applied sciences

MDPI

Article

A Novel Covert Channel for IEEE 802.11 Networks Utilizing MAC Address Randomization

Geovani Teca [†] **and Marek Natkaniec** [*,†]

Institute of Telecommunications, AGH University of Science and Technology, al. Mickiewicza 30, 30-059 Krakow, Poland; teca@agh.edu.pl
* Correspondence: natkanie@agh.edu.pl
† These authors contributed equally to this work.

Abstract: Vendors implement the MAC address randomization technique to prevent IEEE 802.11 client station devices from being tracked. Although it conceals device identity, it cannot hide its occurring data transmission. This paper presents a novel covert channel that leverages the MAC address randomization technique to create a covert channel to hide data transmission inside IEEE 802.11 networks. The secret data are a disposable random MAC address generated by the IEEE 802.11 station as part of the probe request frame while scanning the network. The paper presents the concept of the covert channel, its implementation, and performance metrics. The study covers diverse scenarios, including the adaptation of the modified Selective Repeat ARQ protocol to alleviate the impact of the number of client stations and their offered loads on the covert channel. The results show that with the appropriate parameter selections, we can adapt the covert channel to produce excellent throughput, efficiency, delay, and jitter according to the environment in which it is installed.

Keywords: IEEE 802.11 networks; covert channels; MAC address randomization; ARQ protocol

Citation: Teca, G.; Natkaniec, M. A Novel Covert Channel for IEEE 802.11 Networks Utilizing MAC Address Randomization. *Appl. Sci.* **2023**, *13*, 8000. https://doi.org/10.3390/app13148000

Academic Editor: Juan-Carlos Cano

Received: 18 June 2023
Revised: 5 July 2023
Accepted: 6 July 2023
Published: 8 July 2023

1. Introduction

As time has progressed, there has been a significant proliferation in the number of mobile devices connected to the Internet. Wireless local area networks (WLANs) are the predominant solution to guarantee Internet connection for those devices. WLANs constitute a fundamental infrastructure for building smart cities, enabling the Internet of Things (IoT), machine-to-machine (M2M) communication, and network traffic offloading from cellular networks, such as LTE and 5G. A forecast anticipates that there will be approximately 628 million public Wi-Fi hotspots by 2023 compared to 169 million hotspots in 2018 [1].

The IEEE 802.11 standard [2] defines the protocols for the physical (PHY) layer and medium access control (MAC) layer for a WLANs, commercially known as Wi-Fi. The PHY describes techniques to regulate transmission rates, while the MAC specifies the procedures for channel access control and frame formats. An access point (AP) bridges client stations (STAs) to the Internet within a WLAN. The STAs associated with an AP form the basic service set (BSS), and before joining the BSS, an unassociated STA has to discover the network by scanning the wireless channel. The standard defines two methods for channel scanning. The first method is passive scanning, where the STA listens to beacon frames transmitted by the AP on the channel. However, passive scanning is disadvantaged due to the longer beacon interval, typically 100 milliseconds (ms). If an STA has a short beacon timeout, it may miss beacons, prolonging the scanning process. The second scanning method is active scanning, in which the STA broadcasts probe request (PR) frames and waits for probe responses from the AP. The STA sends PR frames using its unique global MAC address in plaintext, revealing its presence and identity within a specific geographical area. This information can be processed by anyone with a device capable of collecting WLAN traffic, potentially without the user's consent, and based on the user location pattern, third parties might use the information for various purposes, such as creating

a user profile [3,4]. Wi-Fi networks are susceptible to various security threats, including unauthorized access, data interception, network spoofing, and malicious attacks targeting vulnerabilities in routers, bridges and client devices [5,6]. To conceal the device identity and enhance user privacy, modern Wi-Fi devices use disposable random MAC during the scanning process [7].

One particularity of the IEEE 802.11 standard is that devices share the transmission channel [8,9]. Each device can detect when the channel is busy. As a result, there are no hidden or secret data transmissions. However, devices can create covert channels to conceal their transmissions from other devices. A covert channel is a communication channel that operates without interfering with normal network operations, enabling secret data transmission between two endpoints. Covert channels in IEEE 802.11 are implemented in both the PHY and MAC layers by leveraging specific features of each layer. The primary objective of implementing covert channels in WLANs is to enhance data protection and privacy, providing additional security for sensitive information.

This article comprehensively analyzes an IEEE 802.11 covert channel that utilizes MAC address randomization. The study aims to assess the performance of this covert channel and introduces a transmission technique to mitigate the effect of external traffic on it. The research contributions of this study are multi-faceted:

- Updated analysis of MAC address randomization—We provide an up-to-date analysis of MAC address randomization and its significance in the context of covert channels. This analysis offers a comprehensive understanding of the technique's relevance and implications.
- Novel approach to IEEE 802.11 covert channel—We propose and implement a novel approach for covert channels by integrating MAC address randomization within the PR frame. This approach enhances the covert channel's functionality and provides a unique perspective on covert communication.
- Focus on reliability—Unlike many existing covert channel implementations, we emphasize the importance of reliability. Our study addresses the need for robust message transmission and reception to ensure the covert channel's successful operation. This aspect fills a crucial gap in current covert channel research.
- Novel approach to optimize the performance of IEEE 802.11 covert channel—We present a concept and implementation of the modified Selective Repeat ARQ protocol within the covert channel to prevent network congestion generated by the covert channel traffic and maintain QoS metrics at the appropriate level.
- Scenario-based evaluation—We examine the results of three distinct scenarios and provide an evaluation of each. We identify and recommend the most appropriate approach for effective covert communication by considering various network conditions.

This study offers a comprehensive analysis of an IEEE 802.11 covert channel, introduces transmission techniques for dense environments, and bridges gaps in existing covert channel implementations. The findings contribute to the broader understanding of covert communication and provide practical insights for enhancing covert channel performance in real-world scenarios.

The article is structured into nine sections, each addressing specific aspects of the research topic. Section 2 highlights the existing IEEE 802.11 covert channels. Section 3 explores the MAC address randomization technique in detail, including emergence, current status, and plans. The proposed covert channel, presenting the underlying concept and providing in-depth details about its implementation, is introduced in Section 4. Section 5 evaluates the performance of the covert channel in two distinct scenarios, assessing metrics such as throughput, efficiency, delay, and jitter. Section 6 describes the modified Selective Repeat ARQ protocol, its adaptation and integration into the covert channel, discussing the benefits and implications of this implementation. The results of Selective Repeat ARQ protocol integration, showcasing the performance improvements achieved and analyzing the findings, are presented in Section 7. Section 8 discusses the overall results and the uniqueness of the covert channel. Finally, Section 9 concludes the work by summarizing the

key findings, highlighting the significance of the research, and outlining potential directions for future research and advancements in the field.

2. State of the Art

Over the years, extensive research has been conducted to develop various covert channel techniques by leveraging different aspects of the MAC and PHY. The primary objective of these studies is to enhance the effectiveness, transparency and improve the undetectability of covert channels. Two reconnection-based covert channel methods are presented in the research paper [10]. The first method involves transmitting covert data by manipulating the behavior of STAs, without direct communication between the covert sender and receiver. Each STA denoted as S_i, is associated with a secret message M_i. To encode the secret message, the sender induces a reconnection in STA_i, and the covert receiver monitors the network to detect the reconnection event and subsequently decodes the secret message M_i. In the second method, the covert sender and the STAs are directly interconnected through physical wires, with one wire dedicated to downlink communication and another for uplink communication. To transmit the secret message M_i, the sender triggers a reconnection in STA_i by sending a high-voltage level pulse through the corresponding wire.

The research paper [11] introduces a covert channel that utilizes the order of frame transmissions to encode secret messages. In this covert channel scheme, if Station STA_1 transmits a data frame before STA_2, it is interpreted as the transmission of bit 0. Conversely, if the transmission occurs in the reverse order, it represents the encoding of bit 1. This approach requires a minimum of two STAs, and each transmission encodes a single secret bit of information.

The paper [12] introduces a ternary timing covert channel. This covert channel operates by leveraging statistical analysis of the free time intervals within the channel, which both the sender and receiver collect. The information derived from this analysis is then utilized to conceal and decode secret messages. The time interval is divided into three subsets in the ternary timing covert channel. For the sender, these subsets are denoted as H_S^0, H_S^1, and H_S^2, corresponding to the time intervals used to encode trits 0, 1, and 2, respectively. Similarly, for the receiver, the subsets are denoted as H_R^0, H_R^1, and H_R^2, representing the time intervals used to decode trits 0, 1, and 2, respectively. For instance, to transmit a trit 0, the receiver selects a slot s from the subset H_S^0 and waits for s time slots before initiating the transmission. In essence, the sum of the waiting time between consecutive transmissions must be equal to the chosen slot s.

The research presented in [13] presents a covert channel that utilizes the interarrival time of PR or beacon frames. This covert channel enables the encoding of hidden messages in two distinct forms. In the first method, the sender and receiver establish a shared lookup table, where each time interval is associated with a secret message. The sender generates frames with a matching time interval from the lookup table to encode a particular message. The second encoding method in this covert channel involves introducing variations in the time intervals between consecutive frames. Similar to the first method, each variation corresponds to a secret message in the lookup table. The sender encodes the data by generating frames with different time intervals that align with the appropriate message from the lookup table.

The study [14] introduces a practical timing covert channel that leverages the beacon interval (BI). This covert channel enables the encoding and transmission of a secret message from an access point (AP) to a station (STA). The AP encodes the secret message in this method by intentionally introducing a time delay, denoted as δ, in the BI. Specifically, a delay of δ is employed to encode a bit value of 0, while an acceleration of δ is used to encode a bit value of 1.

The work in [15] presents a covert channel that utilizes the supported rates field in PR frames. The supported rates field contains information about the data rates supported by STA or AP and is typically used to ensure compatibility between both devices. The covert channel encrypts secret data in the most significant bit (MSB) of the supported rates field

while transmitting PR frames. Instead of the STA genuinely scanning for available networks, its primary focus is to send covert data. Another approach that modifies the content of the MAC header is presented in [16]. This covert channel technique encodes the secret message within the two-bit protocol version field. It exploits the fact that the 802.11 standards currently allocate only one specific value (binary 00) to this field, while the remaining three combinations (binary 01, 10, 11) are left unused. This allows a covert channel by utilizing unused combinations to transmit hidden information.

Analyzing the current state of IEEE 802.11 covert channels, the focus has mainly been establishing the possibility of creating a covert channel rather than its bandwidth. Our contribution introduces the pioneering concept of an IEEE 802.11 covert channel that utilizes a random MAC address as the secret message, providing a significant bandwidth of 48 bits per frame, high throughput, and minimal delay. This novel covert channel can be replicated in simulated environments and real-life Wi-Fi device drivers, marking a significant advance in the field.

