energies

MDPI

Article

StegoDCF: A New Covert Channel for Smart Grids Utilizing the Channel Access Procedure in Wi-Fi Networks

Marek Natkaniec * and Jakub Dyrcz

Institute of Telecommunications, AGH University of Krakow, al. Mickiewicza 30, 30-059 Krakow, Poland; jdyrcz@student.agh.edu.pl

* Correspondence: natkanie@agh.edu.pl

Abstract: Wi-Fi networks within the smart grid play a vital role in enabling communication between smart meters and data collectors. They are also frequently used in automation and metering, distribution control and monitoring, and distribution protection. However, a significant challenge arises from the uncertainty surrounding the genuine identity of data recipients. In this paper, we propose an efficient and novel covert channel that leverages the IEEE 802.11 DCF to transmit data requiring a high level of security. It is also the world's first covert channel supporting quality of service (QoS). Our protocol was implemented and tested in the ns-3 simulator, achieving very high-performance results. Its performance remains robust even under saturated network conditions with additional background traffic generated by other stations. This covert channel presents a novel approach to securely transmitting large amounts of QoS data within the smart grid.

Keywords: smart grid; IEEE 802.11; covert channel; DCF; backoff procedure; QoS

1. Introduction

The smart grid (SG) [1] leverages advanced communication technologies to enhance the efficiency, reliability, and sustainability of energy delivery systems. By integrating various communication technologies, SGs enable real-time monitoring, control, and optimization of electricity generation, transmission, distribution, and consumption. The internationally acknowledged SG standard, IEC 61850 [2], has formalized the seamless exchange of data across local area networks (LANs), ensuring interoperability among different systems. With appealing features such as cost-effectiveness in installation, high-speed data transfer capabilities, and ease of implementation, wireless local area network (WLAN) technologies are increasingly capturing the interest of power utilities. Wi-Fi can serve as a communication medium for SG devices, such as smart meters, sensors, and control systems. By leveraging existing WLAN networks or deploying dedicated Wi-Fi-enabled devices, utilities can establish robust communication channels for real-time data exchange, enabling better monitoring and control of grid operations. As SGs rely heavily on data exchange and remote control, robust cybersecurity measures are essential to protect against cyber threats and ensure the integrity and privacy of grid data. Advanced encryption, authentication mechanisms, and intrusion detection systems are deployed to safeguard critical infrastructure and sensitive information. While Wi-Fi offers convenience and connectivity, security remains a critical concern, especially in mission-critical SG applications. Utilities must implement robust security measures to safeguard Wi-Fi-enabled devices and prevent unauthorized access or tampering with grid infrastructure. Future applications used in SGs will also require support for the transmission of data with appropriate quality of service (QoS) provided.

A covert channel is a communication channel that allows data to be conveyed using the structure of another, already existing medium in a way that is normally undetectable. Transmitting messages through a covert channel is related to steganography and serves as an alternative to cryptography for securing communication. Cryptographically secured

check for updates

Citation: Natkaniec, M.; Dyrcz, J. StegoDCF: A New Covert Channel for Smart Grids Utilizing the Channel Access Procedure in Wi-Fi Networks. *Energies* **2024**, *17*, 2021. https://doi.org/10.3390/en17092021

Academic Editor: Sen Tan

Received: 24 March 2024
Revised: 21 April 2024
Accepted: 23 April 2024
Published: 25 April 2024

messages, no matter the cryptosystem chosen, and no matter how unbreakable, will arouse interest and may cause trouble for the communicating parties. On the other hand, steganography (from Greek 'steganographia', with 'steganos' meaning covered or concealed and 'graphia' meaning writing) is the practice of embedding hidden information within another message or physical object. Its primary goal is to remain undetected. There are two distinct types of covert channels—timing-based and storage-based channels. Timing-based channels send information by modulating some observable aspect of system behavior over time, while storage-based channels convey information by editing specific bits in the overt message to camouflage another in it.

In this paper, we present a novel covert communication channel, leveraging the IEEE 802.11 [3] DCF. The proposed covert channel and its modifications are of a hybrid variety, containing elements of both storage- and timing-based approaches. Its efficiency is four times higher than our previous covert channel expounded on in [4]. This covert channel serves to enhance communication within the SG network, specifically between smart meters and data collectors, with the primary objective of bolstering security and privacy. It also enables the provision of services that require real-time frame delivery.

In this paper, we present the following contributions:

- Proposal of a new covert channel—we propose a new covert channel mechanism that uses the 'Duration' field of the MAC frame header to hide covert data. We also modify the method presented in [4] to make it resistant to stego-analysis.
- Proposal of a new hybrid solution—we propose an unprecedented solution, where information is hidden in two independent locations of the DCF, which increases its resistance to stego-analysis.
- Proposal of the enhanced cover channel with QoS support—we propose the world's first covert channel, which is capable of transmitting data with varying priorities.
- Evaluation of the covert channel's performance—we assess the covert channel's performance by evaluating its behavior with the UDP transport protocol.
- Assessment of the covert channel's performance across varied IEEE 802.11 parameters—we delve into the performance evaluation of the covert channel, considering variations in duration/ID bits, frame length, and QoS classes.
- Analysis of the covert channel's performance under saturation conditions—we conduct a critical analysis of the covert channel's performance under saturation conditions.
- Examination of loads offered by other stations—our performance studies include an examination of the load imposed by neighboring stations on the covert station while operating under saturation conditions.
- Analysis of covert station signaling—we conduct a thorough analysis of the covert station's signaling required to transmit data with QoS support on the overall channel throughput.

This article presents a pioneering effort that introduces the application of an IEEE 802.11 covert channel to enhance security within the SG network. Our contribution is distinguished by its innovative approach, which leverages the randomness of the IEEE 802.11 backoff mechanism and the operation of the 'Duration' field of the MAC frame transmitted with the DCF to maintain covert channel concealment. By implementing a covert channel within the IEEE 802.11 network, we not only enhance the security and confidentiality of communications in SGs but also improve resilience against potential threats. Moreover, our work paves the way for further exploration of covert communication mechanisms and QoS aspects in SG networks.

The remainder of the paper is organized as follows. First, we provide an overview of the literature in Section 2. Then, in Section 3, we provide an overview of IEEE 802.11 architecture. In Section 4, we depict the proposed algorithm. A comprehensive presentation of the simulation results, including different scenarios, is presented in Section 5. Next, we present an enhanced covert channel mechanism with a virtually enhanced distributed channel access (EDCA) function; Section 7 evaluates its performance. We discuss the results in Section 8. Finally, we summarize the paper and outline future work in Section 9. We hope that this paper will facilitate further development and performance improvements of covert channel solutions for SG.

2. State of the Art

A critical aspect of SGs is in ensuring robust transmission security and cyber resilience. In [5], the authors propose a communication compensation block to bolster the resilience of distributed secondary control against communication impairments in the microgrids operated at the higher bandwidth. The proposed method aims to alleviate malicious time delays and communication imperfections within distributed networked controls utilized in the secondary layer of microgrids. This is achieved through prediction, estimation, and ultimately making decisions on transmitted data. Consequently, the proposed modification elevates the dynamic performance of the microgrids, enhancing system speed and robustness.

In [6], an analysis of the threats and potential solutions related to IoT-based SGs was conducted. The authors delved into various cyberattack types and offered a comprehensive overview of the cyber-security landscape concerning SGs. They specifically concentrated on discussing and examining network vulnerabilities, proposing attack countermeasures, and outlining security requirements. Furthermore, the paper elucidated on cyber-security vulnerabilities and corresponding solutions. Additionally, the authors provided guidance on future research directions concerning cyber-security in SG applications.

In [7], a review of the impact of cyberattacks on the entire SG ecosystem was provided. The authors analyzed the vulnerabilities of all components of the smart grid, including software, hardware, and data transmission. They also explored vulnerabilities related to data management, services, applications, and running environments. Reference also discussed attack strategies, consequences, and detection methods. The potential solutions for cyberattacks on SGs were analyzed in terms of blockchain technology and AI techniques. Reference also reviewed cyberattacks on SGs, documenting events recorded from 2010 to July 2022, including their impacts and consequences. The authors also provided future research directions for the robust cybersecurity of SGs against more sophisticated cyberattacks.

The researchers in [8] explored the application of AI techniques in microgrids with a focus on cybersecurity concerning physical devices and communication networks. Security vulnerabilities were examined under various cyberattacks that targeted sensor measurements, control signals, and information exchange. Their paper also summarized AI-based techniques for detecting and mitigating cyberattacks in microgrids. The authors paid special attention to learning-based AI techniques. Reference also included a case study of a test microgrid where the effectiveness of AI-based cyberattack mitigation in a distributed alternating current microgrid control was demonstrated. Future research directions were also outlined, including the application of AI techniques to enhance trust in AI-based models in microgrids.

The idea of classifying traffic with a minimum amount of information about the source and destination inspired the authors in reference [9]. The work was related to the analysis of threat detection in SGs based on network traffic analysis. They examined various datasets with different frequencies of the occurrence of threats. Long short-term memory, isolation forest, and support vector machine were considered in the study as machine learning techniques. Eight series of results were compared with other studies. The findings revealed notable variations among the techniques, dataset sizes, and the balance of datasets. The authors also showed that more accurate classification could be obtained by increasing the number of analyzed features.

An optimal method for feature selection and comparative techniques for results between different studies in the context of imbalanced datasets and threat identification in SGs were presented in [10]. The authors presented the state of the data science discipline and the most frequently employed methods of data analysis. They also revealed the most common errors and shortcomings in data analysis. The authors proposed new feature sets for training machine learning algorithms on the CSE CIC IDS2018 dataset and suggested effective techniques for feature selection. They also proposed several solutions that merit consideration for future research endeavors, focusing on the analysis of threats and trends in SGs.

In [11], the authors presented an overview of the SG, along with its main components, namely information technology (IT), operational technology (OT), and advanced metering infrastructure (AMI). Various vulnerable devices across IT, OT, and AMI were identified, and a concise description of each was provided. The authors proposed security measures that effectively mitigated the known threats of cyberattacks. The current architecture of the SG, the characteristics of SG devices, and cyberattacks were described. The limitations of current studies for advanced SG security were also explored. Additionally, the authors pinpointed novel research challenges and delved into prospective avenues for future research.

Several covert channels were proposed over the years for IEEE 802.11 networks. The first theoretical hidden channel was described and evaluated in [12,13]. The author proposed three channels—the first two were covert, but had low bandwidth, based on the cipher initialization vector (IV) field and medium access control (MAC) addresses in the MAC frame header, to be used for the configuration of the third one. The third channel used intentionally corrupted frames to more overtly transmit large amounts of data. The researchers in [14] analyzed the potential of hiding data in the frame control field of a MAC header and provided a partial implementation and analysis of the reliability, undetectability, and capacity of their proposed channels. They proposed two hidden channels using their analyzed method of encoding data. The first method relied on packet modification and the second one relied on the duplication of specific packets. Reference [15] proposed two hidden channels and a proposed communication protocol for them. One of the channels was based on modifying the sequence control data of a frame, while the other one was based on sending plain text or encrypted messages, three bytes at a time, using the IV field of a MAC header. Furthermore, in [16], the researchers implemented the proposed communication protocols in a user-friendly way, and proposed modifications to strengthen the channels against steganalysis. In [17], the authors updated the channels proposed in [14]. They also included a very in-depth analysis of the original implementation and their updates, which proved that the updates improved capacity, reliability, and non-detectability of the channels in question.

