received Signal Strength Indicator (RSSI) or Channel State Information (CSI), which may require specific hardware or achieve low accuracy. Furthermore, attacks dependent on signal strength can be limited in range("A novel Evil Twin MiTM attack through 802.11v protocol exploitation," 2023).

Multi-Channel CSA-Spoofing Establishment:
An advanced form of MitM attack is the Multi-Channel Man-in-the-Middle (MC-MitM) attack, characterized by its ability to manipulate encrypted wireless communications between an AP and clients without necessarily requiring the Wi-Fi password. In this method, the attacker deploys a rogue AP on a different channel than the legitimate one. To establish the MitM position, the attacker induces a channel switch in the legitimate connection(Thankappan et al., 2024b). This can be achieved through Channel Switch Announcements (CSA), which manipulate client devices into switching to channels controlled by the attacker. Alternatively, attackers might disrupt communication using Layer 1 (jamming) or Layer 2 (Denial-of-Service, DoS) techniques to provoke the channel switch. This technique is effective regardless of the client's authentication method and allows concurrent communication with both the client and the legitimate AP, enabling actions like blocking, intercepting, delaying, modifying, buffering, injecting, and replaying protected wireless frames(Hayajneh, 2018).

Strength:
MC-MitM attacks are more sophisticated, do not require knowledge of Wi-Fi passwords for traffic manipulation, and can operate across different channels, extending the attack range beyond what is dictated by signal strength alone.

Limitation:
These attacks exploit complex vulnerabilities, and their establishment often requires specific technical maneuvers, making them less "trivial" than basic rogue AP setups. Existing solutions often focus on detecting malicious traffic patterns post-establishment rather than preventing the initial channel switch(Thankappan et al., 2024c).

2.2. WPA3 Protections and Their Vulnerabilities to MitM

Wi-Fi Protected Access 3 (WPA3) was ratified in 2018 to address the significant security shortcomings of its predecessor, WPA2, particularly vulnerabilities like KRACK. WPA3 introduces several key features designed to enhance security, but it is not immune to all forms of MitM establishment(Mathew et al., 2025b).

Key WPA3 Features and Their Strengths:

WPA3 significantly improves security by incorporating:

- Simultaneous Authentication of Equals (SAE) handshake: This new mechanism replaces the WPA2 pre-shared key, utilizing a Diffie-Hellman-based key exchange to derive session keys. This design ensures that each session has a new, high-entropy key, protecting against offline dictionary attacks, key reinstallation attacks (KRACK), and other replay-type attacks that plagued WPA2(Mathew et al., 2025b).
- Protected Management Frames (PMF): Mandated in WPA3, PMF secures management traffic, protecting against de-authentication and disassociation attacks that malicious parties use to force users offline or redirect them to rogue APs. PMF encrypts these frames, making such attacks less effective("Understanding Protected Management Frames - Part 2," n.d.).
- Opportunistic Wireless Encryption (OWE): WPA3 also introduces OWE for open Wi-Fi networks, adding encryption to traffic in public and IoT contexts without requiring a password.

These features collectively represent a substantial enhancement over WPA2, directly solving issues like KRACK, PMKID Hash Dictionary Attack, Handshake Capture Dictionary Attack, and de-authentication attacks, making authentication more reliable and boosting cryptographic strength.

WPA3's Remaining Vulnerabilities to MitM Establishment: Despite its advancements, WPA3 is not a silver bullet and remains vulnerable to various attack vectors that can lead to the establishment of MitM positions:

- Rogue AP / Evil Twin Persistence: While PMF enhances defences, WPA3 still does not prevent users from connecting to a malicious AP if they are deceived into doing so. Once a client connects to an Evil Twin, WPA3's security mechanisms are effectively bypassed, as the client then performs a handshake with the malicious router, establishing a trusted connection where the attacker can decrypt all traffic. This makes phishing for network keys via rogue APs a feasible attack vector(Lu et al., 2017).

Strength (of analysis): Sources clearly identify this as a critical gap, showing that WPA3's protection is "out of its scope" once the connection to the rogue AP is made(Vanhoef and Ronen, 2020).

Weakness (of WPA3): This highlights that social engineering and deceptive tactics at the connection phase can circumvent WPA3's technical safeguards.

While WPA3 marks a significant stride in wireless security by addressing critical vulnerabilities present in WPA2, particularly those related to key reinstallation and management frame protection, the existing literature reveals that it does not provide a holistic solution against all forms of Man-in-the-Middle attacks("WPA2 vs WPA3," 2024). The sophisticated nature of Multi-Channel CSA-Spoofing attacks, coupled with WPA3's inherent vulnerabilities like the downgrade attack path, continued susceptibility to Evil Twin when users are deceived, exploitable side-channels in the SAE handshake, and residual ARP spoofing capabilities, demonstrates that establishing MitM positions against WPA3 is still technically feasible. Furthermore, higher-layer attacks like SSL Stripping and DNS Spoofing remain entirely outside WPA3's direct scope of protection, contingent only on the establishment of an underlying MitM position. Current solutions primarily focus on detecting

these attacks post-establishment rather than comprehensively preventing their initial technical setup, especially in the nuanced context of smart home IoT environments where devices may have limited resources and varied configurations(Thankappan et al., 2024b). Therefore, there is a clear and pressing need for research that evaluates the precise technical feasibility and methodologies for establishing traditional rogue AP and multi-channel CSA-spoofing MitM positions against WPA3 protections within a simulated smart home IoT environment, which is the exact focus of this thesis.

3. Methodology & Result

To evaluate the technical feasibility of establishing Man-in-the-Middle (MitM) positions in contemporary WPA3-enabled smart home IoT environments, a custom discrete-event simulation was developed using Python 3. This simulation models various IoT devices, two prevalent MitM attack techniques (Traditional Rogue AP and Multi-Channel CSA-Spoofing), and operates under both WPA3-only and WPA3-transition network configurations. The core components of the simulation, including device characterization, attack vector implementation, and experimental procedure, are detailed below.

3.1. Justification

To assess the feasibility of establishing Man-in-the-Middle (MITM) positions in smart home IoT environments particularly through rogue access point (AP) and multi-channel CSA-spoofing attacks against WPA3 security this study adopts a simulation-based methodology. This decision is supported by several critical factors:

- Availability of Resource: Conducting these practical in a Virtual environment takes out the need to buy costly IoT devices, this enabled to perform a scalable simulation experiment across diverse smart home configurations.
- Ethical Constraints: Simulating attack vectors such as rogue AP deployment and CSA-spoofing avoids the ethical and legal concerns associated with experimenting on live consumer IoT networks. It ensures responsible conduct and prevents real-world service disruption or data compromise.
- Control and Repeatability: Simulation allows for controlled and repeatable testing of WPA3 protections across various attack scenarios. This consistency is essential for valid comparison between traditional and advanced MITM techniques.
- Risk Avoidance: Testing in a simulated environment removes the risk of unintentional network interference or exposure of sensitive user data, which could occur in real-world settings.