3. MAC Address Randomization

3.1. IEEE 802.11 MAC Address

IEEE 802.11 devices have a unique Layer-2 identifier known as the MAC address. This address identifies the device as the source of a transmitted frame and allows for proper frame processing upon arrival. A MAC address comprises 6 bytes, and its uniqueness is ensured through a hierarchical structure. At the top level, the responsibility of MAC address registration lies with the IEEE Registration Authority (IEEE RA) [17]. The IEEE RA assigns a block of addresses, MAC-Address Block Large (MA-L) or Organizationally Unique Identifiers (OUIs), consisting of 3 bytes. These blocks are then sold to specific manufacturers of IEEE 802.11 devices. Each manufacturer subsequently assigns the remaining 3 bytes to ensure global uniqueness for every network interface controller (NIC) they produce. To optimize the utilization of the available OUI pool, the IEEE Registration Authority (IEEE RA) provides manufacturers with the option to acquire a 3-byte company identifier (CID) for certain connections where a globally unique MAC address is not essential, such as in the case of active scanning. The MAC address format is structured as follows: the first 3 bytes represent the organizationally unique identifier (OUI), while the last 3 bytes denote the network interface controller (NIC) as illustrated in Figure 1. Unicast and multicast addresses can be differentiated based on the value of the least significant bit (LSB) in the first octet, where a clear bit indicates a unicast address. The distinction between global (OUI) and local (CID) MAC addresses is determined by the state of the second LSB in the first octet, with a set bit indicating a globally unique address.

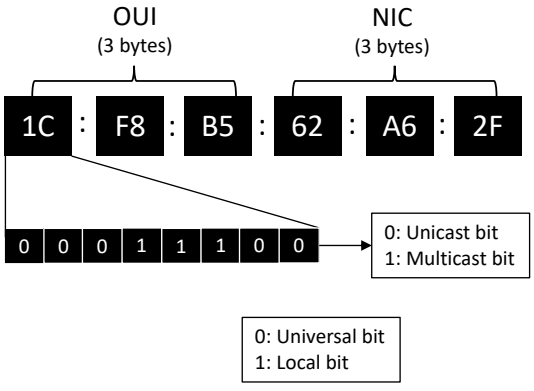

Figure 1. MAC address format.

3.2. User Information Disclosure through MAC Address

Figure 2 presents the format of the PR frame, which allows a STA to discover a proper BSS. This frame consists of a header and a body section. Of particular interest within the header is the source address (SA), which reveals the globally unique MAC address

of the device. It is important to note that the MAC address goes beyond identifying the device's vendor. It can potentially reveal an individual's identity, posing privacy concerns. Moreover, the MAC address enables data collection for various purposes, which we address in this research by highlighting the most prevalent cases.

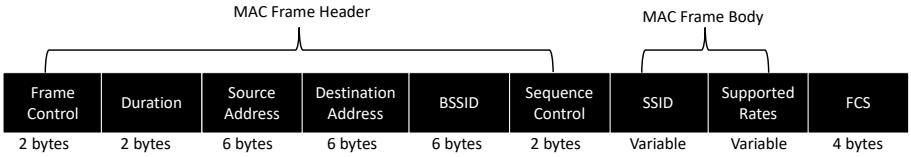

Figure 2. IEEE 802.11 probe request frame structure.

The experiments conducted in [18] reveal concerning findings regarding the frequency of Wi-Fi device probing and the disclosure of their unique identifiers. The study demonstrates that devices send PRs at a high rate, increasing the number of PRs as the device recognizes more SSIDs. Interestingly, devices continue broadcasting PRs even when connected to a specific BSS. The study concludes that some devices generate approximately 55 PRs per hour. Studies have shown that malicious third parties can exploit the broadcast of user device unique identifiers to collect data, build user profiles, and track individuals across multiple locations with precision. These activities occur without the users' endorsement or consent as highlighted in [19–21].

The work presented in [4] introduces two attacks designed to track individuals by linking them to their MAC addresses. The first attack is known as the beacon replay attack. In this attack, the adversary collects SSIDs from a specific geographic area, such as residential neighborhoods, and replicates them by broadcasting fake beacons in different locations, such as workplaces or stadiums. The goal is to bait devices to send probe requests revealing their MAC addresses. This method assumes that the likelihood of two individuals sharing the same MAC address, residing at the same home address, working at the same place, or attending the same event is significantly low. The second attack is called the stalker replay attack. As the name implies, once the target has been identified, the attacker follows the target for a specific duration, collecting Wi-Fi data emitted by their devices. The collected data are then analyzed, and the MAC address with the highest frequency during this period is considered the victim's MAC address.

The study [22] introduces a novel model for estimating the presence of individuals within a scanning area. The model utilizes a specialized tool called Sherlock [23] to capture probe requests (PRs) transmitted by mobile devices. The model can detect and track the user's arrival, presence, and departure from the monitored area by analyzing the PR parameters. The detection process begins by identifying the first probe request from a user's device. To confirm the user's presence, the monitor waits for subsequent probe requests with the same source MAC address within a specified time window of A_T slots. The system confirms the user's presence if additional probe requests are received within this time window. On the other hand, if no probe request is detected from the user's device after the designated time slot, the system considers it a potential departure. Confirmation of departure is made after a defined period of D_T slots elapses without detecting any further probe requests from the user's MAC address.

The article [24] presents a comprehensive system designed to collect, store, and analyze PR frames to estimate crowd density and track user movements in indoor environments. The system comprises specialized software on dedicated hardware that monitors the WLAN and cloud-based services that facilitate data collection, storage, and analysis. The system also includes a dashboard to visualize and present the analyzed data. By capturing and analyzing PRs, the system can calculate crowd density within the monitored area. Specifically, for devices that remain in the vicinity for 2 to 3 min, the collected PRs provide sufficient data to estimate crowd density accurately.

The study [25] introduces two passive analysis methods, namely service set identifier (SSID) analysis and inter-frame arrival time analysis (IFAT), for device identification using

PR frames. These methods leverage the MAC address as a key parameter in the PR frames and other associated values. The first method focuses on SSID fingerprinting, where the MAC address is linked to the SSID contained within the probe request. User behavior or location can be inferred by analyzing the SSID, which often provides information about commercial spots, public places, or private property addresses. The study demonstrates that the SSID fingerprinting method accurately achieves an efficiency rate of 73.19%. The second method, IFAT analysis, examines the inter-frame arrival time values within the probe requests. Unique device characteristics can be extracted by analyzing the timing patterns between successive PR frames. However, the study shows that the IFAT fingerprinting method has a lower efficiency rate of 33.73% compared to SSID fingerprinting.

The study [26] explores utilizing Wi-Fi data for estimating passenger mobility on buses. To facilitate this, buses have Wi-Fi sensors that continuously collect real-time data. Each data capture includes the MAC address, signal strength, and timestamp, which are stored alongside GPS coordinates and timestamps in separate files. These files link the Wi-Fi and GPS data, enabling the analysis of passenger movements. A similar approach is demonstrated in the research [27], where Wi-Fi data are employed to estimate the number of passengers using public transportation. This method relies on identifying devices based on probe requests transmitted during discovery. In this case, the buses are equipped with multiple sensors, and the accuracy of determining whether a device is inside the vehicle depends on factors such as the frequency of MAC addresses and additional sensor information. To map user movements on a map based on MAC addresses, a combination of Wi-Fi and GPS data is employed as outlined in the research [28]. This integration allows for visualizing user trajectories and their corresponding MAC addresses.

3.3. MAC Address Randomization Implementation

MAC address randomization enhances user privacy by generating frames with temporary and disposable source MAC addresses, thereby concealing the device's global MAC address. By decoupling the MAC address from the user device, MAC randomization adds a layer of security, preventing the disclosure of user information through the global MAC address. As depicted in Figure 1, MAC randomization is achieved by setting the second most significant bit (MSB) in the first octet of the MAC address. The implementation of MAC address randomization by the major's OS vendors is as follows:

- Apple Inc. from iOS 8, 2014 [29].
- Linux from Kernel version 3.18, 2014 [30].
- Google LLC from Android 6.0 Marshmallow, 2015 [31].
- Microsoft Corporation from Windows 10, 2016 [32].

Over time, MAC randomization techniques have experienced significant improvements. As of the writing of this article, each operating system (OS) has implemented its approach to MAC randomization. Windows 11, for instance, now has MAC randomization enabled by default and offers two randomization options. Users can either have a single random MAC address for connecting to all networks or utilize one random MAC address specific to a particular network. In the case of iOS devices, MAC randomization is enabled by default starting from iOS 14. The generated random MAC address remains associated with the SSID, even after reconnection. If the device forgets the SSID and reconnects, a new MAC address is generated for that specific connection. Similarly, Android devices running Android 10 or higher also have MAC randomization enabled by default. The random MAC address is linked to the SSID and persists even after reconnection. If the device forgets the SSID and reconnects, the same random MAC address is utilized to establish the connection. In Linux systems, a random MAC address is generated for each SSID. If the device forgets the network, Linux generates a new random MAC address when reconnecting to that network.

Various studies focusing on MAC randomization have revealed inconsistencies in the schemes employed by different devices. Some devices adopt a fixed company identifier (CID) while randomizing the remaining 24 bits of the MAC address. Others choose to

randomize the entire 48 bits while setting the local bit. In contrast, some devices even randomize the complete MAC address using the organizationally unique identifier (OUI), thereby giving the appearance of a global address when it is not the case [7]. During this research, MAC address randomization lacked a standardized approach. In addition to the various schemes, implementing MAC randomization has evolved over the years, showcasing varying deployment strategies across devices. Observations indicate that devices may employ randomization consistently, only in idle states, in a mixed manner using both global and local addresses, or not at all, with the specific approach depending on the device vendor [33].

3.4. Not as Random as It Appears

Recent studies have delved into various aspects of MAC address randomization, including its effectiveness and techniques for resolving to a global address. The research [34] focused on demonstrating that MAC address randomization alone does not guarantee privacy. The study revealed that when combined with predictable sequence numbers, the PR information elements (IEs) in MAC addresses create a device fingerprint that allows tracking of the device, even in the presence of MAC randomization. The report indicated that approximately 50% of devices could be tracked for up to 20 min. In addition, the authors proposed several attack techniques, including fake AP attacks, karma attacks, and hotspot 2.0 honeypot attacks. In the karma attack, a fake AP broadcasts a known SSID, anticipating that the victim device, while scanning using a random MAC address, will associate with the network using its global MAC address (a behavior observed in many devices). In the hotspot 2.0 [35] attack, the fake AP is configured to provide minimal information in the beacon frames, prompting the STA (station) to send an access network query protocol (ANQP) request. When the STA transmits the ANQP request, it uses a unique MAC address, and the frame also contains a dialog token field that can be predicted.

The research outlined in [36] sheds light on the limitations of MAC address randomization. While using a random MAC address can obscure the true identity of a device, it does not guarantee protection against tracking. The authors identified two specific attacks that exploit vulnerabilities in MAC randomization: content-based attacks and timing-based attacks. Content-based attacks exploit the predictability of certain fields within the PR frame, such as the sequence number, OFDM scrambler seed, and information elements (IEs). By analyzing these elements, adversaries can overcome MAC randomization and track the device. On the other hand, timing-based attacks rely on the periodicity of the PR frames. Even though the device changes its MAC address, the intervals at which the PR frames are generated, as well as the sequence in which the device scans the channel, contain sufficient information to circumvent MAC randomization and facilitate tracking. The research presented in [37] introduces a machine learning technique called Cappucino, based on self-supervised learning. Unlike other methods that aim to resolve random MAC addresses to their original values, Cappucino focuses on associating PR frames with their respective source devices for statistical analysis purposes, such as device counting and trajectory reconstruction. The reported results indicate that Cappucino achieves a V-measure score higher than 85, showcasing its effectiveness in performing these tasks.