An innovative technique was proposed in [18], seeking to protect against replay attacks. The proposed covert channel used the IEEE 802.11b rate-switching algorithm as a cover for transmitting a one-time password, which authenticated the client to the access point. Reference also showed the minimal performance impact of the technique on the wireless network. The authors of [19] explored the possibility of using an interference channel in IEEE 802.11 networks to transmit hidden data. They demonstrated that it would be practical to have a covert sender, parallel to legitimate, authenticated senders in a network using this technique. The first OFDM (orthogonal frequency-division multiplexing)-based hidden channel was proposed in [20]. The scheme was based on the insertion of data into the padding of frames at the physical layer of IEEE 802.11a/g standards. The method offered very low detectability and bandwidths up to 1.1 Mbps or 0.44 Mbps, depending on the frame type used. Another innovative work [21] proposed hiding communication by dynamically switching from infrastructure mode to ad hoc mode, while simultaneously scrambling data at the MAC layer with optional data encryption using the VMPC algorithm. This proposal was primarily intended for military networks, although it also has potential for civilian covert communication. The channel provided great bandwidth without overcomplicating the protocol structure, although, while the messages would be hard to read as an adversary, they would not be hard to detect.

Reference [22] sought to design a new timing covert channel by exploiting the random backoff in the distributed coordinated function (DCF). The result was a relatively high-throughput covert channel that maintained 99% accuracy and could adapt to various network conditions. The researchers in [23] analyzed the viability of a hidden channel dependent on the modification of the protocol version field in the MAC header of clear-to-send (CTS) and acknowledgment (ACK) frames, as well as its robustness to errors. They conducted tests on the proposed channel, including measurements of the available data rate, channel errors, and channel detectability, as well as proposed techniques not used previously in similar channels, such as forward error correction and interleaving. To protect against rogue access points, the authors of [24] proposed a system based on sending access point authentication using the least significant bits of the timestamp field and beacon frames. The proposed mechanism had two modes of operation. The first one was based on writing information directly in the four least significant bits of the timestamp field. The second one was based on the modulation of the time difference between timestamps and the beacon interval. The authors noted the possibility of the general use of the proposed covert channel, but advised against it as it was a one-way method of communication.

The authors of [25] created an extensible application, which allowed detecting previously proposed MAC layer steganographic channels, as well as manual packet inspection for better clarity, minimizing false positives to prevent cluttering the output with duplicate or false warnings. As the detector application was entirely passive, it remained entirely undetectable to other network users. Covert channels remained largely unavailable to the general public, either because of difficult implementation or hardware costs. Reference [26] proposed a software radio implementation of systems proposed in [22]. The study also included tests of the viability of such a system on off-the-shelf hardware. Although only half of the simulated throughput of the implemented system could be achieved on real hardware, the work further proved that practical implementations allowed for a better judgment of the feasibility of proposed covert channel communication systems.

In [27], the authors proposed a novel high-capacity, covert channel through the use of simulated noise in the physical layer of IEEE 802.11a/g networks. The work also included a hardware implementation and a series of tests that confirmed the high degree of undetectability and high throughput of the proposed system. In time, new schemes for higher throughput channels were created, such as the one proposed in [28]. The researchers decided to modify cyclic prefixes in OFDM symbols, which when simulated was the fastest proposed covert channel at the time of publication while having a very high degree of undetectability. Reference [29] proposed the exploitation of IEEE 802.11e to create two new covert channels, which were low bandwidth but could be used with no disruption to the network traffic pattern, thus avoiding detection. The proposed channels use previously unused quality of service (QoS) bits in the header and also provide signaling to improve reliability.

The researchers in [30] analyzed the benefits of using multiple-input, multiple-output (MIMO) technology over single-input, single-output (SISO) for covert channels and proposed a new MIMO-exclusive covert channel using eigenbeam-space division multiplexing. The MIMO channel was superior to the SISO in terms of both lower bit error rates and higher undetectability. Inspired by the exploiting modification direction (EMD) method used in Joint Photographic Experts Group (JPEG) steganography, the authors of [31] proposed a new timing channel for the distributed coordination function (DCF). Their goal was to increase embedding efficiency and achieve higher throughput without compromising security. The idea was based on free time intervals in the network. Reference [32] analyzes further possibilities of OFDM-based physical channels for IEEE 802.11a/g networks and provides an analysis of the proposed channels in contrast to the previously described ones.

The researchers in [33] proposed a new covert channel with the goals of very low detectability and very high ease of implementation on off-the-shelf hardware. The included analysis concluded that while the proposed channel was feasible, it had a rather high error rate and very low bandwidth compared to alternatives, but accomplished goals of being very hard to detect and having a very simple implementation, requiring a change in the configuration of the adapter. To further research into MIMO-based covert channels, the authors of [34] proposed two new methods of transmitting hidden data in the uplink.

They rely on modifying the control and data channels of regular communication. Their work also discusses how to determine the parameters of proposed channels and validates the effectiveness of proposed schemes through implementation. Reference [35] described a novel wireless covert channel, based on intentionally causing errors in constellation shaping to transmit data. The proposed method was highly undetectable but lacked reliability to become viable.

The idea of a covert channel that does not decrease the signal-to-noise ratio of the primary channel inspired reference [36], which proposed a novel method that optimized the use of phase-shifting modulations to create a covert channel. The proposed mechanism encoded information by changing the amplitudes of primary symbols while keeping their phase intact. The covert channel was also readable with off-the-shelf hardware in testing. With the development of the IEEE 802.11ad standard, a new high-throughput covert channel was proposed in [37]. The authors proposed a channel that leveraged modulation and coding schemes along with link adaptation mechanisms to achieve a throughput of up to 150 Mbps over the covert channel, while only slightly degrading the quality of primary channel communication. In [38], K. Sawicki proposed a couple of mechanisms to covertly send control information to devices on the network, mostly using previously described methods with slight modifications.

The authors of [39] set out to improve the undetectability of MIMO-based covert channels compared to the state of the art at the time. Their proposed channel used generated artificial noise, modulated into the signaling of the primary channel to deliver a low error rate and hard-to-detect messaging. In [40], the researchers analyzed how to improve the covertness of OFDM-based physical layer hidden channels by using a cover signal to decrease the SNR of a warden. Successfully masking the signal had a measurable impact on the warden's awareness and ability to detect the covert message. The impact on the legitimate receiver was not measured. In [41], the authors proposed a more robust, adaptable dirty constellation-based system for high-speed covert communication. The proposed method was inspired by the usage of a drift correction modulation approach previously used to watermark audio.

The researchers in [42] conducted a mathematical analysis on the use of cover signals in OFDM to reduce the detectability of a hidden channel with minimal impact on the actual channel's performance. To do this, the authors analyzed the bit error rate (BER) and the codeword error rate (CER) at the warden. With the advent of internet-connected cars and the increasing presence of the IEEE 802.11p standard, the authors of [43] analyzed and simulated the viability of hiding data in the physical layer using wireless padding for cross-vehicle communication in non-ideal conditions. Their analysis revealed that throughput decreases as traffic rate, number of vehicles, and packet size increase, alongside BER. To further research into the usage of cover signals in OFDM-based wireless steganography for IoT, reference [44] analyzed the performance of such systems using simulations in varying parameters. The work also evaluated the secrecy of the proposed channel in the case of eavesdropping. The simulations confirmed that the proposed system was viable as information rates and CER guaranteed successful decoding of embedded data and the system's secrecy was within expectations.

In [45], a covert channel that used the MAC address randomization technique to create a covert channel was proposed. Researchers introduced the concept of the covert channel, its implementation, and performance evaluation. The authors analyzed different scenarios, including the adaptation of the modified selective repeat ARQ protocol to alleviate the impact of the number of stations and their offered loads on the covert channel. The results showed that with the appropriate parameter selections, the covert channel could be adapted to produce excellent throughput, high efficiency, low delay, and low jitter values.

A completely new approach was proposed in [4]. It exploits the same random backoff mechanism as in [22], but in a completely new, more covert way. It is more covert as it does not cause the covert sender to access the channel in an unfair way, which might draw suspicion. The main mechanism that was proposed and analyzed uses the parity of the backoff time of a station to broadcast information bit by bit. The method is obviously slow when transmitting large frames, but it inspired the authors of this contribution. This work aims to expand the proposed mechanism with a throughput that is four times higher. Furthermore, we propose a solution to provide QoS support in covert channels, a feature that is currently lacking in the literature.

3. Background

To properly apply steganographic techniques, the cover chosen for embedding must be thoroughly investigated in advance. The characteristic selected as the cover should not disrupt the normal operation of the network when tampered with. This section begins with a brief paragraph, discussing mechanisms employed to secure data transmission in the production environment, utilizing Wi-Fi networks. Then, we go over the relevant parts of normal IEEE 802.11 network operations and how regular packets and their distribution can be tampered with to create a hidden message of our choice.

The standard security mechanisms used in the context of data transmission protection over Wi-Fi networks includes the following: Wi-Fi-protected access (WPA), WPA2, and WPA3. WPA was introduced as an improvement over the older and less secure wired equivalent privacy (WEP) protocol. It uses the temporal key integrity protocol (TKIP) for encryption. TKIP dynamically generates encryption keys for each data frame, enhancing security. However, WPA still has vulnerabilities, especially when used with older devices. It provides better security than WEP but is not as robust as WPA2 or WPA3. WPA2 employs the advanced encryption standard (AES) for encryption, which is more secure than TKIP. It offers two modes: WPA2-Personal, which uses a pre-shared key (PSK) for authentication and is suitable for home networks, and WPA2-Enterprise, which requires a central authentication server (such as RADIUS) for user authentication. The second solution is more common in business environments. WPA2 is widely adopted and provides robust security against most attacks. However, it is not immune to vulnerabilities, such as the key reinstallation attack (KRACK), which targets the handshake process. WPA3 is the latest solution, designed to address WPA2's limitations. It uses a stronger encryption algorithm called GCM (Galois/Counter Mode). The other main key differences include the following: the 192-256 bit encryption key, simultaneous authentication of equals (SAE), which provides stronger protection against brute-force attacks during the initial handshake, and forward secrecy, which ensures that compromising one session key does not affect others. WPA3 is recommended for enhanced security, but not all devices support it yet. While WPA2 remains a solid choice for most networks, transitioning to WPA3 as devices become compatible is advisable for better protection against emerging threats. However, it should be noted that the infrastructure based on WPA2 will likely survive for many more years. Despite the development of security mechanisms in IEEE 802.11 networks, hiding additional information in the form of implementing steganographic channels is considered a solution that increases the confidentiality of transmitted data despite limitations usually resulting from the reduced bandwidth of the covert channel.