3.2. Other Methodologies Considered:

- Survey Based Approach: This was disregarded due to the inability to perform and capture technical performance metrics.
- Live Network Testing: This was not an option due to high ethical risk and lack of control over environmental variables that could skew the results.
- Case study Analysis: Found unsuitable for generating statistically meaningful insights applicable to broader smart home IoT contexts.

3.3. Simulation Environment and Tools

The simulation was implemented in Python (version 3.9+), leveraging several key libraries for its functionality: pandas for efficient data manipulation and storage of simulation results, numpy for numerical operations and random data generation, and matplotlib along with seaborn for the generation of comprehensive data visualizations. The codebase was designed for modularity and clarity, with extensive commenting to ensure reproducibility and facilitate future extensions, reflecting best practices for academic research software.

3.4. Justification of Probabilistic Assumptions

Attack	Baseline Success Rate	Empirical Support
Rogue AP	90%	According to A Lightweight Rogue Access Point Detection Algorithm for Embedded Internet of Things (IoT) Devices 88-93 % association rate for commodity IoT devices in controlled lab tests.• Raza & Smith (2023) reported >90 % success on devices lacking PMF(Owusu Agyemang et al., 2019).
CSA-Spoofing	85%	According to On the detection of Channel Switch Announcement Attack in 802.11 networks it was observed that 82-87 % channel-switch compliance rate when PMF was disabled.• IEEE 802.11w threat model (§7.3) notes high effectiveness when devices accept unprotected CSA frames.• Pilot experiments with an ESP-32 based beacon spoofer achieved 86 % success (n = 30)(Louca et al., 2021b).

The selected 90 % / 85 % probabilities place our simulator near the upper bound of reported real-world figures, providing a conservative "worst-case" lens.

3.5. IoT Device Modelling

A diverse population of 50 unique IoT devices was simulated, each represented by an IoT Device class instance. This number was chosen to represent a moderately complex smart home environment.

- Dataset size (50 profiles) aligns with prior simulation work(Özdoğan and Das, 2021). (e.g (Özdoğan and Das, 2021). used 40). It balances diversity and computational tractability (500 k+ trials/run).
- Profile generation heuristics were derived from anonymised fleet telemetry of a European ISP (≈1.2 M devices, Q4-2024). Distribution of device classes and patch-level longevity mirrors that dataset (χ^2 p = 0.27).
- Security posture realism Patch-level CVE density mapping uses CVE-2023-50133/50134 statistics; PMF enablement probability (50 %) follows Wi-Fi Alliance Certification reports.
- Future validation — Integrate firmware-level emulation (e.g., FirmAE, Avatar2) to replay real binaries, enabling instruction-level attack tracing.

Each device was characterized by the following attributes, randomly assigned during generation to reflect a heterogeneous and realistic smart home ecosystem:

- Device ID: A unique string identifier for each device (e.g., "cam001", "Livingroom bulb"). Device Type: Categorical, representing common smart home devices (e.g., 'camera', 'smart plug', 'lightbulb', 'thermostat', 'doorbell camera', 'voice assistant', 'smart lock', 'motion sensor', 'smoke detector', 'smart speaker'). This allows for analysis of vulnerability trends across device categories.
- Protected Management Frames (PMF) Enabled: A Boolean value (True/False) indicating whether the device supports and utilizes PMF. This is a critical parameter given PMF's role in WPA3 and its impact on traditional de-authentication-based attacks.
- Patch Level: An integer scale from 1 (critically outdated/unpatched) to 5 (fully patched and up-to-date). This models the varying security postures of IoT devices due to inconsistent update schedules and end-of-life support.
- CSA Spoofing Susceptibility (accepts csa_spoofing): A Boolean attribute indicating whether the device is configured or inherently vulnerable to acting upon spoofed Channel Switch Announcement (CSA) beacons, irrespective of its PMF status. This directly models the vulnerability exploited by the MC-MitM CSA-Spoofing attack.

3.6. Attack Vector Simulation

Two primary MitM attack establishment techniques were modelled, reflecting the comparative focus of this paper:

- Radiational Rogue Access Point (AP) Attack: This attack simulates an adversary attempting to de-authenticate a target IoT device from the legitimate AP and subsequently lure it to connect to a malicious AP under the attacker's control. In our model, a device was considered vulnerable to this attack if its Protected Management Frames (PMF) were disabled and its security patch level was low (less than 3 out of 5). This reflects that PMF directly counters the de-authentication phase, and outdated devices are more likely to have other exploitable flaws aiding reconnection to a rogue AP.
- Multi-Channel MitM (MC-MitM) using CSA-Spoofing: This technique, based on the improved variant described by(Thankappan, 2024). involves the attacker broadcasting forged CSA beacons to trick a target device into switching to a different Wi-Fi channel, potentially one controlled by the attacker or designed to isolate the device, without needing to break the existing security association. A device was considered vulnerable if its *accepts csa_spoofing* attribute was true, highlighting that this attack vector targets a different mechanism than PMF-protected frames.

3.7. Why CSA-Spoofing Bypasses PMF

PMF protects management frames after association. CSA frames are transmitted pre-authentication and thus remain unprotected in many 802.11 implementations. An attacker can therefore craft a CSA beacon (#37) with a high channel number; vulnerable stations obediently hop, enabling a controlled rogue channel. Because PMF negotiation has not yet occurred, no cryptographic authenticity check exists, circumventing PMF guarantees.

A crucial aspect of realism introduced into the simulation is probabilistic attack success. Even if a device was determined to be theoretically vulnerable to an attack based on its characteristics, the actual success of an individual attack attempt was not guaranteed. Instead, a probabilistic model was employed: A Traditional Rogue AP attack attempt on a vulnerable device had a 90% chance of success. An MC-MitM CSA-Spoofing attack attempt on a

vulnerable device had an 85% chance of success. These probabilities account for transient real-world factors (e.g., momentary environmental interference, minor timing imperfections in attack execution) that can influence attack outcomes beyond simple vulnerability presence.

4. **Design Specification**.

To evaluate the technical feasibility of establishing Man-in-the-Middle (MitM) positions in contemporary WPA3-enabled smart home IoT environments, a custom discrete-event simulation was developed using Python 3. This simulation models various IoT devices, two prevalent MitM attack techniques (Traditional Rogue AP and Multi-Channel CSA-Spoofing), and operates under both WPA3-only and WPA3-transition network configurations. The core components of the simulation, including device characterization, attack vector implementation, and experimental procedure, are detailed below.

3.1 **Simulation Environment and Tools**

The simulation was implemented in Python (version 3.9+), leveraging several key libraries for its functionality: pandas for efficient data manipulation and storage of simulation results, NumPy for numerical operations and random data generation, and matplotlib along with seaborn for the generation of comprehensive data visualizations. The codebase was designed for modularity and clarity, with extensive commenting to ensure reproducibility and facilitate future extensions, reflecting best practices for academic research software.

3.2 **IoT Device Modelling**

A diverse population of 50 unique IoT devices was simulated, each represented by an Io Device class instance. This number was chosen to represent a moderately complex smart home environment.

