energies

MDPI

Article

StegoBackoff: Creating a Covert Channel in Smart Grids Using the Backoff Procedure of IEEE 802.11 Networks

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

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

* Correspondence: natkanie@agh.edu.pl

† These authors contributed equally to this work.

Abstract: A smart grid constitutes an electrical infrastructure that integrates communication technologies to optimize electricity production, distribution, and consumption. Within the smart grid, IEEE 802.11 networks play a crucial role in facilitating communication between smart meters and data collectors, operating within a shared transmission medium. However, a notable challenge arises due to the lack of certainty regarding the genuine identity of data recipients. In response, we present a solution—a novel covert channel leveraging the IEEE 802.11 backoff procedure—to transmit data that requires special protection. Implemented using the ns-3 simulator, our covert channel achieved a throughput of 140,000 bps when single covert station realized transmission in the wireless channel, and 880 bps in a populated environment characterized by high traffic volumes. This performance metric shows that our mechanism is better than other covert channels, where the performance in saturated conditions usually does not exceed several hundred bps. This covert channel represents a new approach to fortifying data integrity and privacy within smart grid communication.

Keywords: smart grid; IEEE 802.11 network; covert channel; backoff procedure

Citation: 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. https://doi.org/10.3390/en17030716

Academic Editor: Ahmed Abu-Siada

Received: 31 December 2023
Revised: 24 January 2024
Accepted: 31 January 2024
Published: 2 February 2024

1. Introduction

The Smart Grid (SG) [1,2] represents a transformative evolution in traditional electrical grids, integrating cutting-edge digital technologies and advanced communication networks to enhance the efficiency, reliability, and sustainability of the entire electricity infrastructure. Unlike conventional power grids, the SG leverages real-time data, intelligent devices, and bidirectional communication to optimize energy generation, distribution, and consumption. This interconnected network of smart devices, sensors, and control systems allows utilities, consumers, and grid operators to monitor, analyze, and manage electricity flow dynamically.

In the SG context, the communication infrastructure assumes a crucial role, serving as the backbone that orchestrates the seamless flow of data among distributed energy resources, monitoring systems, and control centers. Adopting diverse communication technologies (depending on the network segment), the SG implements bidirectional data exchange, facilitating communication both from the control center to consumers and vice versa. The globally recognized SG standard, IEC 61850, has already standardized the interoperable exchange of information over Local Area Networks (LANs) [3]. Given the advantages of low installation costs, high data rates, and straightforward deployment, Wireless Local Networks (WLANs) technologies are gaining traction among power utilities. This is particularly true for less critical applications in SG. Amid these technologies, the WLANs, standardized as IEEE 802.11 [4] and commonly recognized as Wi-Fi, emerges as one of the primary communication technologies within the SG network segment [5]. Wi-Fi is strategically employed to establish robust communication links, particularly facilitating interactions between home appliances and Smart Meters (SMs) for collecting electricity consumption data. It is also used in distribution control and monitoring, automation and

metering, and distribution protection. Potential applications include: automatic capacitor bank control, fast distribution bus protection, load tap changer control and monitoring, centralized IED configuration, Watt/VAR measurement by broadcasting voltage phasors, distributed digital fault recording, and distribution feeder overcurrent protection [6].

In an IEEE 802.11 environment, devices operate within a shared transmission medium. A station equipped with an IEEE 802.11 radio interface, engaging in channel surveillance, possesses the ability to detect data transmissions by monitoring the channel signal energy levels. The shared nature of the transmission medium, however, exposes ongoing transmissions, potentially drawing attention and becoming susceptible to attacks. Moreover, practices like Medium Access Control (MAC) spoofing [7], the deployment of rogue access points (APs) [8,9], and other tactics that exploit Wi-Fi vulnerabilities in the functionalities [10–12], raise notable concerns regarding data security over Wi-Fi networks. Specifically, the apprehension pertains to verifying the authenticity of the data source, highlighting the need for robust security measures within the IEEE 802.11 environment in SG.

Steganography, an ancient practice, has found integration within the IEEE 802.11 network to enhance data confidentiality by facilitating the transmission of concealed information, rendering it imperceptible to network monitors or eavesdroppers. This implementation involves the creation of a covert channel, a secondary communication channel that operates concurrently with the standard channel. The conventional channel serves as an envelope or cover for the secret data. This covert channel, in turn, can be leveraged for the transmission of confidential information or for establishing authentication between elements within the SG.

In this paper, we introduce a new covert channel using the IEEE 802.11 backoff procedure. It serves as a secure method for authentication and a safeguarded channel for sharing private information. This covert channel enhances communication between the smart meters and also between the smart meters and the data collectors in a specific SG network [13]. The goal is to improve the security and privacy of data within the SG network [14–17].

The research brings the following contributions:

- Performance Evaluation of Covert Channel with TCP and UDP Variants—assessing the performance of the covert channel involves the evaluation of two variants of transport protocols, namely TCP and UDP.
- Performance Evaluation Across Varied IEEE 802.11 Parameters—the research delves into the performance evaluation of the covert channel, taking into account the variation in frame length as well as two crucial IEEE 802.11 mechanisms—RTS/CTS frames exchange, and MCS modulation index.
- Performance Evaluation Under Saturation Conditions—a critical analysis is conducted to evaluate the performance of the covert channel under saturation conditions, specifically focusing on the impact of external stations associated with the network.
- Analysis of Other Stations Offered Load—the performance studies include an analysis of the surrounding station's offered load on covert stations working under saturation conditions.
- Analysis of Covert Station Offered Load—the research includes an in-depth analysis of the covert station's offered load on the covert channel, particularly in the presence of traffic interference from external stations.

