energies

MDPI

Article

StegoEDCA: An Efficient Covert Channel for Smart Grids Based on IEEE 802.11e Standard

Marek Natkaniec * and Paweł Kępowicz

Institute of Telecommunications, AGH University of Krakow, al. Mickiewicza 30, 30-059 Krakow, Poland; pkepowicz@student.agh.edu.pl
* Correspondence: natkanie@agh.edu.pl

Abstract: Smart grids are continuously evolving, incorporating modern technologies such as Wi-Fi, Zigbee, LoRaWAN or BLE. Wi-Fi are commonly used to transmit data from measurement systems, distribution control and monitoring systems, as well as network protection systems. However, since Wi-Fi networks primarily operate on unlicensed frequency bands, this introduces significant security risks for sensitive data transmission. In this paper, we propose a novel and highly efficient covert channels that utilize IEEE 802.11 Enhanced Distributed Channel Access (EDCA) for data transmission. It is also the first ever covert channel that employ three or four independent covert mechanisms to enhance operational efficiency. The proposed mechanism is also the first to exploit the Transmission Opportunity (TXOP) period and the access categories of the EDCA function. The protocol was developed and tested using the ns-3 simulator, achieving excellent performance results. Its efficiency remains consistent even under heavy network load with additional background traffic. These covert channels provide an innovative solution for securely transmitting large volumes of data within the smart grid.

Keywords: smart grid; covert channel; IEEE 802.11e; QoS; EDCA; TXOP

check for updates

Academic Editor: Juan-José González de la Rosa

Received: 23 December 2024
Revised: 6 January 2025
Accepted: 10 January 2025
Published: 13 January 2025

Citation: Natkaniec, M.; Kępowicz, P. StegoEDCA: An Efficient Covert Channel for Smart Grids Based on IEEE 802.11e Standard. *Energies* **2025**, *18*, 330. https://doi.org/10.3390/en18020330

1. Introduction

IEEE 802.11 networks, commonly known as Wi-Fi, play a key role in the advancement of Smart Grids (SG) [1] by providing a versatile and cost-effective communication medium for real-time data exchange. These networks enable seamless connectivity among SG devices such as smart meters, sensors, and control systems, facilitating efficient monitoring, control, and optimization of energy systems [2]. A key enabler of this functionality is the internationally recognized SG standard IEC 61850, which facilitates seamless data exchange across Local Area Networks (LANs) to ensure system interoperability [3]. Using existing Wi-Fi infrastructure or deploying dedicated networks, utilities can enhance the scalability and flexibility of their operations while reducing installation and maintenance costs. The high-speed data transfer capabilities of Wi-Fi support critical SG functions, including demand response, fault detection, and energy consumption analytics. Although Wi-Fi offers significant benefits, its integration into SGs necessitates strong security measures to address vulnerabilities and safeguard the integrity and reliability of the grid's communication networks. Advanced encryption protocols, authentication mechanisms, and intrusion detection systems are essential to safeguard infrastructure and prevent unauthorized access or tampering.

In today's rapidly evolving internet, data privacy has become an increasingly important topic of discussion. One of the most widely adopted methods to ensure secure communication between two parties is data encryption. Encryption safeguards the data using a key that is known only to communication participants, making the information unreadable to unauthorized third parties. Although encryption effectively conceals the content of the data, it does not obscure the fact that communication has occurred. The term "steganography" is derived from the Greek words *steganós*, meaning "covered" or "concealed", and *graphia*, meaning "writing". Historically, it has seen usage to exchange highly sensitive messages. With the evolution of the digital age, steganography has gained popularity, as individuals can now use specialized software to embed hidden messages within images, videos, or audio files, which can only be deciphered by those who know how to extract them. Over the years, numerous researchers have proposed algorithms that enable the creation of covert communication channels over regular network protocols, allowing two parties to communicate secretly without the knowledge of the network administrator.

This research focuses on developing a covert communication channel for SG based on IEEE 802.11 [4] networks. This standard employs a shared medium for all users, which inherently exposes them to the risk of eavesdropping. In such an environment, a covert channel can be utilized to facilitate secure cryptographic key exchange, verify user identity, or transmit other confidential data. The goal of this research is to propose a set of novel algorithms for covert transmission, introducing an innovative approach to embedding data within the second layer of the IEEE 802.11 standard family by combining various timing-based and storage-based covert channel algorithms. Furthermore, this work aims to refine previously proposed methods to maximize the available bandwidth for covert communication while remaining undetectable and minimizing the negative impact on regular network transmission.

In this paper, we present the following contributions:

- The proposal of the first family of covert channels that allow to switch between high covertness and high throughput mode and use features introduced in the IEEE 802.11e [5] extension.
- The proposal of a first covert channel named StegoTXOP—we propose a new covert channel mechanism that uses the transmission opportunity (TXOP) period of the MAC frame to hide covert data.
- The proposal of a second covert channel named StegoQoS—we propose a new covert channel mechanism that uses access categories of the Enhanced Distributed Channel Access (EDCA) function combined with shift mechanism that uses the 'Duration' field of the MAC frame header to hide covert data.
- The proposal of a third covert channel named StegoEDCA as a new hybrid solution—we propose a novel approach of combining three or four independent covert channels into a single transmission to enhance covert transmission throughput and resistance to steganalysis.
- A comprehensive evaluation of the performance of covert channels under varying network parameters (frame size, bits encoded in single TXOP), covert channel configurations (number of background nodes) and impact of different Quality of Service (QoS) queues within the EDCA function.
- An examination and discussion of the effects of network saturation and loads imposed by neighboring stations on covert channel performance.

The remainder of the paper is organized as follows. Section 2 provides an overview of the relevant literature. Section 3 discusses the technical aspects of the IEEE 802.11 architecture and its mechanisms. Section 4 describes the principles of operation for the covert channels incorporated into the proposed combination. The simulation results and their discussion are presented in Section 5. Section 6 discusses the limitations and risks of the proposed methods. Finally, Section 7 concludes the research findings and highlights potential directions for future work.

2. State of the Art

Over the years, there have been numerous investigations into covert channels within Wi-Fi network environments. The first notable proposal is considered [6], in which the authors proposed three channels. The first channel is based on WEP cipher initialization vectors, the second uses MAC addresses, and the third channel is based on sending frames with intentionally created bad checksums. This approach was evaluated in [7]. The first two channels were covert but offered low bandwidth. The third channel provided nearly 100% of the network bandwidth but introduced anomalous traffic to the network. The researchers in [8] proposed two covert channels: one based on modifying subfields within the IEEE 802.11 MAC frame control field and the other on duplicating packets. They were able to partially implement both ideas in hardware and conducted an extensive study on the throughput, reliability, and covertness of the transmission. The two proposals in [9] utilized the sequence control field and the WEP initialization vector, and could be operated together depending on the network configuration. The authors analyzed performance and proposed mechanisms to protect the covert channel from network sniffers. Furthermore, this idea was implemented in [10] with a user-friendly interface, but the transmissions proved to be vulnerable to frame loss.

The authors of [11] used the IEEE 802.11b MAC multirate protocol as a bearer of covert messages. By utilizing this channel, they were able to create covert authentication for users with one-time passwords to protect the network from replay attacks. The simulations demonstrated minimal performance impact on regular transmission. A different approach to creating wireless covert channels can be found in [12]. In the proposed solution, the covert sender does not need to be connected to the network, as the hidden message is transmitted by introducing interference into the channel. The authors demonstrated the practical utility of this interference channel by watermarking VoIP flows. The first OFDM-based hidden channel was proposed in [13]. The researchers inserted hidden data into the padding of frames at the physical layer. In doing so, they achieved up to 1.1 Mb/s of bandwidth while maintaining low detectability. Another concept of hiding communication in IEEE 802.11 networks can be found in [14], which employs fast switching between infrastructure and ad-hoc mode. Although anomalies of this nature are easy to detect, the proposed algorithm also introduces data scrambling and optional encryption using the VMPC algorithm.

In [15], a novel timing-based covert channel was proposed. It utilizes random backoff in the Distributed Coordination Function (DCF) to disguise transmissions. The authors claim that this proposal can achieve a throughput of 1800 bits/s with high accuracy while remaining undetectable. Furthermore, the throughput can reach up to 8000 bits per second in scenarios where covertness is ignored. In [16], researchers created a covert channel by modifying Clear-To-Send (CTS) and Acknowledgment (ACK) frames. To enhance the robustness of the channel against errors, they implemented forward error correction and bit interleaving. Extensive testing on channel errors, data rate, and detectability demonstrated performance gains from using the mentioned techniques. Additional authentication for access points using a covert channel was introduced in [17]. This method utilizes the Least Significant Bits (LSB) of the Timestamp field in Beacon frames. Using this information, clients can distinguish legitimate access points from rogue ones. However, this approach is limited to one-way communication. Another application for covert channels was discussed in [18]. The researchers used a covert channel based on the rate switching algorithm with One-Time Passwords to implement covert authentication and covert Wi-Fi botnets. They studied the throughput, covertness, and consequences of covert communication on regular network traffic.

Reference [19] implements the system proposed in [15] using off-the-shelf equipment. The researchers used equipment available in almost all laptops and found that, due to hardware fluctuations, only half of the theoretical throughput could be achieved. This highlights the importance of practical implementations to judge the feasibility of covert channels. Due to the increasing popularity of steganography, researchers created an extensible application to detect covert channels as described in [20]. This application passively observes network traffic on the second layer and is currently able to detect only a few covert channels. The results show that it can capture implemented channels with ease and can be expanded to accommodate new and more sophisticated algorithms in the future. Another take on steganography at the physical layer is described in [21]. Scientists call their technique Dirty Constellation because they hide a covert message with noise that resembles hardware imperfections and channel conditions. The hardware implementation confirms the low detectability and high throughput of this idea. The researchers in [22] decided to modify the cyclic prefix of Orthogonal Frequency-Division Multiplexing (OFDM). The simulations showed low detectability and immense available bandwidth, which the authors claimed to be the highest of all known steganography algorithms at the time.

The study in [23] proposed two new covert channels using bits inside the Quality of Service (QoS) header of the IEEE 802.11e frame. These channels were low bandwidth and highly undetectable due to the lack of disruption to network traffic patterns. Additionally, the implemented signaling provided reliable transmission. The authors of [24] proposed and evaluated a covert channel using Multiple-Input, Multiple-Output (MIMO) technology. MIMO proved to be superior to Single-Input, Single-Output (SISO) systems in terms of transmission characteristics and higher undetectability. Reference [25] introduced improvements to a covert channel based on the DCF function, inspired by the Exploiting Modification Direction (EMD) method used in Joint Photographic Experts Group (JPEG) steganography. The goal was to increase embedding efficiency, bandwidth, and security. The researchers in [26] analyze and compare four techniques for creating OFDM-based covert channels at the physical layer of 802.11a/g. They discuss the pros and cons with respect to their performance and detectability. The discussed OFDM covert channels offer high bandwidth but prove vulnerable to signal analysis at the physical layer. However, at higher layers, they are undetectable as they introduce only a slightly increased BER.

The timing-based covert channel introduced by [27] transmits information by manipulating the timing of frames within a DCF-controlled medium. To enhance the stealthiness of this channel, the researchers proposed an adaptive approach in which the timing pattern for transmitting covert information is based on the time intervals observed in the distribution of regular network traffic. The simulation results indicated a moderate bit rate, low error rate, and a high level of covertness. The channel proposed in [28] was implemented using off-the-shelf equipment. It uses intervals of probe request frames or beacon frames to provide bidirectional communication. This channel was proved to be detectable only at the physical layer, with a relatively low error rate, but it offers very low bandwidth. Two new covert channels described in [29] rely on modifying the feedback matrix of data and control channels to send hidden information. The researchers provide a detailed discussion on how to design the parameters of their method. Conducted simulations show an insignificant impact of hidden communication on normal transmission and high covertness, but offer only an uplink connection. In [30], researchers investigate a covert channel based on introducing errors in OFDM constellation shaping to transmit data. Although the experimental results show high undetectability, transmission reliability remains a concern.

The introduction of noise to create covert transmission can also be found in [31]. In this proposal, hidden bits are transmitted by introducing amplitude shifts to phase-shift keying modulations, a technique termed pseudo-noise asymmetric shift keying. Simulations and physical implementation on off-the-shelf network cards yielded impressive results—high throughput, high transmission robustness, and no impact on regular transmission SNR. The authors of [32] exploited the modulation and coding schemes and link adaptation mechanisms introduced in the IEEE 802.11ad standard to create a high-throughput covert channel. In simulation, they were able to achieve a throughput of 150 Mb/s and reliably send data. However, this increased throughput came at the cost of slightly reducing the quality of regular transmission. To increase the covertness of the OFDM-based covert channel, researchers in [33] proposed a novel method to utilize a cover signal to decrease the Signal-to-Noise Ratio (SNR) and thereby conceal the secret signal. Simulations demonstrate this method to be an effective approach for enhancing resistance to steganalysis. However, their study focuses solely on the detectability of hidden transmission, thus lacking an analysis of the impact on the covert receiver and throughput. The work [34] analyzes the possibility of using a covert channel based on hiding transmissions in OFDM padding in vehicular networks. The authors conducted simulations assuming non-ideal conditions, and the results showed the impact of various parameters such as channel conditions, number of vehicles, packet sizes, and transmission data rate on the steganographic channel.

The authors of [35] propose a new, easy-to-implement steganographic channel that embeds hidden bits of information in the relative order of frames. Experiments conducted in real-world scenarios demonstrate high covertness and a low error rate, even when non-informed stations are present in the channel. The main downside of this proposal is its very low bandwidth. In [36], another proposal for an easy-to-implement covert channel can be found. It introduces a small offset to the beacon interval to transmit hidden bits. The authors implemented error correction for robustness and simple data encryption to increase security. The protocol presents a trade-off: while it operates on a low-bandwidth channel with limited unidirectional transmission capacity, it boasts straightforward integration into commercial equipment and ensures covert transmission. The proposal described in [37] utilizes the supported data rates and extended data rates fields found in the probe request frames to establish a covert channel. Due to the active scanning principle of operation, the sender receives responses to their requests, allowing for error detection and retransmission. The simulations demonstrated a maximum throughput of more than 1.2 kb/s with low latency. The covertness of the proposed channel was not discussed in this paper. Another study on OFDM-based channels is conducted in [38]. The authors analyze the performance of a channel hidden in a single-carrier signal for IoT usage. Simulations proved that the signal power ratio was sufficient for successful decoding and low enough not to raise suspicions from observers.

The new channel proposed in [39] uses a randomized MAC address to create a covert channel. The sender embeds hidden information in the MAC address and uses it to send probe requests within the network. To distinguish covert transmissions from regular ones, the authors implemented the Cyclic Redundancy Check (CRC) in the sequence number field. Simulations showed a significant impact of the number of stations in the network on channel performance, but researchers were able to mitigate this with a modified version of selective repeat Automatic Repeat reQuest (ARQ) protocol. The results proved the channel to be stealthy, yielding high throughput and offering low delay and jitter values. Reference [40] introduces another hidden channel built on exploiting the DCF function and its random backoffs called StegoBackoff. Bits of the covert transmission are based on the parity of the sender's backoff time. This simple concept is easy to implement and hard to detect, as the sender does not access the channel unfairly. The bandwidth of this channel is highly dependent on the number of active stations in the network, and transmitting large frames proves to be a challenge. The authors of [41] introduce a novel approach that combines two different steganography algorithms to enhance the transmission parameters of a covert channel. They use a slightly modified StegoBackoff method to send one bit of information per packet and combine it with encoding three bits of information inside the duration/ID field of the MAC header. In addition, they implement a mechanism to support different QoS classes similar to those defined in the IEEE 802.11e standard. The results of the conducted simulations demonstrate that this protocol offers high bandwidth and low delay without disrupting normal network operations, although a large number of background stations could reduce its efficiency.

Although numerous solutions have been proposed over the years, there remains significant potential for novel covert channel concepts and optimization of existing ones. The motivation for this work is to develop a channel characterized by very high throughput, low detectability, and minimal impact on regular network performance. This study aims to refine existing concepts and introduce new approaches to enable covert transmission utilizing QoS features introduced in the IEEE 802.11e standard extension, which have not been explored to date.

3. Background

To gain a thorough understanding of the functioning of the proposed steganographic algorithms, it is essential to examine the specific elements of the IEEE 802.11 standard that will be utilized to create a covert transmission channel. IEEE 802.11 represents a subset of IEEE standards that describe the physical layer and the Media Access Control (MAC) sublayer of WLANs. Over the years, the continuous evolution of these standards has given rise to an advanced ecosystem composed of numerous procedures, making it an ideal framework for proposing novel solutions related to steganography.

3.1. Backoff Mechanism

Since Wi-Fi networks operate over a shared medium, they require a method to manage transmission in a multi-station environment. This task is handled by the Distributed Coordination Function (DCF) and EDCA, which employ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and binary exponential backoff. The sender must listen to the medium before initiating transmission. If the medium is idle, the sender is free to transmit its data. However, both the DCF and the EDCA functions cannot guarantee that collisions will be avoided within the network.