3.5. Current Status

The IEEE 802.11 committee established a dedicated group called the Randomized and Changing MAC Addresses Topic Interest Group (RCM TIG) [38] to standardize MAC address randomization. The primary focus of RCM TIG is to investigate existing MAC randomization techniques, evaluate the impact of MAC randomization on IEEE 802.11 networks, and work toward potential standardization efforts. Since 2014, the organization has actively discussed and addressed MAC address randomization during various meetings [39]. Regarding MAC address randomization, the IEEE 802.11aq pre-association discovery amendment [40] provides recommendations for STA (station) behavior. It suggests that an STA should frequently change its MAC address while not associated with a

BSS to enhance privacy. The amendment also advises two additional measures: resetting the sequence number whenever the MAC address changes and avoiding active scanning or sending probe requests with an empty SSID field if active scanning is enabled. The specific interval at which an STA should change its MAC address during scanning is left to the vendor's discretion and falls outside the scope of IEEE standards. In 2019, two topic interest groups (TIGs) emerged within the IEEE 802.11 committee: IEEE 802.11bh (enhanced service with randomized MAC addresses) and IEEE 802.11bi (enhanced service with data privacy protection). These TIGs aim to safeguard the functionality of network services that the use of MAC address randomization might compromise, while also enhancing data privacy in IEEE 802.11 networks [41].

A study conducted between 2013 and 2017 examined the adoption of MAC randomization. Researchers collected a substantial dataset of nearly 374 million PR frames from various European cities and locations. The findings revealed that the practice of MAC randomization has expanded since its introduction. However, over 95% of the analyzed MAC addresses utilized unregistered organizationally unique identifiers (OUIs), which deviate from the IEEE Registration Authority (RA) recommendations. The adoption rate of MAC randomization remains low, with less than 3% of PR frames in the dataset employing this technique [42]. One contributing factor to the low adoption rate is the need for more familiarity among users regarding the MAC randomization feature on their devices or the need to understand how to enable it [43]. In response, vendors actively engage in initiatives to raise awareness about MAC randomization and enable it as the default device setting [44].

4. The Proposed MAC Address Randomization Covert Channel

4.1. Concept

The underlying concept of the covert channel described in this paper involves the transmission of secret messages by utilizing random MAC addresses. In this method, the secret message is the content of the field source address (SA) in the PR frame as presented in Figure 3. These random addresses are disposable to network observers and hold no meaning apart from their use in channel scanning and concealing the device's identity. The covert channel is disguised as MAC address randomization, leveraging the widespread adoption of this practice in modern Wi-Fi networks. We also use the sequence control (SC) field of the PR frame for the implementation of the covert channel as shown in Figure 3. The SC is a 16-bit field divided into two subfields: 4 bits for fragmentation number (FN) and 12 bits allocated for sequence number (SN). The FN signifies the frame's order in case of fragmentation, facilitating proper reassembly. For non-fragmented frames, such as PR, its value is always set to 0. The SN indicates the sequence in which the frame is transmitted from a single transmitter's perspective, incrementing by one with each transmission.

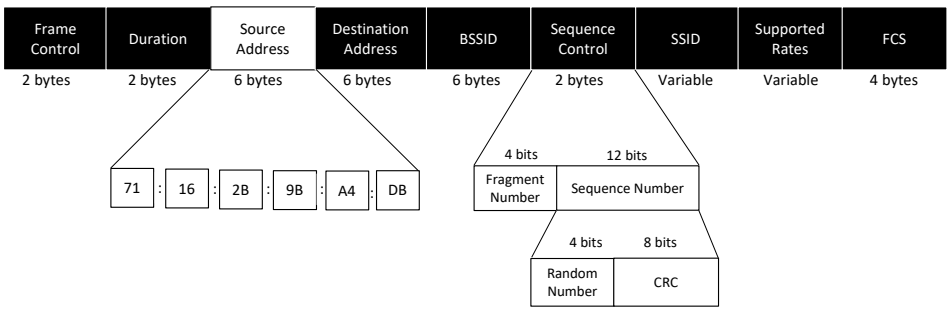

Figure 3. Covert message encoded as random MAC address in probe request frame.

In the proposed covert channel, the AP must differentiate between PR frames containing random MAC addresses from the covert station and PR frames from regular stations. To effectively address this distinction, we implemented the use of the cyclic redundancy

check (CRC), specifically CRC-8, in the SN field. The procedure remains the same as the original algorithm. The covert STA generates a 4-bit random number and appends eight zeros to create a 12-bit initial value (e.g., 101100000000). The STA then divides the initial value by the shared generator polynomial. After the division, the covert STA inserts the 4-bit random number and the remainder of the division (the CRC) into the SN field. To verify the source of the PR frame, the AP takes the SN value and divides it by the shared generator polynomial. If the remainder is zero, it indicates that the PR frame originated from the covert STA. Otherwise, the AP interprets the PR frame as a regular PR.

Changing the sequence number does not have any impact on regular network operations. In fact, it is a recommended practice to modify the sequence number during MAC randomization. This practice further increases the difficulty of reverse engineering the random MAC address and linking it back to the original global address [7].

Detecting the covert channel presents challenges due to two key factors. First, generating disposable random MAC addresses is recommended and lacks standardization. This allows for the creation of various additional randomization schemes to further enhance the disguise. Secondly, in the event of suspicion regarding implicit data transmission within the channel, the sender and receiver can employ a dictionary to encode and decode the covert messages. This dictionary enables the interpretation of seemingly random messages only by parties with the dictionary.

Figure 4 presents the operation of the covert channel. In this scenario, the STA and AP share two specific random MAC addresses: one for indicating the initiation of covert communication, and the other for indicating its termination. To initiate the covert channel, the STA sends a PR frame with the SA field set to the MAC address indicating the initiation of covert communication. From that point onward, each subsequent PR frame is sent at regular intervals (i.e., every 10 ms), and its SA field is interpreted as a secret message. The covert channel is reliable. Employing retransmission, as illustrated in the case of PR number 3 not being acknowledged, STA retransmits PR with the same random MAC address. After transmitting the messages, the STA sends a PR frame with the appropriate random MAC address to signal the channel's termination. Subsequent PR frames are treated as regular requests by the AP.

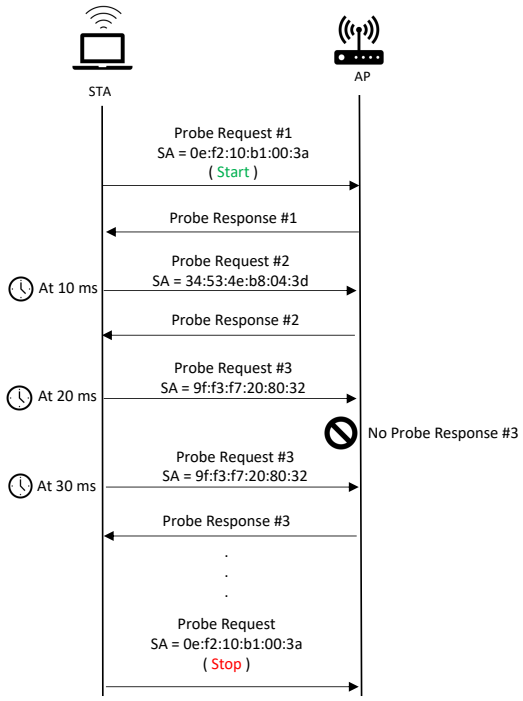

Figure 4. Covert channel operation.

4.2. Simulation Environment

We utilized the network simulator version 3 (NS-3) release 35 as our simulation environment. This simulator allows researchers to model and assess the performance of various networking protocols and scenarios. NS-3 [45] is an open-source tool widely recognized for its extensive use in network technology research and development, as it supports a variety of networks. NS-3 is implemented in C++ and is currently being extended to support Python, enabling researchers to incorporate new models and protocols as required. We modified the NS-3 source code to align with our specific goals. These adjustments include generating random MAC addresses, scheduling transmission events, checking for acknowledgment, and more. Algorithm 1 presents a comprehensive overview of our introduced functionalities.

Two configurations were created for the experiments as depicted in Figure 5. The first configuration consisted of a single STA and an AP, enabling an analysis of covert channel performance without external interference. In the second scenario, the network expanded gradually by adding more stations that generated UDP traffic at a constant rate. This setup allowed us to evaluate the behavior of the covert channel as external network traffic increased and identify factors that could impact covert channel performance. It is important to note that the covert STA did not associate with the network during these transmissions. Table 1 presents the main parameters employed during the simulation. In all figures, the error of each simulation point for the 95% confidence interval does not exceed ±2%.

Algorithm 1: Covert channel based on MAC address randomization pseudocode.

```
while while network card is running do
    macAddr ← GetRandomMac(); msIdg ← GetMsgId();
     SendProbeRequest(macAddr); MsgIdAndMac[msIdg] = macAddr;
     MsgIdAndRsp[msgId] = false; ScheduleNextSendMsgEvent();
     ScheduleVerification(Timer, MsgId);
    if ScheduleVerification() triggered and MsgIdAndRsp[msgId] == false then
        Retransmit(MsgIdAndMac[msIdg])
    else
        SendNextProbeRequest();
    end
end
```

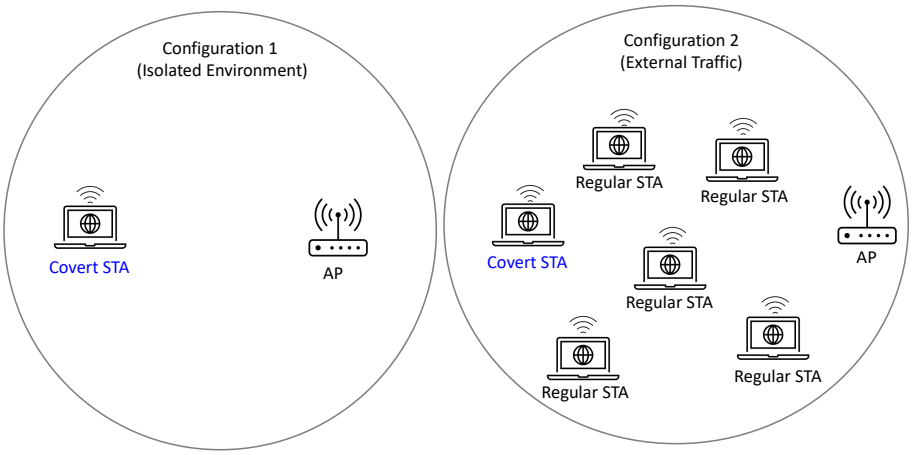

Figure 5. The two configurations used in the simulation.

Table 1. Simulation parameters.

Parameters	Value and Unit
Packet Size	2000 [Bytes]
Offered Load	20 [Mbps]
Transport protocol	UDP
IEEE standard	802.11ac
Frequency band	5 GHz
Channel width	20 MHz
Number of Tx and Rx antennas	1
Mobility Model	Constant mobility
Regular STA Probing	Passive
Probe Request Interval	Constant Interval
MCS Index	VHT9
Guard Interval	800 [ns]

4.3. Covert Channel Metrics

In a standard network transmission channel, it is imperative to establish a comprehensive set of evaluation metrics. These metrics act as performance indicators, facilitating the assessment of the transmission channel's quality, identification of parameters and factors that directly impact it, and implementation of measures to mitigate potential performance degradation caused by these parameters. When evaluating the performance of the proposed covert channel, we employ the same metrics utilized for assessing regular standard transmission channels, namely throughput, delay, and jitter, measured according to the definitions in [46]. We decided to introduce an additional metric, namely covert channel frame efficiency. This metric indicates the ratio of the actual PR frames received to the number of PR frames transmitted. Our observation revealed that many covert channels focus solely on measuring bandwidth, which represents the theoretical throughput but not the actual performance. Furthermore, when measuring throughput, they often consider only the number of frames sent, without emphasizing whether those frames are received or lost. By including covert channel frame efficiency as a metric, we aim to provide a more comprehensive evaluation of the covert channel's health and performance.