To our knowledge, this article is the first of its kind, introducing the application of an IEEE 802.11 covert channel to improve security within the SG network. What sets this contribution apart is its exploration of an innovative approach that is based on the randomness of the IEEE 802.11 backoff mechanism, thereby enabling a covert channel to remain undetectable. In the landscape of utilizing Wi-Fi technology in the SG, our research brings a novel perspective by introducing an additional security layer. We address a critical gap in existing security measures by implementing a covert channel within the IEEE 802.11 network. This not only enhances the SG's resistance to potential threats, but

also opens avenues for further exploration of covert communication mechanisms tailored to the specific challenges posed by SG networks.

The organization of this research paper is structured as follows: Section 2 provides an overview of related works, presenting covert channels for IEEE 802.11 networks applicable for similar purposes and briefly discussing existing mechanisms to improve data security in SG. We delve into the SG and its network architecture, forming the basis for the proposed covert channel implementation in Section 3. In Section 4, we provide a comprehensive overview of the fundamental aspects of IEEE 802.11. This is fundamental to understanding the various scenarios employed to establish the covert channel. Further, Section 5 introduces the covert channel concept, its operation, and the simulation environment. A comprehensive presentation of simulation results, incorporating different scenarios and parameters, is presented in Section 6. We briefly discuss the results in Section 7. The final conclusions and future research directions are presented in Section 8.

2. Related Studies

The implementation of the IEEE 802.11 standard offers numerous possibilities for the creation of covert channels. One effective approach is leveraging fields that permit the use of custom values. The study [18] introduces an innovative covert channel that exploits the MAC address randomization technique for concealing data transmissions within IEEE 802.11 networks. In this covert communication method, disposable random MAC addresses are employed, generated by the IEEE 802.11 station as an integral part of the probe request frame during the network scanning phase. An additional covert channel, centered around the IEEE 802.11 probe request frame, is introduced in [19]. This implementation leverages the probe request frame's role, particularly the supported rates and extended supported rate fields, which convey information about the data rates supported by both the Station (STA) and Access Point (AP) to ensure data rate compatibility. In this covert communication approach, secret data are encoded in the most significant bit (MSB) of the supported rates field during the transmission of probe request frames. Another technique for creating a covert channel involves encoding the secret message in the time difference between consecutive transmissions. The study [20] presents an IEEE 802.11 covert channel that utilizes the interarrival times of either the Beacon frames or the Probe Request frames to encode the message. The method involves changing the generation interval of the frames based on the bit combination that the sender intends to transmit. Another timing covert channel is introduced in [21], which consists of the manipulation of the Beacon interval. The communication is unidirectional from an Access Point (AP) to a station (STA). In this approach, the AP encodes the secret message by deliberately introducing a time delay in the beacon interval parameter.

A covert channel, as proposed in [22], is implemented within CTS and ACK frames, utilizing the protocol version field of the MAC header. The protocol version field, a 2-bit segment, is currently set to zero (binary 00). The covert channel exploits the three remaining combinations, namely 01, 10, 11, for transmitting concealed messages. The transmission process is divided into three distinct phases: Start Message Delimiter, in this phase, involves transmitting a sequence of five frames, each carrying the 01 combination. Secret Message Transmission: During this phase, the covert channel transmits the binary zero as 10 and the binary one as 11. End Message Delimiter: The final phase consists of transmitting another sequence of five frames, all containing the 01 combination.

The StegoFrameOrder method is proposed in [23]. The primary concept involves concealing data within the transmission order of stations. For the method to function correctly, the STAs must synchronize with each other by leveraging information provided in the beacon frame generated by the AP. The covert channels transmit information as follows:

- Transmitting bit 0-Station A initiates the transmission of the first frame immediately after the Beacon frame, preceding any transmission from Station B. During this period, Station B refrains from transmitting until Station A completes its frame transmission.

- Transmitting bit 1-Conversely, Station B initiates the transmission of the first frame after the Beacon frame, preceding any transmission from Station A. In this case, Station A follows a similar protocol, suspending transmissions until Station B completes its frame transmission.

A covert timing channel, denoted as Covert-DCF, is introduced in [24] and implemented in [25]. This method is founded on scenarios similar to the prisoner's problem [26], where a warden oversees communication attempts between a covert sender and a covert receiver. The objective is to establish communication without arousing the warden's suspicion. In the Covert-DCF scheme, the covert sender and receiver collaborate by pre-agreeing to share a codebook associating characters with specific backoff values. Suppose, for example, that the covert receiver aims to transmit the message "BAD". Before each transmission, the covert sender and receiver share a dictionary linking characters to respective backoff values. In this case, the covert sender employs backoff values of 0.3 ms, 0.1 ms, and 0.7 ms, respectively. This covert communication strategy allows the covert receiver to monitor the wireless channel and decode the hidden message by observing the backoff values used by the sender. Two covert channels based on dirty constellation are introduced in [27]. These covert channels involve covert senders strategically manipulating transmission parameters to introduce imperceptible variations in the received signal quality. The covert receiver, possessing knowledge of the encoding scheme, interprets these variations to reconstruct the hidden message. This method capitalizes on the inherent noise and fluctuations in wireless communication channels, offering a discreet means of transmitting information without raising suspicion.

In Table 1, we offer a comprehensive summary and concise overview of various existing covert channels. This compilation aims to provide a quick reference to the methodologies involved in the construction of a covert channel.

This study distinguishes itself from related works by creating a covert channel designed to address the data privacy needs of SG. Unlike existing IEEE 802.11 covert channels originally intended for different purposes, our channel is purposefully targeting the SG security concern.

Table 1. Related Studies Overview.