The first element that the proposed algorithm will utilize differently from its intended purpose is the DCF. DCF provides the logic for access to the shared medium that all stations (STAs) within a given basic service set (BSS) use for communication. To contend for access, all STAs desiring to initiate the transfer of data frames or management frames invoke the carrier sense (CS) mechanism to determine whether the medium is in a busy or idle state. If the medium is busy, the STA should defer until the medium is determined to be idle, with no interruptions for a period equal to the extended inter-frame space (EIFS) if the last transmission is not received correctly or DCF inter-frame space (DIFS) otherwise. After that idle period, the STA must generate a random backoff count for additional deferral time before transmitting. If the backoff counter already contains a non-zero value, it should continue using the previously established count. The random value is an integer drawn from an inclusive interval between 0 and the contention window (CW). The CW parameter starts at CWmin and increases in a predetermined manner until it reaches CWmax or a frame is successfully transmitted.

The second and final element that the proposed algorithm will utilize differently from its intended use is the duration/ID field in the MAC frame header, as described in [3], Section 9.2.4.2 (see Table 1). The contents of the duration/ID field vary depending on the frame type and subtype, as well as the QoS capabilities of the sending station STA. The contents of the field are defined in three groups:

1. In the control frames of the subtype PS-Poll (power save polling) other than PS-Poll+BDT (bi-directional transmit opportunity) frames, and for broadcast transmissions in S1G PPDUs (sub 1 GHz physical layer protocol data units), the duration/ID field carries the association identifier (AID) of the STA that transmits the frame in the 14 least significant bits (LSBs), and the 2 most significant bits (MSBs), both set to "1".
2. In all other frames sent by non-QoS STAs and other control frames sent by QoS STAs, the duration/ID field contains a duration value as defined individually for each frame type in the standard (described more in-depth below).
3. In data and management frames sent by QoS STAs and extension frames, the duration/ID field contains a duration value, but it is not relevant to this paper's contents.

Within all non-QoS data frames, the 'Duration' field is set according to the following rules:

- If the 'Address 1' field contains a group address, the 'Duration' field is set to 0.
- If the 'More Fragments' bit is 0 in the frame control field of a frame and the 'Address 1' field contains an individual address, the 'Duration' field is set to the time, in microseconds, required to transmit one ACK frame, plus one short inter-frame Space (SIFS).
- If the 'More Fragments' bit is 1 in the frame control field of a frame and the 'Address 1' field contains an individual address, the 'Duration' field is set to the time, in microseconds, required to transmit the next fragment of this data frame, plus two ACK frames, plus three SIFSs.

The 'Duration' field calculation depends on the data rate at which control frames are transmitted. If the calculated duration includes a fractional microsecond value, it is rounded up to the nearest integer. All STAs process the value of the 'Duration' field—as long as it fits within the range of 0–32,767—of all valid data frames (not regarding the receiver address (RA), destination address (DA), and/or basic service set identifier (BSSID) address values that might be present in these frames) to upgrade the network allocation vector (NAV) settings, depending on the coordination function rules.

Table 1. Duration/ID field encoding (taken from [3], page 767, Table 9-9).

Bits 0-13	Bit 14	Bit 15	Usage
0–32,767		0	Duration value (in microseconds) within all frames except PS-Poll frames that are not PS-Poll+BDT.
0–16,383	0	1	Reserved
0	1	1	AID 0 is used for broadcast transmission in S1G PPDU, reserved if not in S1G PPDU.
1–2007	1	1	AID in PS-Poll frames other than PS-Poll+BDT.
2008–8191	1	1	Additional AIDs in S1G PS-Poll frames other than PS-Poll+BDT. Reserved if not in S1G PS-Poll frames.
8192–16,383	1	1	Reserved

4. Proposal for a StegoDCF Covert Channel

The proposed covert channel uses both the CW and the duration/ID field to send a hidden transmission of 4 bits per MAC frame. The CW approach is possible thanks to the random nature of CSMA/CA used in IEEE 802.11 networks. This method was taken with some modifications from [4] and is used to send the first secret bit per frame (see Figure 1). To send a "1" or a "0", the receiving STA reads the backoff time of the sender. A backoff of an even number of slot times since the last transmission translates to a "0" in a message and an odd number of slot times translates to a "1". What is new in the proposed mechanism is the method of determining backoff slots, depending on the number of frame retransmission attempts, which makes it resistant to stego-analysis. To modulate the backoff time and, thus, the sent data, the transmitter manipulates the number of slots. If the sender is nearing the end of their backoff period and the number of waited slots is less than expected, the sender will delay broadcasting by waiting an additional slot, unless this delay is due to a third or subsequent attempt to transmit following collisions. In that situation, the sender decrements the backoff counter to give themselves an unfair advantage in an effort to balance out the transmission delays that backoff time manipulation has caused.

The proposed algorithm used for creating a covert channel will not interfere with the regular operation of this network as the covertly transmitting STA will manipulate its random backoff value mostly against its own interests (by increasing it), thus allowing other clients to—at times—assume the preferred position in the contention queue. To avoid being infinitely delayed, the random backoff may be reduced by the covertly transmitting STA, but only after two consecutive transmission failures, to prevent placing it at too much of a disadvantage.

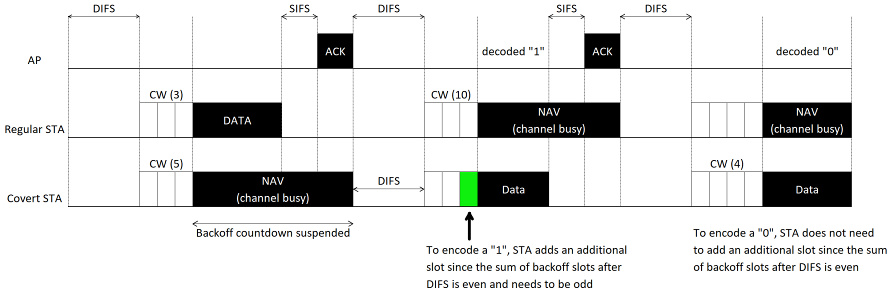
DIFS
SIFS
DIFS
SIFS
DIFS
AP
ACK
decoded "1"
ACK
decoded "0"
Regular STA
CW (3)
DATA
CW (10)
NAV
(channel busy)
NAV
(channel busy)
Covert STA
CW (5)
NAV
(channel busy)
DIFS
Data
CW (4)
Data
Backoff countdown suspended
To encode a "1", STA adds an additional slot since the sum of backoff slots after DIFS is even and needs to be odd
To encode a "0", STA does not need to add an additional slot since the sum of backoff slots after DIFS is even

Figure 1. Covert STA sending "0" and "1", encoded using the contention window (based on [4], Figure 1).

Our new proposed mechanism for encoding the next three bits of the message uses the three least significant bits of the duration/ID field (not counting bit 15 as it is always 0 if the field describes duration) in the MAC header of the frame, as shown in Figure 2. They are read as-is by the receiver. This allows for increasing the efficiency of the entire mechanism by another 300%. However, it must be admitted that this mechanism has the side effect of causing a slight timing deviation in the network. The choice of the three least significant bits in the 'Duration' field is deliberate as the maximum timing deviation it may cause is 7 µs, which is less than the shortest xIFS time (SIFS) for the analyzed IEEE 802.11ax network (see Table 2). Using 4 bits would cause it to cause deviations of up to 15 µs, so to reduce the risks of making the network unstable it was forgone. In Section 5.2, we present a study on the impact of the number of duration/ID field bits on the covert channel performance.

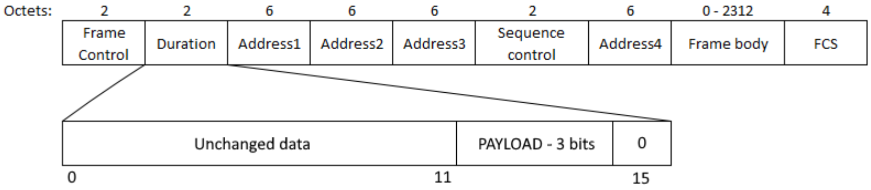

Figure 2. Data hidden in the duration/ID field.

The algorithm creating a covert channel, as proposed, will not interfere with the normal operation of the IEEE 802.11 network, because the only bits manipulated for the purpose of concealing data are the 3 least significant bits (bits 12–14, not counting bit 15 as it is always set to 0), which allows the duration to be shortened or lengthened by up to 7 µs, which is an insignificant amount of time in almost all IEEE 802.11 standards as it is shorter than the SIFS time. With the only exception being IEEE 802.11ad (operating at 60 GHz) with an µs SIFS time of 3, all other standards such as IEEE 802.11b/g/n (operating at 2.4 GHz) with a SIFS of 10 µs, IEEE 802.11a/n/ac/ax (operating at 5 GHz) with a SIFS of 16 µs, or IEEE 802.11ah (operating at 900 MHz) with a SIFS of 160 µs will work without issues with this scheme.

Table 2. SIFS in IEEE 802.11 standard extensions (data from [3,46]).

Standard	SIFS (µs)
IEEE 802.11-1997 (FHSS)	28
IEEE 802.11-1997 (DSSS)	10
IEEE 802.11b	10
IEEE 802.11a	16
IEEE 802.11g	10
IEEE 802.11n (2.4 GHz)	10
IEEE 802.11n, IEEE 802.11ac (5 GHz), IEEE 802.11ax	16
IEEE 802.11ah (900 MHz)	160
IEEE 802.11ad (60 GHz)	3

The pseudocode in Algorithms 1 and 2 illustrates how the sender encodes and transmits a message:

Algorithm 1 Encoding a message bit in CW.

```
$m$—bit to encode
$d$—slots since the last transmission
$r$—retransmission count

procedure ENCODEBITINCW($m, d, r$)
    if $m = 0$ then
        if $d$ is odd then
            if $r < 3$ then
                Increment the number of slots left in the backoff
            else
                Decrement the number of slots left in the backoff
            end if
        end if
    else if $m = 1$ then
        if $d$ is even then
            if $r < 3$ then
                Increment the number of slots left in the backoff
            else
                Decrement the number of slots left in the backoff
            end if
        end if
    end if
end procedure
```

Algorithm 2 Encoding a fragment in the duration/ID field.

```
$m$—bits to encode [0 < length(m) <= 3]
$d$—Duration/ID field in MAC Header

procedure EncodeBitInDuration($m$, $d$)
    if $length(m) < 3$ then                ▷ zero-fill all fields with no relevant data
        Zero-fill the $m$ array
    end if
    $d[12] \leftarrow m[0]$
    $d[13] \leftarrow m[1]$
    $d[14] \leftarrow m[2]$
end procedure
```

5. Performance Evaluation of the StegoDCF Covert Channel Algorithm

In this section, we describe the simulation environment and simulation results for different network topologies and configurations.