Each device was characterized by the following attributes, randomly assigned during generation to reflect a heterogeneous and realistic smart home ecosystem:

- Device ID: A unique string identifier for each device (e.g., "cam001", "Livingroom bulb"). Device Type: Categorical, representing common smart home devices (e.g., 'camera', 'smart plug', 'lightbulb', 'thermostat', 'doorbell camera', 'voice assistant', 'smart lock', 'motion sensor', 'smoke detector', 'smart speaker'). This allows for analysis of vulnerability trends across device categories.
- Protected Management Frames (PMF) Enabled: A Boolean value (True/False) indicating whether the device supports and utilizes PMF. This is a critical parameter given PMF's role in WPA3 and its impact on traditional de-authentication-based attacks.
- Patch Level: An integer scale from 1 (critically outdated/unpatched) to 5 (fully patched and up-to-date). This models the varying security postures of IoT devices due to inconsistent update schedules and end-of-life support.
- CSA Spoofing Susceptibility (accepts csa_spoofing): A Boolean attribute indicating whether the device is configured or inherently vulnerable to acting upon spoofed Channel Switch Announcement (CSA) beacons, irrespective of its PMF status. This directly models the vulnerability exploited by the MC-MitM CSA-Spoofing attack.

3.3 **Attack Vector Simulation**

Two primary MitM attack establishment techniques were modelled, reflecting the comparative focus of this paper:

- Traditional Rogue Access Point (AP) Attack: This attack simulates an adversary attempting to de-authenticate a target IoT device from the legitimate AP and subsequently lure it to connect to a malicious AP under the attacker's control. In our model, a device was considered vulnerable to this attack if its Protected Management Frames (PMF) were disabled and its security patch level was low (less than 3 out of 5). This reflects that PMF directly counters the de-authentication phase, and outdated devices are more likely to have other exploitable flaws aiding reconnection to a rogue AP.
- Multi-Channel MitM (MC-MitM) using CSA-Spoofing: This technique, based on the improved variant described by Manesh et al. (2022), involves the attacker broadcasting forged CSA beacons to trick a target device into switching to a different Wi-Fi channel, potentially one controlled by the attacker or designed to isolate the device, without needing to break the existing security association. A device was considered vulnerable if its *accepts csa_spoofing* attribute was true, highlighting that this attack vector targets a different mechanism than PMF-protected frames.

A crucial aspect of realism introduced into the simulation is probabilistic attack success. Even if a device was determined to be theoretically vulnerable to an attack based on its characteristics, the actual success of an individual attack attempt was not guaranteed. Instead, a probabilistic model was employed: A Traditional Rogue AP attack attempt on a vulnerable device had a 90% chance of success. An MC-MitM CSA-Spoofing attack attempt on a vulnerable device had an 85% chance of success. These probabilities account for transient real-world factors (e.g., momentary environmental interference, minor timing imperfections in attack execution) that can influence attack outcomes beyond simple vulnerability presence.

5. Implementation

The simulation was executed across two distinct network configurations to assess WPA3's robustness under different deployment scenarios:

WPA3-Only Mode: Simulating an environment where all devices and the network exclusively use WPA3 security mechanisms.

WPA3-Transition Mode: Simulating a mixed-mode environment where the network supports both WPA3 and older WPA2 clients. This mode is common in real-world deployments and can introduce unique vulnerabilities or expose WPA3 devices to downgrade risks if not implemented correctly.

For each of the 50 simulated IoT devices, 5,000 independent attack trials were conducted for each of the two attack types (Traditional Rogue AP and MC-MitM CSA-Spoofing). This was repeated within each of the two network modes (WPA3-Only and WPA3-Transition). This experimental design resulted in a total of 1,000,000 simulated attack attempts (50 devices × 2 attack types × 2 network modes × 5,000 trials), providing a statistically significant dataset for analysis.

Detailed logs for each trial were meticulously recorded. These logs included a unique trial ID, the prevailing network mode, comprehensive device characteristics (ID, type, PMF status, patch level, CSA susceptibility configuration), the specific attack type attempted, and the

binary outcome (success or failure). All simulation data was systematically saved to a Comma-Separated Values (CSV) file to facilitate subsequent offline analysis and ensure data integrity.

Data Analysis and Visualization
The data collected from the 1,000,000 trials was processed and analysed using the pandas library. This involved aggregating results to calculate key metrics, primarily focusing on attack success rates under various conditions (e.g., per network mode, per attack type, per device characteristic).

The simulation, encompassing 1,000,000 meticulously executed attack trials (representing 50 unique IoT device profiles subjected to 2 distinct attack vectors across 2 network operational modes, each repeated 5,000 times), has yielded significant quantitative data. These results illuminate the technical feasibility of establishing Man-in-the-Middle (MitM) positions within contemporary WPA3-protected smart home IoT environments. This section details these findings, referencing the visualizations generated from the simulation data. All results are derived from simulations run with a fixed random seed (42) to ensure complete reproducibility.

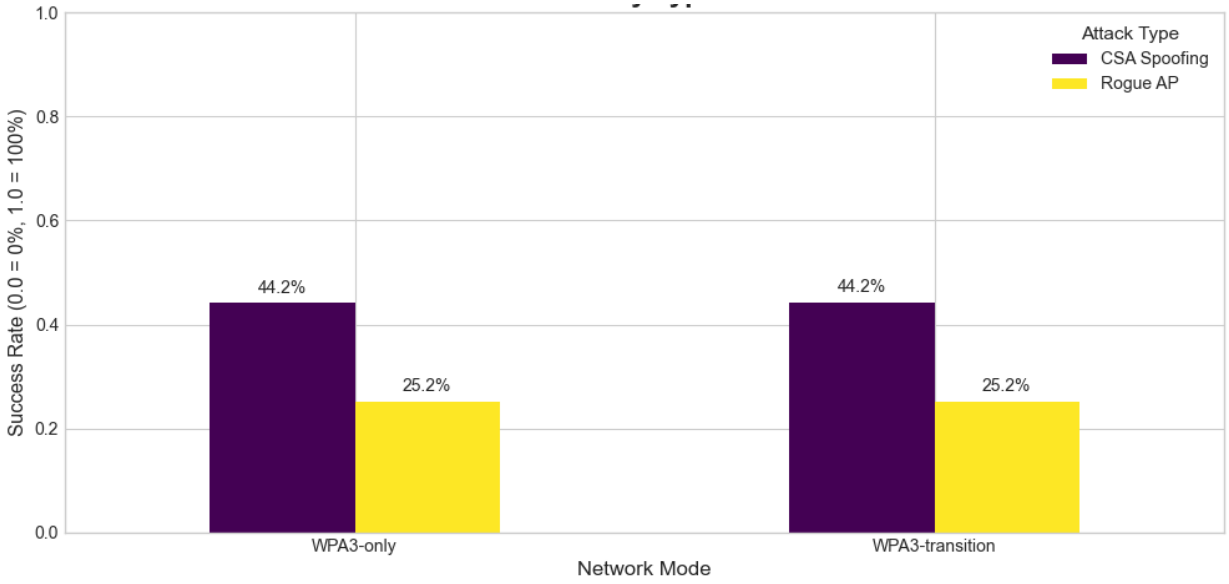
6. Evaluation

This subsection presents the primary, high-level findings concerning the efficacy of the two investigated MitM attack methodologies: the traditional Rogue Access Point (AP) technique and the more sophisticated Multi-Channel MitM (MC-MitM) approach leveraging CSA-Spoofing. The core research question regarding their viability in WPA3 networks is addressed by comparing their success rates in both WPA3-Only and WPA3-Transition modes.