Ref.	Overview	Evaluation Method	802.11 Layer	Efficiency	Covertness	Year
[22]	The covert channel employs two bits within the PV field of an IEEE 802.11 CTS frame to convey hidden information. These PV bits serve multiple purposes in the covert channel, indicating the start and end of the transmission and carrying information one bit at a time.	Atheros AR5212 network adapter	MAC	Low	Low	2012
[25]	The covert sender initially converts symbols to back-off values. These values serve as back-offs during data transmission. The receiver initially monitors the wireless channel, filtering the back-offs from the covert sender to extract the hidden message.	Atheros AR5212 network adapter	MAC	Low	High	2013
[20]	The secret data is encoded within the interarrival times of either probe request frames or beacon frames.	Alpha network adapter	MAC	High	Medium	2017
[23]	The technique conceals bits of data in the sequential order of frames transmitted by wireless terminals sharing the same radio channel. For instance, Station A transmitting before Station B represents bit 0, while Station B transmitting before Station A represents bit 1.	Atheros AR9271 network adapter	MAC	Very low	High	2021
[27]	A dirty modulation method based on phase drift, creating covert channels through radio transmissions using N-ary PSK or QAM modulations. The proposed solution utilizes a random change in the dirty constellation parameters as the carrier for the secret message.	USRP-2920 hardware platform	PHY	N/A	High	2021
[19]	The secret message is hidden in the supported rate and extended supported rate fields and sent in the probe request frame.	NS-3	MAC	Medium	Medium	2023
[18]	The hidden information consists of a one-time-use random MAC address created by the IEEE 802.11 station during the network scanning process within the probe request frame.	NS-3	MAC	High	High	2023

3. Smart Grid

The Electric Grid (EG) [28] is a chain of components comprising distinct yet interdependent segments, each playing a crucial role in the generation, transmission, distribution, and consumption of electrical energy. It is an interconnected infrastructure consisting of various key components that collaboratively ensure the seamless flow of electrical energy from its generation to its consumption.

The conventional EG encounters various challenges, including unpredictable failures induced by natural elements (e.g., heavy rain, strong winds, or accidents), failures resulting from the aging of components with a limited lifespan, and the incorporation of renewable energy sources such as wind turbines and solar power. These challenges compel EG operators to implement intelligence into the EG, allowing for proactive responses to unforeseen circumstances and the ability to predict events before they occur. In response to this need, the concept of the SG has emerged, revolutionizing the way we manage and harness electrical energy. The SG leverages advanced technologies to sense small imbalances, enabling proactive adjustments to prevent the escalation of potential issues. Through the strategic deployment of sensors across various parts of the grid, the SG continuously measures and monitors the status of its components. This real-time monitoring allows for the prediction and prevention of faults, minimizing downtime and enhancing overall grid resilience.

One of the key features of the SG is its establishment of a networked infrastructure, where components seamlessly exchange information about the state of the grid. This interconnection enables faster and more intelligent decision-making processes, reducing the reliance on manual interventions that were prevalent in traditional grids. The integration of new technologies enhances the capabilities of the current grid, making it more secure, reliable, efficient, and self-sufficient.

The SG harnesses and integrates existing communication technologies to establish seamless bidirectional communication between its various segments [29] as presented in Figure 1. The first segment in this interconnected system is the Home Area Network (HAN) [30]. The HAN creates a network that connects home appliances throughout the household to the SM. This connectivity is achieved through diverse wireless network technologies, including Zigbee, as well as Wi-Fi or Ethernet, and Bluetooth. At the heart of the HAN is the smart meter, a standalone device designed to collect and aggregate power consumption data from individual home appliances. The smart meter acts as a pivotal point within the grid, serving as a bridge that facilitates the flow of information between the connected appliances and the broader SG infrastructure.

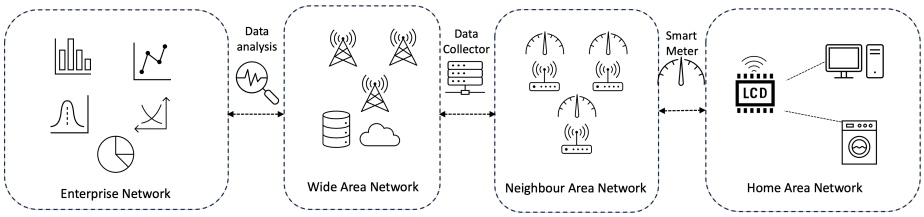


Figure 1. Smart Grid Overview.

The Neighbor Area Network (NAN) [31] represents an expansive interconnection of SMs distributed across a wide geographical area. Within this segment, the SG efficiently gathers substantial volumes of diverse data from various sources. Commonly utilized communication technologies for NAN include WiMAX and Wi-Fi, chosen for their long-range capabilities. The collected data are subsequently relayed to a broader network segment for more extensive processing and analysis.

Within the Wide Area Network (WAN) of the SG infrastructure, data streams seamlessly flow in from the HAN. Once in the WAN, the data are processed, which involves storage and analysis. This segment serves as the central hub for aggregating and assimilating data obtained from diverse points across the network. The primary objective of processing within the WAN is to refine the raw data into meaningful insights. These

insights can then be made available to energy providers in the Enterprise Network using a user-friendly format, often presented through intuitive charts and graphs. The data analysis yields valuable indicators that empower operators to make informed decisions and take proactive actions, ensuring the optimal functioning of the SG and addressing any anomalies or issues that may arise.

Security Threats

As consumer and data-related information traverse through a network of interconnected devices, it becomes imperative to exercise caution and diligence throughout the entire process. This is particularly critical due to the sensitivity of the data involved. A meticulous analysis of consumption data from the customer's end can unveil patterns that indicate peak or low energy usage, potentially revealing specific times of the day when a residence is occupied or unoccupied. Beyond merely sensitive data, information containing unique fingerprints can inadvertently pass through the network, allowing for the identification of customers and their associated devices, often recognized by MAC addresses. To prevent inadvertent data leakage, such data require meticulous treatment. Moreover, the integrity of measurement data is paramount, as tampering attempts may compromise the accuracy of readings. Additionally, potential threats from third parties may be directed at the communication links between home appliances and smart meters, or even the interconnections between different smart meters within the network. Vendor-related data, encompassing crucial details such as electricity costs and the number of customers, is also susceptible to exposure. Competitors may exploit such information. In the era of information technology, where every piece of data passing through a network holds value, comprehensive safeguards are essential to protect it from unauthorized access by third parties. Simultaneously, there is a parallel need to ensure that data remain readily available to operators whenever required.