5.1. Simulation Environment

The covert channel was implemented using the ns-3 discrete-event network simulator (version 3.40) [47]. This open-source simulator—constructed using C++ and Python 3—offers a plethora of functionalities, notably encompassing robust support for simulating IEEE 802.11 networks. NS-3 emerged as the prime selection owing to its seamless alignment with the latest IEEE 802.11ax standard, its dynamic and helpful community, and its continual growth over time. Within simulations, NS-3 provides adaptability, effectively simplifying the intricacies of IEEE 802.11 networks within a simulated domain. Table 3 shows the general network parameters used for all simulations, unless specified otherwise in the description of a specific simulation. All figures in simulations had errors and run-to-run variances under 1% and, thus, were omitted from graphs for better readability.

Table 3. Simulation parameters.

Parameter	Value
IEEE standard	802.11ax
Transport protocol	UDP
Frequency band	2.4 [GHz]
Channel width	40 [MHz]
Guard interval	400 [ns]
SIFS	16 [µs]
DIFS	34 [µs]
Time slot	9 [µs]
MCS index	9
RTS/CTS	Disabled
Number of Tx and Rx antennas	1

5.2. Impact of the Number of Duration/ID Bits Used on the Covert Channel

The first scenario involves five covert STAs connected to a single AP (as shown in Figure 3). The STAs exchange user datagram protocol (UDP) data under non-saturation conditions with 50 Mbps of the total offered load. The experiment examined how changing the number of duration/ID field bits used to encode covert channel transmissions, starting from 0 and ending with 12 data bits (in addition to the single bit encoded in the backoff mechanism), affects the performance of the covert channel. The results are illustrated in Figures 4–7.

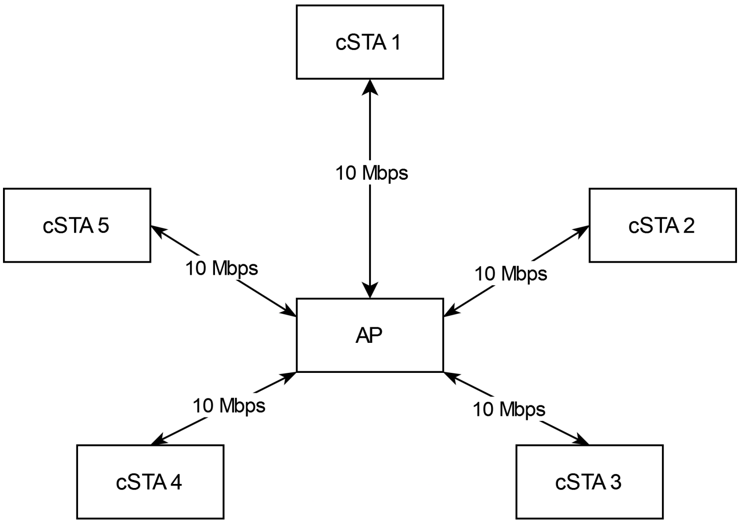

Figure 3. Topology of the first simulation scenario.

Figure 4 shows that the efficiency of the covert channel decreases with the growth of the number of duration/ID bits used in transmission. This is due to the increasing error in the reported transmission duration, which leads to further collisions, especially between stations that are not the recipient of a given transmission and make subsequent transmission decisions based on the NAV vector. Using more than seven bits leads to efficiency degradation. At that point, the deviation from the correct transmission duration value reaches 128 µs or slightly more than DIFS and 10 time slots. From the 9th bit onward, the efficiency rapidly declines, reaching 60% at 11 bits and going below 40% at 12 bits.

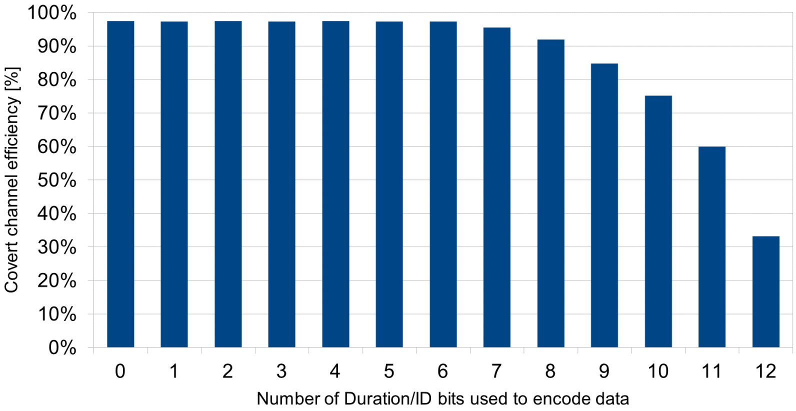

Figure 4. Covert channel efficiency vs. the number of duration/ID bits used to encode data.

Figure 5 shows that the impact of the number of duration/ID field bits used to encode data on covert channel throughput is not straightforward. The graphed outcome of the experiment shows a curve with a local maximum at 9 bits, where the covert channel nearly reaches 7 kbps. This peak is due to significant increases in the amount of data being sent in one frame, which offsets the efficiency issues. However, it is worth noting that immediately after this point, the throughput consistently plummets, aligning with previous results.

Figures 6 and 7 show that changes in the duration/ID field slightly impact delays and jitters experienced by the network in which the covert channel is active, but these effects remain within acceptable limits regardless of the parameters. The delay peaks at about 1.8 ms, which is just a 0.6 ms increase over the baseline observed when the covert channel is disabled. Meanwhile, the jitter reaches just above 1.2 ms at its peak, which is only slightly less than 0.5 ms higher than under normal conditions for the tested network.

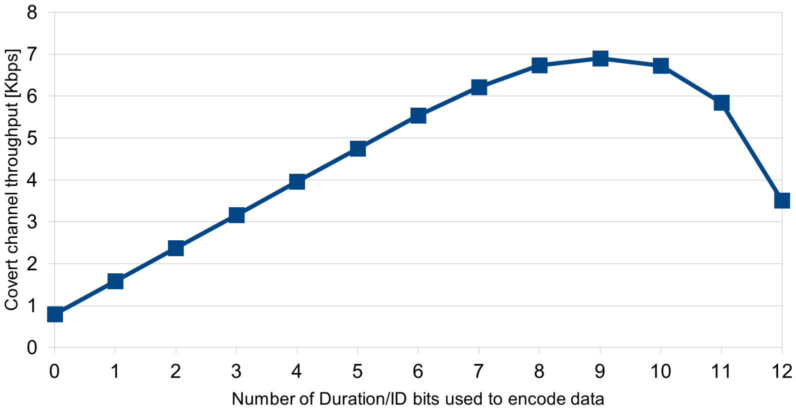

Figure 5. Covert channel throughput vs. number of duration/ID bits used to encode data.

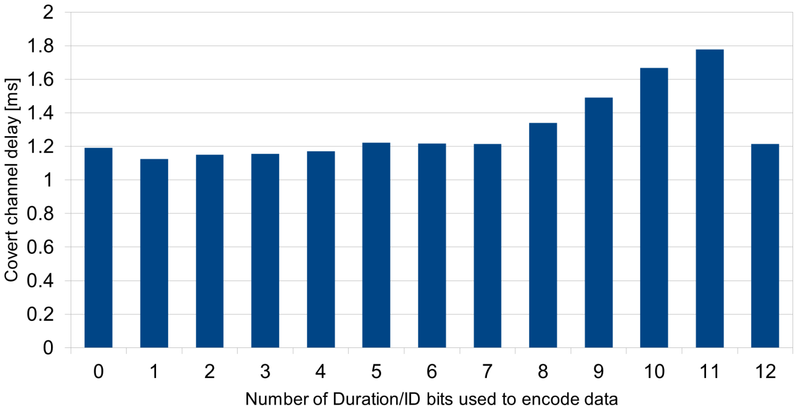

Figure 6. Covert channel delay vs. number of duration/ID bits used to encode data.

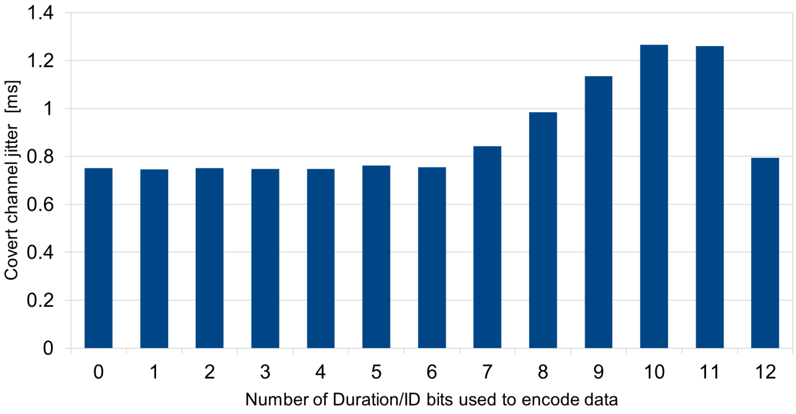

Figure 7. Covert channel jitter vs. number of duration/ID bits used to encode data.

5.3. Covert STA with No Background Traffic

The second experiment involves a single covert STA and a single AP with no background STAs and no background traffic in the network (see Figure 8). The STA generates UDP traffic at a constant frame size with an increasing generated network load. The covert STA uses three duration/ID field bits to carry its payload, as this is determined to be both safe for channel health and difficult to detect due to the low amount of generated anomalies. The experiment is repeated with different frame sizes and aims to measure the impact of the covert STA's load on the covert channel's throughput and delay.

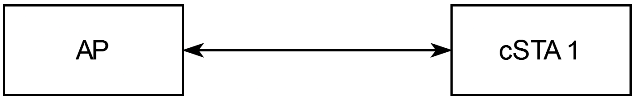

Figure 8. Topology of the second simulation scenario.

Figure 9 shows the impact of the generated load on the throughput of the covert channel. The findings indicate that the channel throughput increases linearly up to a certain point and then remains constant. The frame size significantly impacts the overall channel throughput; smaller frames occupy the channel for shorter durations, thus allowing more frames to be sent within the same timeframe, which directly increases the throughput. Another thing worth noting is that the plateau point can be directly correlated with the point of network saturation and scales slightly with the size of the frames sent. The smaller frames lead to more network overhead, which leads to faster network saturation. The obtained results confirm that the efficiency of the proposed covert channel is four times higher than the covert channel described in [4].

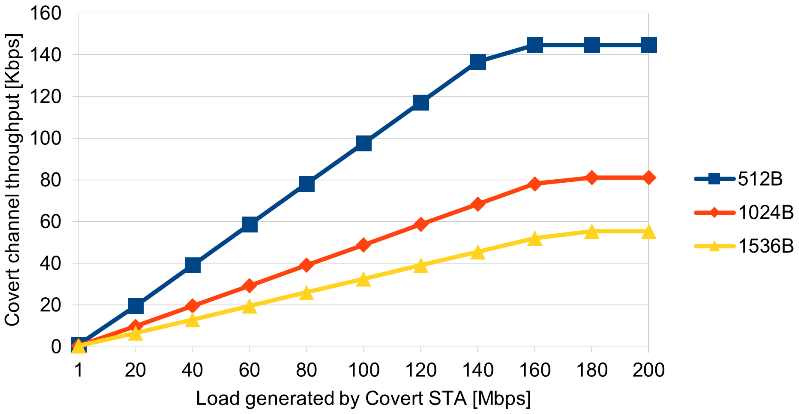

Figure 9. Covert channel throughput vs. frame size and network load generated by the covert STA.