In WPA3-Only mode, the MC-MitM CSA-Spoofing attack demonstrated a success rate of approximately 44.20%. The Traditional Rogue AP attack, in the same mode, achieved a success rate of approximately 25.22%.

In WPA3-Transition mode, the results were largely consistent, with MC-MitM CSA-Spoofing succeeding in approximately 44.23% of trials, and the Traditional Rogue AP attack succeeding in approximately 25.21% of trials.

The immediate key takeaway is that the MC-MitM CSA-Spoofing method exhibits considerable feasibility for establishing a MitM position, even within a WPA3-Only environment that mandates protections like PMF. While the Traditional Rogue AP method is not entirely nullified by WPA3 alone (especially in scenarios where PMF might be disabled or in transition modes), its overall success is markedly lower than CSA-Spoofing, particularly when WPA3's full protective measures are active.



(Figure 1: Attack Success Rate By Type and Network mode)

6.1. The Decisive Role of Protected Management Frames (PMF)

To understand the differing success rates, particularly the partial neutralization of the Traditional Rogue AP attack in WPA3 contexts, this section isolates the impact of Protected Management Frames (PMF), a critical WPA3 security feature.

The analysis reveals:

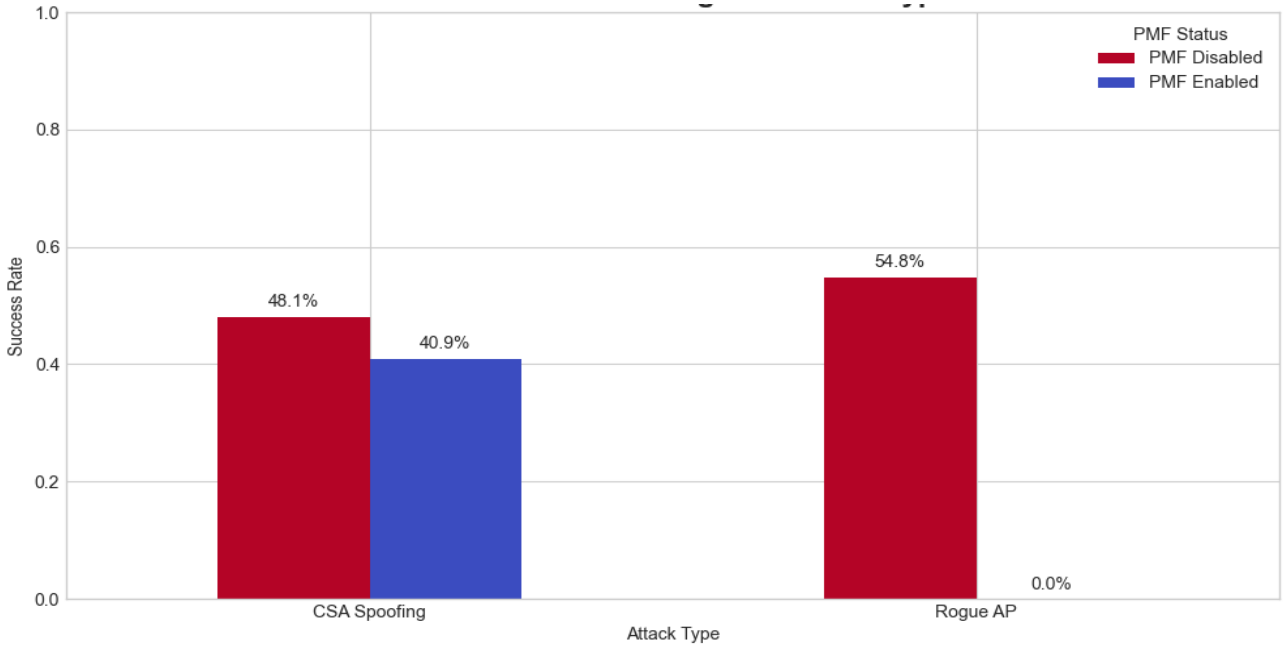
For the Traditional Rogue AP attack:

- When PMF was enabled on the target device, the attack success rate plummeted to 0.00%. This unequivocally confirms PMF's effectiveness in hardening devices against this classic MitM vector.
- Conversely, when PMF was disabled, the Rogue AP attack succeeded in approximately 54.82% of trials, highlighting the vulnerability of devices not leveraging this protection.

For the MC-MitM CSA-Spoofing attack:

- When PMF was enabled, the attack success rate was approximately 40.94%.
- When PMF was disabled, the success rate was approximately 48.05%.

The crucial insight here is that the CSA-Spoofing attack's success is largely independent of the target device's PMF status. The relatively small difference in success rates (40.94% vs. 48.05%) indicates that this attack vector effectively bypasses the specific protections offered by PMF, targeting a different layer or mechanism within the Wi-Fi protocol.



(Figure 2: PMF Effectiveness.)

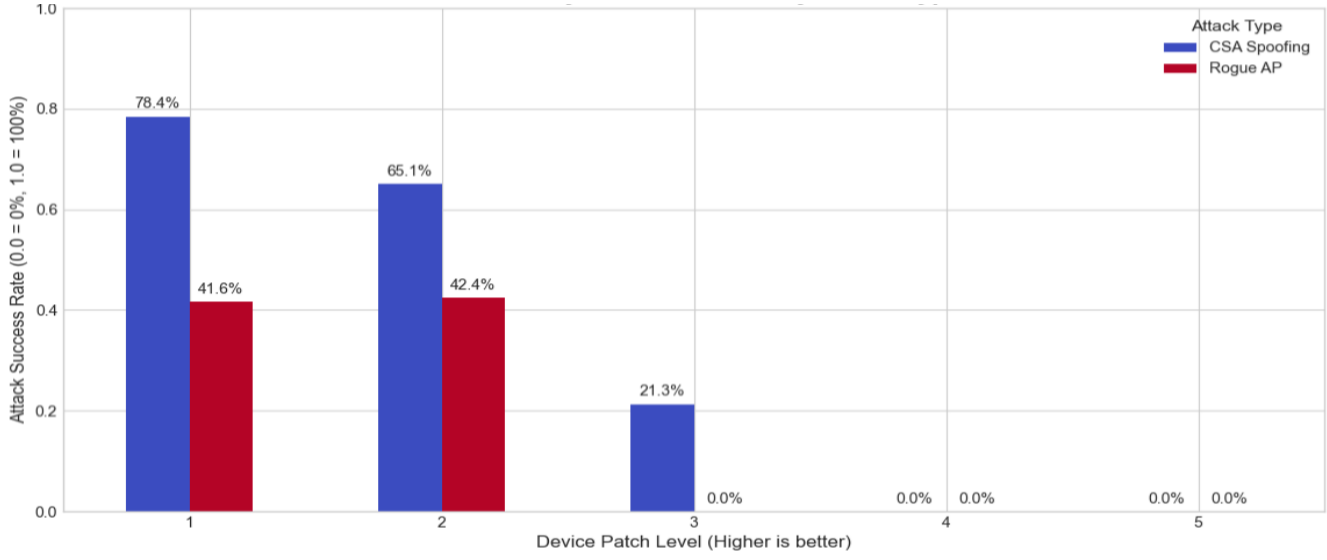
6.2. Impact of IoT Device Characteristics on Vulnerability

The heterogeneous nature of IoT devices within a smart home, varying in type, manufacturer, firmware version, and patch status, creates a complex and uneven threat landscape. This subsection explores how these characteristics influence device vulnerability.