To underscore the significance of the presented covert channel in enhancing the security of the SG, we highlight the existing threats and attacks the smart grid is susceptible to. The extended research conducted in [32] provides a comprehensive taxonomical classification of attacks within the SG framework. It systematically delineates the various components, vulnerabilities, and corresponding countermeasures, revealing a total of 33 distinct vulnerabilities across SG components. The identified attacks strategically target the availability, integrity, confidentiality, authenticity, and accountability of elements within the SG ecosystem. In a closer analysis of the SM, specific attacks were discerned, including Spoofing, Sniffing, Message Replay, and Impersonation.

The study covered in [33] conducts a thorough survey of the threat landscape concerning SG systems, emphasizing three primary target domains: confidentiality, integrity, and availability. Integrity attacks, prevalent in wireless networks, include eavesdropping on the channel, man-in-the-middle attacks [34], and spoofing attacks [35]. Instances of attacks on integrity involve the injection of false data, where adversaries insert altered data packets to provide misleading information to the energy provider [36]. Another identified attack involves the modification of time in the node to present inaccurate information regarding the time of measurement and location [37]. Regarding attacks on availability, a denial-of-service approach is employed, aiming to exhaust the resources of the host, thereby disrupting its normal functionality in receiving, sending, or processing data across different layers of the OSI model.

The paper [38] analyzes the communication security for SG and points to the deficiency in robust security measures for the Advanced Metering Infrastructure (AMI), which constitutes a distributed network of measuring devices tasked with collecting and processing the energy consumption data from the HAN. The study, particularly in the context of authentication, identifies various threats to these devices. Key concerns are the rogue access point problem, reply attacks, as well as message modification and injection. In response to these identified threats, the authors advocate for the establishment of a secure SG

framework. Their proposed framework places a specific emphasis on device authentication and data confidentiality.

Another article dedicated to the analysis of SG attacks is the [39]. The article delves into the analysis of SG attacks, providing a comprehensive overview of the attack types, their effects, and specific segments of the network impacted. Similar to other studies, it emphasizes the vulnerability of SM meters, attributing their susceptibility to attacks to the characteristics of the connection technology employed in both HAN and NAN.

The presented set of researches has exposed the vulnerabilities inherent to the use of the IEEE 802.11 network in the SG infrastructure. To address these critical issues, our research proposes the development of a covert channel as a strategic solution. This covert channel serves a dual purpose: first, as an authentication mechanism, ensuring the secure identification of involved parties during Wi-Fi communication. Second, it functions as a secure means for the transfer of sensitive data, concealing transmissions within the shared medium. By adding this new layer of privacy through a covert channel, we aim to enhance the overall security of communication within segments where IEEE 802.11 networks are deployed, thereby fortifying data integrity and improving the confidentiality of smart grid communications.

4. IEEE 802.11 Standard

As demonstrated the IEEE 802.11 network is one of the primary communication technologies in the SM, serving essential roles in HAN and NAN. In the HAN, Wi-Fi enables seamless communication among smart appliances and meters within homes. Meanwhile, in NAN, it facilitates communication between neighboring smart meters, creating a network that enhances grid efficiency. Wi-Fi is cost-effective to deploy and adaptable to the evolving needs of the grid. Its scalability allows for easy expansion, making it a practical choice for smart grid implementations, and promotes seamless communication between smart meters, sensors, and other components. Wi-Fi supports high data rates, and this capability is crucial for transmitting substantial data volumes generated by smart meters and appliances, enabling real-time monitoring and control. This section offers a concise overview of essential topics, laying the groundwork for a comprehensive understanding of the covert channel concept. These discussions will highlight key parameters directly influencing the performance of the covert channel.

The IEEE 802.11 standards require the Distributed Coordination Function (DCF) to enable asynchronous channel access for devices sharing the transmission medium. In DCF, a station that wants to send a frame must first sense the channel. If the channel is busy due to ongoing transmission by another station, the sender waits until the end of the current transmission plus a specific time known as DCF Inter Frame Space (DIFS). After DIFS, the station selects a random integer backoff slot from 0 to a value of CW (Contention Window), calculated according to Formula (1), where the values of x are specific to the IEEE 802.11 amendment [40]. Initially, every station sets CW to CW_{min}, but upon collision, it doubles until it reaches CW_{max}. However, after every successful transmission attempt, the CW is reset to CW_{min}. After drawing the backoff, the station starts the countdown until it reaches zero. At this point, the station has won the contention to access the channel. During this time, other stations suspend their backoff countdown. The time interval between frames belonging to the same transmission (such as Data and ACK frames) is called Short Inter Frame Space (SIFS). After a transmission plus a DIFS period ends, the stations whose backoff has not reached zero resume their backoff countdown. The station that wins the contention for access to the channel gets a new backoff slot. The Figure 2 summarizes the IEEE 802.11 backoff procedure.