4.3.1. Covert Channel Throughput

The throughput indicates how fast STA can actually send secret messages over the network channel. The covert channel throughput, as expressed in Equation (1), is measured as the total number of transmitted PR frames successfully acknowledged by AP multiplied by the number of covert bits carried in a single frame over the simulation time. In our case, since the covert payload is the MAC address, each frame carries 48 covert bits. The throughput is expressed in bits per second (bps). The throughput metric holds significant relevance in the performance evaluation of covert channels, as it quantifies the amount of covert data that can be transmitted within a specified timeframe. It serves as a vital factor for capacity planning, as it offers insights into whether the covert channel meets the required throughput to effectively function within a given scenario.

$$Throughput = \frac{Rx\ PR\ Frames \times 48}{Simulation\ Time}\ [\text{bps}] \quad (1)$$

4.3.2. Covert Channel Efficiency

As demonstrated in Equation (2), we decided to define the covert channel efficiency as the received-to-transmitted PR frames ratio expressed in percentage (%). Covert channel frame efficiency is a vital metric, as it provides insights into the actual delivery of data, enabling us to assess the extent of data loss within the covert channel. By evaluating this metric, we can gain valuable information about the overall health of the transmission

channel and identify any parameters that may be causing interference with the covert channel, and pinpoint areas that require improvement or mitigation strategies:

$$Efficiency = \frac{Rx\ PR\ Frames}{Tx\ PR\ Frames} \times 100\ [\%] \quad (2)$$

4.3.3. Covert Channel Delay

The network channel delay refers to the duration it takes for a message to travel from the source to the destination, measured in time units. This delay is influenced primarily by four factors: propagation time, transmission time, queuing time, and processing delay. Therefore, the delay is defined as the cumulative duration of time from the moment a PR is sent to the time it takes to receive the corresponding probe response. The delay metric carries significant relevance in the context of the covert channel, as it assists in identifying potential bottlenecks within the channel. Since delay is influenced by various parameters, it aids in pinpointing the factors that may result in untimely frame arrival at different stages of the transmission process, including the sender, the channel itself, and the receiver. By analyzing the delay, we gain insights into the external factors that impact frame arrival, such as the number of frames and the offered load. This information allows for effective planning and identifying suitable environments for implementing the covert channel, ensuring optimal performance and reliable frame delivery:

$$Delay = \frac{Tx\ PR\ Frame\ Delay + Rx\ PR\ Frame\ Delay}{Simulation\ Time}\ [\text{ms}] \quad (3)$$

4.3.4. Covert Channel Jitter

The jitter, in the network context refers to the delay variation of a frame over the channel, measuring the irregularity of frame arrival. It is expressed in Equation (4) in ms, where N is the frame number. The jitter plays a critical role, as it quantifies the variation in delay within the covert channel. By measuring jitter, we can assess how the delay fluctuates throughout the transmission, revealing periodic improvements or degradations in the network condition. This parameter is crucial for identifying variations in network behavior throughout the entire simulation:

$$Jitter = \frac{Delay\ PR\ Frame_{N-1} - Delay\ PR\ Frame_{N}}{Simulation\ Time}\ [\text{ms}] \quad (4)$$

5. Covert Channel Performance Evaluation

5.1. Scenario 1—Periodic Transmission with No Retransmission

Figure 6 depicts the covert channel throughput analysis. Two parameters directly influence the throughput: the transmission interval (TI) and the number of regular STAs connected to the same network as the covert STA. As the TI is extended, the throughput decreases regardless of the number of regular STAs connected to the network. For instance, when the TI is set to 100 ms in the isolated environment configuration, the throughput experiences a tenfold reduction from its initial value (from 4.8 Kbps to 0.48 Kbps), representing a significant drop. Notably, longer TI leads to throughput values that converge to the extent that having 10 additional STAs is nearly equivalent to having 50 STAs generating traffic. This decline in throughput can be attributed to the latency introduced by longer TIs during transmission. The impact of adding regular STAs to the network is illustrated in Figure 6. Increasing the number of STAs in the network leads to a degradation in throughput for a TI. For instance, when the shortest TI of 10 ms was used, it was observed that the throughput significantly decreased as soon as 10 STAs joined the network (from 4.8 Kbps to 2.9 Kbps). Furthermore, with the addition of 20 STAs, the throughput further dropped to 2.3 Kbps, which is half the initial value. In denser environments, where 20 to 50 STAs were considered, the difference in throughput reductions tended to become less evident. This indicates that the effects of having 20 STAs are nearly equivalent to having 50 STAs.

The impact of additional STAs on the throughput can be attributed to increasing collisions as more STAs compete for channel access.

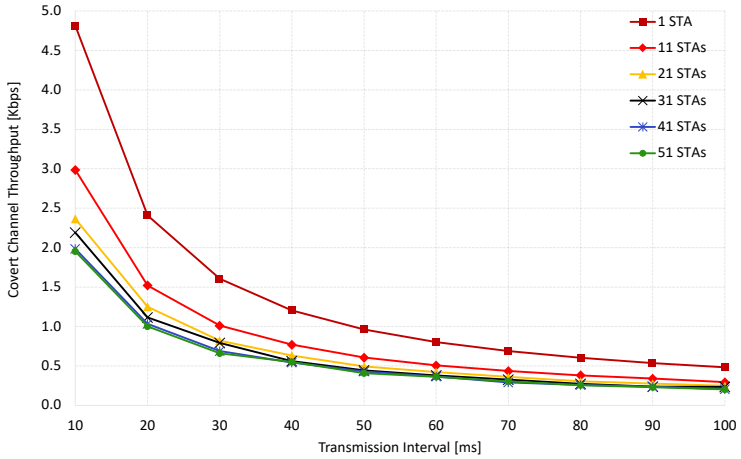

Figure 6. Covert channel throughput as a function of transmission interval in scenario with retransmission disabled.

Next, we evaluate the transmission efficiency of the covert channel. In Figure 7, it is evident that the TI does not significantly impact the transmission efficiency. However, the number of regular STAs connected to the network affects the transmission efficiency. This observation indicates that the response-to-request ratio is not solely dependent on the frequency of frame transmission but on the presence of external traffic generated when the frame is sent. As depicted in Figure 7, in an isolated environment with no external traffic interference, no frame loss was initially detected in the covert channel. However, upon adding ten STAs to the network, a significant decrease in efficiency was immediately observed, resulting in approximately 63% efficiency. Furthermore, the inclusion of 20 STAs led to a frame loss of nearly 50%. In more congested environments with 30, 40, and 50 STAs, the covert channel experienced a further decline, with over 50% of frames being lost.

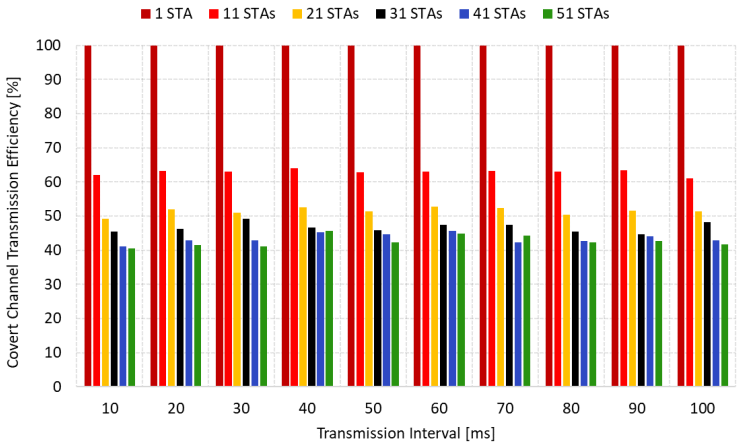

Figure 7. Covert channel efficiency as a function of transmission interval in scenario with retransmission disabled.

The delay analysis is presented in Figure 8. In an isolated environment, a nearly constant delay of approximately 0.5 ms is recorded, regardless of the TI. However, the delay increases when additional STAs are added to the network. Notably, the shortest TI exhibits similar delays across different numbers of STAs, oscillating around 4 ms. From 20 ms and beyond, the delay slightly rises as the transmission interval increases. This observation

highlights the impact of multiple factors, including TI and the number of STAs, on the delay. As more STAs join the network, channel resources are exhausted, and the AP frame queue grows, affecting the response time.

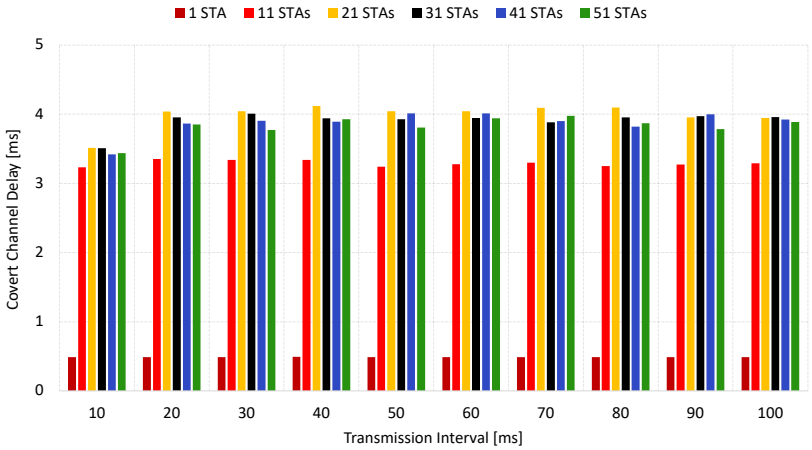

Figure 8. Covert channel delay as a function of transmission interval in scenario with retransmission disabled.

As shown in Figure 9, the covert channel exhibits jitter based on the delay. In the isolated scenario, the jitter was relatively insignificant compared to the scenario with an external load. Observations revealed that with a transmission interval of 10 ms, the jitter remained below 3.5 ms. However, as the transmission window expanded due to consecutive frame transmissions adding to the congestion, the delay increased to values exceeding 4 ms.

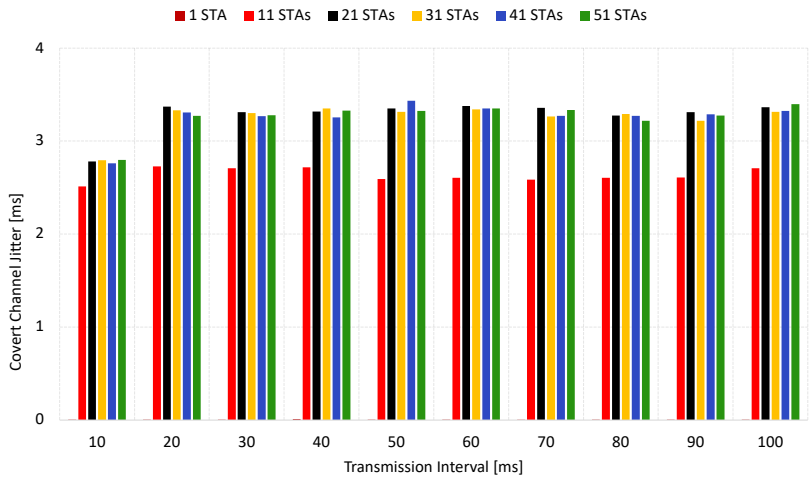

Figure 9. Covert channel jitter as a function of transmission interval in scenario with retransmission disabled.