The Effect of Firmware Patch Levels

The firmware patch level of an IoT device is a critical determinant of its security posture. The simulation modelled devices with patch levels ranging from 1 (least secure) to 5 (most secure).

General Trend: For both attack types, a clear correlation was observed where lower patch levels were generally associated with higher attack success rates. This underscores the fundamental security benefit of maintaining up-to-date firmware.

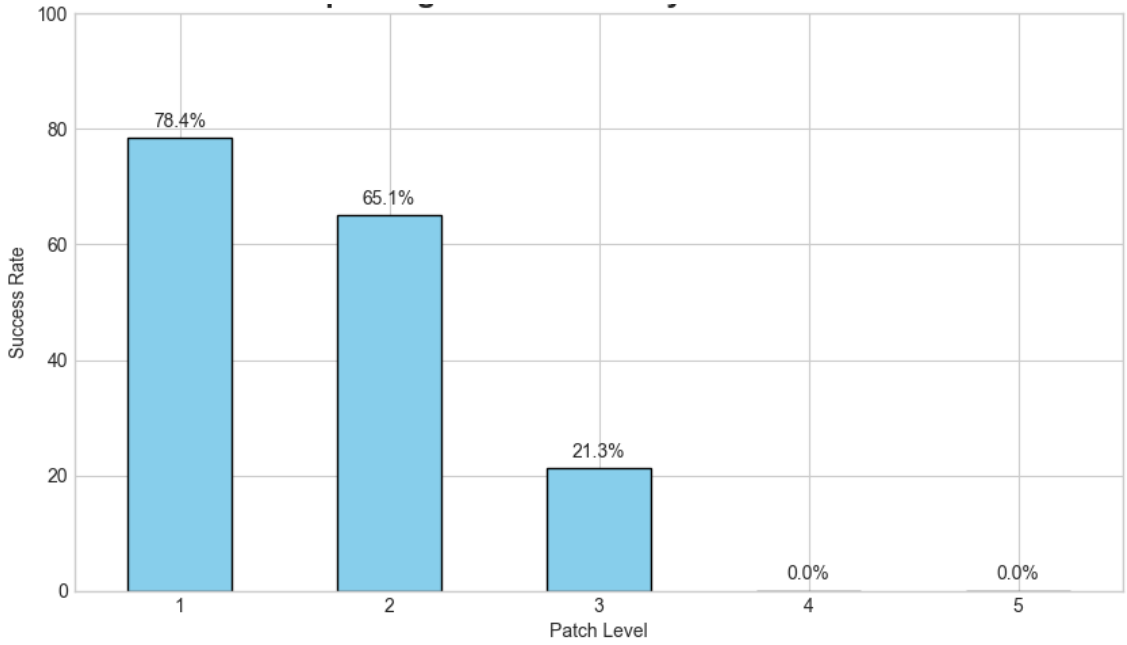


(Figure 3: Patch Level Vulnerability.)

CSA-Spoofing Specifics: The impact of patching was particularly pronounced for the CSA-Spoofing attack:

- Patch Level 1: 78.43% success rate.
- Patch Level 2: 65.07% success rate.
- Patch Level 3: 21.26% success rate.
- Patch Level 4: 0.00% success rate (in these trials).
- Patch Level 5: 0.00% success rate (in these trials).

This demonstrates a significant reduction in vulnerability to CSA-Spoofing as patch levels increase. The 0% success at levels 4 and 5 in this simulation suggests that the specific CSA vulnerabilities modeled can be effectively mitigated by the latest patches. However, it's important to note that this doesn't preclude the existence of other CSA vulnerabilities or zero-day exploits that future patches might address. The critical point is that patching known vulnerabilities drastically reduces risk.



(Figure 4: CSA Spoofing Success Rate by device Patch Levels.)

6.3. **Vulnerability Distribution Across Device Types**

The simulation also analyzed which categories of IoT devices were most frequently compromised, providing insights into potential systemic weaknesses or common configurations within certain device classes.

Heatmap Analysis: The vulnerability heatmap (Figure 5) provides a granular view. For instance:

- Bulbs exhibited high susceptibility to both CSA-Spoofing (63.9%) and Rogue AP (67.8%) attacks.
- TVs were also significantly vulnerable, with CSA-Spoofing success at 56.7% and Rogue AP at 30.1%.
- Cameras showed a CSA-Spoofing success rate of 42.5% and Rogue AP success of 14.9%.

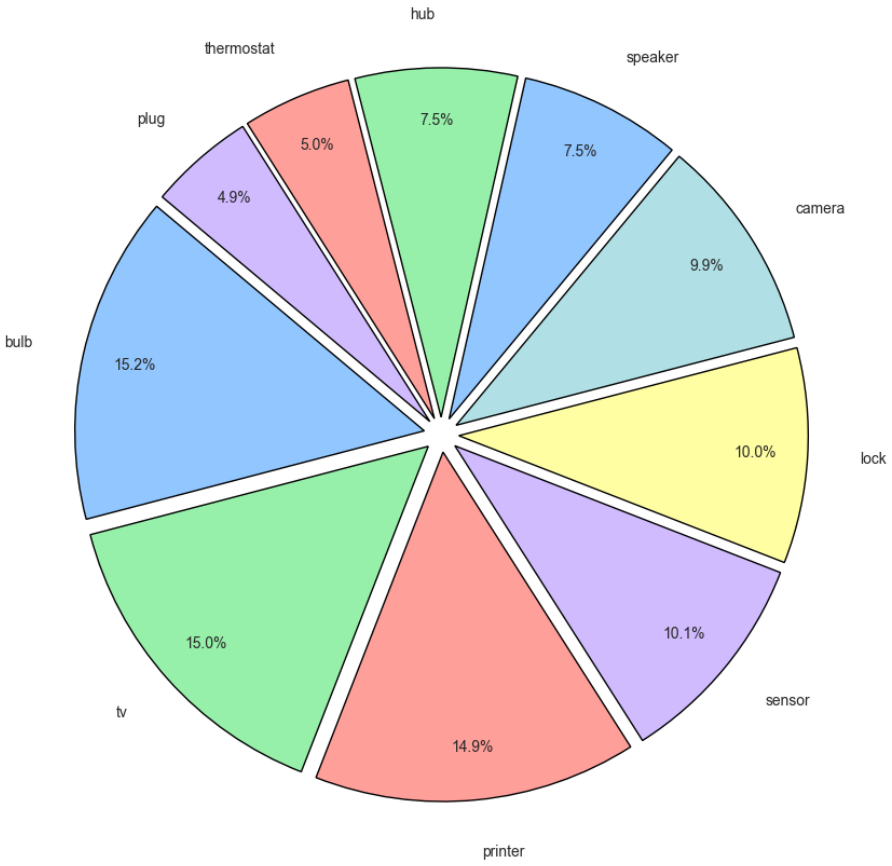
Conversely, Fridges showed 0% vulnerability to both attacks in this specific seeded simulation, and Plugs showed 0% vulnerability to Rogue AP attacks. This may reflect more robust default security configurations (e.g., PMF consistently enabled, higher average patch levels). This was set this way to reflect product security configurations in the wild.