$$CW = 2^x - 1 \tag{1}$$

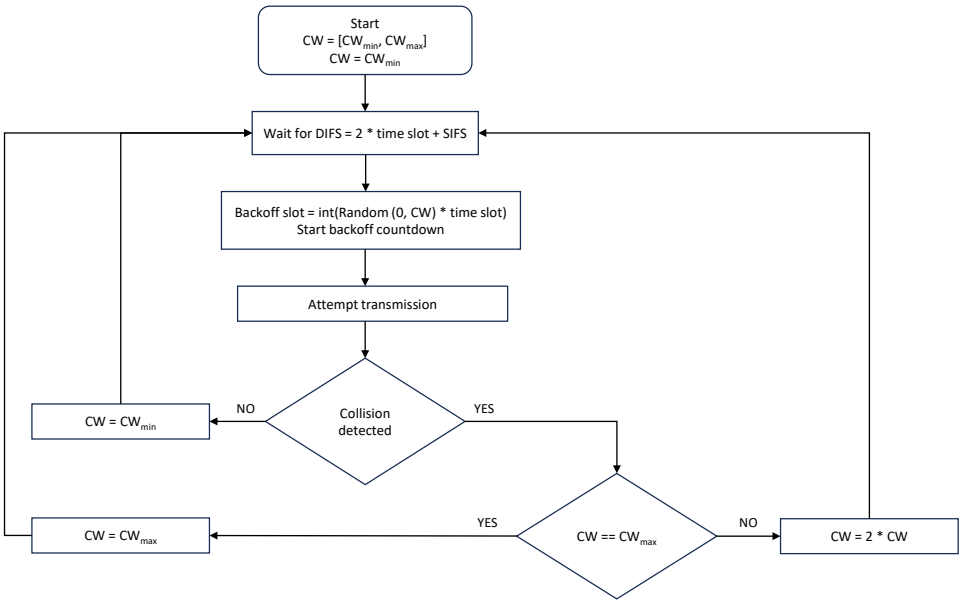


Figure 2. IEEE 802.11 DCF with random backoff procedure.

The DCF still encounters two challenges when employing the random backoff procedure, namely, the exposed node and hidden node problem. The exposed node problem occurs when a node refrains from transmitting data, thinking the channel is busy leading to the underutilization of the channel. The hidden node problem occurs when two nodes within the same range wireless network are communicating with a common access point but are unable to detect each other's presence. In both cases, these problems can lead to inefficiencies in the utilization of the wireless channel, potentially causing collisions, increased latency, and decreased overall network performance. The Request-to-Send (RTS) and Clear-to-Send (CTS) frames are employed to address these issues in the IEEE 802.11 standard. With the RTS/CTS mechanism when a device intends to transmit data, it sends an RTS frame to the intended receiver, requesting permission to send. The receiver responds with a CTS frame, granting permission and notifying other devices to defer their transmissions. The mechanism prevents a station from refraining from its transmission under the mistaken assumption that the channel is busy. It also prevents the station from sending a frame under the assumption that the intended recipient is available to receive it.

The IEEE 802.11 network standard defines the Modulation and Coding Scheme (MCS) index, which represents a set of parameters. These parameters determine the efficiency of data transfer within the available bandwidth. They include modulation and coding rate, channel size, spatial streams, and guard interval. Modulation and coding rate affect data transfer efficiency, channel size represents network capacity, spatial streams indicate the number of physically separated channels, and the guard interval is a brief period between packet transmissions. This index serves as a comprehensive grouping mechanism, offering insights into achievable throughput.

5. Proposal for a Covert Channel in a Smart Grid Network

The backoff procedure allows stations to determine the time slots that have elapsed before a transmission can start, using the DIFS and the remaining backoff time. By exploiting this property, a covert channel can be created by encoding a secret message in the parity of the backoff slot. The bit 0 corresponds to an even backoff slot, while an odd backoff slot transmits a bit 1. This covert channel has a bandwidth of one bit per frame, and any node on the channel can be the recipient, whether it is another station or an AP. The pseudocode to implement the covert sender is illustrated in Algorithm 1. Following the determination of the backoff slot to defer transmission, the sender intentionally introduces a delay in its transmission based on the covert bit to be transmitted. The corresponding pseudocode

for the receiver can be found in Algorithm 2 as well. The receiver actively monitors the channel, measuring the time elapsed from DIFS to the moment the packet is sent across the network. Subsequently, subtracting the DIFS from this elapsed time, the receiver identifies the backoff slots the sender waited for before transmitting the data.

Algorithm 1: Pseudocode for the sender procedure.

```
while network card is running do
    for i ← 0 to N − 1 do
        covert_bit ← message[i];
        backoff ← Random(0, CW);
        if covert_bit = 0 then
            if backoff is odd then
                backoff ← backoff + 1;
            end
        end
        else
            if backoff is even then
                backoff ← backoff + 1;
            end
        end
    end
end
```

Algorithm 2: Pseudocode for the receiver procedure.

```
while network card is running do
    DIFS ← SIFS + 2 × time_slot;
    slots_elapsed ← (time_elapsed_since_difs − DIFS)/time_slot;
    for i ← 0 to N − 1 do
        if slots_elapsed is even then
            decoded_bit ← 0;
        else
            decoded_bit ← 1;
        end
    end
end
```

In the preliminary considerations, the identification of the sender relies on its MAC address, a unique physical address associated with the hardware, and a shared secret between the sender and the receiver. The covert channel is designed to serve as a communication means for SMs and between SMs and the data collector. This mechanism assures the sender's identity to the data receiver, as the secret is known exclusively to both parties. Moreover, the covert channel ensures data integrity. Another noteworthy application of the covert channel is in maintaining data privacy and confidentiality. The channel facilitates the exchange of secret messages which remain unpredictable to third parties, due to the inherently random nature of the backoff mechanism, making it an ideal vehicle for concealing sensitive information.

The covert channel is notable for its transparency and resilience against steganalysis. In terms of transparency, the implementation of the channel exhibits no functional interference with the regular operations of the standard channel. This characteristic became evident during the simulation, as reflected in the results presented in the following sections. While collecting data on the covert channel, we observed consistent performance metrics (throughput, delay, efficiency, etc.) comparable to scenarios without the covert channel.

Its operations remain imperceptible, and no disruptions in transmission were observed. The resistance to steganalysis is a critical aspect that indicates the covert channel's ability to withstand scrutiny and detection techniques. This parameter not only defines the channel's efficiency but also its robustness against attempts at exposure. Anomalies in behavior, such as modifications to a reserved field or frequent adjustments in periodic parameters (e.g., beacon or probe request intervals), tend to arouse suspicion among network observers, potentially revealing the existence of a covert channel. The presented covert channel demonstrates strong resilience to steganalysis, primarily due to the inherently random nature of the backoff mechanism. To external observers or networks undergoing scrutiny, each backoff event following transmission is perceived as an integral part of the DCF.