In subsequent transmissions, or if the sensed medium was busy or a collision occurred, the Wi-Fi station must initiate the backoff procedure. Backoff is a component of the DCF and EDCA functions that delays the station from accessing the medium. It is measured in terms of time slots with their length depending on the specific IEEE 802.11 standard. The backoff value represents the number of time slots the station must wait before attempting to transmit again. It is calculated as follows:

$$Backoff = random\_int[0, CW - 1]$$

where CW (Contention Window) is determined based on the number of retransmission attempts i, the minimum contention window size (CWmin), and the maximum contention window size (CWmax) values:

$$CW = min(2^i \cdot CWmin, CWmax)$$

It starts at CWmin, and with each unsuccessful transmission it increases exponentially until it caps at CWmax. The values of CWmin and CWmax are configurable and may vary between different IEEE 802.11 standards. Each Access Category (AC) in EDCA has its own minimum CWmin and maximum CWmax contention window values. The backoff timer decrements only when the channel is detected as idle. The channel is considered idle once the Distributed Inter-Frame Space (DIFS) duration has elapsed.

3.2. EDCA Function

The IEEE 802.11e amendment introduces enhancements to Wi-Fi networks aimed at enabling Quality of Service (QoS) provisioning. It defines a new channel access mechanism known as EDCA, which operates similarly to the DCF but includes additional support for QoS features. EDCA achieves this by utilizing a variation of the CSMA/CA mechanism that incorporates four independent priority queues, each characterized by distinct Arbitration Inter-Frame Space (AIFS) and contention window (CWmin and CWmax) values. AIFS represents the time interval for which a specific queue waits before the channel is deemed idle. Queues with higher priority are assigned shorter AIFS values, increasing their likelihood of accessing the channel. Similarly, high-priority queues are assigned lower CWmin and CWmax values, further enhancing their access to the channel by reducing contention periods. This ensures that time-sensitive data, like voice and video, get preferential treatment over less-critical traffic. The EDCA channel access procedure is illustrated in Figure 1.

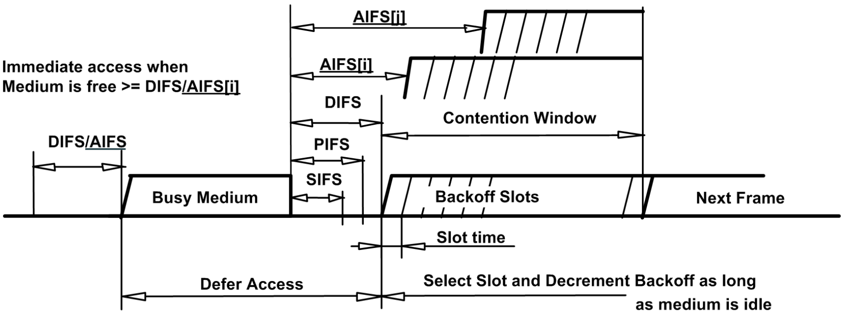


Figure 1. EDCA channel access [5].

The IEEE 802.11e amendment also introduces the concept of a Transmission Opportunity (TXOP) period. A TXOP is a defined time interval during which a station that has gained access to the shared medium can transmit multiple frames, as long as the total transmission time does not exceed the TXOP limit. This mechanism eliminates the need for the station to perform backoff procedures between successive transmissions of high-priority frames. If the maximum TXOP duration for a queue is set to zero, the station is restricted to transmitting only a single frame before initiating a new backoff procedure. The TXOP period effectively reduces the time lost in backoff processes for consecutive high-priority transmissions. The default configuration for the access categories defined in the IEEE 802.11e amendment is provided in Table 1.

Table 1. Default values for access categories.

QoS Class	CWmin	CWmax	AIFSN	TXOP Limit
Background	15	1023	7	0
Best effort	15	1023	3	0
Video	7	15	2	3.008 ms
Voice	3	7	2	1.504 ms

3.3. Frame Aggregation

The IEEE 802.11n [42] standard amendment focused on improving the performance of Wi-Fi networks. To achieve increased throughput, it introduced, among other innovations, frame aggregation. This allowed multiple frames to be transmitted in a single transmission with a single Physical Layer Convergence Protocol (PLCP) header, thereby reducing signaling overhead. The standard defined two types of frame aggregation: MAC Service Data Unit (MSDU) aggregation, resulting in the creation of aggregated MSDUs (A-MSDUs), and Aggregate MAC Protocol Data Unit (A-MPDU).

An A-MSDU frame uses a single PLCP header and a shared Media Access Control (MAC) header across all subframes. This minimizes transmission overhead, but eliminates the Frame Check Sequence (FCS) for individual subframes, which can reduce the effectiveness of error detection. In contrast, A-MPDU shares the PLCP header across all subframes, but each subframe retains its own MAC header. While this method provides a lesser reduction in overhead, it maintains the integrity of error detection. These aggregation methods are illustrated in Figure 2.

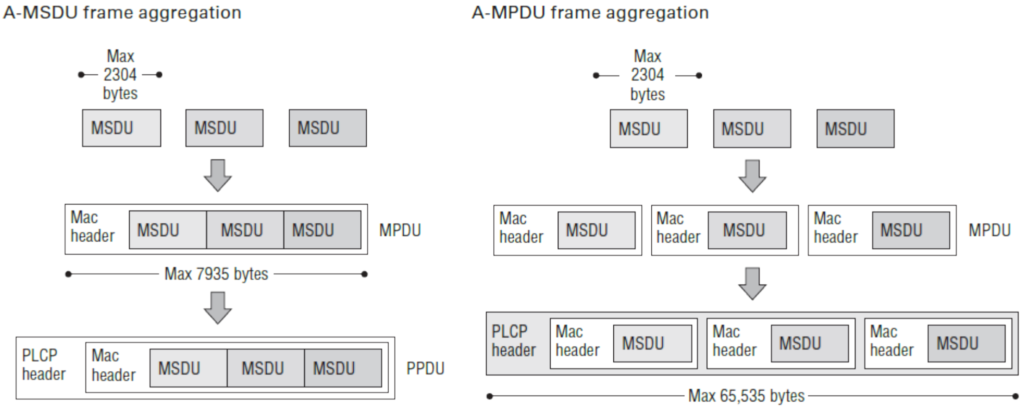


Figure 2. Aggregation method comparison [43].

4. Algorithm Proposal

4.1. StegoQoS

The IEEE 802.11e standard amendment specifies four different priority queues which can be exploited to send covert data. This number allows for the encoding of two covert bits per frame. How different queues are mapped to specific bit sequence is specified in Table 2.

Table 2. Encoding table.

QoS Class	Bit Sequence
Voice	00
Video	01
Best effort	10
Background	11

It is not always the case that all four queues are used simultaneously by a single station. Furthermore, the transmission of frames from different queues in random order may raise suspicion, potentially compromising the covert channel. To address these scenarios, the proposed algorithm incorporates a new concept of a shift mechanism embedded in two least significant bits (LSB) of the duration field. The encoding procedure is presented in pseudocode for Algorithm 1. To decode the bit sequence, the covert receiver must map the QoS class of the received frame and perform an XOR operation between the mapped sequence and the two least significant bits of the duration field. This mechanism allows the covert station to maintain transmission without the need to utilize all four queues and increases resistance to steganalysis.

Algorithm 1: Encoding in QoS.

```
Input: $m$ — Bits to encode
Input: $q$ — QoS bit sequence of current frame
Input: $d$ — Duration/ID field in MAC Header
Function EncodeBitInQoS($m, q, d$):
    while $m \neq null$ do
        if $length(m) < 2$ then
            Zero-fill the $m$ array;
        end
        $d[13, 14] \leftarrow$ XOR$(m, q)$;
    end
```

Due to the existence of A-MPDU frame aggregation in the Wi-Fi network, the covert channel can operate in two distinct modes: high covertness and high throughput. In high covertness mode, the covert station attempts to transmit the secret bit sequence only once per A-MPDU, with the corresponding duration value replicated across all headers of the aggregated frames. This method sacrifices throughput for increased transmission secrecy. In a scenario where compromise of the covert channel is unlikely or bandwidth is crucial, high-throughput mode should be used. In this mode, the covert sender sets the duration field in every aggregated frame, thereby increasing throughput from 2 bits per A-MPDU up to 128 bits per A-MPDU.

In a previous research on hiding information in the duration field [41], researchers stated that in networks of the IEEE 802.11ax standard, up to three bits might be used to send a covert message without having a negative impact on network operation and performance. StegoTXOP needs only two bits for the shift mechanism, but to maximize combined algorithm throughput, the third bit will be used for conveying information and will be referred to as a separate covert channel called StegoDuration.

4.2. StegoTXOP

EDCA function features the TXOP mechanism, which enhances throughput for high-priority data and is enabled by default for voice and video queues. This mechanism can be used by the covert sender to transmit additional bits of hidden data. The receiver can interpret the transmission of a predefined number of frames within a single TXOP period as a specific bit sequence. The maximum number of frames within a single TXOP may vary depending on the IEEE 802.11 standard version. To adapt to specific network conditions, this algorithm employs adaptive encoding, dynamically setting the maximum number of encoded bits per TXOP to two, three, or four. Each step in this progression requires an exponentially greater number of frames to be transmitted within a single TXOP. An example encoding of up to three bits in a single TXOP can be found in Table 3.

To avoid introducing unnecessary delays for regular transmission, an option is provided to send a single frame within a TXOP that does not carry any covert information. Before initiating another TXOP period, the covert scheduler should check the number of frames in the buffer and attempt to transmit the longest possible covert bit sequence using the available buffered frames. This ensures that regular transmission buffers do not overflow. StegoTXOP algorithm that encodes up to three bits in a single TXOP for the voice queue is described by the pseudocode presented in Algorithm 2.

Table 3. TXOP Encoding table.

Number of Frames Sent	Encoded Bits
1	–
2	00
3	01
4	10
5	11
6	000
7	001
8	010
9	011
10	100
11	101
12	110
13	111

Algorithm 2: Encoding in TXOP

```
Input: $m$ — Bits to encode
Input: $q$ — Queue buffer
while $m \neq null$ do
    if $len(q) \geq 13$ then
        len$(m) = 3$;
    end
    else if $len(q) \geq 5$ then
        len$(m) = 2$;
    end
    else if $len(q) = 0$ then
        len$(m) = 0$;
    end
    send number of frames for sequence $m$ as specified in Table 3;
end
```

In case of frame aggregation, each A-MPDU is interpreted by the covert receiver as a single frame during the decoding process. Therefore, the threshold parameters for queues with aggregation enabled should be set based on the specific network parameters that may differ between standard versions.

4.3. StegoBackoff in EDCA Function

An additional channel can be integrated into the previously proposed stack of covert algorithms. The proposal presented in [40] operates independently of the previous two algorithms and, as demonstrated in the, does not degrade transmission performance. The difference is that this time we use the backoff with respect to a given traffic class in the EDCA function. This method leverages the backoff procedure to encode a single bit, where the receiver interprets an even backoff slot as "0" and an odd backoff slot as "1". If the sender intends to transmit a "0" but the current backoff value is odd, the sender should increment the backoff by one to ensure the correct bit is transmitted. However, in the edge case where the backoff is already equal to CWmax, the sender is permitted to decrement the backoff value to align with the required bit transmission. The complete encoding procedure is detailed in Algorithm 3.

Algorithm 3: Encoding in EDCA backoff

```
Input: $m$ — next message bit
Input: $b$ — current backoff lenght in specific EDCA class
Input: $cwMax$ — backoff slots limit in specific EDCA class
while $m \neq null$ do
    if $m = 1$ then
        if $b$ isOdd then
            return $b$
        else
            if $b \neq cwMax$ then
                return $b + 1$;
            else
                return $b - 1$;
            end
        end
    else
        if $m = 0$ then
            if $b$ isEven then
                return $b$
            else
                if $b \neq cwMax$ then
                    return $b + 1$;
                else
                    return $b - 1$;
                end
            end
        end
    end
end
```

It should be noted that the backoff procedure does not occur during the TXOP period. Consequently, the throughput of StegoBackoff is significantly reduced, as it can only be utilized by the first frame that initiates the TXOP period.

4.4. Combined StegoEDCA Algorithm

Combining all previously proposed covert channels into one and performing a single coherent transmission requires strict order in which covert bits are sent and then received by covert stations. The first bit of the hidden message is encoded using the stegoBackoff mechanism. The subsequent set of bits are concealed within the duration field, where the 14th bit is utilized by the stegoDuration mechanism, and the 15th and 16th bits are employed by the stegoQoS shift mechanism. Finally, if the transmission utilizes the TXOP mechanism, the last set of bits is determined by the number of frames transmitted during a single TXOP period. Detailed encoding and decoding procedures are depicted in Figures 3 and 4.

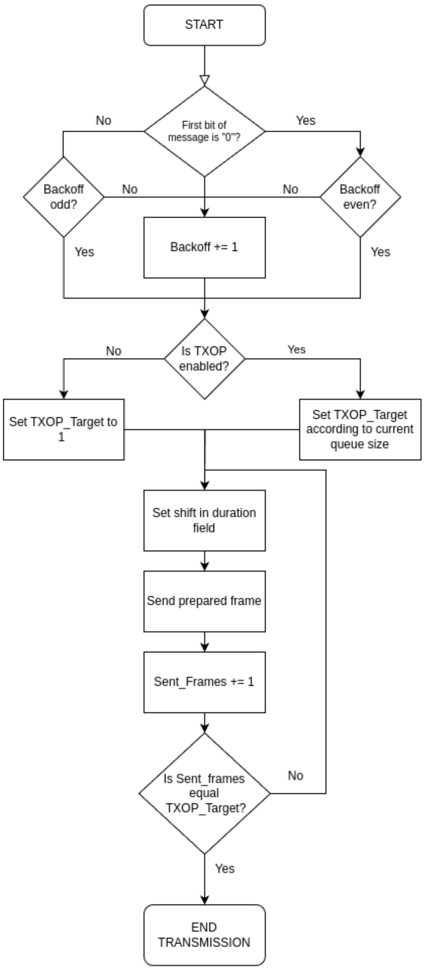


Figure 3. Encoding procedure.

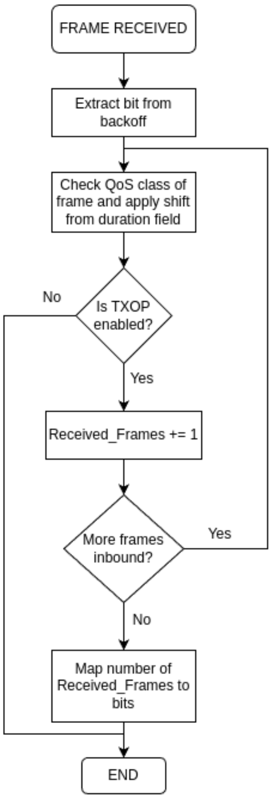


Figure 4. Decoding procedure.

5. Performance Evaluation

5.1. Simulation Environment

All covert channels were implemented and analyzed in the NS-3 simulator, version 3.42. NS-3 is a free, open-source, discrete-event network simulator developed using C++20 and Python 3.6. It is a mature solution supported by a vast community and numerous universities worldwide. It provides comprehensive support for various network types, including IEEE 802.11 and its latest 802.11ax extension. NS-3 was selected as the platform for this research due to its extensive functionality, active developer community, continuous updates and user-friendly interface, which facilitates the modification of network behavior and the collection of data. The base simulation parameters are listed in Table 4 and remain unchanged unless otherwise specified in the simulation scenario. All simulations were repeated multiple times, with different seed values. It should be noted that, in all figures, the error for each simulation point within the 95% confidence interval did not exceed ±2%. Consequently, error bars have been omitted from all graphs.

Table 4. Simulation parameters.

Parameter	Value
IEEE standard	802.11ax
Transport protocol	UDP
Frequency band	2.4 [GHz]
Channel width	40 [MHz]
Guard interval	800 [ns]
Channel Number	6
TX power	30 [dBm]
Time slot	9 [µs]
SIFS	16 [µs]
DIFS	34 [µs]
AC_VO TXOP time limit	1.504 [ms]
AC_VO CW min	3
AC_VO CW max	7
AC_VI TXOP time limit	3.008 [ms]
AC_VI CW min	7
AC_VI CW max	15
MCS index	9
RTS/CTS	Disabled
Number of Tx and Rx antennas	1
Propagation and Loss Model	Log-Distance Path Loss Model
Mobility model	Constant
Distance between AP and STA	5 [m]

5.2. Simulation Scenarios

5.2.1. Scenario 1—Voice Queue in Non-Competetive Environment

The topology of the first scenario consists of a single station and an Access Point (AP), as shown in Figure 5. The objective of this experiment was to evaluate the performance of the combined EDCA covert channel and its impact on regular transmission in a non-competitive environment depending on frame size, offered load, and maximum number of bits encoded in a single TXOP with stegoTXOP channel.