Figure 10 shows that the impact of the covert channel on network delay is negligible until the network saturation point. The figure also very clearly shows the approximate saturation point for each frame size as we can clearly notice a sharp increase in network delays for each frame size (160 Mbps for 512 B and 180 Mbps for 1024 B and 1536 B, just becoming worse at 200 Mbps). Below the 160 Mbps mark, the delays are entirely within acceptable limits for an IEEE 802.11ax standard network.

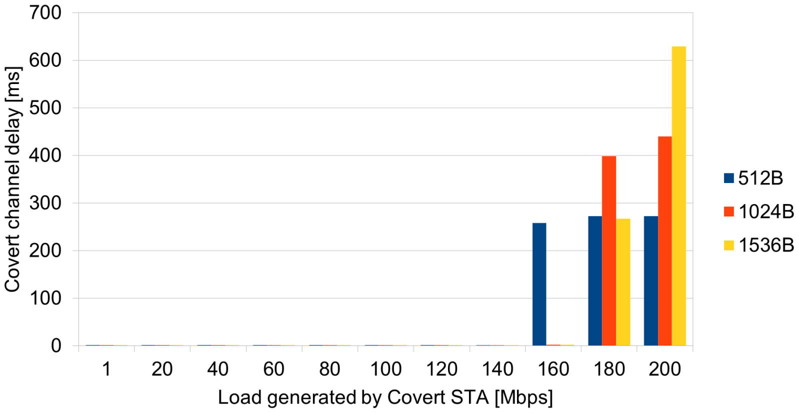

Figure 10. Covert channel delay vs. frame size and network load generated by covert STA.

5.4. Covert STA with Background Traffic

The third and final experiment for the basic algorithm involves a single covert STA communicating with a single AP with a set number of background stations generating background traffic (Figure 11). All STAs generate UDP traffic at a constant frame size. The covert STA uses the same frame size as background STAs and uses three duration/ID fields to carry the data on top of the backoff mechanism. Additionally, the covert STA constantly sends data at 200 Mbps. The experiment is repeated for different numbers of background STAs and different frame sizes.

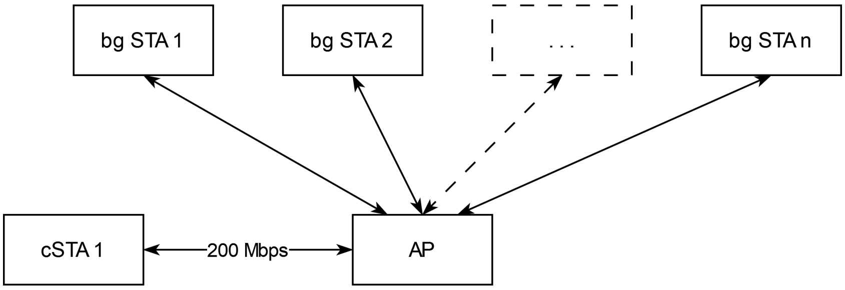

Figure 11. Topology of the third simulation scenario.

Figures 12–14 show the throughput of the covert channel for 512 B, 1024 B, and 1536 B frames. This simulation shows that an increase in the number of background stations has a much greater impact on channel throughput than the total load they provide. Additionally, the three figures show that the frame size scales identically to that without any background load.

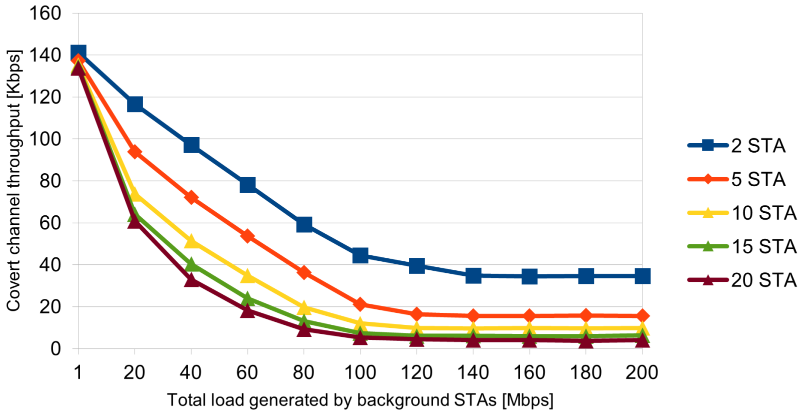

Figure 12. Covert channel throughput vs. number of background STAs and background network load for 512 B frames.

Figures 15–17 show how the number of background STAs impacts the channel efficiency for 512 B, 1024 B, and 1536 B frames. The efficiency, as opposed to throughput, is not so sensitive to the transmitted frame size. As the traffic generated by background STAs increases, the effectiveness of the covert channel decreases. The greater the number of STAs generating background traffic, the lower the effectiveness of the covert channel for a given value of the offered load. The longer the data frame transmitted by the covert station, the greater the efficiency, but the differences between the shortest (512 B) and the longest (1536 B) frames are not large, especially for large traffic values.

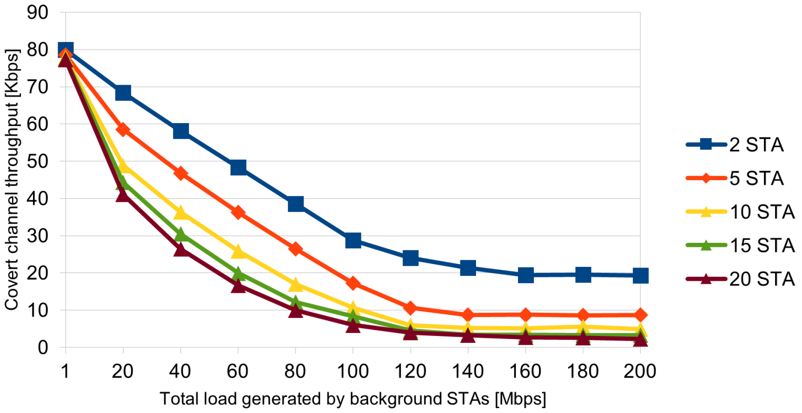

Figure 13. Covert channel throughput vs. number of background STAs and background network load for 1024 B frames.

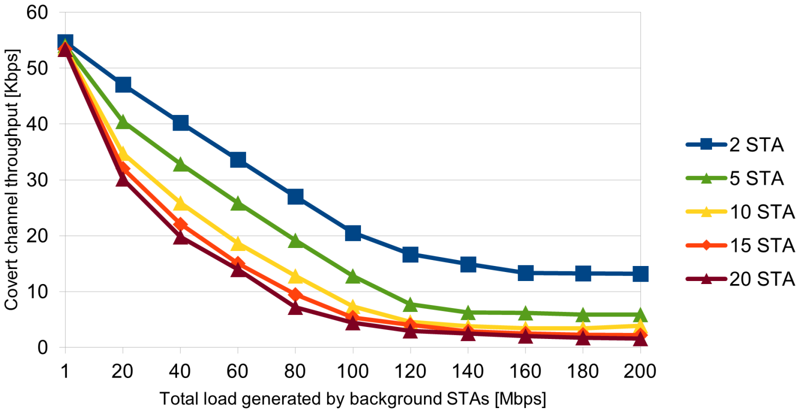

Figure 14. Covert channel throughput vs. number of background STAs and background network load for 1536 B frames.

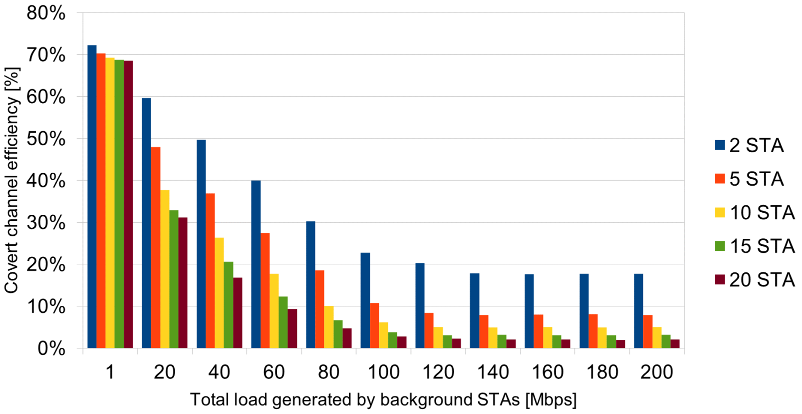

Figure 15. Covert channel efficiency vs. number of background STAs and background network load for 512 B frames.

Finally, Figures 18–20 show the impact of background STAs on jitter. Here, the impact of the frame size and the number of background stations are the most evident. For lower frame sizes, the jitter always remains at acceptable levels, staying well below 1.8 ms even for 200 Mbps of load and 20 background STAs. The use of longer frames, as expected, increases the jitter value, but the obtained values do not exceed 2.5 ms for 1024 B frames and 3.6 ms for 1536 B frames (in both cases for 20 background STAs and saturation conditions).

For small values of offered traffic that do not yet saturate the network, jitter is minimal, regardless of the frame size and the number of STAs generating background traffic.

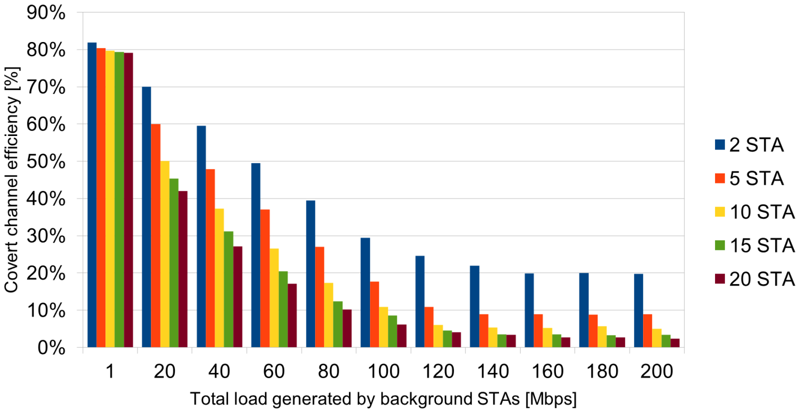

Figure 16. Covert channel efficiency vs. number of background STAs and background network load for 1024 B frames.