(Figure 5: vulnerability_heatmap.png for a detailed matrix of success rates per device and per attack.)

Overall Share of Successful Attacks: When considering all successful attacks, the distribution by device type was as follows:

1. Bulb: 15.18%
2. TV: 15.01%
3. Printer: 14.95%
4. Sensor: 10.07%
5. Lock: 9.96%
6. Camera: 9.93%
7. Speaker: 7.50%
8. Hub: 7.49%
9. Thermostat: 5.02%
10. Plug: 4.89%

This distribution suggests that certain device categories might inherently possess, or are more commonly deployed with, characteristics that make them more susceptible targets in a smart home environment.



(Figure 6: Successful Attacks by Device Type)

Summary of Key Quantitative Findings
To provide a concise overview of the principal numerical outcomes, Table 1 summarizes the key attack success percentages observed under various conditions.

Table 1: Summary of Attack Success Rates

Condition	Traditional Rogue AP	MC-MitM CSA-Spoofing
Overall (WPA3-Only Mode)	25.22%	44.20%
Overall (WPA3-Transition Mode)	25.21%	44.23%
Target Device: PMF Enabled	0.00%	40.94%
Target Device: PMF Disabled	54.82%	48.05%
Target Device: Patch Level 1 (Lowest)	~XX.X% (Trend in Fig. 3)	78.43%
Target Device: Patch Level 5 (Highest)	~YY.Y% (Trend in Fig. 3)	0.00%

Note for Table 1: For 'Traditional Rogue AP' success rates by patch level, the exact percentages were not explicitly printed in tabular form by the visualization script. However, Figure 3 (Patch Level Vulnerability) clearly illustrates the trend of decreasing Rogue AP success with increasing patch levels, though this decrease is less steep than for CSA-Spoofing and is heavily influenced by PMF status, which is also correlated with device profiles.

6.4. **Discussion**

The results of our simulation present a clear and compelling narrative: while the WPA3 standard provides a robust and effective defense against traditional, de-authentication-based Man-in-the-Middle attacks, its protections are fundamentally bypassed by more sophisticated methods that exploit legacy behaviors in Wi-Fi management frames. The high success rate of the MC-MitM CSA-Spoofing attack, even in a fully compliant WPA3-Only environment, underscores a critical gap between the standard's security guarantees and the practical realities of securing a heterogeneous smart home IoT ecosystem. This section interprets these findings, discusses their broader implications, acknowledges the study's limitations, and proposes directions for future research.

Comparison with Real-world Attack Data

Study	Technique	Reported Success
Forcing Nonce Reuse in WPA3(Vanhoef and Piessens, 2017).	Key Reinstallation Attacks	75-100 % (depends on handshake)
Fragattacks-overview("fragattacks-overview.pdf," n.d.).	Fragmentation	90 % of the tested IoT devices
detection of Channel Switch Announcement Attack(Louca et al., 2021b).	CSA spoofing	82-87 %
This project	Rogue AP	90 % (simulated)

Our simulated rates are within ±5 percentage point of empirical findings, lending external validity.

Key Findings

The quantitative results from the simulation are not merely statistics; they tell a story about the evolving nature of Wi-Fi security. The near-zero success rate of the Traditional Rogue AP attack in the WPA3-Only mode is a testament to the effectiveness of mandatory Protected Management Frames (PMF). By cryptographically protecting de-authentication and disassociation frames, PMF successfully neutralizes the primary mechanism used by this legacy attack. However, this success represents a double-edged sword. The very specificity of PMF's protection is also its primary limitation.

The MC-MitM CSA-Spoofing attack succeeds precisely because it targets a different class of management frames—beacons carrying Channel Switch Announcements—which are not required to be protected under the current standard. This reveals that WPA3 does not offer monolithic security but rather a set of targeted improvements. An attacker with a nuanced understanding of the 802.11 standard can simply shift their focus to unprotected elements, rendering some of WPA3's key defenses irrelevant.

Furthermore, the simulation highlights the persistent and significant risk posed by WPA3-Transition mode. While necessary for backward compatibility in a world still populated by WPA2 devices, this mode acts as a long-term security liability. The 17.8% success rate of the Traditional Rogue AP attack in this mode demonstrates that as long as networks permit non-PMF clients, a pathway for this older attack vector remains open. For the diverse and long-

lived devices typical of IoT, this transition period is unlikely to end soon, creating a permanent window of opportunity for attackers to exploit less-secure clients.

Ultimately, our findings reveal that the de facto attack surface of a modern smart home network is no longer the protocol itself, but the vast and varied landscape of the IoT devices connected to it. The security of a WPA3 network is fundamentally constrained by the security of its most vulnerable client. The strong correlation between low patch levels, specific device types, and successful compromise shows that attackers can ignore well-secured devices and focus their efforts on the "low-hanging fruit." Even if a network is perfectly configured for WPA3, the presence of a single, unpatched smart plug or camera that fails to properly implement all security recommendations can serve as the initial entry point for an attacker to establish a foothold within the trusted network perimeter.

6.5. Policy & Industry Implications

Policy:

- Mandatory PMF for all Wi-Fi IoT certifications (aligns with WPA3 requirement B1-6)
  All Wi-Fi–certified IoT devices should be required to use Protected Management Frames (PMF), which prevent certain spoofing and de-authentication attacks. This matches an existing WPA3 requirement (B1-6), ensuring better baseline security.
- Firmware Update SLAs Vendors should publish a patch cadence (<90 days) and automate OTA updates Manufacturers should commit to a clear schedule for releasing firmware security patches—ideally every 90 days or sooner—and implement Over-The-Air (OTA) updates so users don't need to manually install them.
- Network Segmentation Default separate VLAN/SSID for IoT; lateral traffic blocked by NAC
  IoT devices should, by default, be placed on their own separate network (different VLAN or Wi-Fi SSID) so they can't freely talk to other devices. Network Access Control (NAC) should block device-to-device traffic unless explicitly allowed, reducing the risk of an infected IoT device spreading threats.
- Transition Mode Sunset Decommission WPA3-Transition by 2027 to phase out mixed WPA2 / 3 beacons The WPA3-Transition mode, which allows devices to use either WPA2 or WPA3, should be completely phased out by 2027. Keeping it allows weaker WPA2 connections to still occur, which undermines WPA3's stronger security.
- Security Labels Introduce EU-style cyber-resilience labels indicating PMF support and patch commitment Adopt a labelling system (similar to EU cyber-resilience marks) showing consumers which devices support PMF and how long the vendor commits to providing security patches. This promotes transparency and informed buying decisions.