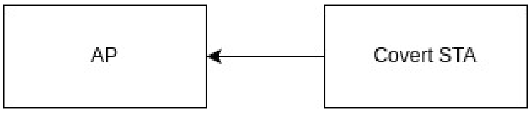
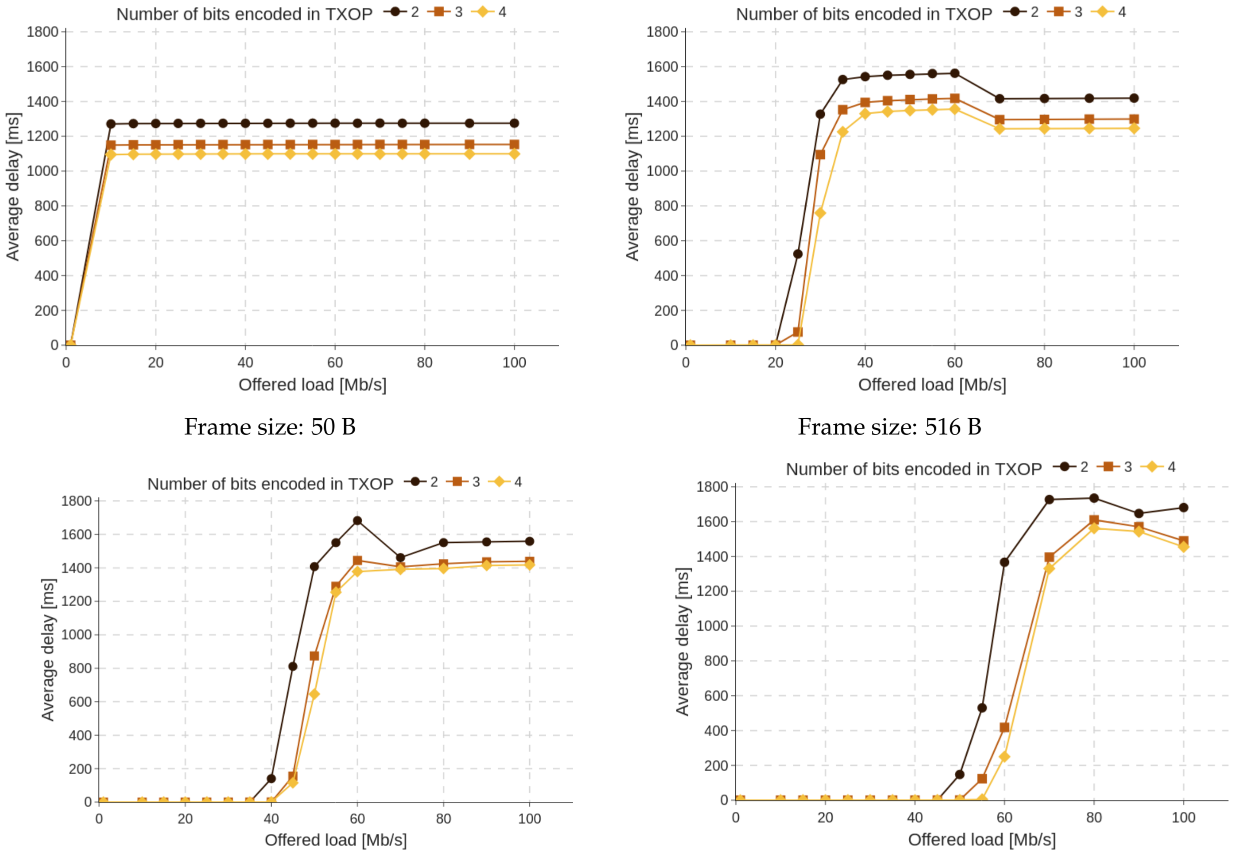


Figure 5. Network topology with single station.

The mean frame delay of transmission with the covert channel enabled is shown in Figure 6. It can be observed that increasing the number of bits encoded within a single TXOP period reduces the negative impact on covert channel performance, as it allows the covert station to send more frames before starting another backoff procedure. Frame size remains the primary factor determining the oversaturation point, and the performance differences between various stegoTXOP settings appear to be invariant to changes in frame length.



Frame size: 50 B

Frame size: 516 B

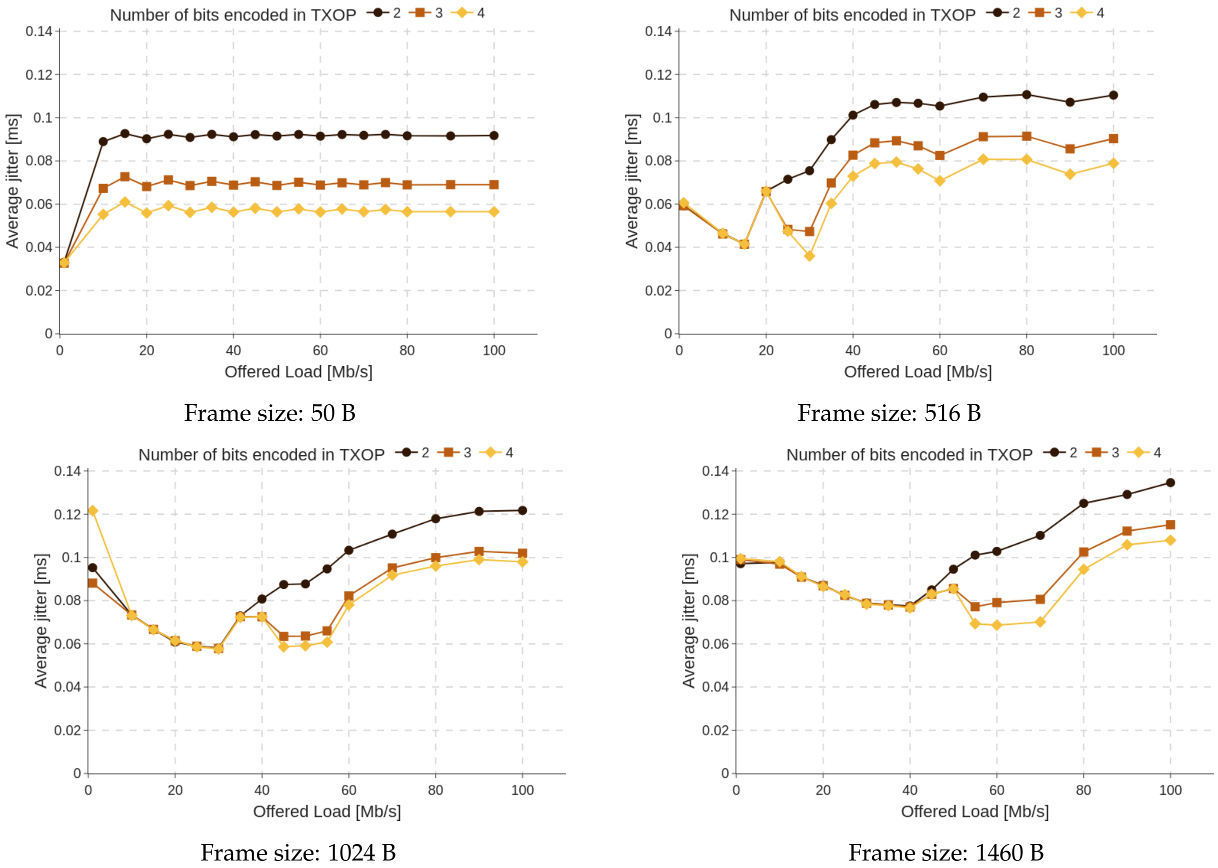
Frame size: 1024 B

Frame size: 1460 B

Figure 6. Average frame delay vs. offered load for different frame size.

A similar observation can be made by analyzing the mean jitter graphs presented in Figure 7. Once again, transmitting more frames within a single TXOP period demonstrates superior performance, as it minimizes downtime between consecutive transmissions and maximizes overt channel throughput.

The throughput of the combination of all considered channels is shown in Figure 8. Since the number of covert bits is correlated with the number of frames transmitted by the covert station, the highest throughput is observed in networks that utilize the shortest frames. The maximum throughput achieved for the voice queue in all simulations was over 24 kb/s. The simulations indicate a minimal disparity in throughput when encoding 2 or 3 bits within a single TXOP, whereas encoding 4 bits appears to result in noticeably reduced performance.



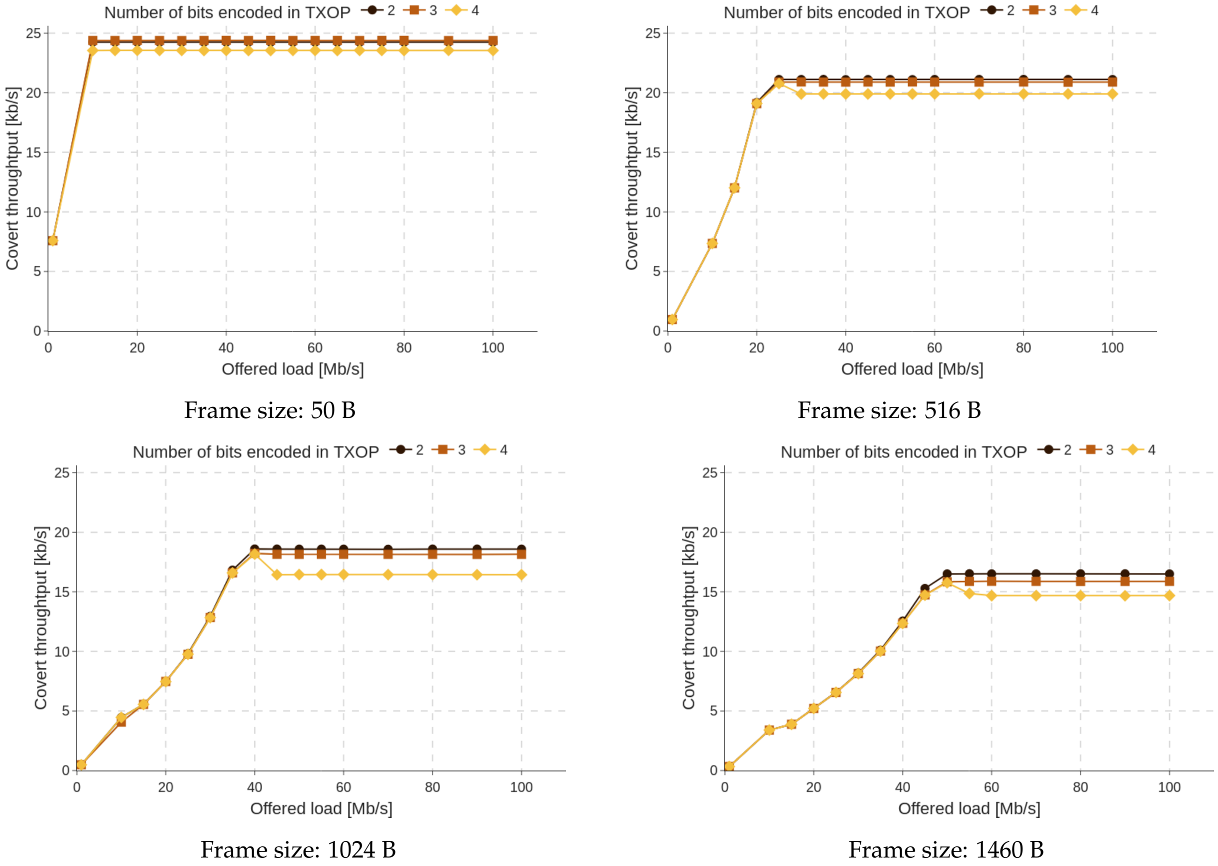
Frame size: 50 B

Frame size: 516 B

Frame size: 1024 B

Frame size: 1460 B

Figure 7. Average frame jitter vs. offered load for different frame size.



Frame size: 50 B

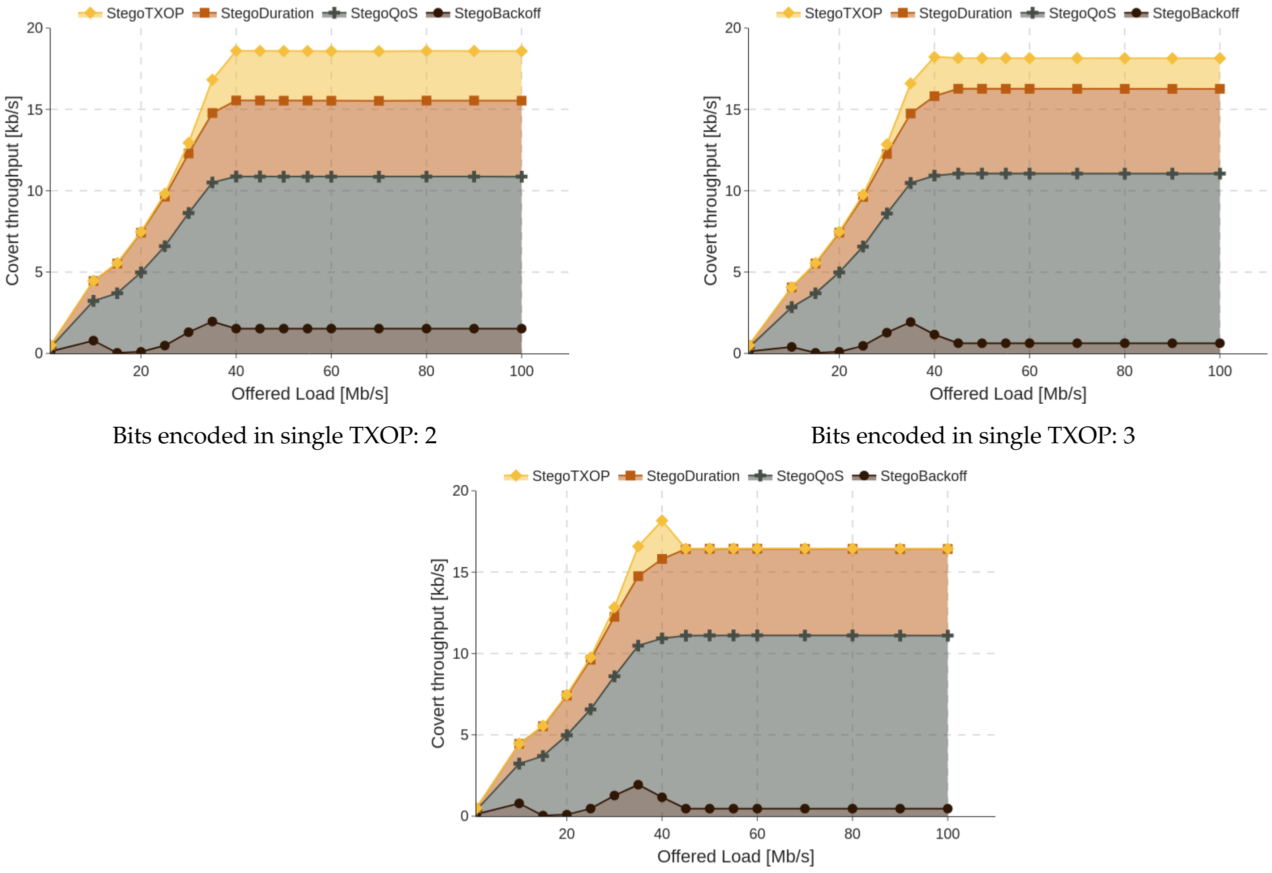
Frame size: 516 B

Frame size: 1024 B

Frame size: 1460 B

Figure 8. Combined EDCA covert channel throughput vs. offered load for Voice queue.

The throughput of each component of the combined EDCA covert channel for a frame size of 1024 bytes is presented in Figure 9. Similar proportional trends are observed for other frame sizes. The largest portion of the throughput is contributed by the StegoQoS and StegoDuration channels, which are mostly unaffected by changes in the number of bits encoded within a TXOP. In contrast, the throughput of the StegoTXOP channel decreases as TXOP periods become longer. Longer bit sequences fail to compensate for the reduction in the number of TXOP periods. Similarly, the throughput of the StegoBackoff channel decreases with longer bit sequences in StegoTXOP, as it can transmit bits only with the first message of each TXOP period. It is also worth noting that a 4-bit sequence length for StegoTXOP is unable to reliably convey hidden data.