The covert channel finds application in the SG network when one SM needs to communicate with another SM, or when the grid operator aims to enhance authentication methods. In scenarios where SMs need to establish communication, they can use a pre-shared data sequence as a secret, and before the communication, deploy the covert channel to allow both entities to exchange that secret as an authentication method. This prevents attacks where a third party attempts to impersonate a legitimate SM through tactics such as packet reply attacks, MAC address spoofing, or rogue Access Points. The covert channel ensures that communication stays confidential, restricting it to authorized parties and providing assurance about the legitimacy of the communicating peers. Another use of the covert channel is in transmitting sensitive data in untrusted environments. When an SM wants to transfer a secret message, the covert channel allows it to do so without being perceived or detected by observers or third-party attackers. This ensures a secure transmission of information in situations where privacy and confidentiality are paramount.

To illustrate how this covert channel operates in practice, please consider Figure 3, where a covert sender has a queue of secret messages consisting of two bits, with the first being 1 and the second being 0. After DIFS, the covert sender draws a random backoff of 5 slots and begins the countdown. Meanwhile, another regular station also has a frame to transmit and compete for access to the channel. It draws a lower backoff of 3 slots and wins the contention, causing the covert station to suspend its backoff countdown timer and wait until the regular station's transmission is complete. After the regular station's transmission and another DIFS interval, the covert station resumes its backoff countdown with only two slots remaining. When the backoff countdown reaches zero, the covert station waits for one more slot, making the total number of slots after DIFS an odd number since it intends to send bit 1. When the first secret data transmission finishes, the covert station draws a new backoff of four when the regular station is still counting down from the backoff of 10. After DIFS, the covert sender wins the contention as it had a lower backoff value than the regular station and sends the frame without delay since the total number of slots passed after DIFS is even, and it intends to send a bit 0.

The entire backoff procedure is perceived as random, including the insertion of an additional slot when needed, seamlessly blending with the randomly drawn backoff values by the stations. As illustrated in Figure 3, the covert channel exhibits flexibility, as the receiver is not constrained to a specific type (AP or station). In a shared medium, each station that participates in sharing the transmission medium can decode the secret message if it is aware of it. By monitoring channel activities, this covert channel adapts well to the diverse roles played by devices in Wi-Fi networks, where devices serve in various capacities such as repeaters, access points, stations, and more.

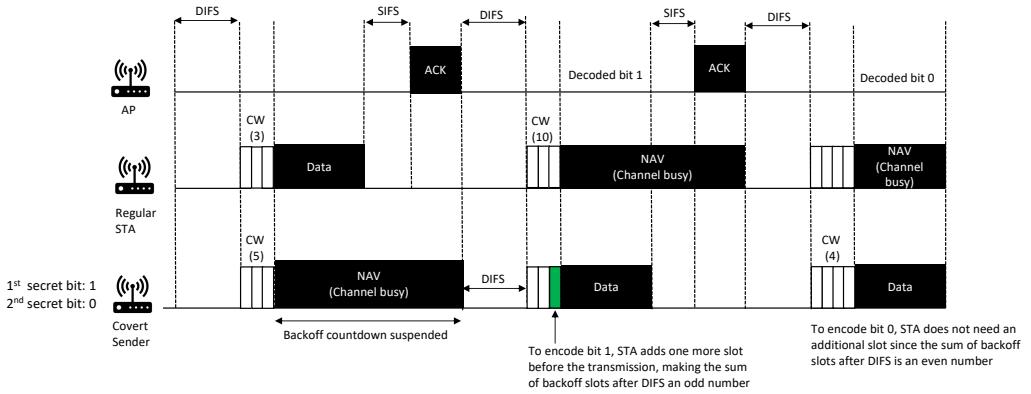


Figure 3. Covert Channel Operation.

Simulation Environment

The covert channel was implemented using the ns-3 network simulator [41], a robust discrete-event network simulator widely employed for modeling and simulating diverse network types. This open-source simulator, developed in C++ and Python, supports numerous features, including comprehensive support for simulating IEEE 802.11 networks. NS-3 (version 3.40) was the optimal choice due to its compatibility with the latest IEEE 802.11ax standard, its active and supportive community, and its maturation over the years. It offers flexibility during simulation, abstracting the complexities of IEEE 802.11 networks in a simulated environment. Table 2 outlines the key parameters configured for the simulations. The MAC PDU size employed is 1472 bytes, and unless explicitly stated otherwise, this payload size is consistently utilized across various scenarios. It is noteworthy that, in all figures, the error for each simulation point within the 95% confidence interval did not exceed ±2%.

Table 2. Simulation Parameters.

Parameter	Value
IEEE specification	802.11ax
Transport protocol	UDP and TCP
MAC PDU Size	1472 [bytes]
Frequency	5 [GHz]
Channel width	40 [MHz]
Guard Interval	800 [µs]
Time slot	9 [µs]
SIFS	16 [µs]
DIFS	34 [µs]
Time slot	9 [µs]
MCS index	11
Mobility model	Constant
RTS/CTS	Enabled and Disabled
Propagation and Loss Model	Log-Distance Path Loss Model
Number of Tx and Rx antennas	1

The simulator offers a ready-to-use API while also allowing developers to extend or tailor it for specific purposes. In our approach, we combined existing functionalities with our implementations to craft the covert channel. The implementation was as follows: In the `txop.h` file, we introduced the variable `latestBackoff` to store the updated backoff when the station needs to pause the countdown for later resumption. Within `txop.cc`, specifically in `Txop::UpdateBackoffSlotsNow()`, we handle the update of the backoff. The covert channel is embedded within the `channel-access-manager.cc` file, specifically in the method `ChannelAccessManager::DoGrantDcfAccess()`. Once the station is granted channel access, we first check the covert bit and then examine the parity of `latestBackoff`

variable to determine whether to wait for an additional slot or not. The slot value in the simulator is obtained through the `GetSlot()` method of the `class ChannelAccessManager`.