We also conducted an analysis to assess the impact of a covert channel on network throughput. The primary objective was to ensure that the covert channel does not consume network resources intended for regular stations and operates without negatively affecting the network. To conduct this experiment, we utilized the same network infrastructure and introduced traffic generation from multiple STAs, causing the saturation of the network throughput. We assumed a worst-case scenario, where PR frames are generated by covert station every 10 ms. Our network configurations included 1, 10, 20, 30, 40, and 50 STAs. The increasing number of STAs in saturation conditions resulted in a significant increase in the number of collisions and a decrease in the overall efficiency of the network. In each

scenario, we compared the saturation throughput without the covert STA and subsequently introduced the covert STA to observe the resulting changes in saturation throughput (see Figure 10).

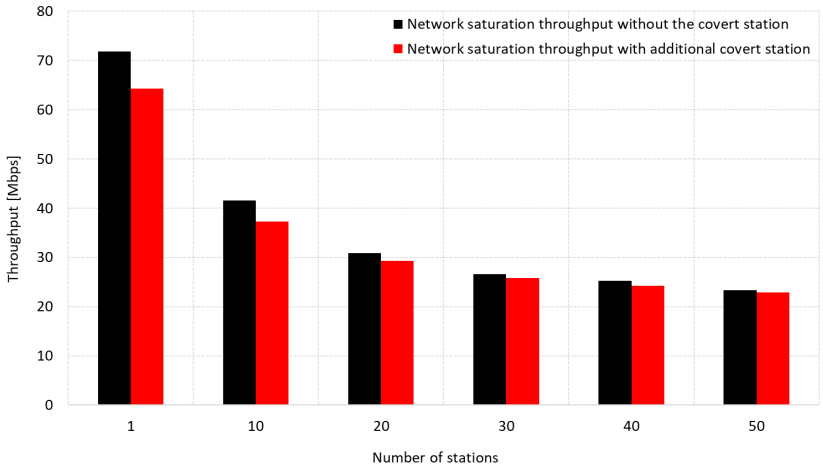

Figure 10. The impact of the covert station on the network saturation throughput.

The impact on saturation throughput is most pronounced when there is only one regular STA and one covert STA, leading to a significant drop of nearly 6 Mbps. This effect is clearly evident. This underscores the heightened competition for channel resources in such a scenario. Nevertheless, as the number of STAs increases to 10, the impact gradually diminishes, resulting in a drop of approximately 3 Mbps. In scenarios involving 20, 30, 40, and 50 STAs, the inclusion of the covert STA has a minimal observable impact, with the throughput drop not exceeding 1 Mbps. These findings lead us to conclude that in scenarios with a limited number of STAs, the presence of a covert channel adversely affects saturation throughput (a decrease of about 8%). However, as the number of STAs grows, this effect becomes less pronounced (in the last case, it is a decrease of only about 2.5%). As a result, covert channels are better suited for networks that resemble typical Wi-Fi networks encountered in everyday situations with a large number of STAs.

5.2. Scenario 2—Periodic Transmission with Retransmission

In the second scenario, the presence of a covert STA introduces retransmission, thereby increasing the probability of successful frame delivery. As depicted in Figure 11, the impact of retransmission is initially not perceptible in the isolated environment since no frames are lost, as in the first scenario. However, as more STAs join the network, the retransmission effect becomes more apparent compared to the first scenario. To compare the two extremes of TI used in the experiments, 10 ms as the shortest and 100 ms as the longest, we observed that the covert channel's behavior remains similar to the previous scenario, where the throughput decreases as the TI increases. However, when retransmission is enabled, and additional STAs are added, significant throughput improvements are observed. For the shortest transmission interval, with ten more STAs, the throughput increased by 1169 Kbps. Adding 20 more STAs increased to approximately 1098 Kbps. In denser environments, where 30, 40, and 50 additional STAs were added, throughput gains of 763 bps, 1069 bps, and 900 bps were achieved, respectively. Notably, the benefits of retransmission extend to even the longest TI, as in the case of 100 ms for each case from 10 to 50 additional STAs, the gain of more than 100 bps was consistently observed.

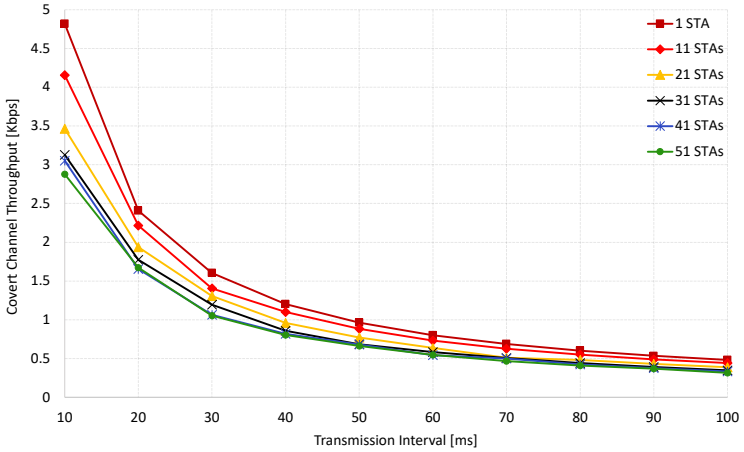

Figure 11. Covert channel throughput as a function of transmission interval in scenario with retransmission enabled.

The introduction of retransmission significantly enhances the efficiency of the covert channel. It is worth noting that, as observed, the transmission efficiency is closely correlated with the number of regular STAs rather than the values of the TI. Comparing it to the first scenario, when having ten additional STAs, efficiency improved from approximately 60% to values exceeding 80% (see Figure 12). When 20 more STAs were added, the efficiency experienced a notable increase of 22%. Furthermore, as 30, 40, and 50 more STAs joined the network, the transmission efficiency improved by 19%, 22%, and 18%, respectively. In contrast to the first scenario, none of the configurations in the second scenario exhibited frame loss exceeding 50%.

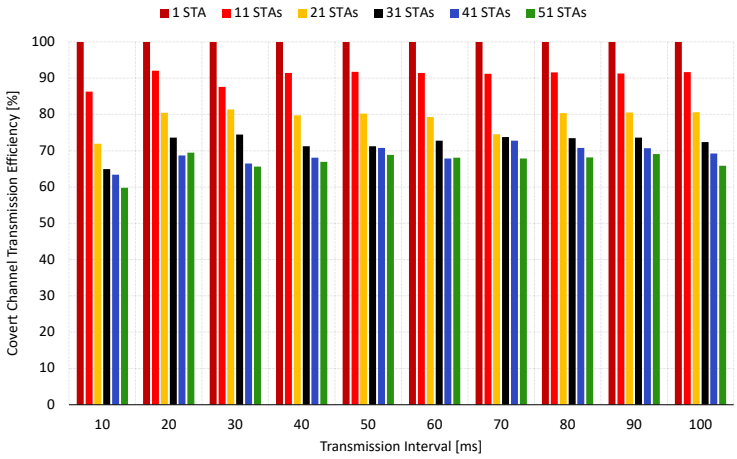

Figure 12. Covert channel efficiency as a function of transmission interval in scenario with retransmission enabled.

While retransmission enhances throughput and efficiency, it is necessary to note that it introduces an additional delay, as evidenced by the results presented in Figure 13. The retransmissions lead to an increase of up to 2.5 ms in each configuration compared to the delays observed in the first scenario. This effect can be attributed to the additional traffic generated by the covert STA. As more STAs join the network, many frames require retransmission, increasing collisions and amplifying channel delays. Despite introducing this additional delay, the benefits of retransmission, including improved throughput and transmission efficiency, outweigh the observed delay. Likewise, as illustrated in Figure 14, it was noticed that retransmissions contribute to increased channel jitter. Enabling retransmissions resulted in an average jitter increment of 1.5 in scenarios involving external traffic.

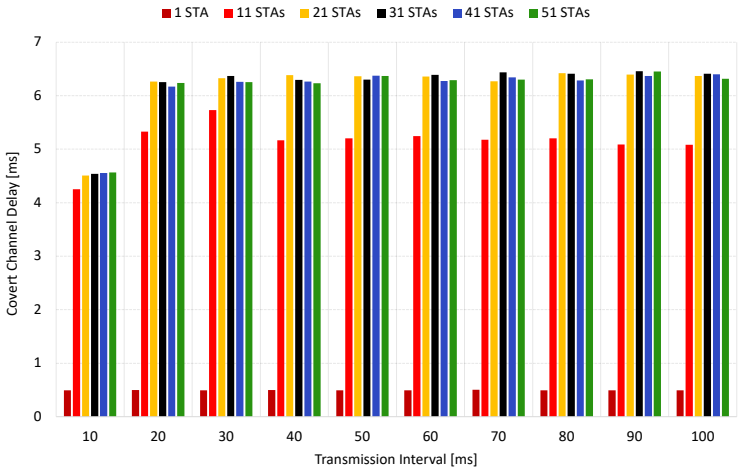

Figure 13. Covert channel delay as a function of transmission interval in scenario with retransmission enabled.

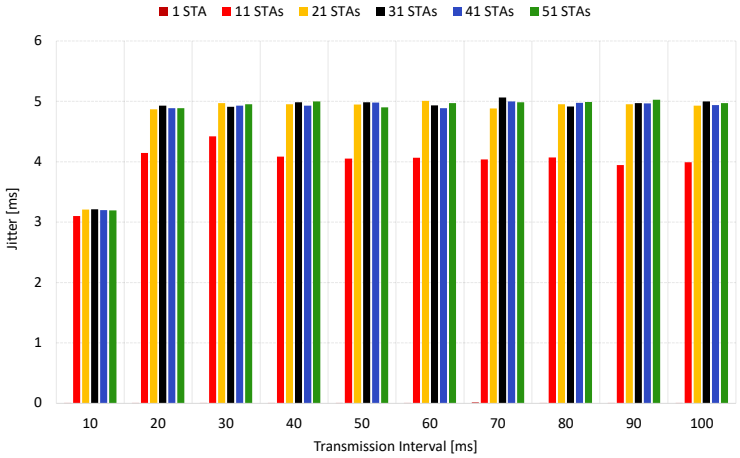

Figure 14. Covert channel jitter as a function of transmission interval in scenario with retransmission enabled.

6. Adapting the Selective Repeat ARQ Protocol—The Concept of the Discontinuous Sliding Window Protocol

The obtained results demonstrate that the performance of the covert channel is significantly influenced by the number of stations associated with the BSS and their respective loads. As the number of stations increases, several factors are impacted, including decreased throughput, reduced efficiency, increased delay, and elevated jitter. This effect is particularly noticeable in dense environments, where the presence of additional stations (30 to 50) worsens the impact of external traffic on the covert channel. To address the challenges posed by external traffic, especially in dense environments, we propose the adaptation of the modified selective repeat (SR) ARQ (automatic repeat request) protocol called in our paper SWP (sliding window protocol) [47]. This protocol allows the covert stations to monitor the channel's state and transmit frames only under favorable conditions. Consequently, the adoption of this protocol leads to linear throughput growth, improved frame efficiency, and reduced overall delay and jitter within the covert channel.