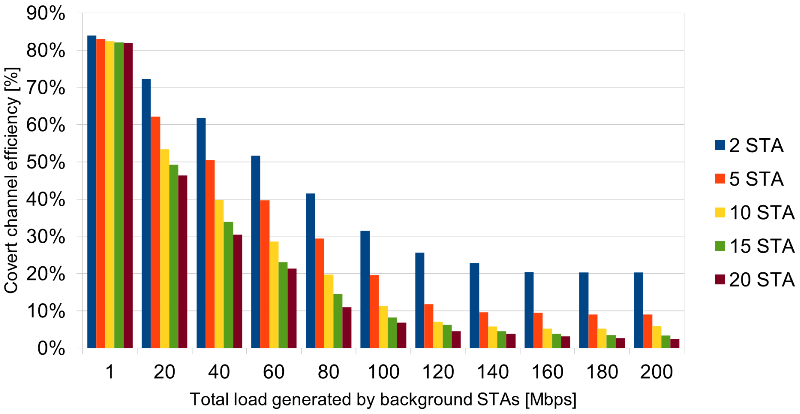

Figure 17. Covert channel efficiency vs. number of background STAs and background network load for 1536 B frames.

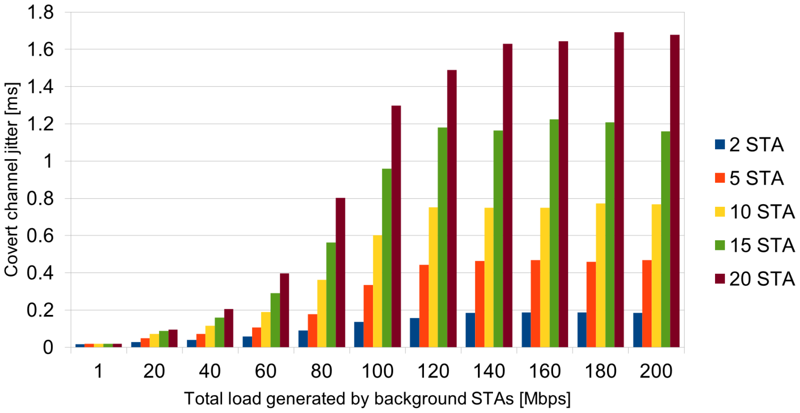

Figure 18. Covert channel jitter vs. number of background STAs and background network load for 512 B frames.

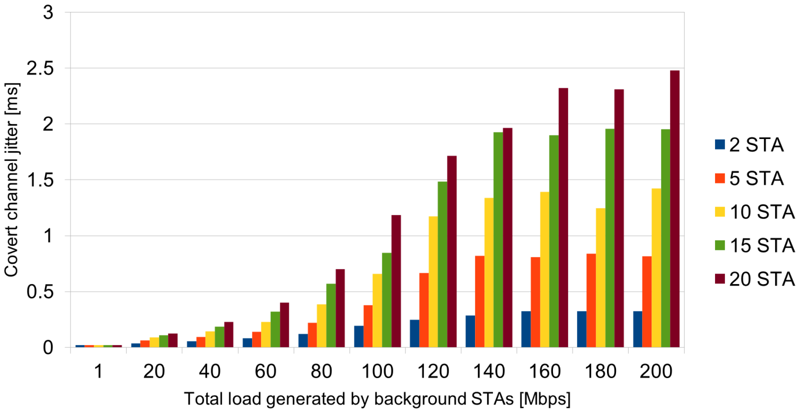

Figure 19. Covert channel jitter vs. number of background STAs and background network load for 1024 B frames.

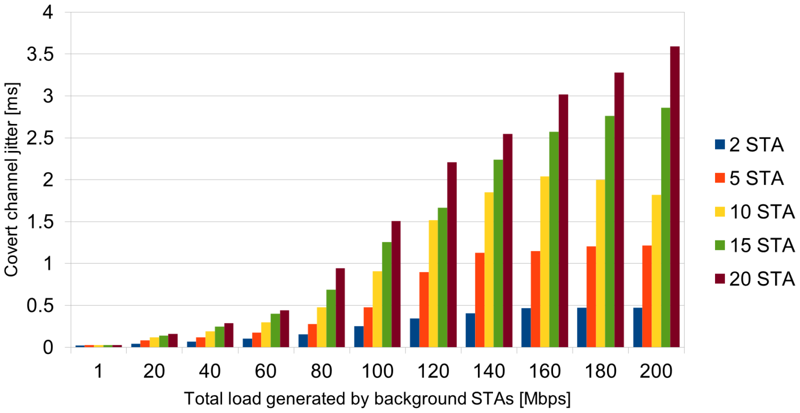

Figure 20. Covert channel jitter vs. number of background STAs and background network load for 1536 B frames.

6. Enhancements to the Algorithm—Covert Channel with QoS Support

The covert channel can be enhanced with the use of virtual QoS queues to allow for multiple concurrent data streams with varying priorities. The simplest QoS mechanism to implement is a strict priority queue—the populated queue with the highest priority items being emptied first. The proposed signaling mechanism is a basic code, indicating a class change. The difficulty in designing such a code for a covert channel is in keeping the code both covert and clearly readable at the same time; another problem is ensuring its low overhead.

The proposed mechanism enhancement has four QoS classes, similar to the number of QoS classes defined in the IEEE 802.11e standard. They are, from the highest to the lowest priority, voice (VO), video (VI), best effort (BE), and background (BK). To signal which class is used, the covert STA broadcasts a code when changing the QoS class. The code is a continuous sequence of the request to send (RTS) frames of given lengths. This type of mechanism is covert, as RTS retransmissions occur in IEEE 802.11 networks, especially ones with higher error rates and higher collision rates. To keep the QoS signaling distinct, the codes need to be longer than usual retransmission counts. To minimize the overhead, as the highest priority messages are switched to more often than lower priority ones, the higher priority classes use shorter codes. The proposed values meeting the mentioned criteria are listed in Table 4.

The process of sending QoS traffic over the covert channel consists of two parts—signaling and transmission. First, the covert STA needs to describe which class the next message will belong to. If the class remains unchanged from the previous message, there is no need to do any signaling. If the class changes, covert STA needs to transmit a code, consisting of a given number of "signals" in a row. We should note that, here, "in a row" means in consecutive transmission, only counting ones originating from the given STA not consecutive in the network. A "signal" consists of sending an RTS frame and awaiting a CTS. Sending "consecutive" RTS frames is not considered suspicious in an otherwise regular network as it would be normal behavior if the requesting station fails to receive a CTS. In this mechanism, "signals" do not carry data—any bits read from backoff or duration/ID performed by the covert receiver should be discarded if they come from RTS frames.

Table 4. Class change signal definitions.

QoS Class	Code
Voice (VO)	5× RTS
Video (VI)	6× RTS
Best Effort (BE)	7× RTS
Background (BK)	8× RTS

After the proper class is established, covert STA should return to sending data over non-RTS frames, as described in the base variant of the covert channel. Message fragmentation does not occur at the covert channel level; signaling a class change to the same class is a wasteful error and should be avoided. Class switching occurs based on strict priority—if data from a more important class are waiting in a queue, the current transmission should be immediately interrupted. After switching classes, the higher priority message should be sent instead. Figure 21 presents a very simplified illustration of the aforementioned class-switching mechanism (please note that the figure does not contain other frames such as CTS or ACK).

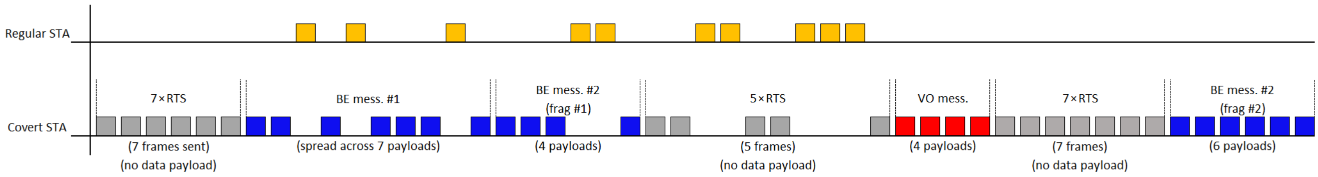

Figure 21. QoS class switching—a simplified view showcasing transmitted frames, purposefully omitting the AP.

7. Performance Evaluation of Covert Channel with QoS Support

For the covert channel with QoS support, the experiment simulates the impact of signaling on the overall channel throughput and counts the percentage of throughput lost to signaling, as the signaling RTS frames cannot contain covert data. The scenario simulates switching between two traffic classes, depending on the percentage of classes in overall traffic. Additionally, this scenario assumes a constant frame size for each class, as depicted in Table 5.

Table 5. Average frame size per class as used for the simulation scenario.

QoS Class	Frame Size [B]
Voice (VO)	128
Video (VI)	512
Best Effort (BE)	1024
Background (BK)	1536

Figure 22 shows the results for VO as the main class, and from it, we can conclude that the most taxing scenarios are when traffic is a combination of VO and VI frames. The largest signaling losses at 1.7% can be observed when VO and VI each make up 50% of covert traffic, so the signaling sequence of 5 or 6 RTS frames is constantly being broadcasted.

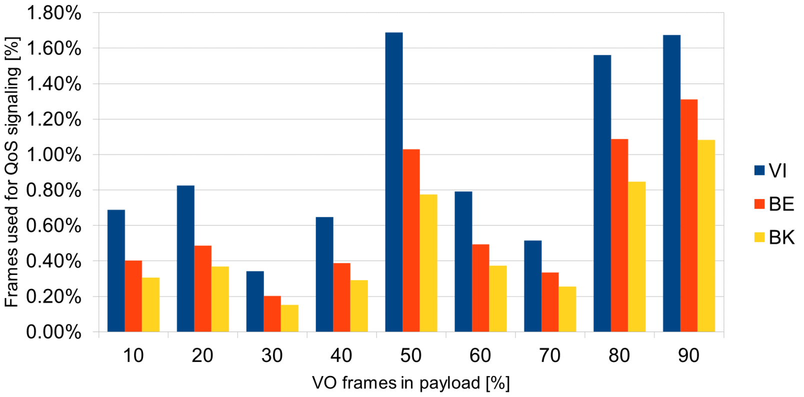

Figure 22. Percentage of channel throughput used for QoS signaling (by VO percentage).

Figures 23–25 show the results of other frame types, but they all show the same tendency—the more the traffic consists of smaller and higher priority frames on average, the greater the covert channel throughput needed for signaling. Additionally, signaling usage increases in scenarios where an even mix of classes is sent through the covert channel.

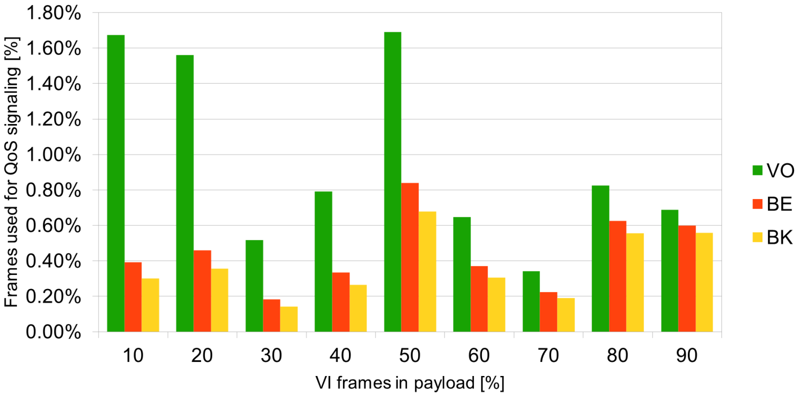

Figure 23. Percentage of channel throughput used for QoS signaling (by VI percentage).