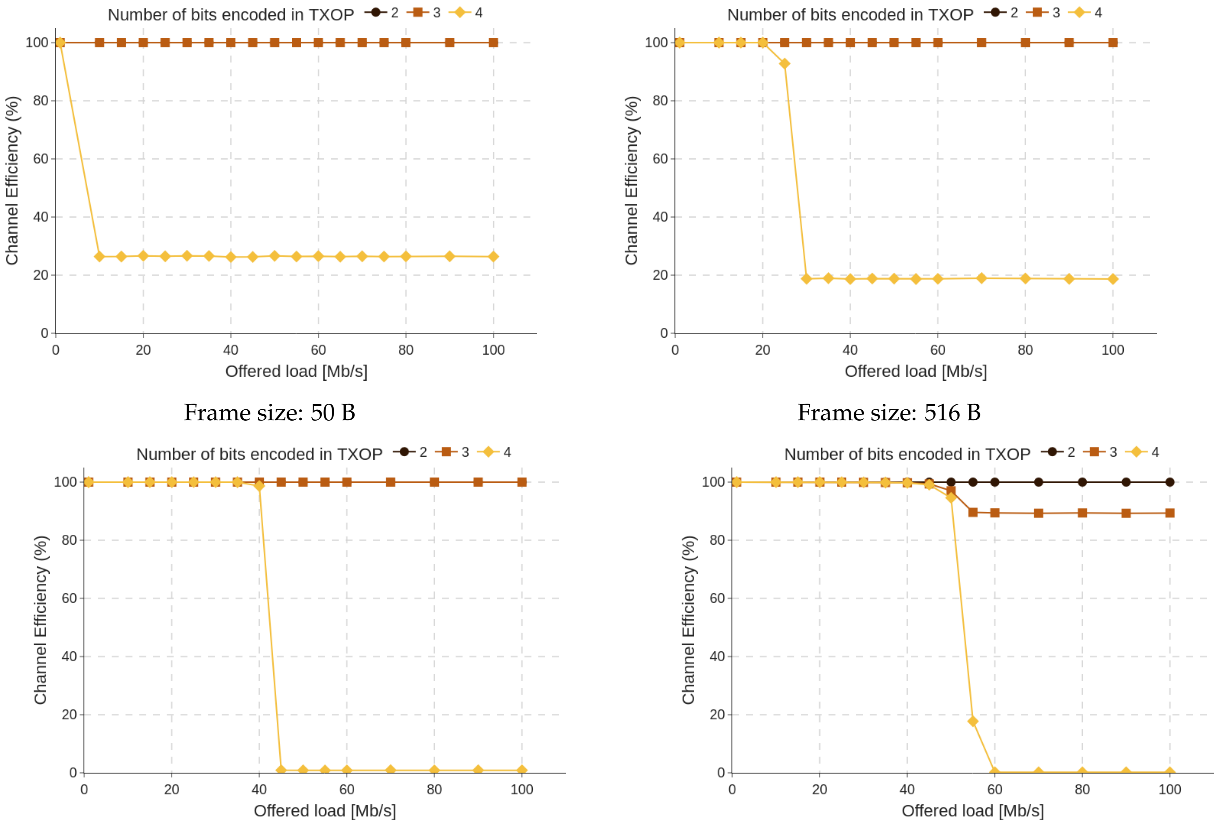
Bits encoded in single TXOP: 2

Bits encoded in single TXOP: 3

Bits encoded in single TXOP: 4

Figure 9. StegoEDCA covert channel throughput vs. offered load for frame size 1024 B.

Figure 10 illustrates the channel efficiency for StegoTXOP. Channel efficiency is defined as the ratio of correctly decoded TXOP periods to the total number of transmitted TXOP periods. It can be observed that channels encoding 2 or 3 bits per TXOP period reliably transmit data without errors. However, encoding 4 bits makes the channel unstable. This instability appears to arise because, for correct message transmission, the station needs to send more frames within a single TXOP period than is permitted by the network configuration and parameters. Consequently, the channel efficiency in this scenario is significantly reduced, reaching 0% with the longest frame size considered.



Frame size: 50 B

Frame size: 516 B

Frame size: 1024 B

Frame size: 1460 B

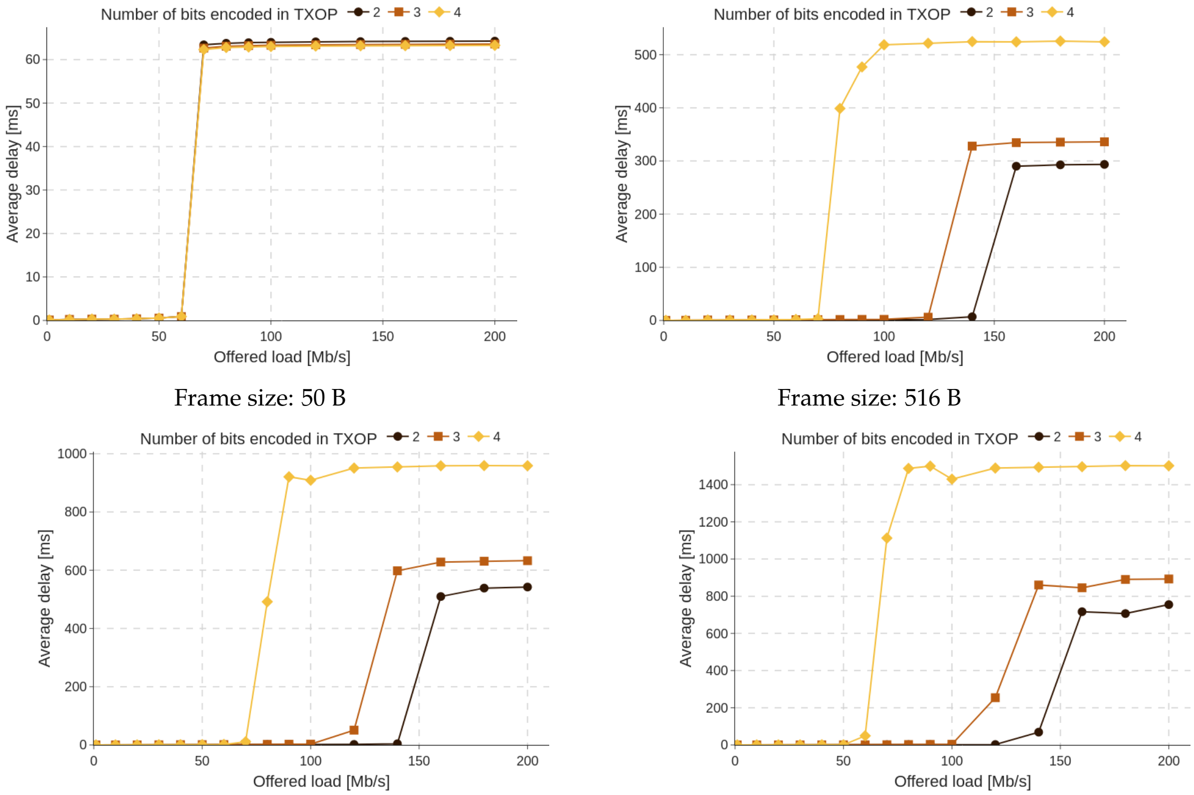
Figure 10. Channel efficiency vs. offered load for different frame size.

5.2.2. Scenario 2—Video Queue in Non-Competetive Environment

The topology of the second scenario is identical to that of the first scenario depicted in Figure 5.The key difference lies in the use of the video queue instead of the voice queue for overt channel transmission. The default parameters specified in the IEEE 802.11e standard extension for the video access category, compared to those for the voice access category, allow for longer TXOP periods and do not require immediate acknowledgments, thereby enabling frame aggregation in the form of A-MPDU.

The average delay, as shown in Figure 11, reveals significant performance discrepancies based on the maximum number of bits encoded within a single TXOP period. In contrast to the results observed in the first scenario, the best-performing configuration for StegoTXOP in terms of delay is encoding only up to two bits. This setting minimizes the impact on network performance by reducing unnecessary signaling to a minimum. To transmit more A-MPDU within a single TXOP, the covert station must aggregate fewer frames per A-MPDU than the maximum allowed by the standard. This results in an increased number of block acknowledgment frames, which, in turn, reduces the time available for transmitting user data. This phenomenon is not observed in simulations with a frame size of 50 bytes, as such short frames reach the limit of 64 frames per A-MPDU even before StegoTXOP interference occurs.

Similar observations can be made by analyzing the mean jitter graphs in Figure 12. Once again, the 50-byte frame size does not show any noticeable differences between the stegoTXOP modes. However, under network saturation, it can be observed that encoding 3 bits has a slight advantage over encoding 2 bits. This is because more frequent block acknowledgments enable faster error detection and retransmission of incorrectly received frames. This advantage does not extend to networks with 4-bit encoding enabled, as the difference in transmission throughput and signaling overhead between 4-bit encoding and lower-level encodings is too important.



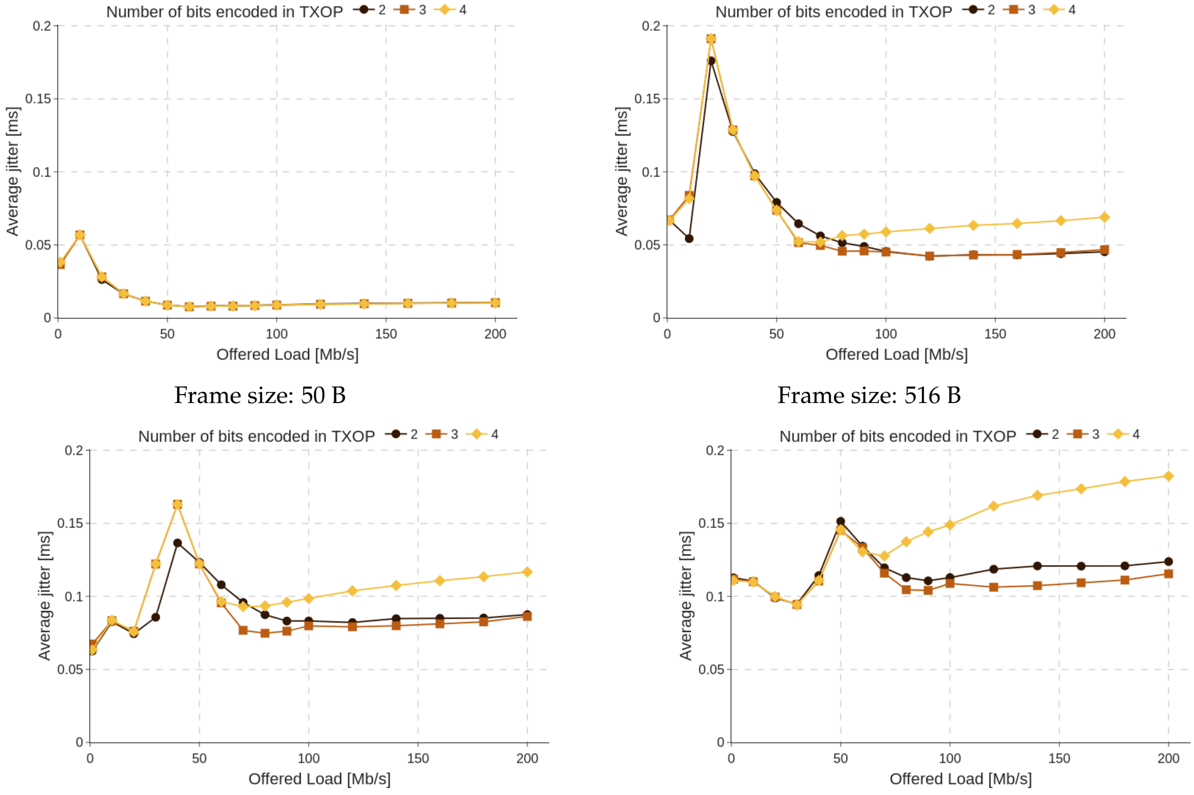
Frame size: 50 B

Frame size: 516 B

Frame size: 1024 B

Frame size: 1460 B

Figure 11. Average frame delay vs. offered load for different frame size.



Frame size: 50 B

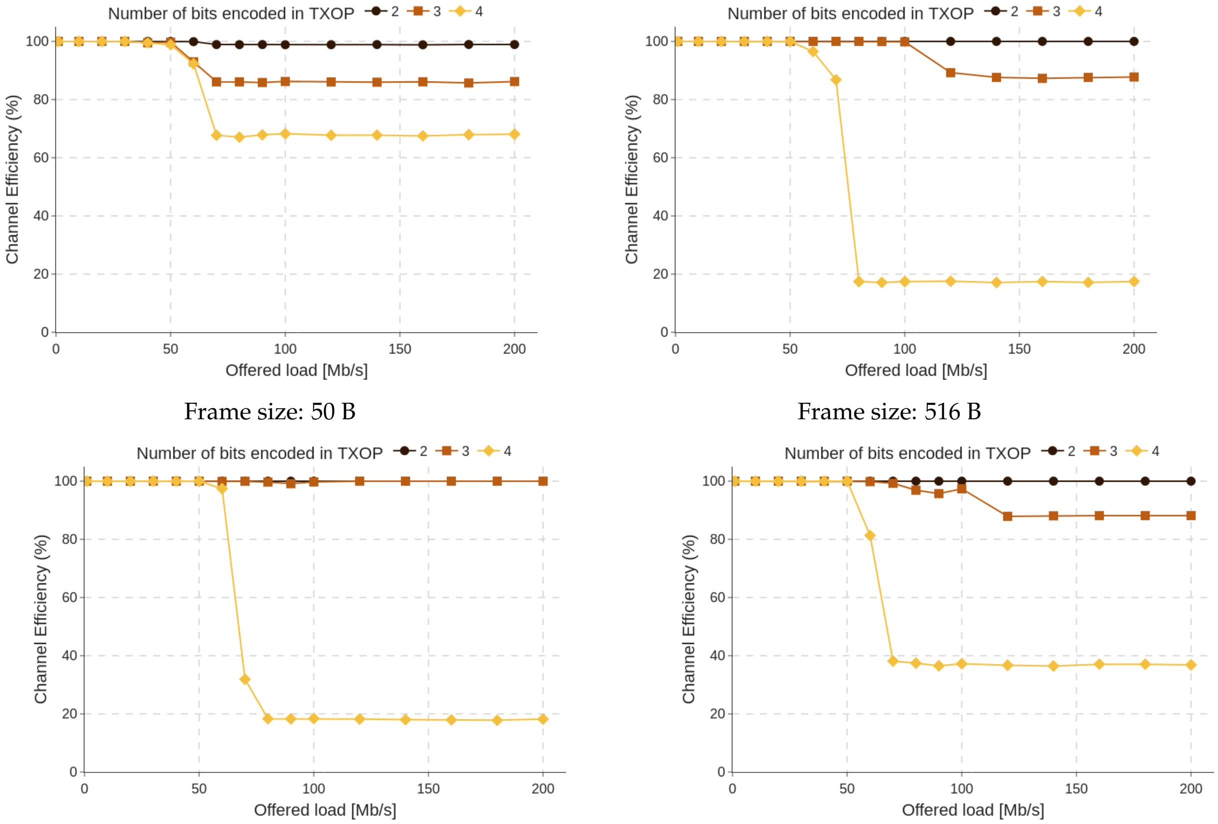
Frame size: 516 B

Frame size: 1024 B

Frame size: 1460 B

Figure 12. Average frame jitter vs. offered load for different frame size.

StegoTXOP efficiency in both modes within the video queue is illustrated in Figure 13. The results indicate that the frame aggregation slicing implemented for the StegoTXOP mechanism is suboptimal and introduces errors in data transmission. Although the 2-bit sequence length achieves near-perfect efficiency, reaching almost 100%, the 3-bit sequence length experiences a performance decline to approximately 85% across all simulations with an increase in offered load. Furthermore, the 4-bit encoding efficiency falls below the acceptable threshold for reliable data transmission.



Frame size: 50 B

Frame size: 516 B

Frame size: 1024 B

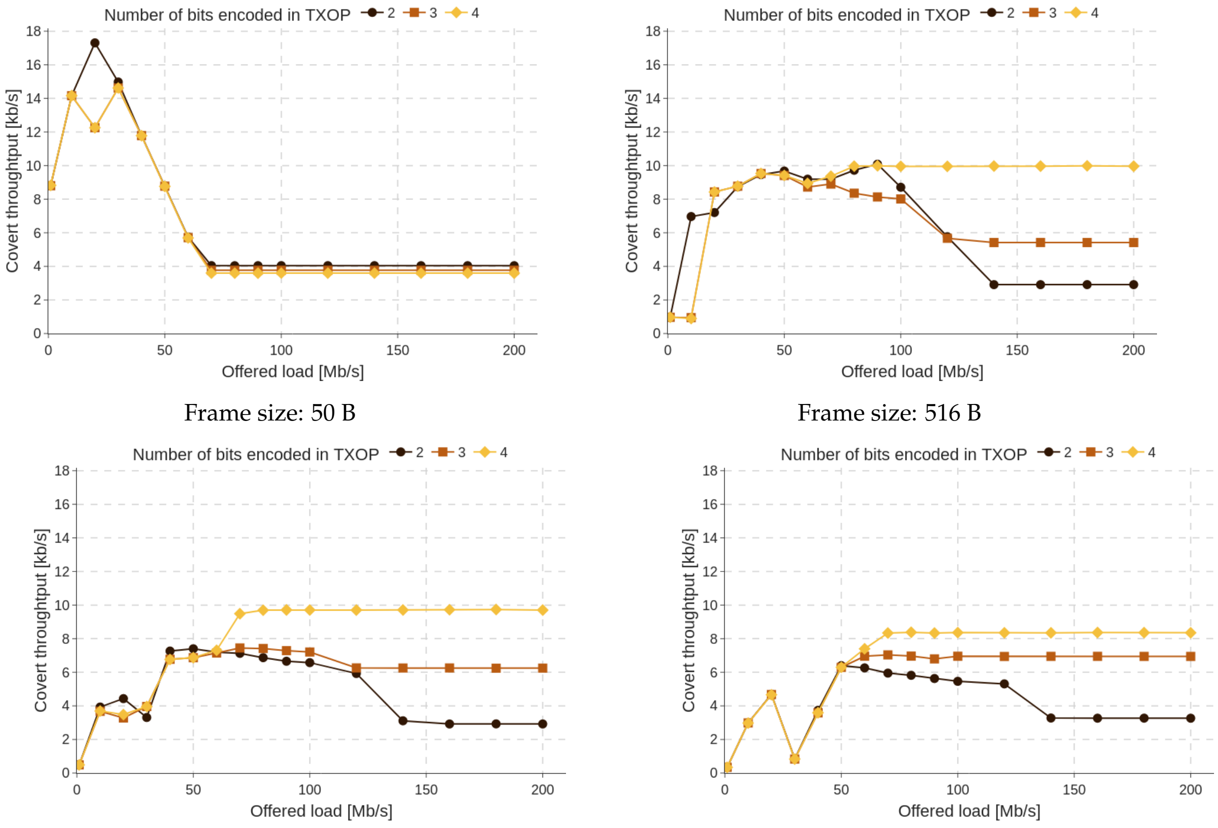
Frame size: 1460 B

Figure 13. Channel efficiency vs. offered load for different frame size.