The operation of the covert channel, following the adoption of SWP, is depicted in Figure 15. The window size refers to the number of frames an STA can transmit consecutively without receiving acknowledgment. Each probe request is assigned a unique sequence number and has an associated timeout. The first probe request, which does not contain a covert message, utilizes a customized MAC address content to signal the readiness

of the STA for covert communications. Upon receiving a probe response, subsequent frames transmitted by the STA are interpreted as covert messages. When an STA sends a covert message, it decrements the window size by one and sets a timeout for the corresponding probe response. Upon receiving a response, the window size is incremented by one (sliding the window). If the probe response timeout event is triggered, the STA checks whether it has received the expected probe response. If no probe response is detected, the STA considers the frame lost and schedules a retransmission event (note that retransmission does not decrement the window size).

The protocol proposed by us differs from the original SR ARQ protocol in that both the sender and receiver's windows can be discontinuous, meaning that only the maximum number of sent and unacknowledged frames is important, which cannot exceed the window size. This implies that the transmission process continues constantly, as long as the number of received acknowledgments is not less than the total number of sent frames minus the window size. The algorithm used during the simulation to implement the scheme in Figure 15 is also demonstrated in Algorithm 2.

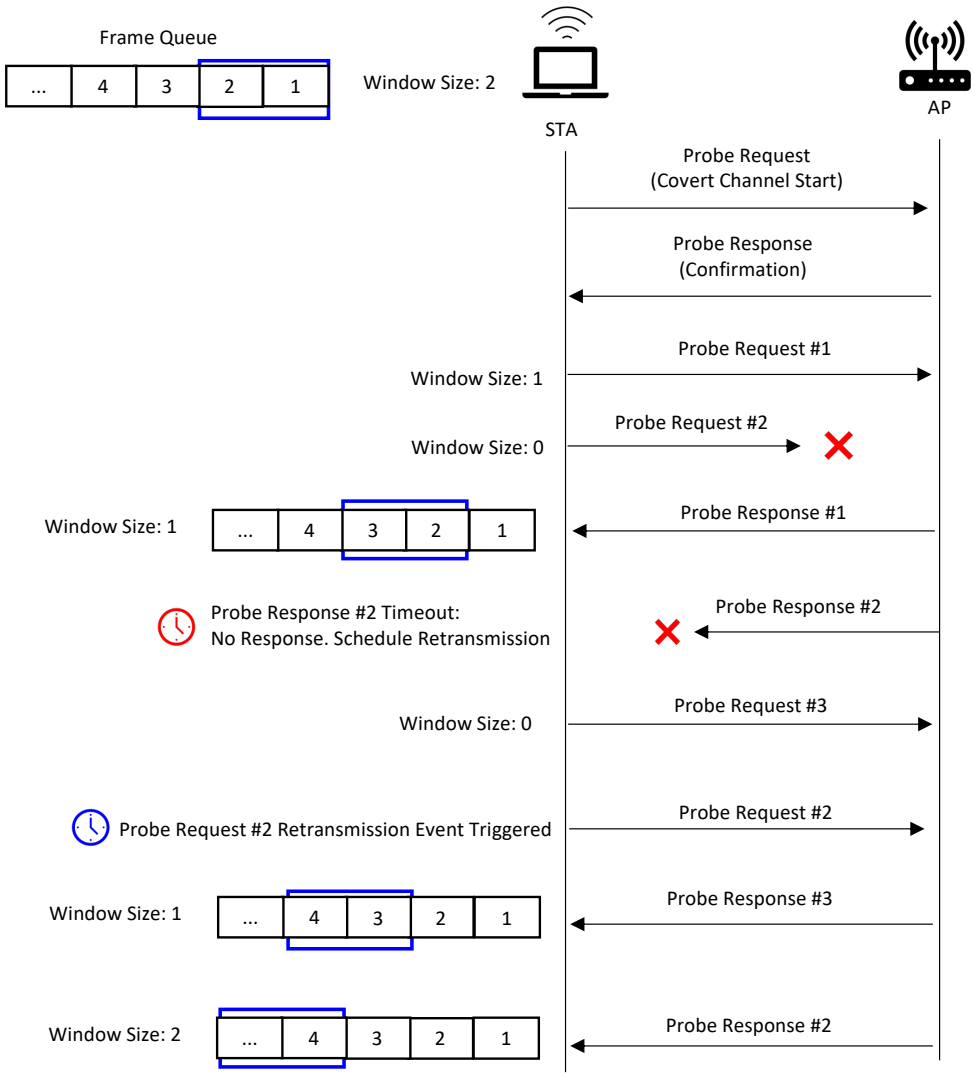

Figure 15. Adoption of sliding window protocol into the covert channel.

Algorithm 2: Pseudocode for adopting the sliding window protocol into the covert channel.

```
while while network card is running do
    if windowSize > 0 then
        macAddr ← GetRandomMac();
        msIdg ← GetMsgId();
        SendProbeRequest(macAddr);
        MsgIdAndMac[msIdg] = macAddr;
        MsgIdAndRsp[msIdg] = false ;
        ScheduleNextSendMsgEvent() ;
        ScheduleVerification(msIdg) ;
        windowSize = windowSize + 1 ;
    end
    ScheduleNextSendMsgEvent() ;
    if ScheduleVerification(msIdg) triggered and MsgIdAndRsp[msIdg] == false
     then
        ScheduleRetransmission(Timer, msIdg)
    else
        windowSize = windowSize − 1 ;
    end
end
```

7. Scenario 3—Covert Channel with Sliding Window Protocol

We conducted an analysis of the covert channel performance by varying the window size from 1 to 100,000. The parameters used are consistent with those listed in Table 1, and a regular 10 ms transmission interval was maintained throughout the experiments. In isolated scenarios, as anticipated, we found that the window size did not impact the throughput, which remained constant (see Figure 16). This observation aligns with the results obtained from the previous two scenarios. However, the effect of the SWP became noticeable as more stations joined the network. For instance, when an additional 10 stations were introduced, we observed that increasing the window size led to a corresponding increase in throughput, eventually reaching a point of saturation.

The advantages of employing SWP became even more evident in dense environments, where the number of stations ranged from 30 to 50. Comparing these results to those shown in Figure 11, we noticed a significant average improvement of 1.45 Kbps in the throughput. The pattern remained consistent: as more stations associated with the BSS, we observed a linear and proportional relationship between the throughput and window size until saturation.

The results clearly demonstrated that employing SWP effectively mitigated the impact of the increased station count and their respective offered loads, leading to a substantial improvement in throughput. This improvement became particularly evident when using larger window sizes, as it resulted in a constant throughput. The underlying reason for this observation is that, with small window size, the transmission window fills up quickly, thereby reducing transmission opportunities. Contrariwise, as the window size increases, more frames can be transmitted before awaiting acknowledgment, enabling the STA to send more frames than possible with the mechanisms employed in the previous scenarios.

Figure 17 clearly demonstrates the unpaired frame efficiency provided by SWP. When comparing these results with those shown in Figure 12, it becomes evident that increasing the number of stations leads to more frame losses, even with retransmission. In fact, in scenarios involving external traffic, it was observed that no efficiency above 90% was achieved, except for the isolated scenario. However, when employing SWP, the frame efficiency consistently reached 90% or higher across all scenarios. Focusing specifically on congested environments, such as those with 40 and 50 stations, notable efficiency gains

of 30% and 31%, respectively, were observed compared to the previous scenario. This highlights the significant advantages of utilizing SWP in improving frame efficiency.

The utilization of SWP significantly altered the dynamics of frames within the covert channel as evidenced by the data presented in Figures 18 and 19, showcasing the delay and jitter, respectively. It was observed that delay and jitter are directly proportional to the window size: smaller window sizes resulted in reduced delay and jitter, while larger windows led to increased delay and jitter. When comparing these results with those shown in Figures 13 and 14, specifically in scenarios involving external traffic with 10 to 50 additional stations, it is worth noting that no delays exceeding 1 ms were observed. In densely populated environments, such as those with 30, 40, and 50 additional stations, there was an average reduction in delay of 4.2 ms and a decrease in jitter of 3.8 ms when compared to the previous scenario.

These findings highlight the positive impact of SWP on mitigating delay and jitter, resulting in more efficient and reliable frame transmission within the covert channel.

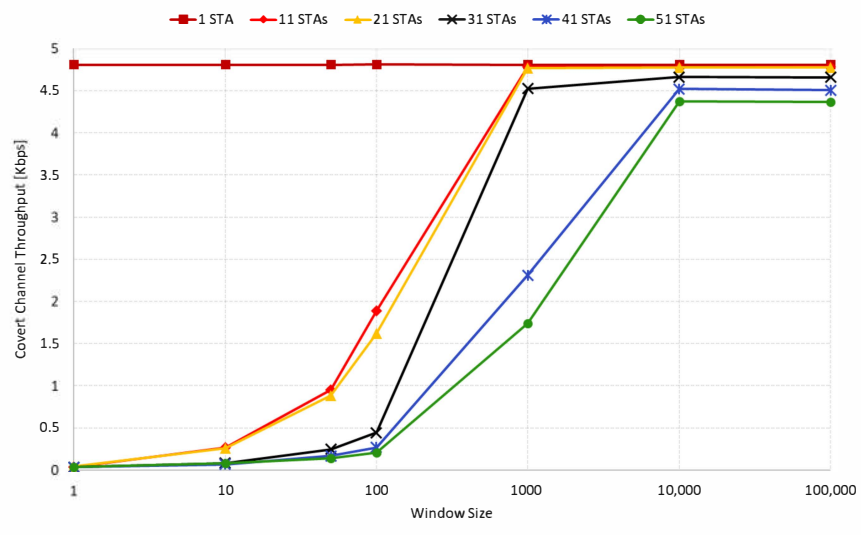

Figure 16. Covert channel throughput after the adoption of sliding window protocol.

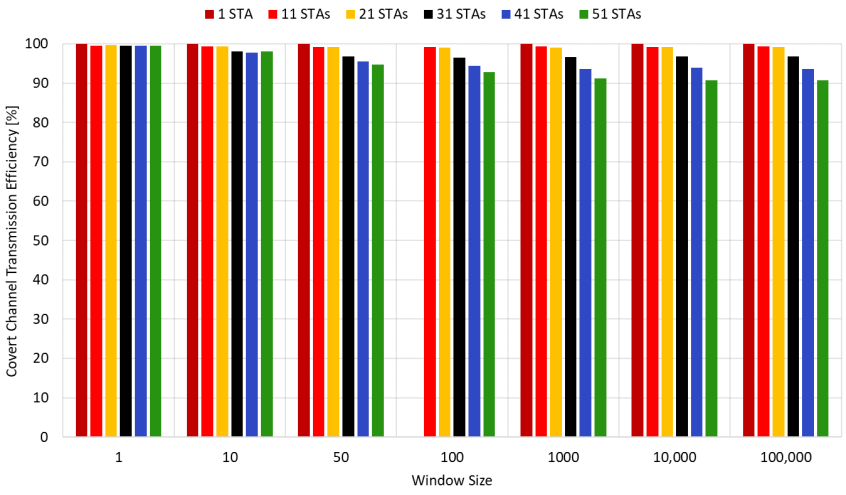

Figure 17. Covert channel efficiency after the adoption of sliding window protocol.