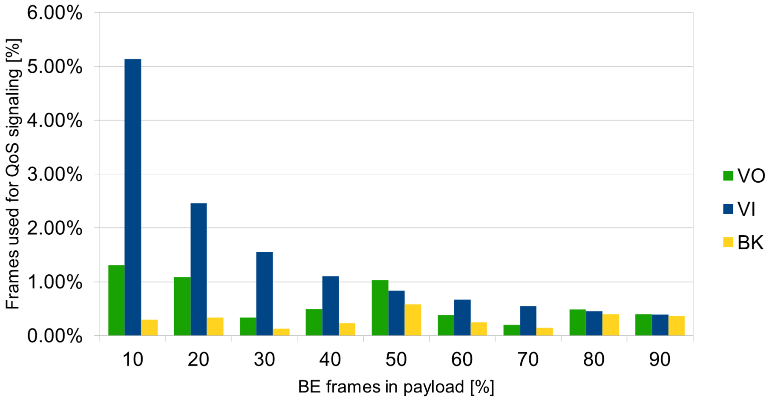

Figure 24. Percentage of channel throughput used for QoS signaling (by BE percentage).

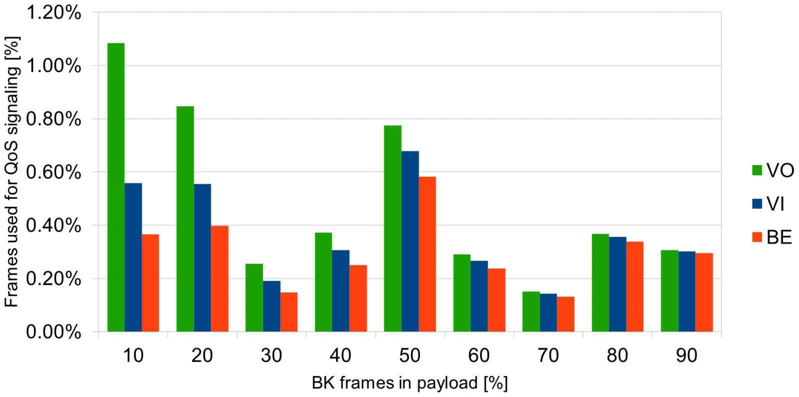

Figure 25. Percentage of channel throughput used for QoS signaling (by BK percentage).

Overall, it is worth noting that the QoS signaling mechanism is very efficient, as in the absolute worst-case scenario, it lowers the cover channel throughput by less than 2%, and in the majority of scenarios, its impact is less than 1%, while providing the ability to send four traffic classes concurrently.

8. Discussion

Unfortunately, like any protocol, the proposed covert channel also comes with certain limitations. When only one covert station is transmitting traffic without any background traffic, the throughput is determined by the frame size and offered load—smaller frame sizes help achieve higher throughput of the covert channel, but in turn, have a moderately negative impact on channel efficiency. Additionally, increasing the offered load increases the channel capacity up to a certain point, beyond which, it has an adverse effect on the network as a whole. Table 6 summarizes the result for a single covert station, and Table 7 collects the results for a single covert STA working when additional background STAs saturate the wireless channel.

Table 6. Covert channel throughput and delay depending on the payload size and offered load for a single station using 3 bits of the duration/ID field.

Frame Size [B]	Offered Load [Mbps]	Covert Channel Throughput [kbps]	Covert Channel Delay [ms]
512	20	19.53	0.22
512	80	78.12	0.38
512	140	136.72	1.33
512	200	144.80	272.64
1024	20	9.77	0.12
1024	80	39.06	0.38
1024	140	68.36	0.99
1024	200	81.19	439.74
1536	20	6.51	0.15
1536	80	26.04	0.39
1536	140	45.57	1.74
1536	200	55.36	629.23

To quote specific numbers, for a single STA, the maximum achieved throughput is 144.81 Kbps with 512 B frames and 160 Mbps of offered load, with further increases in the offered load impacting the throughput marginally while moderately decreasing efficiency—from 92.68% for 160 Mbps down to 74.14% for 200 Mbps. The decreased efficiency goes hand in hand with the increased network delays. Below 160 Mbps, the maximum measured delay is 1.33 ms, while at a 160 Mbps offered load, the delay increases to 257.57 ms. Changing the frame size to 1024 B decreases the maximum throughput to just 81.19 kbps with an offered load of 180 Mbps while keeping the efficiency at 92.37%, causing the delays to reach 398.37 ms. Similarly, further increasing the offered load does not change the throughput, while harming the network performance and latency. Table 6 contains sample values and describes the impact of the frame size and offered load on the covert channel throughput and delay.

Table 7. Covert channel throughput, jitter, and efficiency, depending on the background load and the number of background stations for a covert station using 3 bits of the duration/ID field, a payload size of 1024 B, and an offered load of 200 Mbps.

Background Load [Mbps]	#Background STA	Covert Channel Throughput [kbps]	Covert Channel Jitter [ms]	Covert Channel Efficiency [%]
0	0	81.19	0.02	83
20	2	68.35	0.04	70
20	10	48.86	0.09	50
20	20	41.07	0.12	42
80	2	38.59	0.12	40
80	10	16.98	0.39	17
80	20	10.00	0.70	10
140	2	21.40	0.29	22
140	10	5.26	1.34	5
140	20	4.92	1.96	3
200	2	19.35	0.33	20
200	10	3.30	1.42	5
200	20	2.29	2.48	2

For a covert STA with a variable number of background STAs and variable offered background loads, both have a drastic impact on throughput and efficiency. The increase in background stations has a more significant impact on channel throughput than the total load they generate. Unlike throughput, efficiency is not as sensitive to the transmitted frame size. With a greater number of stations generating background traffic, the effectiveness of the covert channel decreases for a given offered load. While longer data frames transmitted by the covert station lead to higher efficiency, the differences are not substantial.

For example, 20 background STAs offering a combined load of 20 Mbps result in a covert channel throughput of 41.07 kbps and an efficiency of 42%. Conversely, 2 background STAs offering 80 Mbps lead to a covert throughput of 38.59 kbps and a channel efficiency of 40%. Moreover, 20 STAs providing a background load of just 80 Mbps result in half the performance of a covert channel impacted by 2 STAs generating 200 Mbps of background load. In this scenario, the 20 STAs lead the channel to have a throughput of 10.00 kbps and an efficiency of 10%, while 2 STAs achieve 20% efficiency and a covert throughput of 19.35 kbps. Table 7 contains sample values and describes the impact of background loads and the number of background stations on covert channel throughput, jitter, and efficiency.

It is worth noting that the simulation conditions were rather more extreme than the usual real-world scenarios, especially the network load offered. Such conditions were deliberately chosen to test the operation of the covert channel under the most adverse conditions and to prove that it worked under such conditions.

9. Conclusions

The integration of Wi-Fi technology into SGs has revolutionized the way electricity is managed and distributed. Wi-Fi enables seamless and secure communication between various components of the SG infrastructure, such as smart meters, sensors, and control systems. This paper introduces a new type of covert channel for IEEE 802.11 networks applied in SGs, which expands our previously proposed mechanism using backoff and introduces a novel solution of combining two different mechanisms of sending data to create a single, wider, and faster covert channel. Additionally, the proposed channel can be used to send four concurrent data streams, the flow of which can be controlled using a QoS mechanism also proposed in this work. Both the basic and the QoS-enhanced mechanisms were analyzed using the NS-3 network simulator, which has a very mature implementation of IEEE 802.11ax networks. The simulations investigated how the frame size, offered load, and the number of stations in the background impact the proposed covert channel. Metrics, such as covert channel throughput, jitter, and efficiency were analyzed. The simulation studies confirmed that the proposed covert channel achieves a throughput four times higher than the covert channel proposed in [4]. Based on simulation findings, we can conclude that the proposed mechanism is suited to be deployed in real networks as it provides a framework to establish a covert channel, which is able to maintain reasonable throughput without increasing network jitter or decreasing network efficiency below acceptable levels, thus causing disruption to the normal network operation.

Future Work

In the future, this research could be expanded by conducting more simulations involving a variable number of duration/ID bits utilized for covert channels, aiming to determine the optimal parameters for maximizing the throughput or efficiency of the basic version of the channel. Another potential expansion could involve implementing a more sophisticated quality of service (QoS) mechanism to replace the proposed strict priority. For instance, this could entail utilizing a weighted fair queue, where a certain percentage of bandwidth is allocated to specific data classes, or implementing a mechanism based on transmit credit, akin to the one employed in CBSA in IEEE 802.11aa. Such an approach would facilitate multiple streams per class and ensure fair channel access for all of them.

Author Contributions: Conceptualization, M.N. and J.D.; methodology, M.N. and J.D.; software, J.D.; validation, M.N. and J.D.; formal analysis, M.N. and J.D.; investigation, M.N. and J.D.; writing—original draft preparation, M.N. and J.D.; writing—review and editing, M.N.; visualization, J.D.; 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 National Research Institute, grant number POIR.04.02.00-00-D008/20-01, the “National Laboratory for Advanced 5G Research” (acronym PL-5G), as part of Measure 4.2, ‘Development of modern research infrastructure of the science sector’ 2014–2020, financed by the European Regional Development Fund.