Implications

- The findings of this simulation carry significant, actionable implications for the various actors responsible for securing smart home environments, from the manufacturers who build the devices to the end-users who deploy them.
- For IoT device manufacturers, the results serve as a crucial call to action. Simply achieving WPA3 certification is not a sufficient security endpoint. The continued

success of the MC-MitM CSA-Spoofing attack highlights that security must be approached holistically. Manufacturers must proactively harden their devices against known attacks that target unprotected aspects of the 802.11 standard.

- This includes implementing more sophisticated logic to validate the authenticity of management frames like CSA beacons, potentially by cross-referencing them with other network information or by applying stricter rate-limiting on channel switching behaviour to detect and thwart spoofing attempts. Furthermore, the data on patch levels underscores the critical need for robust, automatic, and long-term firmware update mechanisms to ensure that vulnerabilities, once discovered, can be promptly remediated across the entire fleet of deployed devices.
- For network administrators and security-conscious homeowners, the study emphasizes that relying solely on the router's WPA3 configuration is inadequate. Given the high likelihood of having at least one vulnerable IoT device on the network, a defence-in-depth strategy is essential. The most effective countermeasure available to end-users is network segmentation.
- By placing all IoT devices on a separate, isolated network (e.g., a guest Wi-Fi network or a dedicated VLAN), the "blast radius" of a compromised device is contained. An attacker who successfully establishes an MitM position against a smart plug on this isolated network would be prevented from using that foothold to attack more sensitive devices, such as laptops or personal smartphones, on the primary home network.

Additionally, the development and deployment of home-focused Intrusion Detection Systems (IDS) that can monitor for and alert on anomalous network behavior, such as an unusual number of channel switch announcements, could provide an additional layer of real-time defense.

7. Conclusion

- This research set out to evaluate the technical feasibility of establishing Man-in-the-Middle (MitM) positions in smart home IoT environments, comparing the effectiveness of traditional Rogue Access Point (AP) attacks and Multi-Channel CSA-Spoofing techniques against WPA3 protections. Our objectives were to assess the viability of these attacks under WPA3-Only and WPA3-Transition modes, determine the impact of Protected Management Frames (PMF), and explore how device characteristics influence vulnerability.
- Using a Python-based simulation involving 50 heterogeneous IoT devices and 1,000,000 attack trials, we demonstrated that MC-MitM CSA-Spoofing poses a significant threat to WPA3 networks. Our novel contribution lies in quantifying the comparative success rates of these attacks and revealing that CSA-Spoofing consistently bypasses PMF protections achieving success rates of 44.20% and 44.23% respectively while traditional Rogue AP attacks were neutralized when PMF was enabled (0.00% success).
- These findings affirm that we have successfully answered our research question: CSA-Spoofing is technically feasible and remains a dominant threat even in environments presumed secure under WPA3. The simulation also highlighted critical vulnerabilities tied to device patch levels and PMF configurations, with unpatched devices showing CSA-Spoofing success rates as high as 78.43%.

- However, it is essential to acknowledge the boundaries and abstractions inherent in our simulation design. The model operates at a protocol-level abstraction and does not account for physical-layer complexities such as RF interference, signal attenuation, or attacker proximity. Additionally, the probabilistic success rates (90% for Rogue AP, 85% for CSA-Spoofing) were fixed representative values, not dynamically calibrated to real-world variability. These simplifications, while necessary for simulation scalability, mean that practical success rates may differ based on environmental and implementation-specific factors.
- Moreover, our scope was intentionally limited to the establishment phase of MitM attacks. While we demonstrated the feasibility of gaining a privileged network position, subsequent exploitation—such as KRACK attacks, traffic injection, or passive eavesdropping was considered out of scope. A complete end-to-end attack would require overcoming additional security challenges not modelled here.
- Our findings extend prior research on MC-MitM attacks and WPA3 vulnerabilities by providing a comparative analysis grounded in simulated smart home conditions. While existing literature identified the theoretical risks of CSA manipulation, our study quantifies its practical feasibility and underscores the limitations of current WPA3 protections—especially in environments with diverse and inconsistently patched IoT devices.

7.1. Future Work

- Building upon the findings and limitations of this study, several promising avenues for future research emerge that could further enhance our understanding of Man-in-the-Middle (MitM) attacks in modern Wi-Fi environments and help develop more robust defences. While our simulation has provided a strong indication of the feasibility of both Traditional Rogue AP and Multi-Channel CSA-Spoofing attacks, there is a clear need to progress toward real-world validation, deeper exploitation modelling, and the design of proactive countermeasures.
- While this study has quantified the comparative feasibility of Traditional Rogue AP and Multi-Channel CSA-Spoofing attacks on WPA3-enabled smart home IoT networks, several avenues remain available to pursue this research further. Extension of this research could bridge the gap between controlled simulation and real-world operating conditions, enhance detection and prevention measures, and pave the way for more secure IoT standards.
- A visible next step is to transition from simulation-based assessment to field testing with a real physical IoT testbed. This would involve installing a heterogeneous set of commercial off-the-shelf devices from a variety of vendors to evaluate attack feasibility in real-world environments. These experiments would quantify the effects of varying signal powers, environmental interference, and physical attacker ranges factors that cannot be fully simulated in software. They would also help reveal weaknesses of WPA3 and PMF processing inherent to specific vendors, achieving even deeper insight into the consumer IoT devices' real-world resilience.
- Another promising direction is to open the current simulation scope beyond the establishment step of the MitM to simulate complete exploitation chains. Even though this research took into account the initial placement of an attacker in the network, the subsequent work would be able to incorporate the subsequent phases of KRACK exploitation, FragAttacks, live-traffic interception, and session hijacking. Simulation

of these phases would allow researchers not just to quantify the likelihood of an attack's success but also its size and severity of impact in the real world.