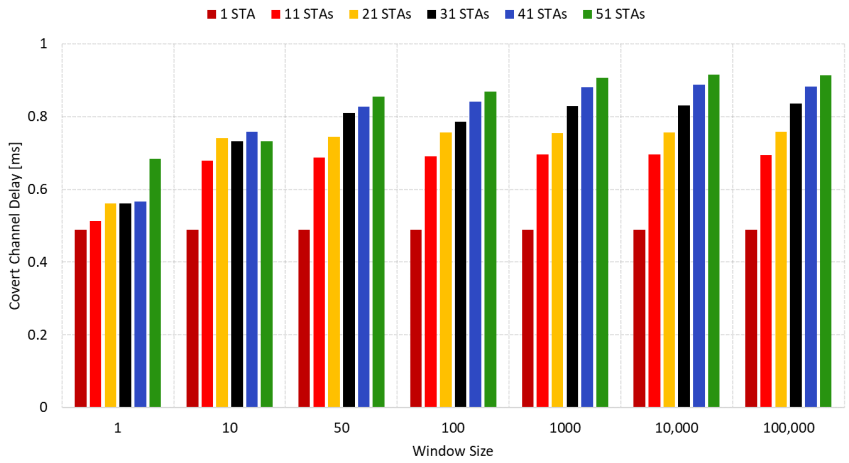

Figure 18. Covert channel delay after the adoption of sliding window protocol.

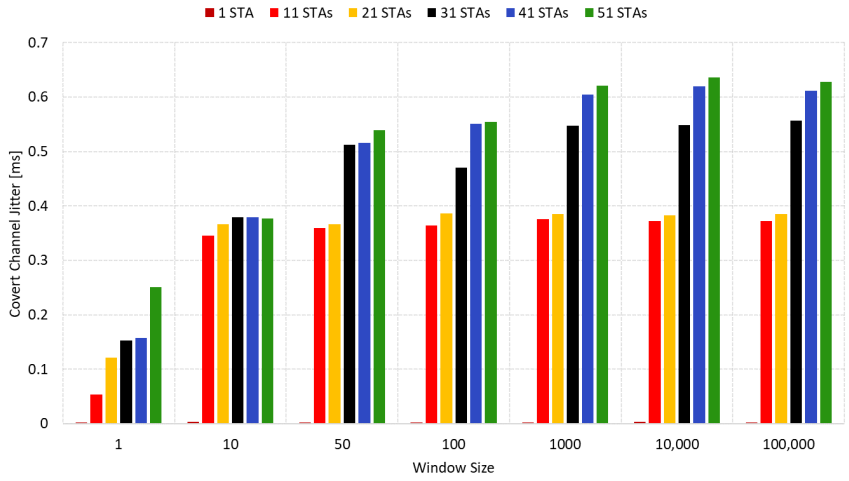

Figure 19. Covert channel jitter after the adoption of sliding window protocol.

8. Discussion

In this study, we investigated two scenarios for covert data transmission and explored a transmission technique to enhance its performance in dense environments. Our findings indicate that the number of stations and the TI has a direct impact on network performance and delay. To address longer transmission intervals or an increased number of stations, retransmission can be employed, resulting in significant improvements in network throughput and efficiency. However, it also introduces additional delay and jitter.

On the other hand, the adoption of the SWP allows stations to consecutively send messages without waiting for acknowledgment or freezing when there is a high external load. Our observations demonstrate that implementing SWP leads to enhanced throughput, improved efficiency, and reduced delay and jitter. This technique proves to be highly beneficial in dense environments.

Furthermore, the covert channel exhibits versatility and can operate in three different modes depending on network conditions, including the number of stations, offered load, and desired sender throughput. Table 2 provides a summary of the key aspects of each experiment, including the highest throughput values, corresponding frame efficiency, delay, and the methods employed to achieve these results. It is worth noting that all transmission techniques utilized a uniform transmission interval of 10 ms.

Table 2. Comparison of the three simulated scenarios based on the highest achieved throughput.

Number of Stations	Scenario	Throughput [Kbps]	Delay [ms]	Jitter [ms]	Frame Efficiency
1 STA	1—w/o retrans.	4.8	0.4	0.002	100
	2—with retrans.	4.8	0.4	0.002	100
	3—with SWP	4.8	0.4	0.002	100
11 STAs	1—w/o retrans	2.98	3.23	2.51	62
	2—with retrans.	4.15	4.25	3.09	86.27
	3—with SWP	4.78	0.69	0.37	99.29
21 STAs	1—w/o retrans	2.3	3.5	2.7	49
	2—with retrans.	3.46	4.5	3.2	71.93
	3—with SWP	4.77	0.75	0.38	99.11
31 STAs	1—w/o retrans	2.19	3.51	2.79	45
	2—with retrans.	3.12	4.54	3.21	64.96
	3—with SWP	4.66	0.83	0.54	96.8
41 STAs	1—w/o retrans	1.98	3.42	2.76	41.18
	2—with retrans.	3.05	4.55	3.2	63.39
	3—with SWP	4.52	0.88	0.61	93.86
51 STAs	1—w/o retrans	1.95	3.4	2.7	41
	2—with retrans.	2.87	4.56	3.19	59.79
	3—with SWP	4.37	0.91	0.62	90.68

We also outline some of the key distinguishing characteristics of our research on covert channels compared to existing implementations based on the IEEE 802.11 MAC layer. We emphasize the significance of these characteristics in advancing the field of IEEE 802.11 networks steganography, with the ultimate goal of designing and implementing covert channels that are both resilient and secure while maintaining transparency and reliability.

- **High covertness**: The covert messages are based on the IEEE 802.11 specifications and recommendations and exploit the open aspects of the standard. The covert channel is camouflaged as a MAC randomization technique in the PR frames. The MAC address is randomly disposable, carrying no special meaning. If detected, the frames can be considered one of the many flavors of MAC randomization. MAC randomization is an advocated practice during scanning, is not standardized, and currently is a vendor specification.
- **Robust security**: If the covert channel is detected due to the random nature of the message content, to interpret the message correctly, the third party still needs the dictionary shared between sender and receiver, which adds an extra layer of security. Even though the MAC address is plain text, the covert message is not.
- **Data reliability**: Data reliability needs to be addressed in the IEEE 802.11 covert channel. To demonstrate the importance of reliability, we compared a covert channel with and without retransmission, and the results confirmed the profits of enabling retransmission.
- **Transparency**: A covert channel should not have any interference with regular network functionality. This study proves we can implement a covert channel that coexists with everyday devices generating regular application traffic, such as UDP or TCP.
- **High throughput**: It is crucial to mention that the primary focus of the covert channel is to enable secret data flow within a regular transmission channel. In this work, we combine allowing secret data exchange with high throughput in the order of kilobytes per second. Compared to the existing IEEE 802.11 MAC covert channel, it is multiples times higher and considered a very satisfactory result.

Considering the inherent nature of IEEE 802.11 networks, where all stations sharing the transmission channel can hear each other, it becomes possible for any IEEE 802.11 devices to capture and potentially decrypt the traffic within that channel. The proposed covert channel primarily finds its application in Wi-Fi networks. To prevent the covert

frame from being targeted, one can deploy the proposed covert channel to send messages to the AP without establishing an association or transmitting any meaningful data frames that could draw attention. Another significant application of the proposed covert channel is in monitored networks, where all data traffic is under surveillance. In such scenarios, the covert channel can be employed to send secret messages that remain imperceptible within the network, bypassing detection mechanisms. Furthermore, the covert message can serve as an authentication mechanism for device authentication. This application becomes particularly relevant in highly secure networks, where the MAC address can be easily spoofed, potentially compromising the true identity and legitimacy of a station. By utilizing the covert channel as an authentication message, a station can provide genuine proof of its legitimacy in a private network.

9. Conclusions

This study focuses on the design and implementation of a covert channel disguised as MAC address randomization. The implementation was thoroughly tested through simulations on IEEE 802.11ac wireless networks, and it involved three distinct scenarios to assess the covert channel's performance. One significant advantage of the presented covert channel is its potential to remain unnoticed. It achieves this by utilizing disposable random MAC addresses for wireless network scanning, which are typically perceived as having no purpose other than concealing the device's identity. This attribute allows the covert channel to be deeply camouflaged within the network infrastructure. Moreover, the implementation of the covert channel is straightforward, transparent, and capable of coexisting harmoniously with other stations generating regular network traffic without causing any disruptions.

One limitation of the covert channel is its reliance on an AP as the intended recipient of covert messages to ensure reliability. This requirement may introduce some level of suspicion since the covert channel needs to maintain the appearance of regular scanning processes by generating probe requests at the expected rate. This aspect should be taken into consideration when deploying the covert channel to mitigate any potential suspicions or anomalies that may arise.

In terms of future research directions, there are two key aspects to consider: improving the robustness and resistance to steganalysis by adopting the recommended MAC randomization practices and analyzing the impact of the offered load on the covert channel. To enhance the covert channel's robustness and make it more resilient against steganalysis techniques, it is crucial to explore strategies beyond MAC randomization. Current techniques based on probe request fingerprinting can easily detect MAC randomization and retrieve the global MAC address. To address this limitation, randomizing additional fields, such as sequence numbers, and altering device fingerprints could provide an added layer of undetectability, making the covert channel more effective and covert. Additionally, investigating the impact of the offered load on the covert channel is essential. While it is established that the number of stations has an impact on the covert channel, understanding the influence of the offered load is equally important. By examining how the offered load affects the covert channel's performance, it becomes possible to better estimate the covert channel throughput during implementation and adapt it to match the network conditions.

The impressive throughput, efficiency, minimal delay, and jitter achieved through the use of SWP make this covert channel an excellent choice for modern IEEE 802.11 wireless networks for dense environments. In typical network scenarios, the attained throughput is more than sufficient to establish a stable and reliable communication channel. In the context of a covert channel, it can be regarded as a high-throughput covert communication solution. Moreover, the covert channel offers versatility with its three modes of operation, allowing for flexibility in adapting to different environmental conditions. The proposed covert channel offers applications in Wi-Fi networks to prevent targeting, in monitored networks to send imperceptible secret messages, and in device authentication to ensure

the real identity of a station in a highly private network, where MAC address spoofing is a concern.