The network topology is exhibited in Figure 4, the simulation environment provides the capability to model nodes that emulate various home appliances. The network topology employed is a Basic Service Set (BSS), characterized by a central Access Point (AP) through which all communications traverse. In this configuration, the covert station is embodied by Smart Meter 1, serving as a representative node within a network of smart meters, all equipped with IEEE 802.11 cards. This network is dynamic, enabling the addition or removal of nodes, while also incorporating static nodes strategically positioned within a specified range from the AP. This scenario provides a level of control over the covert station independent of the other nodes, allowing for a focused examination of its behavior. Additionally, the regular stations are managed in a set, allowing to make changes on them collectively.

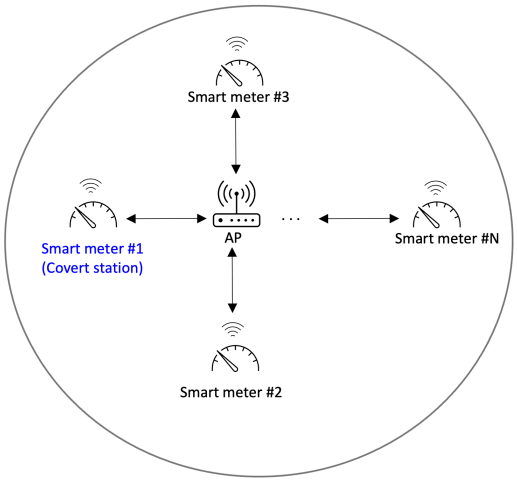


Figure 4. Network topology.

6. Performance Assessment

6.1. Non-Competitive Channel Access

The first scenario examined comprises solely the covert Station (STA) and the Access Point (AP), without the presence of any other STAs. Within this context, the covert STA generates UDP traffic, and the investigation involves incrementing the offered load while keeping a consistent frame size. This process is iterated with varying frame sizes to evaluate how the covert channel's throughput is affected as the offered load increases.

Simulated results of the isolated scenario are depicted in Figure 5. The findings indicate a direct correlation between payload size and covert channel throughput. Notably, smaller payload sizes yield higher covert throughput values, whereas larger payload sizes yield lower throughput values. This phenomenon arises because a smaller payload occupies the channel for a shorter duration, affording the covert stations more transmission opportunities within the overall transmission time.

Moreover, our observations reveal that payload size influences the network saturation threshold. Specifically, the network attains saturation with less offered load for small payload sizes, whereas larger payload sizes necessitate more load to achieve saturation. This observation is attributable to the fact that, as payloads become more substantial, a greater volume of traffic must be generated to reach or surpass the saturation threshold.

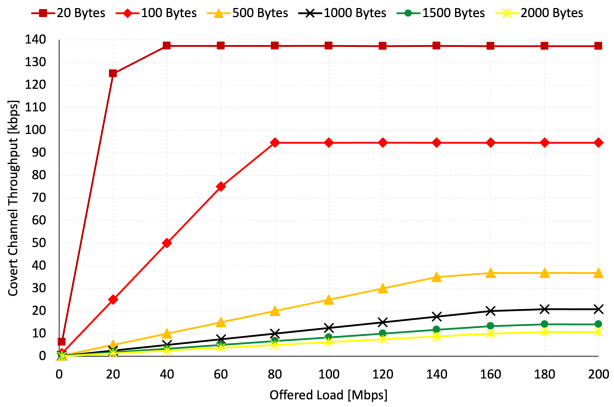


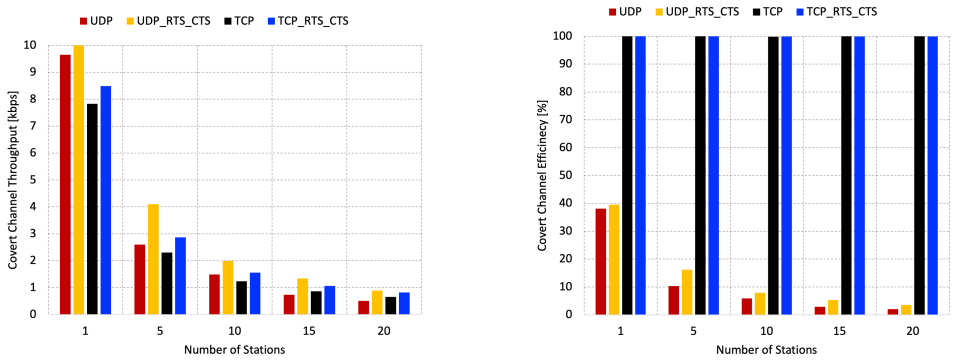
Figure 5. Covert channel throughput vs. offered load for different payload sizes and 1 STA.

6.2. Increasing Station Density

In this experiment, our objective was to observe the dynamic behavior of covert channel parameters in response to an increasing number of stations joining the network. Each station represents either adjacent SMs or Wi-Fi-enabled home appliances associated with the same Access Point AP. The experimental setup began with a single regular station, followed by increments of five stations until reaching a total of 20 stations generating traffic at their maximum capacity. Additionally, we conducted experiments using two distinct variants of the transport protocol, namely UDP and TCP traffic. This allowed us to explore how these protocols, in conjunction with the growing number of stations causing interference, impact the performance of the covert channel.