High Covertness Mode

This subsection presents the results of the covert channel throughput, where StegoQoS and StegoDuration operate in high covertness mode. The set of plots in Figure 14 illustrates the cumulative performance of all proposed methods. It can be seen that the highest bandwidth is achieved by the channel utilizing the longest available encoding mode in StegoTXOP. The 2-bit and 3-bit sequence lengths show reduced performance as the offered load increases. In contrast, the 4-bit mode stands out as the only configuration that maintains consistent performance.

Figure 15 provides insight into the significant performance gap between different modes of StegoTXOP. In high covertness mode, the most critical carrier of covert bits is the A-MPDU, where increasing the number of aggregated frames yields no performance gains. This implies that in heavily loaded networks where the A-MPDU approaches its length limit, the proportion of time spent transmitting frames that do not carry covert information increases. The slicing of A-MPDUs introduced by StegoTXOP increases the number of A-MPDUs sent by the covert station. The longer the sequence encoded within a TXOP period, the shorter A-MPDUs need to be transmitted, thereby enhancing the performance of StegoQoS and StegoDuration.



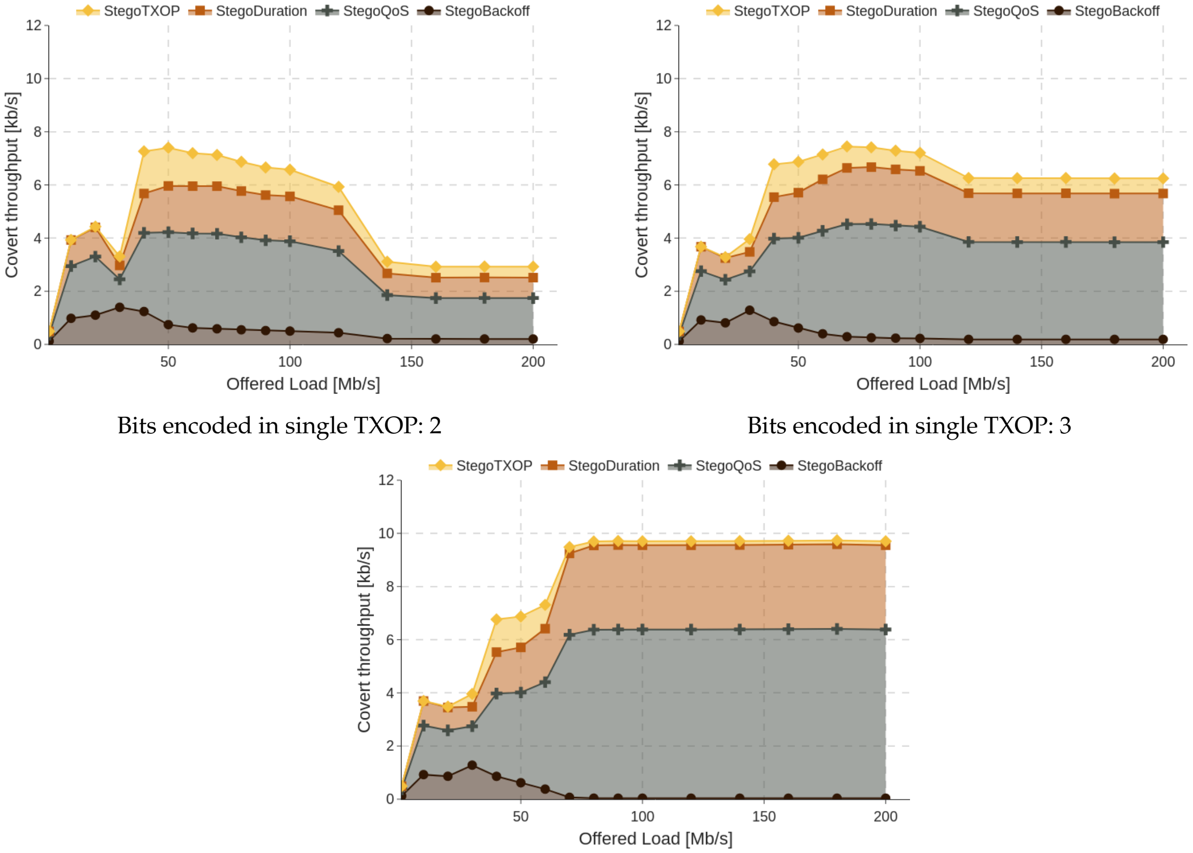
Frame size: 50 B

Frame size: 516 B

Frame size: 1024 B

Frame size: 1460 B

Figure 14. Channel throughput vs. offered load for different frame size.



Bits encoded in single TXOP: 2

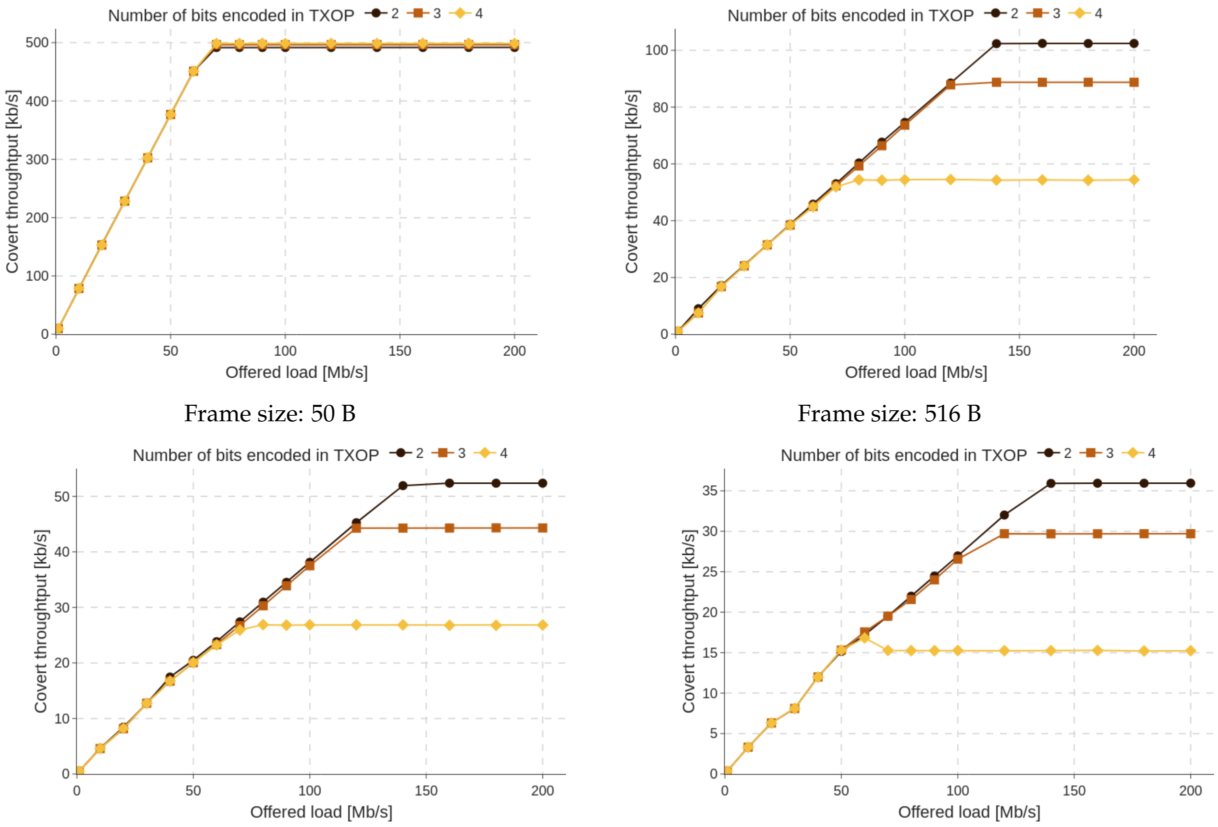
Bits encoded in single TXOP: 3

Bits encoded in single TXOP: 4

Figure 15. Channel throughput vs. offered load for frame size 1024 B.

High Throughput Mode

This subsection shows the maximum throughput possible to achieve by this proposal. Here, StegoQoS and StegoDuration run in high throughput mode which greatly reduces resistance to steganalysis, but in turn provides incredible bandwidth. The simulation results depicted in Figure 16 demonstrate a performance of approximately 500 kb/s for a frame size of 50 B. In this mode, frame size plays an important role in determining the achievable covert throughput. Additionally, significant discrepancies are observed among different StegoTXOP sequence length limits, with throughput losses reaching nearly 50% when transitioning from 2-bit sequence encoding to 4-bit sequence encoding within the TXOP period.



Frame size: 50 B

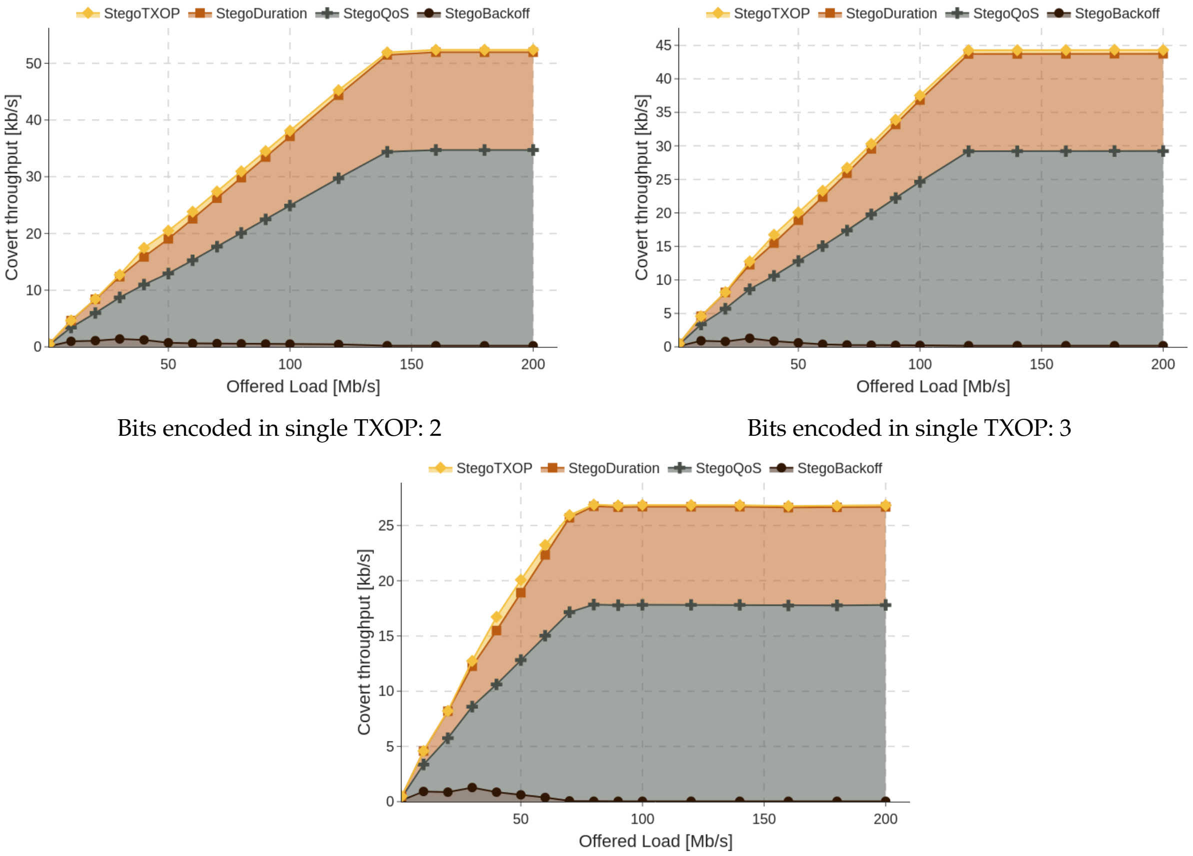
Frame size: 516 B

Frame size: 1024 B

Frame size: 1460 B

Figure 16. Channel throughput vs. offered load for different frame size.

A better understanding of channel behavior is provided by Figure 17, which illustrates the contributions of individual channels to cumulative throughput. In this mode, as opposed to high covertness mode, frames themselves become the covert information carriers for StegoQoS and StegoDuration. This allows the covert channel to fully exploit the additional bandwidth gains from frame aggregation. As these two channels, which rely on frames to transmit data, account for almost 100% of the combined channel throughput, any reduction in overt transmission performance introduced by StegoTXOP directly results in a corresponding reduction in the total combined channel throughput.



Bits encoded in single TXOP: 2

Bits encoded in single TXOP: 3

Bits encoded in single TXOP: 4

Figure 17. Channel throughput vs. offered load for frame size 1024 B.

5.2.3. Scenario 3—Voice Queue in Competitive Environment

In the second simulation scenario, the research focuses on evaluating covert channel performance for voice queue in a multi-station network environment as presented in Figure 18. All background stations share the same offered load, divided equally among all non-covert stations, and use the same QoS queue as the covert station to transmit data. Similarly to Scenario 1, this analysis examines the delay, jitter, efficiency, and throughput achieved by the proposed methods.

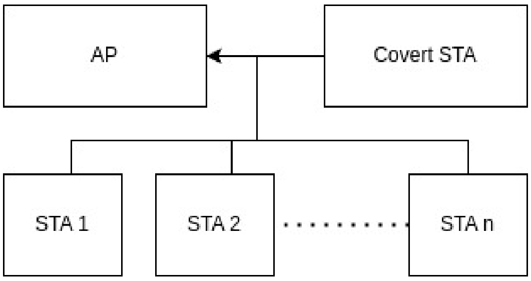
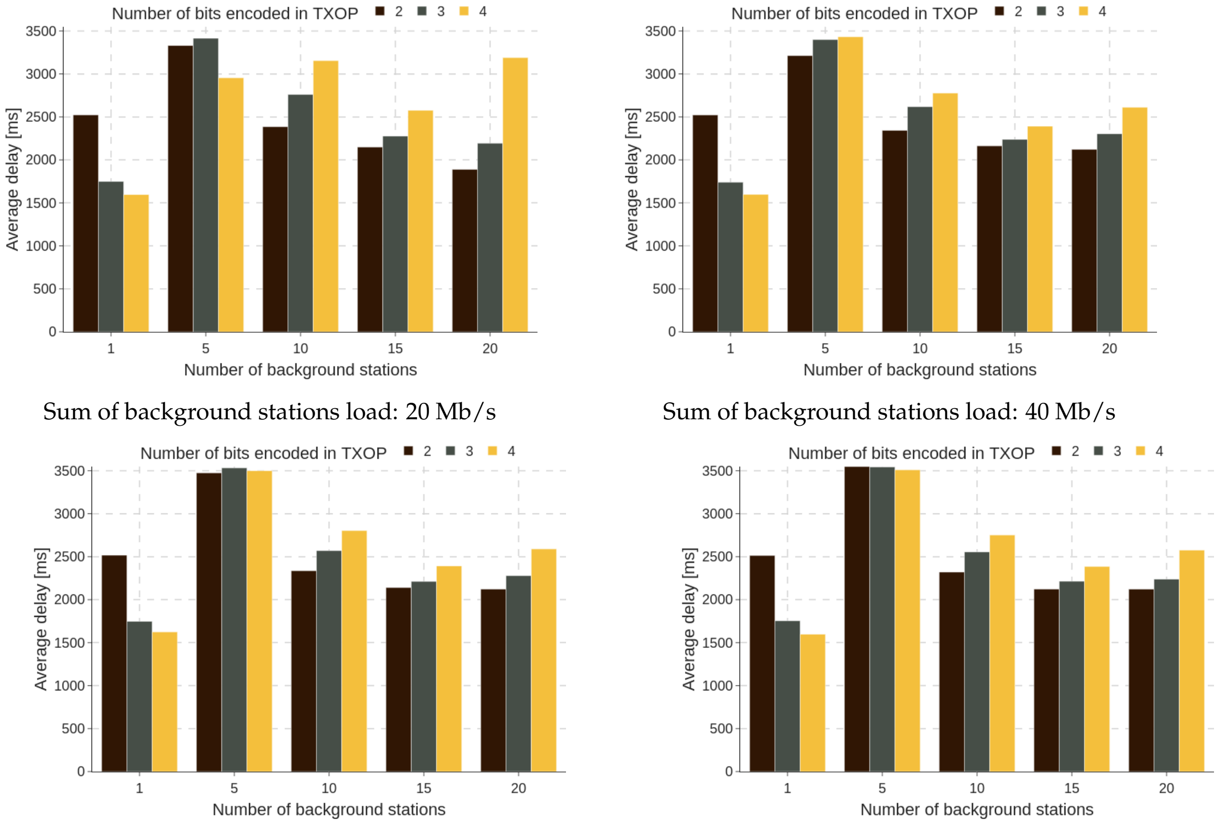


Figure 18. Network topology with multiple stations generating background traffic.