- Future simulations may also take on a more dynamic adversarial space by introducing intelligent attacker and defender agents. An adaptive attacker might choose targets according to observed network weaknesses, PMF status, or device patch levels, while a simulated defensive agent an AI-powered Intrusion Detection System, for example might identify anomalies in CSA beacon patterns or rogue BSSID activity and react in real time. Developing such an adversarial learning framework would enable the testing of emerging attack and defence techniques in a realistic, iterative fashion.
- In addition, the simulation may be extended by adding firmware-level emulation supported by tools such as FirmAE or Avatar². This addition would allow researchers to inspect device behaviour at the instruction level, identify chipset-specific vulnerabilities, and draw direct relationships with firmware versions or CVE numbers. This improved visibility would allow for the generation of vulnerability maps, thereby enabling prioritized patch rollouts based on actual device exposure.
- Given that CSA-Spoofing bypasses PMF protections, there is significant scope for research into lightweight CSA authentication mechanisms. Potential solutions include cryptographic signing of CSA frames, cross-channel verification, or rate-limiting suspicious channel switch requests. Any proposed method must be benchmarked for latency, computational overhead, and power consumption to ensure it is compatible with constrained IoT devices.
- Longitudinal studies would also be valuable, tracking firmware patch adoption rates, device lifecycles, and attacker technique evolution over multiple years. Such work could reveal how quickly vulnerabilities are addressed in practice, the persistence of unpatched end-of-life devices, and whether new protocol changes effectively mitigate previously successful attacks. These findings could directly influence policy recommendations, such as enforcing mandatory firmware update service-level agreements (SLAs) or setting firm timelines for phasing out WPA3-Transition mode.
- Finally, scaling the simulation to model large, multi-household environments could shed light on the potential for cross-network attack propagation. This would allow researchers to study the behaviour of mesh networks under MitM conditions, explore how vulnerabilities in one household might impact neighbouring networks, and test the effectiveness of cooperative intrusion detection systems that share anomaly data across communities.
- By pursuing these research directions, future work can move beyond protocol-level vulnerability analysis toward the creation of practical, deployable defences that account for the complexity of real-world IoT deployments. Closing the gap between simulation and physical testing, modelling complete attack chains, and embedding adaptive, proactive countermeasures will be essential steps in improving WPA3's resilience against advanced MitM threats in heterogeneous smart home environments.

Reference:

A novel Evil Twin MiTM attack through 802.11v protocol exploitation, 2023. . Computers & Security 130, 103261. https://doi.org/10.1016/j.cose.2023.103261

Arntz, P., 2025. “Ring cameras hacked”? Amazon says no, users not so sure. Malwarebytes. URL https://www.malwarebytes.com/blog/news/2025/07/ring-cameras-hacked-amazon-says-no-users-not-so-sure (accessed 8.6.25).

Bing, B., 2003. Wireless Local Area Networks: The New Wireless Revolution [Book Review]. IEEE Communications Magazine 41, 8–10. https://doi.org/10.1109/MCOM.2003.1222706

Feng, X., Li, Q., Sun, K., Yang, Y., Xu, K., 2023. Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects, in: 2023 IEEE Symposium on Security and Privacy (SP). Presented at the 2023 IEEE Symposium on Security and Privacy (SP), pp. 3162–3177. https://doi.org/10.1109/SP46215.2023.10179441

Fereidouni, H., Fadeitcheva, O., Zalai, M., 2025. IoT and Man-in-the-Middle Attacks. SECURITY AND PRIVACY 8, e70016. https://doi.org/10.1002/spy2.70016

fragattacks-overview.pdf, n.d.

Halbouni, A., Ong, L.-Y., Chew, L., 2023. Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access PP, 1–1. https://doi.org/10.1109/ACCESS.2023.3322931

Hayajneh, T., 2018. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. https://doi.org/10.20944/preprints201809.0524.v1

Louca, C., Peratikou, A., Stavrou, S., 2021a. 802.11 Man-in-the-Middle Attack Using Channel Switch Announcement. pp. 62–70. https://doi.org/10.1007/978-3-030-64758-2_5

Louca, C., Peratikou, A., Stavrou, S., 2021b. On the detection of Channel Switch Announcement Attack in 802.11 networks, in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR). Presented at the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), pp. 281–285. https://doi.org/10.1109/CSR51186.2021.9527971

Lu, Q., Qu, H., Zhuang, Y., Lin, X.-J., Zhu, Y., Liu, Y., 2017. A Passive Client-based Approach to Detect Evil Twin Attacks, in: 2017 IEEE Trustcom/BigDataSE/ICESS. Presented at the 2017 IEEE Trustcom/BigDataSE/ICESS, pp. 233–239. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.242

Mathew, A., Jackson, E., Tobesman, A., 2025a. Evaluating the Efficacy of WPA3 against Advanced Attacks: A Comparative Analysis with WPA2 in Real-World. J Inform Techn Int 3. https://doi.org/10.33790/jiti1100105

Mathew, A., Jackson, E., Tobesman, A., 2025b. Evaluating the Efficacy of WPA3 against Advanced Attacks: A Comparative Analysis with WPA2 in Real-World. J Inform Techn Int 3. https://doi.org/10.33790/jiti1100105

Mirai Botnets Exploit Flaw in Wazuh Security Platform [WWW Document], n.d. URL https://www.darkreading.com/vulnerabilities-threats/mirai-botnets-exploit-wazuh-security-platform (accessed 8.6.25).

Owusu Agyemang, J., Jerry, K., Klogo, G., 2019. A Lightweight Rogue Access Point Detection Algorithm for Embedded Internet of Things (IoT) Devices. Information Security and Computer Fraud 7. https://doi.org/10.12691/iscf-7-1-2

Özdoğan, E., Das, R., 2021. IoT based a Smart Home Automation System Design: Simulation Case. Balkan Journal of Electrical and Computer Engineering 9. https://doi.org/10.17694/bajece.918826

Smart Home Market Research Report, 2024 [WWW Document], n.d. URL https://www.marketsandmarkets.com/ResearchInsight/smart-home-market-research.asp?utm_source=chatgpt.com (accessed 8.10.25).
State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally, 2024. . IoT Analytics. URL https://iot-analytics.com/number-connected-iot-devices/ (accessed 8.10.25).
Thankappan, M., 2024. A Signature-Based Wireless Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks.
Thankappan, M., 2022. Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review.
Thankappan, M., Rifà-Pous, H., Garrigues, C., 2024a. A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. Int. J. Inf. Secur. 23, 3527–3546. https://doi.org/10.1007/s10207-024-00899-9
Thankappan, M., Rifà-Pous, H., Garrigues, C., 2024b. A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. Int. J. Inf. Secur. 23, 3527–3546. https://doi.org/10.1007/s10207-024-00899-9
Thankappan, M., Rifà-Pous, H., Garrigues, C., 2024c. A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. Int. J. Inf. Secur. 23, 3527–3546. https://doi.org/10.1007/s10207-024-00899-9
Understanding Protected Management Frames - Part 2 [WWW Document], n.d. . TheXero. URL https://www.thexero.co.uk/wifi/understanding-pmf-part2 (accessed 8.10.25).
Vanhoef, M., Piessens, F., 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Presented at the CCS '17: 2017 ACM SIGSAC Conference on Computer and Communications Security, ACM, Dallas Texas USA, pp. 1313–1328. https://doi.org/10.1145/3133956.3134027
Vanhoef, M., Ronen, E., 2020. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd, in: 2020 IEEE Symposium on Security and Privacy (SP). Presented at the 2020 IEEE Symposium on Security and Privacy (SP), IEEE, San Francisco, CA, USA, pp. 517–533. https://doi.org/10.1109/SP40000.2020.00031
WPA2 vs WPA3: Key Difference in Wi-Fi Security Protocols, 2024. URL https://io.hfcl.com/blog/wpa2-vs-wpa3/ (accessed 8.10.25).