Author Contributions: Conceptualization, M.N. and G.T.; methodology, M.N. and G.T.; software, G.T.; validation, G.T.; formal analysis, M.N. and G.T.; investigation, M.N. and G.T.; writing—original draft preparation, M.N. and G.T.; writing—review and editing, M.N.; visualization, G.T.; supervision, M.N.; project administration, M.N.; funding acquisition, M.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Polish Ministry of Science and Higher Education with the subvention funds of the Faculty of Computer Science, Electronics and Telecommunications of AGH University of Science and Technology.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

5G	Fifth Generation of Wireless Cellular Technology
ANQP	Access Network Query Protocol
AP	Access Point
ARQ	Automatic Repeat Request
BI	Beacon Interval
BSS	Basic Service Set
CID	Company Identifier
CRC	Cyclic Redundancy Check
GPS	Global Position System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IEEE RA	IEEE Registration Authority
IFAT	Inter-Frame Arrival Time Analysis
LSB	Least Significant Bit
LTE	Long Term Evolution
MA-L	MAC-Address Block Large
MAC	Medium Access Control
MCS	Modulation and Coding Scheme
MSB	Most Significant Bit
NIC	Network Interface Controller
NS-3	Network Simulator Version 3
OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
OUI	Organizationally Unique Identifier
PHY	Physical Layer
PR	Probe Request
RA	Registration Authority
RCM TIG	Randomized and Changing MAC Addresses Topic Interest
SSID	Service Set Identifier
STA	Client Station
SC	Sequence Control
SN	Sequence Number
SWP	Sliding Window Protocol
SR	Selective Repeat
TCP	Transmission Control Protocol

TI	Transmission Interval
TIGs	Topic Interest Groups
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network
WS	Window Size
Wi-Fi	Wireless Fidelity

References

1. Cisco Annual Internet Report (2018–2023). Available online: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (accessed on 6 June 2023).
2. *IEEE Std 802.11-2020* ; IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks–Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Redline. IEEE: Piscataway, NJ, USA, 2021.
3. Ryan, F.; Schukat, M. Wi-Fi User Profiling via Access Point Honeynets. In Proceedings of the 2019 30th Irish Signals and Systems Conference (ISSC), Maynooth, Ireland, 17–18 June 2019; pp. 1–4.
4. Cunche, M. I know your MAC address: Targeted tracking of individual using Wi-Fi. *J. Comput. Virol. Hacking Tech.* **2014**, *10*, 219–227. [CrossRef]
5. Uszko, K.; Kasprzyk, M.; Natkaniec, M.; Chołda, P. Rule-Based System with Machine Learning Support for Detecting Anomalies in 5G WLANs. *Electronics* **2023**, *12*, 2355. [CrossRef]
6. Natkaniec, M.; Bednarz, M. Wireless Local Area Networks Threat Detection Using 1D-CNN. *Sensors* **2023**, *23*, 5507. [CrossRef]
7. Martin, J.; Mayberry, T.; Donahue, C.; Foppe, L.; Brown, L.; Riggins, C.; Rye, E.C.; Brown, D. A Study of MAC Address Randomization in Mobile Devices and When it Fails. *Proc. Priv. Enhancing Technol.* **2017**, *4*, 268–286. [CrossRef]
8. Natkaniec, M.; Bieryt, N. An Analysis of the Mixed IEEE 802.11ax Wireless Networks in the 5 GHz Band. *Sensors* **2023**, *23*, 4964. [CrossRef]
9. Natkaniec, M.; Bieryt, N. An analysis of BSS coloring mechanism in IEEE 802.11ax dense networks. *Int. J. Electron. Telecommun.* **2022**, *68*, 855–862.
10. Zillien, S.; Wendzel, S. Reconnection-Based Covert Channels in Wireless Networks. In Proceedings of the ICT Systems Security and Privacy Protection, Oslo, Norway, 22–24 June 2021; Springer International Publishing: Cham, Switzerland, 2021; pp. 118–133.
11. Sawicki, K.; Bieszczad, G.; Piotrowski, Z. StegoFrameOrder—MAC Layer Covert Network Channel for Wireless IEEE 802.11 Networks. *Sensors* **2021**, *21*, 6268. [CrossRef] [PubMed]
12. Tahmasbi, F.; Moghim, N.; Mahdavi, M. Adaptive ternary timing covert channel in IEEE 802.11. *Secur. Commun. Netw.* **2016**, *9*, 3388–3400. [CrossRef]
13. Walker, T.O.; Fairbanks, K.D. An off-the-shelf, low detectability, low data rate, timing-based covert channel for IEEE 802.11 wireless networks. In Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 835–840.
14. Seong, H.; Kim, I.; Jeon, Y.; Oh, M.K.; Lee, S.; Choi, D. Practical covert wireless unidirectional communication in IEEE 802.11 environment. *IEEE Internet Things J.* **2022**, *10*, 1499–1516. [CrossRef]
15. Teca, G.; Natkaniec, M. An IEEE 802.11 MAC Layer Covert Channel Based On Supported Rates. *Int. J. Electron. Telecommun.* **2023**, *69*, 293–299.
16. Gonçalves, R.; Tummala, M.; McEachen, J.C. Analysis of a MAC Layer Covert Channel in 802.11 Networks. *Int. J. Adv. Telecommun.* **2012**, *5*, 131–140.
17. About the Registration Authority. Available online: https://standards.ieee.org/products-programs/regauth/ (accessed on 6 June 2023).
18. Freudiger, J. How Talkative is Your Mobile Device? An Experimental Study of Wi-Fi Probe Requests. In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, New York, NY, USA, 22–26 June 2015. [CrossRef]
19. Cunche, M.; Kaafar, M.A.; Boreli, R. Linking wireless devices using information contained in Wi-Fi probe requests. *Pervasive Mob. Comput.* **2014**, *11*, 56–69. [CrossRef]
20. Schauer, L. 2–Wi-Fi Tracking Threatens Users' Privacy in Fingerprinting Techniques. In *Geographical and Fingerprinting Data to Create Systems for Indoor Positioning and Indoor/Outdoor Navigation*; Conesa, J., Pérez-Navarro, A., Torres-Sospedra, J., Montoliu, R., Eds.; Intelligent Data-Centric Systems; Academic Press: Cambridge, MA, USA, 2019; pp. 21–43.
21. Barbera, M.V.; Epasto, A.; Mei, A.; Perta, V.C.; Stefa, J. Signals from the Crowd: Uncovering Social Relationships through Smartphone Probes. In Proceedings of the 2013 Conference on Internet Measurement Conference. Association for Computing Machinery, Barcelona, Spain, 23–25 October 2013; pp. 265–276.
22. Oliveira, L.; Schneider, D.; De Souza, J.; Shen, W. Mobile Device Detection through WiFi Probe Request Analysis. *IEEE Access* **2019**, *7*, 98579–98588. [CrossRef]
23. Oliveira, L.; Henrique, J.; Schneider, D.; de Souza, J.; Rodriques, S.; Sherr, W. Sherlock: Capturing Probe Requests for Automatic Presence Detection. In Proceedings of the 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanjing, China, 9–11 May 2018; pp. 848–853.

24. Alam, S.; AL-Qurishi, M.; Souissi, R. Estimating indoor crowd density and movement behavior using WiFi sensing. *Front. Internet Things* **2022**, *1*, 967034. [CrossRef]
25. Djervbrant, K.J.; Häggström, A. A Study on Fingerprinting of Locally Assigned MAC-Addresses. Bachelor's Thesis, Halmstad University, School of Information Technology, Halmstad, Sweden, 2019.
26. Fabre, L.; Bayart, C.; Bonnel, P.; Mony, N. The potential of Wi-Fi data to estimate bus passenger mobility. *Technol. Forecast. Soc. Chang.* **2023**, *192*, 122509. [CrossRef]
27. Moser, I.; McCarthy, C.; Jayaraman, P.P.; Ghaderi, H.; Dia, H.; Li, R.; Simmons, M.; Mehmood, U.; Tan, A.M.; Weizman, Y.; et al. A Methodology for Empirically Evaluating Passenger Counting Technologies in Public Transport. In Proceedings of the Australasian Transport Research Forum, Canberra, Australia, 30 September–2 October 2019.
28. Hidayat, A.; Terabe, S.; Yaginuma, H. Mapping of MAC Address with Moving WiFi Scanner. *Int. J. Artif. Intell.* **2017**, *1*, 34–40. [CrossRef]
29. Fisher, D. iOS 8 Will Randomize MAC Addresses to Help Stop Tracking. 2014. Available online: https://threatpost.com/ios-8-will-randomizemac-addresses-to-help-stop-tracking/106527/ (accessed on 6 June 2023).
30. Grumbach, E. iwlwifi: Mvm: Support Random MAC Address for Scanning. 2014. Available online: https://github.com/torvalds/linux/commit/effd05ac479b80641835f9126bbe93146686c2b8 (accessed on 6 June 2023).
31. "Android 6.0. (Marshmallow)". Android Developers. Available online: https://developer.android.com/about/versions/marshmallow/android-6.0-changes (accessed on 6 June 2023).
32. Huitema, C. Experience with MAC Address Randomization on Windows 10. 2015. Available online: https://www.ietf.org/proceedings/93/slides/slides-93-intarea-5.pdf (accessed on 6 June 2023).
33. Fenske, E.; Brown, D.; Martin, J.; Mayberry, T.; Ryan, P.; Rye, E. Three Years Later: A Study of MAC Address Randomization In Mobile Devices And When It Succeeds. *Proc. Priv. Enhancing Technol.* **2021**, *2021*, 164–181. [CrossRef]
34. Vanhoef, M.; Matte, C.; Cunche, M.; Cardoso, L.S.; Piessens, F. Why MAC address randomization is not enough: An analysis of Wi-Fi network discovery mechanisms. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 30 May–3 June 2016; pp. 413–424.
35. *IEEE Std 802.11u-2011*; IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 6: Interworking with External Networks. IEEE: Piscataway, NJ, USA, 2011.
36. Cunche, M.; Matte, C. On Wi-Fi tracking and the pitfalls of MAC address randomization. In Proceedings of the National Internet of Things Day. New Challenges of the Internet of Things: Human-Computer Interaction and Human Factors, September 2016. Available online: https://ido2016.sciencesconf.org/122873/Privacy_v4.pdf (accessed on 6 June 2023).
37. He, T.; Tan, J.; Chan, S.H.G. Self-Supervised Association of Wi-Fi Probe Requests Under MAC Address Randomization. *IEEE Trans. Mob. Comput.* **2022**, 1–14. [CrossRef]
38. Status of IEEE 802.11 Randomized and changing MAC Address Study Group. Available online: https://www.ieee802.org/11/Reports/rcmtig_update.htm (accessed on 6 January 2023).
39. Andersdotter, A. Ongoing Developments in IEEE802.11 WLAN Standardization. Available online: https://petsymposium.org/2019/files/hotpets/andersdotter-wlan.pdf (accessed on 15 January 2023).
40. *IEEE Std 802.11aq-2018* ; IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems Local and Metropolitan Area Network–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Preassociation Discovery. IEEE: Piscataway, NJ, USA, 2018.
41. IEEE 802.11bh and 802.11bi: Short Introduction and Update. Available online: https://datatracker.ietf.org/meeting/112/materials/slides-112-madinas-ieee-80211bhbi-update-01 (accessed on 15 January 2023).
42. Matte, C.; Cunche, M. *Spread of MAC Address Randomization Studied Using Locally Administered MAC Addresses Use Historic*; Research Report RR-9142; Inria Grenoble Rhône-Alpes: Montbonnot-Saint-Martin, France, 2018.
43. Vasilevski, I.; Blazhevski, D.; Pachovski, V.; Stojmenovska, I. Five Years Later: How Effective Is the MAC Randomization in Practice? The No-at-All Attack. In Proceedings of the ICT Innovations 2019—Big Data Processing and Mining, Ohrid, North Macedonia, 17–19 October 2019; Springer International Publishing: Cham, Switzerland, 2019; pp. 52–64.
44. Gomez, C.A.; Guerrero, L.J.; Pedraza, L.F. Evolution of the Use of Random MAC Addresses in Public Wi-Fi Networks. *J. Eng. Sci. Technol. Rev.* **2022**, *15*, 147–152. [CrossRef]
45. NS-3 a Discrete-Event Network Simulator. Available online: https://www.nsnam.org/ (accessed on 6 June 2023).
46. Forouzan, B.A. *Data Communications and Networking*, 3rd ed.; McGraw-Hill, Inc.: New York, NY, USA, 2003.
47. Tanenbaum, A.S.; Wetherall, D. *Computer Networks*, 5th ed.; Prentice Hall: Boston, MA, USA, 2011.