The covert station offered load for all simulations that utilized the voice queue was set to 40 Mb/s, with a frame size of 1024 kb/s. Figure 19 presents the average delay for covert station transmissions. In scenarios with a low number of background stations, the 2-bit sequence length in StegoTXOP lags behind other options in terms of performance. However, as the number of network users increases, its performance remains relatively stable, while the average delay for other options increases significantly. The 4-bit encoding option appears to be the most susceptible to performance degradation with an increasing number of network users.



Sum of background stations load: 20 Mb/s

Sum of background stations load: 40 Mb/s

Sum of background stations load: 60 Mb/s

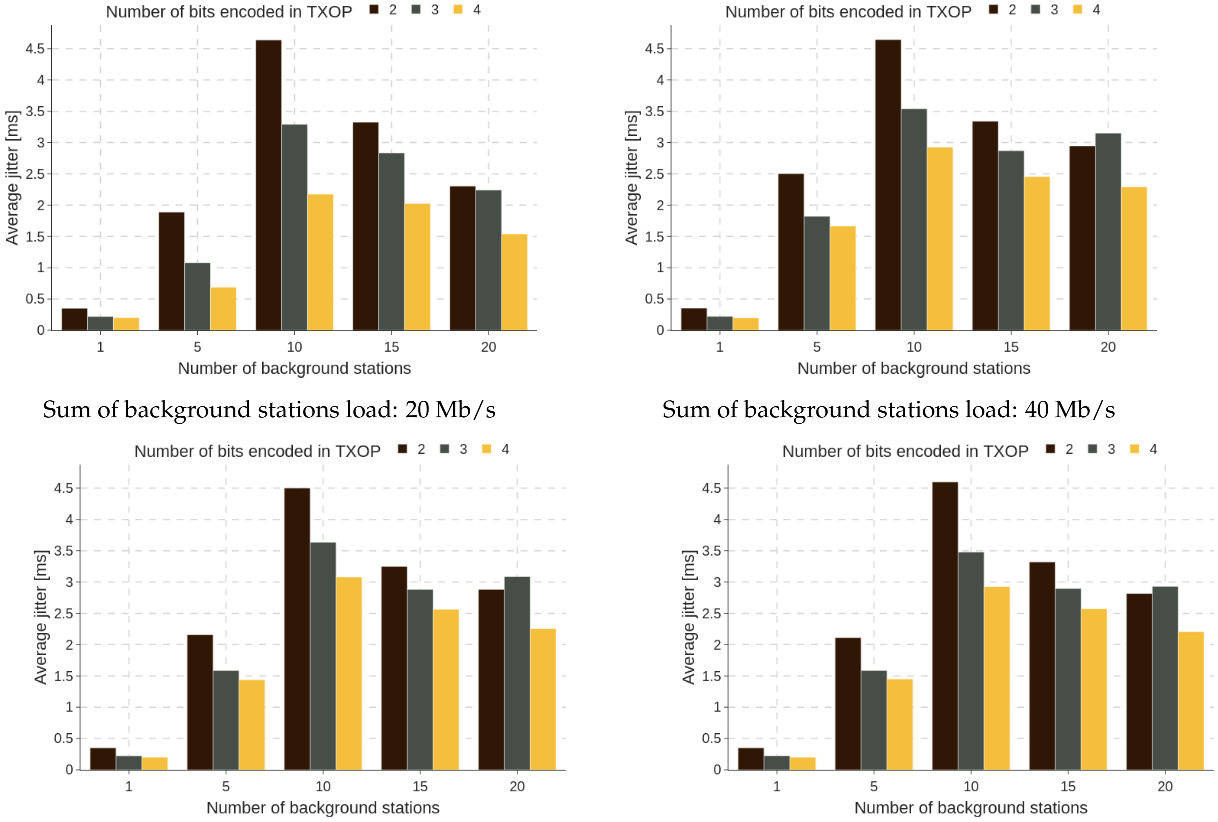
Sum of background stations load: 80 Mb/s

Figure 19. Average frame delay for different number of background stations and offered load.

Figure 20 shows the average jitter for the covert station. It appears that ending prematurely TXOP periods with stegoTXOP increases the average jitter. This indicates that the best-performing mode for stegoTXOP is the one with 4-bit sequences, while the mode that introduces the highest jitter is the 2-bit option. Basically, jitter remains relatively consistent in all simulated background station loads.

In networks where competition for channel access is high, underutilizing the TXOP period by terminating it prematurely proves detrimental to covert transmission. All covert channels are closely correlated with the number of frames transmitted; therefore, increasing the number of background stations or the load they generate significantly reduces the throughput of all utilized covert channels (as shown in Figure 21). Notably, encoding only two bits within a single TXOP period experiences the greatest performance degradation, as it imposes the most severe limitations on the bandwidth available for regular transmission.

The channel efficiency for StegoTXOP under high network congestion remains similar to the observations from scenario 1. As shown in Figure 22, encoding 2 or 3 bits per TXOP period proves to be a reliable method of transmission, achieving nearly 100% efficiency. However, encoding 4 bits remains unstable, particularly under low network load, due to constraints imposed by the network configuration. Despite this unreliability, throughput results indicate that the highest results in a multi-user network were achieved with 4-bit encoding. These findings lead to the conclusion that completely disabled StegoTXOP for voice queue may be the optimal approach in high-congestion scenarios to ensure consistent and efficient network performance.



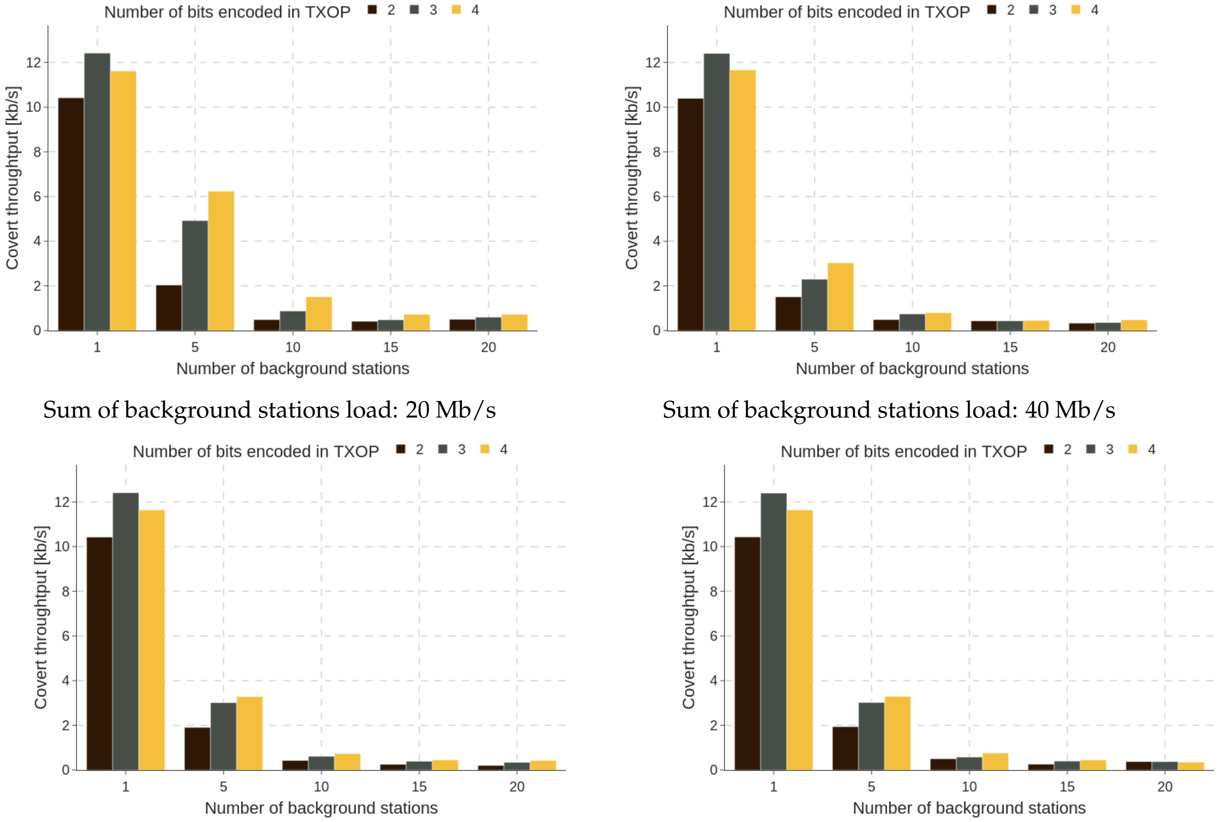
Sum of background stations load: 20 Mb/s

Sum of background stations load: 40 Mb/s

Sum of background stations load: 60 Mb/s

Sum of background stations load: 80 Mb/s

Figure 20. Average frame jitter for different number of background stations and offered load.



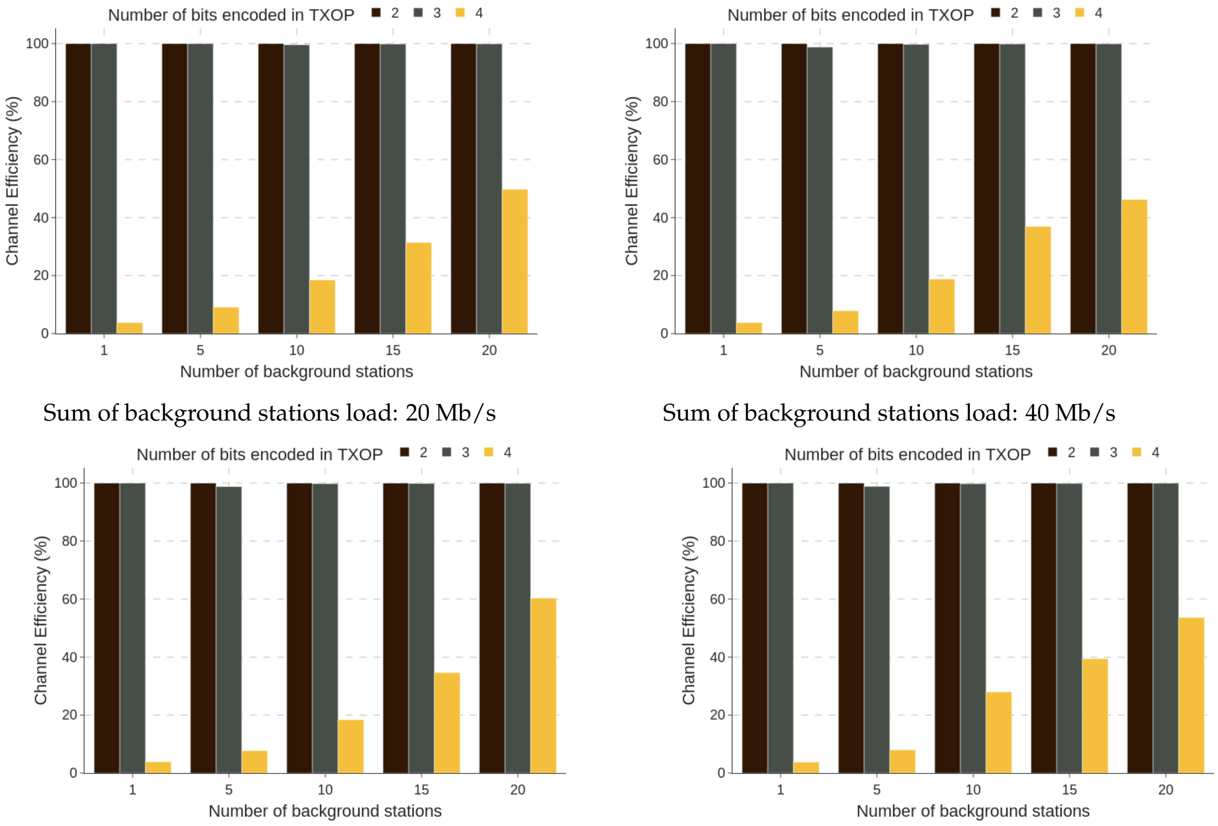
Sum of background stations load: 20 Mb/s

Sum of background stations load: 40 Mb/s

Sum of background stations load: 60 Mb/s

Sum of background stations load: 80 Mb/s

Figure 21. Covert channel throughput for different number of background stations and offered load.



Sum of background stations load: 20 Mb/s

Sum of background stations load: 40 Mb/s

Sum of background stations load: 60 Mb/s

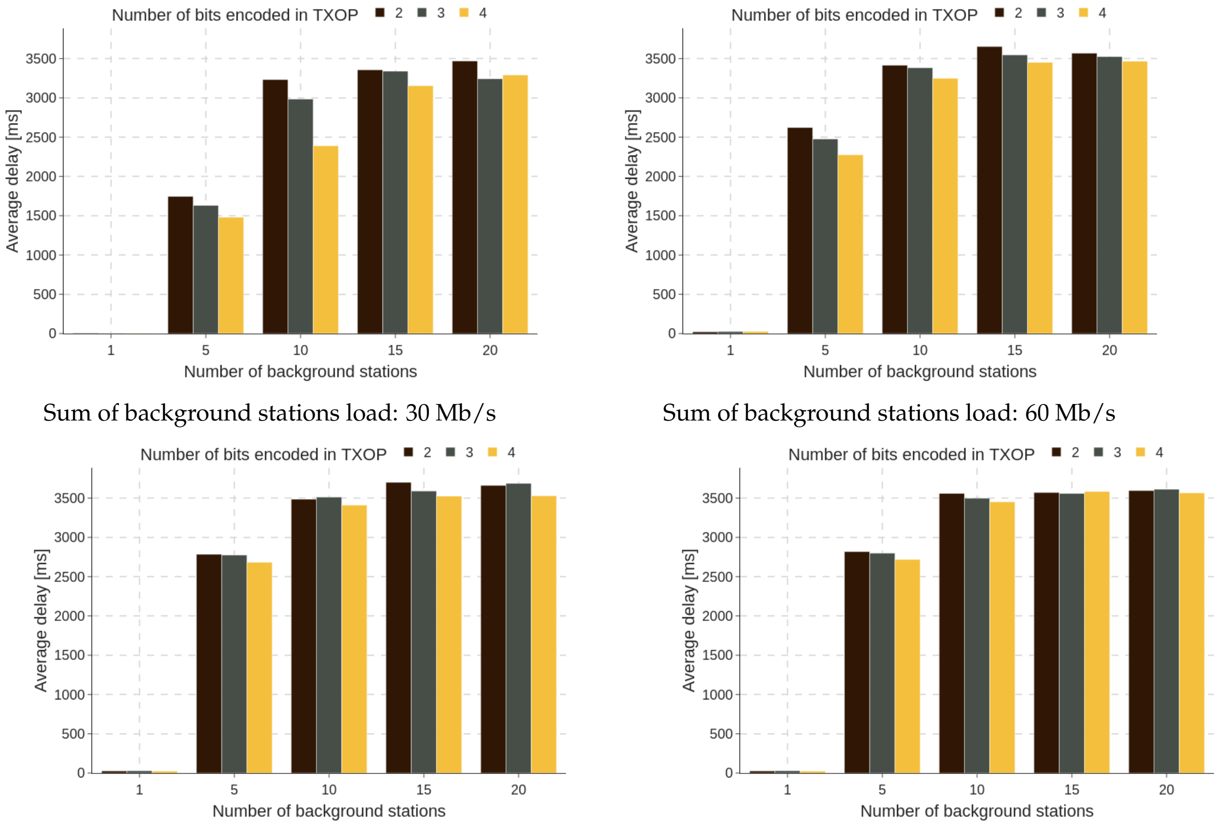
Sum of background stations load: 80 Mb/s

Figure 22. Channel efficiency for different number of background stations and offered load.

5.2.4. Scenario 4—Video Queue in Competetive Environment

The topology for this scenario is the same as depicted in Figure 18. This part of the research focuses on the throughput of a covert channel in a multi-user scenario with the utilization of the video queue for overt transmission. The covert station in all the following simulations uses 1024 B frame size and generates a load of 60 Mb/s. The average delay is presented in Figure 23. The combined load generated by the covert station and a single background station is insufficient to saturate the network, which explains the low results observed in this scenario compared to others. In the remaining scenarios, delay appears to depend primarily on the load generated by background stations. When the background load is low, the best-performing mode of StegoTXOP is that utilizing 4-bit sequences. However, as the background load increases, the performance differences between the different modes become less pronounced.

The average frame jitter for covert station transmissions, as depicted in Figure 24, reveals that under high network congestion, aggregating fewer frames into a single A-MPDU results in reduced average jitter. This is because smaller aggregates facilitate faster retransmissions in the event of errors. Consequently, the 4-bit encoding in StegoTXOP achieves the lowest mean jitter, whereas the 2-bit encoding consistently exhibits the poorest performance across nearly all scenarios.