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

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

Abbreviations

The following abbreviations are used in this manuscript:

ACK	acknowledgement
AES	advanced encryption standard
AI	artificial intelligence
AID	association identifier
AMI	advanced metering infrastructure
AP	access point
BE	best effort
BER	bit error rate
BK	background

BSS	basic service set
BSSID	basic service set identifier
CBSA	credit-based shaping algorithm
CER	codeword error rate
CTS	clear-to-send
CW	contention window
CS	carrier sense
CSMA/CA	carrier sense multiple access/collision avoidance
DA	destination address
DCF	distributed coordination function
DIFS	DCF inter-frame space
EG	electric grid
EIFS	extended inter-frame space
GCM	Galois/Counter Mode
HAN	home area network
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IT	information technology
IV	initialization vector
JPEG	joint photographic experts group
KRACK	key reinstallation attack
LAN	local area network
LSB	least significant bit
MAC	medium access control
MCS	modulation and coding scheme
MIMO	multiple-input, multiple-output
MSB	most significant bit
NAN	neighborhood area network
NAV	network allocation vector
OFDM	orthogonal frequency-division multiplexing
OT	operational technology
QoS	quality of service
PDU	protocol data unit
PG	power grid
PS-Poll	power save polling
RA	receiver address
RTS	request to send
SAE	simultaneous authentication of equals
SIFS	short interframe space
SNR	signal-to-noise ratio
SG	smart grid
SM	smart meter
STA	station
TCP	transmission control protocol
TKIP	temporal key integrity protocol
UDP	user datagram protocol
VI	video
VMPC	variably modified permutation composition
VO	voice
WEP	wired equivalent privacy
WLAN	wireless local area network
WPA	Wi-Fi-protected access

References

1. Borlase, S. *Smart Grids: Infrastructure, Technology, and Solutions*; Electric Power and Energy Engineering; CRC Press: Boca Raton, FL, USA, 2017.
2. *IEC 61850-1*; IEC Standard for Communication Network and Systems in Substations, Part 1 Introduction and Overview. IEC: Geneva, Switzerland, 2003.
3. *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)—Redline*; 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; pp. 1–7524.
4. Teca, G.; Natkaniec, M. StegoBackoff: Creating a Covert Channel in Smart Grids Using the Backoff Procedure of IEEE 802.11 Networks. *Energies* **2024**, *17*, 716. [CrossRef]
5. Heydari, R.; Khayat, Y.; Amiri, A.; Dragicevic, T.; Shafiee, Q.; Popovski, P.; Blaabjerg, F. Robust High-Rate Secondary Control of Microgrids With Mitigation of Communication Impairments. *IEEE Trans. Power Electron.* **2020**, *35*, 12486–12496. [CrossRef]
6. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
7. Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. *Energies* **2022**, *15*, 6799. [CrossRef]
8. Beg, O.A.; Khan, A.A.; Rehman, W.U.; Hassan, A. A Review of AI-Based Cyber-Attack Detection and Mitigation in Microgrids. *Energies* **2023**, *16*, 7644. [CrossRef]
9. Stryczek, S.; Natkaniec, M. Internet Threat Detection in Smart Grids Based on Network Traffic Analysis Using LSTM, IF, and SVM. *Energies* **2023**, *16*, 329. [CrossRef]
10. Gwiazdowicz, M.; Natkaniec, M. Feature Selection and Model Evaluation for Threat Detection in Smart Grids. *Energies* **2023**, *16*, 4632. [CrossRef]
11. Kim, Y.; Hakak, S.; Ghorbani, A. Smart grid security: Attacks and defence techniques. *IET Smart Grid* **2023**, *6*, 103–123. [CrossRef]
12. Szczypiorski, K. HICCUPS: Hidden communication system for corrupted networks. In Proceedings of the Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, Miedzyzdroje, Poland, 22 October 2003.
13. Szczypiorski, K. A performance analysis of HICCUPS—A steganographic system for WLAN. *Telecommun. Syst.* **2009**, *49*, 255–259. [CrossRef]
14. Kraetzer, C.; Dittmann, J.; Lang, A.; Kühne, T. WLAN steganography: A first practical review. In Proceedings of the 8th Workshop on Multimedia and Security, Geneva Switzerland, 26–27 September 2006; pp. 17–22. [CrossRef]
15. Frikha, L.; Trabelsi, Z. A New Covert Channel in WIFI Networks. In Proceedings of the 2008 Third International Conference on Risks and Security of Internet and Systems, Tozeur, Tunisia, 28–30 October 2008; pp. 255–260. [CrossRef]
16. Frikha, L.; Trabelsi, Z.; El-Hajj, W. Implementation of a Covert Channel in the 802.11 Header. In Proceedings of the 2008 International Wireless Communications and Mobile Computing Conference, Crete, Greece, 6–8 August 2008; pp. 594–599. [CrossRef]
17. Kraetzer, C.; Dittmann, J.; Merkel, R. WLAN steganography revisited. In Proceedings of the Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, San Jose, CA, USA, 27 January 2008. [CrossRef]
18. Calhoun, T.; Newman, R.; Beyah, R. Authentication in 802.11 LANs Using a Covert Side Channel. In Proceedings of the 2009 IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009; pp. 1–6. [CrossRef]
19. Shah, G.; Blaze, M. Covert channels through external interference. In Proceedings of the WOOT, Montreal, QC, Canada, 10–14 August 2009.
20. Szczypiorski, K.; Mazurczyk, W. Hiding Data in OFDM Symbols of IEEE 802.11 Networks. In Proceedings of the 2010 International Conference on Multimedia Information Networking and Security, Nanjing, China, 4–6 November 2010. [CrossRef]
21. Piotrowski, Z.; Sawicki, K.; Mariusz, B.; Gajewski, P. New Hidden and Secure Data Transmission Method Proposal for Military IEEE 802.11 Networks. In Proceedings of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Darmstadt, Germany, 15–17 October 2010; pp. 179–183. [CrossRef]
22. Holloway, R.; Beyah, R. Covert DCF: A DCF-based covert timing channel in 802.11 networks. In Proceedings of the 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia, Spain, 17–22 October 2011; pp. 570–579. [CrossRef]
23. Goncalves, R.; Tummala, M.; McEachen, J. Analysis of a MAC Layer Covert Channel in 802.11 Networks. *Int. J. Adv. Telecommun.* **2012**, *5*, 131–140.
24. Sawicki, K.; Piotrowski, Z. The proposal of IEEE 802.11 network access point authentication mechanism using a covert channel. In Proceedings of the 2012 19th International Conference on Microwaves, Radar & Wireless Communications, Warsaw, Poland, 21–23 May 2012; Volume 2. [CrossRef]
25. Grabski, S.; Szczypiorski, K. Network steganalysis: Detection of steganography in IEEE 802.11 wireless networks. In Proceedings of the 2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Almaty, Kazakhstan, 10–13 September 2013; pp. 13–19. [CrossRef]
26. Radhakrishnan, S.; Uluagac, S.; Beyah, R. Realizing an 802.11-based covert timing channel using off-the-shelf wireless cards. In Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 9–13 December 2013; pp. 722–728. [CrossRef]

27. Dutta, A.; Saha, D.; Grunwald, D.; Sicker, D. Secret Agent Radio: Covert Communication through Dirty Constellations. In *Information Hiding, Proceedings of the 14th International Conference, IH 2012, Berkeley, CA, USA, 15–18 May 2012, Revised Selected Papers 14*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 7692. [CrossRef]
28. Grabski, S.; Szczypiorski, K. Steganography in OFDM Symbols of Fast IEEE 802.11n Networks. In Proceedings of the 2013 IEEE Security and Privacy Workshops, San Francisco, CA, USA, 23–24 May 2013; pp. 158–164. [CrossRef]
29. Zhao, H. Covert channels in 802.11e wireless networks. In Proceedings of the 2014 Wireless Telecommunications Symposium, Washington, DC, USA, 9–11 April 2014. [CrossRef]
30. Hokai, K.; Sasaoka, H.; Iwai, H. Wireless steganography using MIMO system. In Proceedings of the 2014 IEEE Fifth International Conference on Communications and Electronics (ICCE), Danang, Vietnam, 30 July–1 August 2014; pp. 560–565. [CrossRef]
31. Tahmasbi, F.; Moghim, N.; Mahdavi, M. Code-based timing Covert channel in IEEE 802.11. In Proceedings of the 2015 5th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 29 October 2015; pp. 12–17. [CrossRef]
32. Classen, J.; Schulz, M.; Hollick, M. Practical covert channels for WiFi systems. In Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 28–30 September 2015; pp. 209–217. [CrossRef]
33. 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. [CrossRef]
34. Wang, X.; Liu, Y.; Lu, X.; Lv, S.; Shi, Z.; Sun, L. CovertMIMO: A covert uplink transmission scheme for MIMO systems. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6. [CrossRef]
35. Cao, P.; Liu, W.; Liu, G.; Ji, X.P.; Zhai, J.; Dai, Y. A Wireless Covert Channel Based on Constellation Shaping Modulation. *Secur. Commun. Netw.* **2018**, *2018*, 1214681. [CrossRef]
36. D'Oro, S.; Restuccia, F.; Melodia, T. Hiding Data in Plain Sight: Undetectable Wireless Communications Through Pseudo-Noise Asymmetric Shift Keying. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019. [CrossRef]
37. Harley, P.; Tummala, M.; McEachen, J. High-Throughput Covert Channels in Adaptive Rate Wireless Communication Systems. In Proceedings of the 2019 International Conference on Electronics, Information, and Communication (ICEIC), Auckland, New Zealand, 22–25 January 2019; pp. 1–7. [CrossRef]
38. Sawicki, K. Sposób Skrytego Zarzadzania Heterogenicznymi Sieciami Teleinformatycznymi Oraz Metoda Przeciwdziałania Skrytym Transmisjom. Ph.D. Thesis, Military University of Technology (Wojskowa Akademia Techniczna), Warszawa, Poland, 2019.
39. Cao, P.; Liu, W.; Liu, G.; Zhai, J.; Ji, X.P.; Dai, Y. A Novel Wireless Covert Channel for MIMO System. In Proceedings of the InInternational Conference on Artificial Intelligence and Security, Hohhot, China, 17–20 July 2020; Springer: Singapore, 2020; pp. 351–362. [CrossRef]
40. Yamaguchi, R.; Ochiai, H.; Shikata, J. A Physical-Layer Security Based on Wireless Steganography Through OFDM and DFT-Precoded OFDM Signals. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–5. [CrossRef]
41. Grzesiak, K.; Piotrowski, Z.; Kelner, J. A Wireless Covert Channel Based on Dirty Constellation with Phase Drift. *Electronics* **2021**, *10*, 647. [CrossRef]
42. Hama, Y.; Ochiai, H.; Shikata, J. Performance Analysis of Wireless Steganography based on OFDM and DFT-s-OFDM Signals over Frequency-Selective Rayleigh Fading Channels. In Proceedings of the 2021 24th International Symposium on Wireless Personal Multimedia Communications (WPMC), Okayama, Japan, 14–16 December 2021; pp. 1–6. [CrossRef]
43. Almohammedi, A.; Shepelev, V. Saturation Throughput Analysis of Steganography in the IEEE 802.11p Protocol in the Presence of Non-Ideal Transmission Channel. *IEEE Access* **2021**, *9*, 14459–14469. [CrossRef]
44. Hama, Y.; Hanazawa, K.; Ochiai, H.; Shikata, J. Performance Analysis for Coded Wireless Steganography System with OFDM Signaling. In Proceedings of the 2023 IEEE Radio and Wireless Symposium (RWS), Las Vegas, NV, USA, 22–25 January 2023; pp. 7–10. [CrossRef]
45. Teca, G.; Natkaniec, M. A Novel Covert Channel for IEEE 802.11 Networks Utilizing MAC Address Randomization. *Appl. Sci.* **2023**, *13*, 8000. [CrossRef]
46. *IEEE Std 802.11ax-2021 (Amendment to 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 Amendment 1: Enhancements for High-Efficiency WLAN. IEEE: Piscataway, NJ, USA, 2021; pp. 1–767.
47. NS-3 a Discrete-Event Network Simulator. Available online: https://www.nsnam.org/ (accessed on 24 March 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.