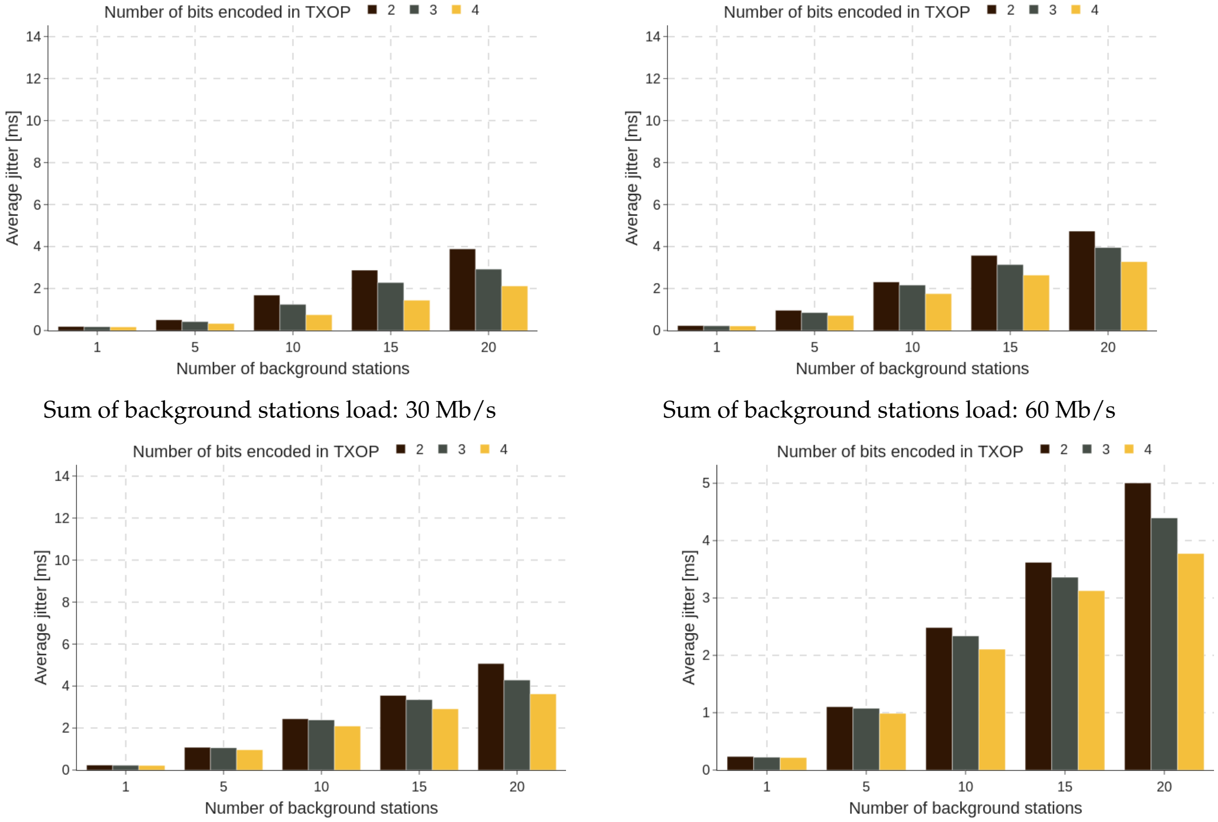
Sum of background stations load: 30 Mb/s

Sum of background stations load: 60 Mb/s

Sum of background stations load: 90 Mb/s

Sum of background stations load: 120 Mb/s

Figure 23. Average frame delay for different number of background stations and offered load.



Sum of background stations load: 30 Mb/s

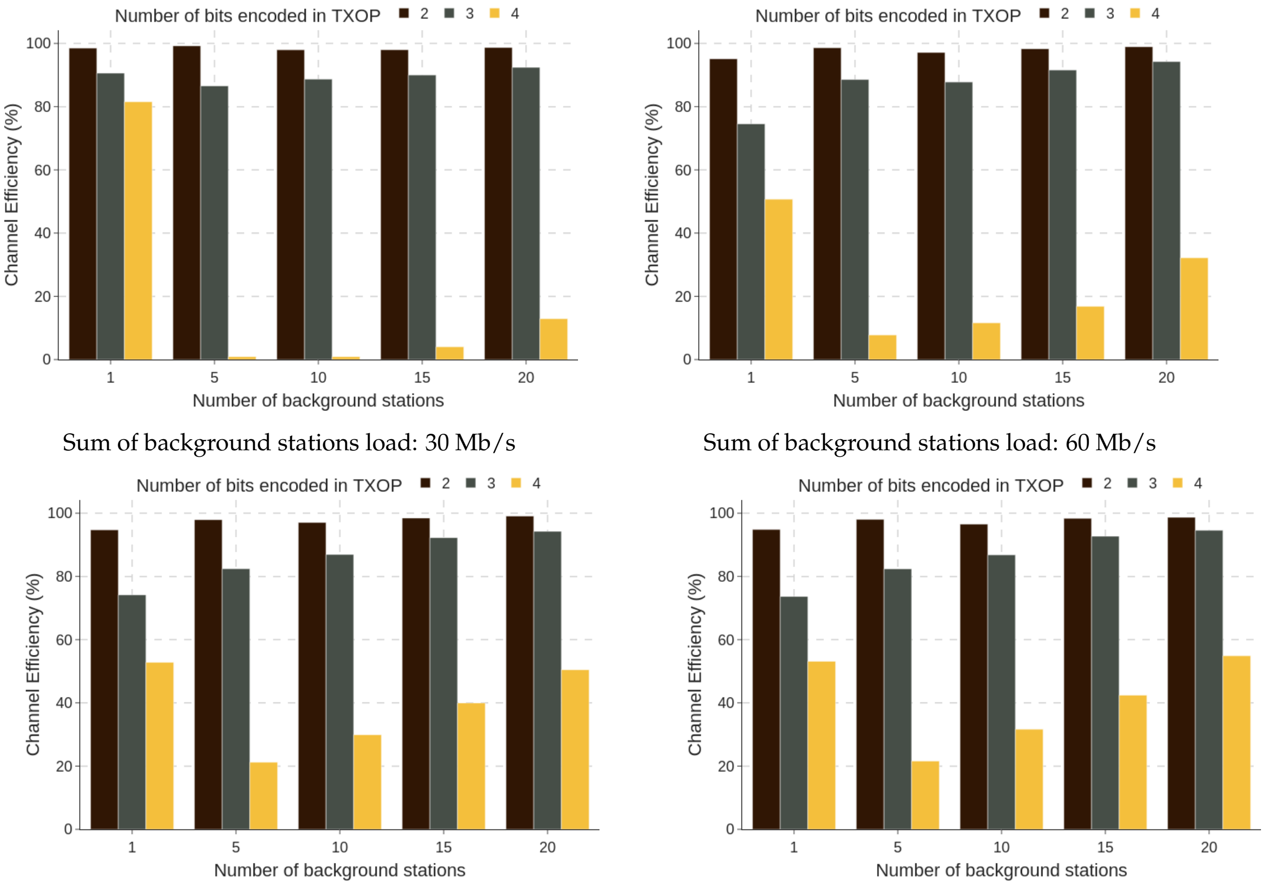
Sum of background stations load: 60 Mb/s

Sum of background stations load: 90 Mb/s

Sum of background stations load: 120 Mb/s

Figure 24. Average frame jitter for different number of background stations and offered load.

Figure 25 shows the channel efficiency of StegoTXOP achieved in both high throughput and high covertness modes. StegoTXOP with a 2-bit sequence length remains unaffected by an increasing number of background stations or their load, maintaining an efficiency of over 95% in all simulations. The 3-bit option performs slightly worse, experiencing a significant drop in efficiency with a low number of background stations and high load. The 4-bit option shows promising performance with a single background station, but as mentioned previously, the network is not in saturation state, meaning that there are not enough frames in the queue for the algorithm to consistently employ 4-bit encoding. In other scenarios, performance improves considerably with an increased number of background stations and their load, but still fails to achieve an efficiency of over 60%.



Sum of background stations load: 30 Mb/s

Sum of background stations load: 60 Mb/s

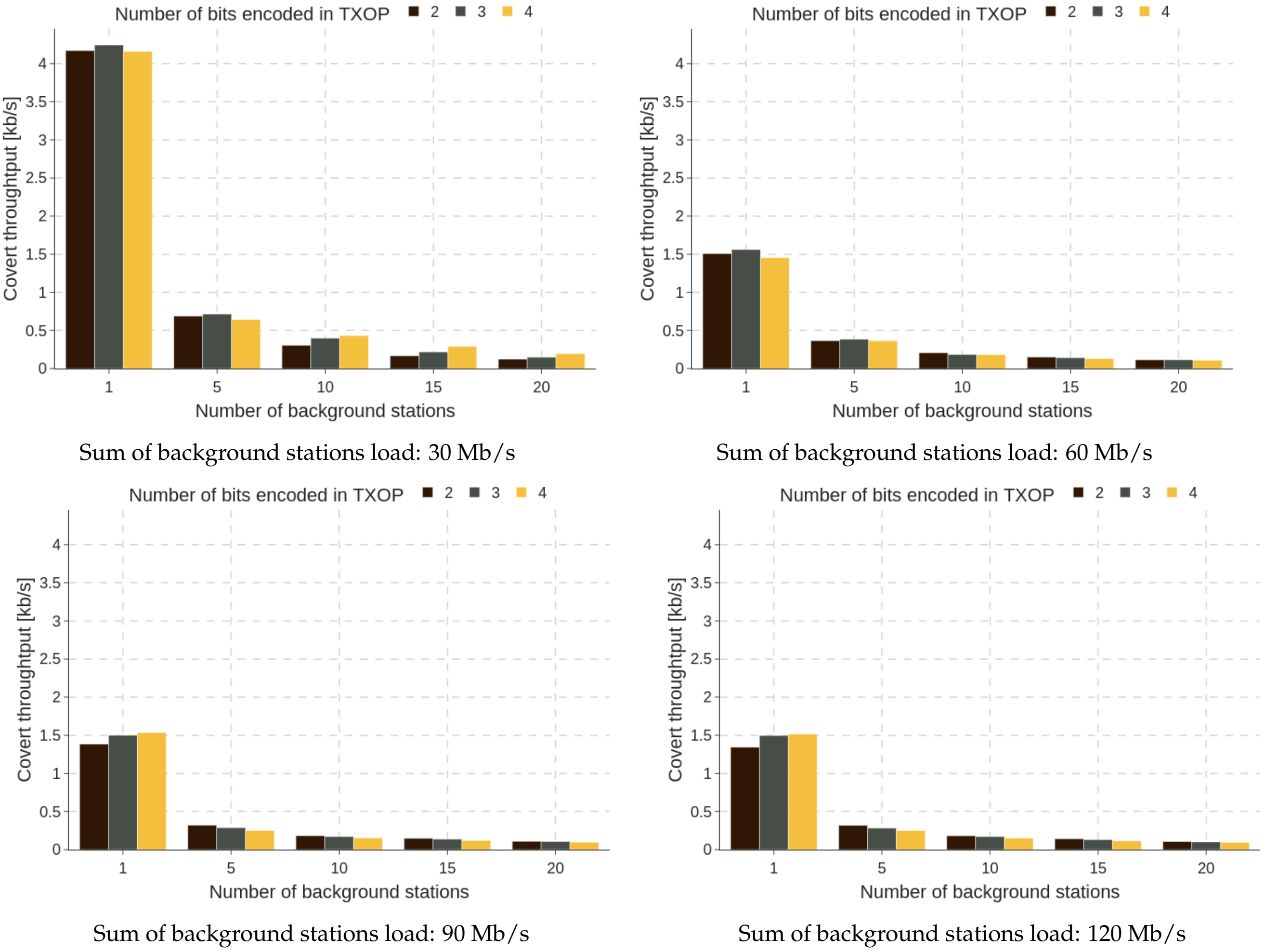
Sum of background stations load: 90 Mb/s

Sum of background stations load: 120 Mb/s

Figure 25. Channel efficiency for different number of background stations and offered load.

High Covertness Mode

In high covertness mode, encoding a maximum of two bits per TXOP period appears to be the most resilient to the increased load generated by background stations. As shown in Figure 26 with a background load of 30 Mb/s and discussed in Scenario 2, shorter sequences in StegoTXOP provide a lower maximum throughput under light load. However, as the load generated by background stations increases, the performance of two-bit encoding catches up to, and eventually surpasses, that of four-bit sequences under high network load. It is important to note that while increasing the number of background stations reduces the throughput of all encoding options by a similar amount, their relative distribution remains consistent. In contrast, increasing the load generated by these stations has a greater negative impact on three-bit and four-bit encoding than on two-bit encoding.



Sum of background stations load: 30 Mb/s

Sum of background stations load: 60 Mb/s

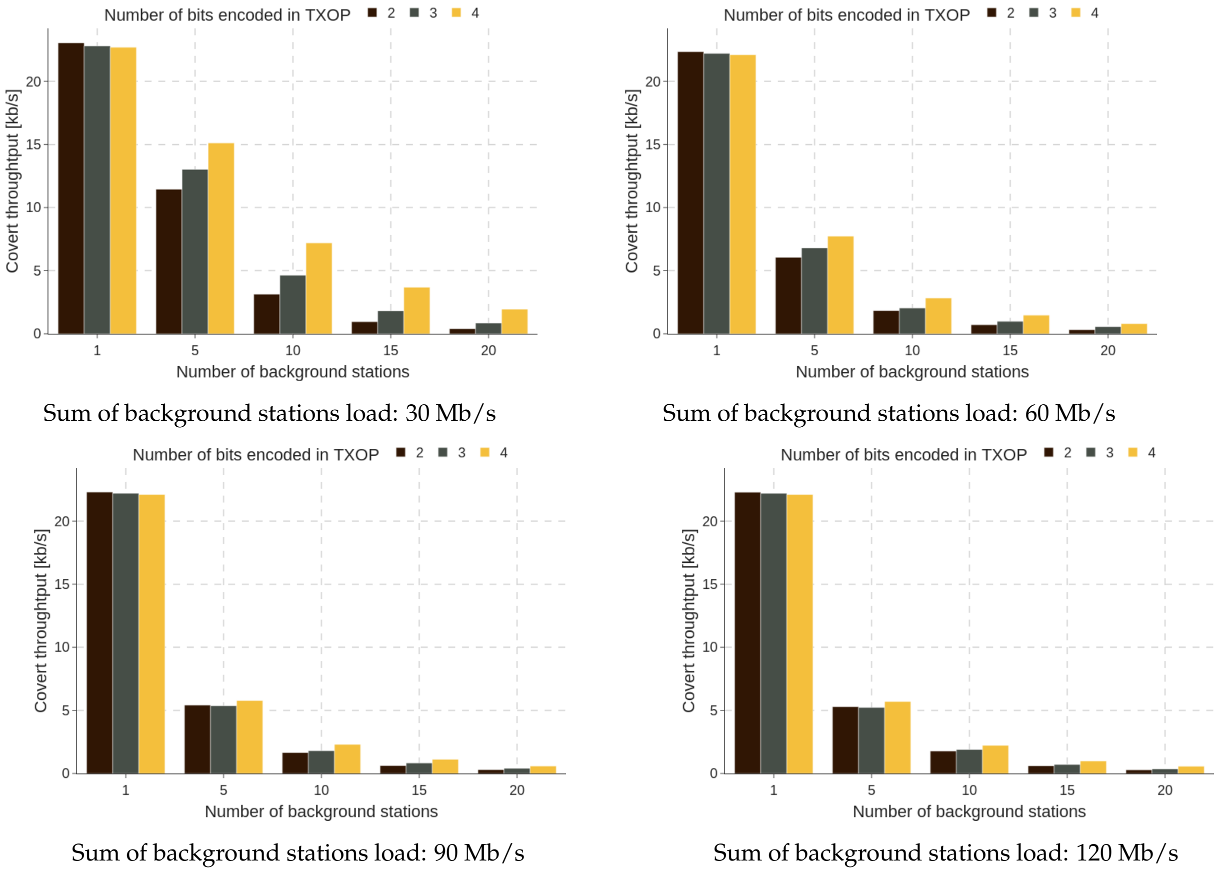
Sum of background stations load: 90 Mb/s

Sum of background stations load: 120 Mb/s

Figure 26. Channel throughput for different number of background stations and offered load.

High Throughput Mode

Contrary to the results observed in high covertness simulations, in high throughput mode, the best-performing channel is the one utilizing four-bit encoding. In all simulations, except for the scenario with a single background station, it achieved the highest throughput compared to the other encoding options (see Figure 27). Once again, increasing the background load tended to equalize the performance differences between the StegoTXOP sequence lengths. However, increasing the number of active stations in the network did not significantly alter the performance relationships among the different StegoTXOP modes.



Sum of background stations load: 30 Mb/s

Sum of background stations load: 60 Mb/s

Sum of background stations load: 90 Mb/s

Sum of background stations load: 120 Mb/s

Figure 27. Channel throughput for different number of background stations and offered load.

6. Limitations and Risks

The algorithms proposed in this work, like other algorithms used for creating covert channels, have certain limitations, and their implementation involves some risks. The primary limitation of the StegoEDCA method is the strong dependence of the covert channel's performance on the length of transmitted frames. Since the transmission of hidden information is closely correlated with the number of transmitted frames, from the perspective of the covert channel, it is advantageous to transmit as many short frames as possible. However, it is well known that transmitting short frames in a wireless network is inefficient due to significant overhead, as the performance of a wireless network without additional mechanisms like TXOP or frame aggregation can decrease by several dozen percent. The length of frames transmitted in computer networks is largely dependent on the types of applications being used. Very short frames are typical for voice services, whereas the transmission of high-quality video streams requires the use of very long frames. A potential solution for controlling the length of frames transmitted in a Wi-Fi network—and consequently setting the throughput of the covert channel—could be the use of additional mechanisms such as frame fragmentation. Although this approach allows for obtaining frames of a specific length, it can also significantly reduce the efficiency of regular data transmission for other stations.

It is also important to remember that a covert channel can only be established if there is ongoing transmission in the regular data transmission channel. For certain types of applications, this requirement may pose a limitation. Another factor influencing performance is undoubtedly the number of frames sent during the TXOP period. As studies have shown, it is not possible to definitively determine whether transmitting more or fewer frames during the TXOP period is better, as the performance of the covert channel depends on many factors, including the operating mode (high covertness vs. high throughput), the length of transmitted frames, and the volume of offered traffic.

There also remains the issue of selecting an appropriate operating mode for the proposed covert channel. In the opinion of the authors, this may depend on the specific application that uses the covert channel for transmission. If the application requires high throughput, such as transmitting several tens of megabytes of measurement data in a SG without providing sensitive data e.g., identifying specific users, the algorithm may switch to “high throughput” mode. However, if sensitive data are being transmitted and real-time transmission is not required, the algorithm should choose the “high covertness” mode for transmission.

Finally, since the covert channel solutions proposed in the article utilize only elements of the data link layer, their implementation in real hardware is entirely feasible. The data link layer in WLAN cards is typically implemented at both the driver and firmware levels. Naturally, there should be no issue implementing selected elements of the proposed covert channels in Linux operating system drivers (e.g., setting bits in the Duration field based on traffic class). However, modifying the firmware is a significantly more complex process (e.g., altering the number of time slots in the backoff mechanism). Firmware code is most often written in low-level languages such as assembler, often using dedicated tools and libraries provided by WLAN chipset manufacturers (e.g., Qualcomm, Broadcom, Intel). Access to such tools and firmware source code is typically beyond the reach of the average user due to costs and licensing issues.

When it comes to risks, it is important to remember that any manipulation of the contention window is non-compliant with the IEEE 802.11 standard and may lead to issues such as unfairness in access to the radio channel. Although the proposed solution, based on the backoff mechanism, in some cases changes the backoff by only one slot—sometimes benefiting the station creating the hidden channel and at other times causing it a disadvantage—this may be perceived by other stations as improper behavior. Considering also that the covert station mostly increases its window size (unless it reaches the CWmax value), effectively acting to its own detriment, this should not be regarded as a violation of correctness in relation to other stations.

Using the proposed steganographic mechanisms, resource consumption such as CPU usage or memory should be taken into account. Compared to other mechanisms requiring significant processing power, which are utilized in modern Wi-Fi networks—such as data encryption, frame fragmentation at transmission rates of tens of Gb/s, CRC calculations, support for MU-MIMO, beamforming, Credit-Based Shaper Algorithm (CBSA) traffic shaping or the operation of the OFDMA scheduler in access points—the presented mechanisms employ very simple calculations. These include operations like XOR, counting individual slots in the contention window, and reading/writing values in MAC frame headers. Considering that modern Wi-Fi devices are often equipped with very powerful processors (typically specialized multi-core SoCs) operating at speeds exceeding 2 GHz, along with substantial memory for frame buffering (necessary at such high transmission rates), the proposed covert channel mechanisms will have a negligible impact on both CPU load and memory usage. The data rates achievable in covert channels (several hundred Kbps), despite significant progress in this field observed in recent years, are still incomparably smaller than the regular data rates exchanged between users and networking devices (which today exceed 36 Gb/s).

7. Conclusions

This research proposes the family of novel covert channels built on features introduced in IEEE 802.11e aimed at enhancing data integrity and communication security within the SG.

The proposed approach utilizes access categories of the EDCA function combined with a shift mechanism that uses the 'Duration' field of the MAC frame header, the TXOP mechanism, and the parity of the EDCA backoff slots. Its resistance to steganalysis is mainly due to the fact that hidden data are transferred using three or four independent covert channels. In addition, these channels operate transparently, preventing disruption of normal network operations, thereby enabling them to function seamlessly and remain inconspicuous. A combination of these channels was implemented in the NS-3 network simulator, and multiple tests were conducted to investigate how different frame sizes, offered load, and background activity impacted channel performance. The study also discusses how various covert channel settings affect regular network performance. The simulations concluded that the channel is capable of providing sufficient throughput in all network scenarios.

With properly configured settings, it demonstrates the ability to avoid introducing any negative impact on regular network transmissions. The key to achieving optimal performance in various scenarios lies in determining the most suitable StegoTXOP sequence length configuration. The best-performing configuration for the voice queue in terms of throughput is the encoding of 2-bit-long sequences within a single TXOP. However, this option introduces the highest increase in average delay and jitter among all available configurations. The 3-bit-long encoding emerges as a viable intermediate solution, balancing throughput performance with reduced delay and jitter compared to the 2-bit one. With A-MPDU aggregation enabled in the video queue, it is challenging to identify a clear winner. In high covertness mode, the highest throughput was achieved using 4-bit-long encoding within a TXOP, albeit at the expense of significantly increased average jitter and delay. In contrast, the 2-bit encoding exhibited the lowest performance impact on regular transmissions. This characteristic made 2-bit encoding the optimal choice in high throughput mode, as covert bits were strongly correlated with the overall number of frames transmitted. The selective throughput results of the simulations are summarized in Table 5, showcasing the highest channel performance achieved under specific parameter configurations. These results underscore the potential of the proposed algorithm to achieve high covert transmission rates while maintaining efficiency. Despite some shortcomings, the algorithm shows great promise and, with fine-tuning, could be implemented in real-world scenarios to enhance the security of SG and their users.

Table 5. Selected simulation results for single station scenario.

Frame Size	Offered Load [Mb/s]	Access Category	StegoQoS Mode	Throughput [kb/s]
50	60	Voice	-	24.25
50	120	Video	High covertness	4.04
50	120	Video	High throughput	496.52
1024	60	Voice	-	18.58
1024	120	Video	High covertness	9.7
1024	120	Video	High throughput	45.26
1460	60	Voice	-	16.51
1460	120	Video	High covertness	8.35
1460	120	Video	High throughput	29.7

In the multi-station scenario, the 2-bit encoding within a TXOP for the voice queue was the most susceptible to the increasing number of stations in the network. This susceptibility significantly reduced the available time for transmission, consequently decreasing covert throughput and introducing higher jitter and delay. For the video queue, all configurations performed similarly regardless of settings, with only minor differences observed.

In high covertness mode, the 2-bit encoding exhibited a slight advantage, whereas in high throughput mode, the 4-bit encoding performed marginally better. The 3-bit sequence length consistently emerged as a balanced option in all situations, providing sufficient throughput while minimizing the impact on regular transmissions. Table 6 presents the highest channel throughput achieved in a congested network environment, measured with a frame size of 1024 bytes.

Table 6. Selected simulation results for multi station scenario.

Offered Load [Mb/s]	Background STA	Background Load [Mb/s]	Access Category	StegoQoS Mode	Throughput [kb/s]
40	5	80	Voice	-	3.02
80	5	120	Video	High covertness	0.32
80	5	120	Video	High throughput	5.7
40	15	80	Voice	-	0.83
80	15	120	Video	High covertness	0.14
80	15	120	Video	High throughput	0.99

Table 7 provides a comparison of the combined StegoEDCA algorithm with previously developed covert channels. The results demonstrate that this proposal achieves the highest throughput ever recorded for a covert channel constructed at the MAC layer of IEEE 802.11 networks. To be fair in evaluating performance relative to other covert channel protocols, the throughput value has been reduced by half to correspond to operating in a 20 MHz channel. Although this exceptional bandwidth is achieved with specific network configurations optimized for the algorithm, the simulations presented in this study indicate that the channel consistently delivers one of the highest covert transmission throughputs up to date. High bandwidth is achieved with the high throughput mode, which maintains a satisfactory level of covertness, ensuring the channel remains secure. The combination of multiple subchannels significantly improves the security of the proposed covert channel. A potential transmission listener would need to uncover all the embedded mechanisms used for data concealment before the covert user data could be compromised. This multi-layered approach increases the complexity of detection and mitigates the risk of channel exposure, making it a robust solution for secure covert communication. Covertness can be further enhanced if necessary, but at the cost of reduced covert channel throughput. This flexibility enables the proposal to adapt to varying network conditions and user requirements.

Table 7. Covert Channels comparison.

Ref.	Covert Data	Performance	Covertness
Proposed StegoEDCA method	Uses 3 or 4 different covert channels exploiting TXOP, EDCA Backoff, Access Category and Duration field	248,260 bit/s	Very high—multiple covert channels ensure that even when one is discovered the transmission as a whole remains secure.
[40]	Stego-Backoff	14,000 bit/s	High—random backoff procedure is an integral part of IEEE 802.11 standard.
[15]	DCF backoff time	8000 bit/s	Low—covert transmission decreases performance of other nodes. Covertness can be increased at the cost of bandwidth.
[39]	Random MAC Address in Probe Request	4770 bit/s	High—MAC randomization during probing.
[25]	The sum of the intervals between two consecutive transmission	1800 bit/s	High—time gaps introduced by the covert channel closely align with time gaps in regular network traffic.
[37]	Supported data rates and extended data rates fields probe request frames	806.67 bit/s	Medium - multiple probe scans with different values in Supported Rates field might arouse suspicion.

Table 7. *Cont.*

Ref.	Covert Data	Performance	Covertness
[16]	Information in Protocol Version field	127.4 bit/s	Low—default protocol version value is 0, and all other values are reserved.
[28]	Intervals of probe request frames and beacon frames to provide bidirectional communication	50 bit/s	High—detectable only at physical layer when investigating probe request frames.
[36]	Offset of the beacon interval	9.766 bit/s	Medium—ness might be broken by some pattern of time interval.
[35]	Embeds hidden bits of information in the relative order of frames	9.76 bit/s	High—sequence of frames are highly unpredictable.

Future Work

This research can be expanded further by conducting additional simulations focused on optimizing channel configurations in scenarios with mixed access categories. Although the StegoTXOP algorithm shows promise, more work is required to determine the appropriate thresholds for sequence lengths, a challenge that could benefit from the use of machine learning techniques. There is also potential to improve channel performance by incorporating additional covert channels into the mix. Another idea for future work is to try to implement this proposal on existing hardware and conduct experiments in similar scenarios for comparison, as references [15,19] suggest that real-world implementations may deviate from simulation results.

Author Contributions: Conceptualization, M.N.; methodology, M.N. and P.K.; software, P.K.; validation, M.N. and P.K.; formal analysis, M.N. and P.K.; investigation, M.N. and P.K.; writing—original draft preparation, M.N. and P.K.; writing—review and editing, M.N.; visualization, P.K.; 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.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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:

AC	access category
ACK	acknowledgement
AIFS	arbitrary inter-frame space
AP	access point
ARQ	automatic repeat request
BE	best effort
BK	background
BLE	bluetooth low energy
CBSA	credit-based shaper algorithm
CRC	cyclic redundancy check

CTS	clear-to-send
CW	contention window
CSMA/CA	carrier sense multiple access/collision avoidance
DCF	distributed coordination function
DIFS	distributed inter-frame space
EMD	exploiting modification direction
IEEE	institute of electrical and electronics engineers
JPEG	joint photographic experts group
LSB	least significant bit
MAC	medium access control
MCS	modulation and coding scheme
MIMO	multiple-input, multiple-output
MPDU	mac protocol data unit
MSDU	mac service data unit
OFDM	orthogonal frequency-division multiplexing
QoS	quality of service
PLCP	physical layer convergence protocol
RTS	request to send
SNR	signal-to-noise ratio
SG	smart grid
STA	station
TXOP	transmission opportunity
UDP	user datagram protocol
VI	video
VO	voice
WLAN	wireless local area network

References

1. Borlase, S. *Smart Grids: Infrastructure, Technology, and Solutions (Electric Power and Energy Engineering)*; CRC Press: Boca Raton, FL, USA, 2017.
2. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart Grid — The New and Improved Power Grid: A Survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980. [CrossRef]
3. *IEC 61850-1*; IEC Standard for Communication Network and Systems in Substations, Part 1 Introduction and Overview. IEC: Geneva, Switzerland, 2003.
4. *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.
5. *802.11e-2005*; IEEE Standard for Information Technology–Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. IEEE: Piscataway, NJ, USA, 2005; pp. 1–212. [CrossRef]
6. Szczypiorski, K. HICCUPS: Hidden communication system for corrupted networks. In Proceedings of the 10th International Multi-Conference on Advanced Computer Systems, Miedzyzdroje, Poland, 22–24 October 2003; pp. 31–40.
7. Szczypiorski, K. A Performance Analysis of HICCUPS–A Steganographic System for WLAN. In Proceedings of the 2009 International Conference on Multimedia Information Networking and Security, Wuhan, China, 18–20 November 2009; Volume 1, pp. 569–572. [CrossRef]
8. Krätzer, 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.
9. 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.
10. 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.
11. Calhoun, T.E.; 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.

12. Shah, G.; Blaze, M. Covert Channels through External Interference. In Proceedings of the WOOT, Montreal, QC, Canada, 10 August 2009; pp. 1–8.
13. 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; pp. 835–840.
14. Zbigniew, P.; Krzysztof, S.; Mariusz, B.; Piotr, G. 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.
15. 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.
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. 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, pp. 656–659.
18. Calhoun, T.E., Jr.; Cao, X.; Li, Y.; Beyah, R. An 802.11 MAC layer covert channel. *Wirel. Commun. Mob. Comput.* **2012**, *12*, 393–405. [CrossRef]
19. Radhakrishnan, S.V.; Uluagac, A.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.
20. 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.
21. Dutta, A.; Saha, D.; Grunwald, D.; Sicker, D. Secret agent radio: Covert communication through dirty constellations. In *Proceedings of the Information Hiding: 14th International Conference, IH 2012, Berkeley, CA, USA, 15–18 May 2012*; Revised Selected Papers 14; Springer: Berlin/Heidelberg, Germany, 2013; pp. 160–175.
22. Grabski, S.; Szczypiorski, K. Steganography in OFDM symbols of fast IEEE 802.11 n networks. In Proceedings of the 2013 IEEE Security and Privacy Workshops, San Francisco, CA, USA, 23–24 May 2013; pp. 158–164.
23. Zhao, H. Covert channels in 802.11 e wireless networks. In Proceedings of the 2014 Wireless Telecommunications Symposium, Washington, DC, USA, 6–9 October 2014; pp. 1–5.
24. 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.
25. 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.
26. 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.
27. Tahmasbi, F.; Moghim, N.; Mahdavi, M. Adaptive ternary timing covert channel in IEEE 802.11. *Secur. Commun. Netw.* **2016**, *9*, 3388–3400. [CrossRef]
28. 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.
29. 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.
30. Cao, P.; Liu, W.; Liu, G.; Ji, X.; Zhai, J.; Dai, Y. A wireless covert channel based on constellation shaping modulation. *Secur. Commun. Netw.* **2018**, *2018*, 1–15. [CrossRef]
31. 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; pp. 1585–1593.
32. Harley, P.M.; Tummala, M.; McEachen, J.C. 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.
33. 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.
34. Almohammedi, A.A.; Shepelev, V. Saturation throughput analysis of steganography in the IEEE 802.11 p protocol in the presence of non-ideal transmission channel. *IEEE Access* **2021**, *9*, 14459–14469. [CrossRef]

35. Sawicki, K.; Bieszczad, G.; Piotrowski, Z. Stegoframeorder—Mac layer covert network channel for wireless ieee 802.11 networks. *Sensors* **2021**, *21*, 6268. [CrossRef]
36. 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]
37. Teca, G.; Natkaniec, M. An IEEE 802.11 MAC Layer Covert Channel Based On Supported Rates. *Int. J. Electron. Telecommun.* **2023**, *69*, 293–299. [CrossRef]
38. 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, NN, USA, 22–25 January 2023; pp. 7–10.
39. Teca, G.; Natkaniec, M. A Novel Covert Channel for IEEE 802.11 Networks Utilizing MAC Address Randomization. *Appl. Sci.* **2023**, *13*, 8000. [CrossRef]
40. 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]
41. 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. [CrossRef]
42. *802.11n-2009*; IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. IEEE: Piscataway, NJ, USA, 2009; pp. 1–565. [CrossRef]
43. Team, I.F. Frame Aggregation in Wireless Networks. Available online: https://inet.omnetpp.org/docs/_images/dataunits3.png (accessed on 12 December 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.