The main parameters under observation include *covert channel throughput*, defined as the number of secret bits transferred over the channel during the simulation period; *covert channel delay*, representing the time taken for data to traverse the network and reach its destination; and *covert channel efficiency*, expressed as the ratio of received to sent data, presented as a percentage. These metrics collectively provide insights into the performance of the covert channel under varying network protocols and traffic interference. In addition, we introduced the RTS/CTS mechanism into our experiment. This allowed us to assess the impact of its usage on the covert channel. The RTS/CTS mechanism introduces overhead into the communication process, and we aimed to investigate how its implementation influences the covert channel's performance. Specifically, we sought to understand whether the overhead introduced by RTS/CTS could potentially mitigate or enhance the covert channel by reducing the probability of collisions, especially in scenarios involving both UDP and TCP traffic protocols. This aspect of the experiment provides valuable insights into the trade-offs associated with employing the RTS/CTS mechanism in the context of covert channel communication.

Figure 6a presents the variations in covert channel throughput, revealing distinct performance characteristics between UDP and TCP traffic. The superiority of UDP is evident due to its best-effort nature, which lacks the reliability mechanisms inherent in TCP, such as congestion control, acknowledgment, and retransmission. TCP's overhead, stemming from these reliability features, consumes a portion of available bandwidth for data traffic. As the number of stations increases, introducing interference, TCP's regulated nature contributes to a decline in throughput, as collisions and competition for the transmission medium become more evident. The introduction of more stations to the network increases the interference with the covert channel, increasing collision probabilities. However, the implementation of the RTS/CTS mechanism brings a noteworthy improvement in throughput, even within densely populated environments. RTS/CTS effectively mitigates collision probabilities, enhancing the chances of successful frame delivery. It is crucial to emphasize that achieving a throughput of 800 bps, even in scenarios with 20 regular stations, is a commendable outcome. In covert communications, where undetectability takes precedence over throughput, reaching such values in a dense network is a significant achievement.

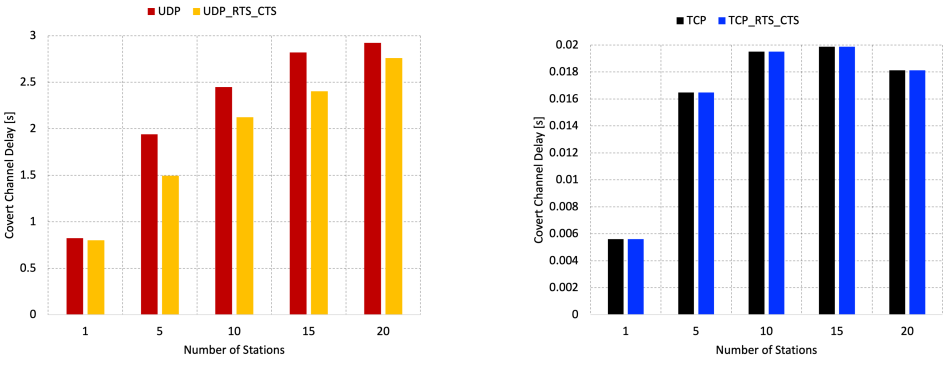


(**a**) (**b**)

Figure 6. Covert channel throughput and efficiency analysis. (**a**) Throughput; (**b**) Efficiency.

In Figure 6b, we present the covert channel efficiency to analyze the volume of frames generated and the channel's response to a large number of frames. We observed an intriguing result: high throughput does not necessarily translate into higher frame efficiency. In the simulation using TCP, we noted a high send-to-receive frame ratio, in contrast to what was observed over UDP. This observation can be explained based on the characteristics of both protocols. When using TCP, the congestion control mechanism assists both sides of communication in regulating the transmission rate, impacting the number of frames sent based on network conditions. The receiver signals the amount of data it can handle, and reliability ensures that each sent frame is acknowledged. Conversely, with UDP and no congestion control mechanism, the sender generates a substantial amount of data and sends it over the channel, overwhelming the receiver. As a result, significant packet loss occurs. From the results, we observe that UDP generates a higher amount of traffic compared to TCP. Choosing the protocol depends on the priority during transmission: prioritizing high reliability or maximizing data rate.

Analyzing the covert channel delay in Figure 7a,b, we initially observed a significant difference in delay between TCP and UDP. This disparity is attributed to the reliable nature of TCP, where the transmission queue is regulated to prevent the sender from overwhelming the network with excessive data in response to feedback from the receiver. As the queue decreases, the delay decreases, as evidenced by the lower number of packets sent over TCP compared to UDP. Examining the delay over UDP, we note that the absence of a congestion control mechanism allows the sender to queue excessive data for transmission over the channel, regardless of the receiver's ability to handle it. The larger the queue, the longer the delay, as reflected in the high number of frames generated while using UDP. Secondly, we also observe that while RTS and CTS have no impact on the delay using TCP, they help to reduce the delay significantly over UDP, as observed in the presence of 5, 10, and 15 stations.



(**a**) (**b**)

Figure 7. Covert channel delay analysis in relation to the number of stations. (**a**) UDP Traffic; (**b**) TCP Traffic.

6.3. Modifying the MCS Index

In this experimental scenario, we manipulated the MCS index of the covert station while maintaining a constant presence of 20 regular stations generating traffic in saturation. This was realized as a change in the distance of stations in relation to the location of the access point. In our research studies we assumed the log-distance propagation loss model. It predicts the path loss of a signal as it traverses through a building or densely populated areas over distance. The objective of this experiment is to observe the variation in covert channel throughput and delay in response to changes in the MCS index, aiming to understand the impact of stations location that influence noise and interference level on the covert channel performance.

Regarding throughput, as illustrated in Figure 8, the observed results align with expectations: a higher MCS index correlates with increased throughput. Notably, with MCS index 0, there is no discernible difference in throughput for both protocols, and variations become apparent starting from MCS 1 and onwards, with MCS 11 exhibiting the highest throughput value. During the MCS index changes, the TCP protocol outperforms UDP. It is essential to note that the MCS index represents a combination of parameters that collectively determine the data transfer capacity over the channel. In this case, when combined with the reliability and high efficiency provided by the use of TCP, a significant increase in throughput is observed.

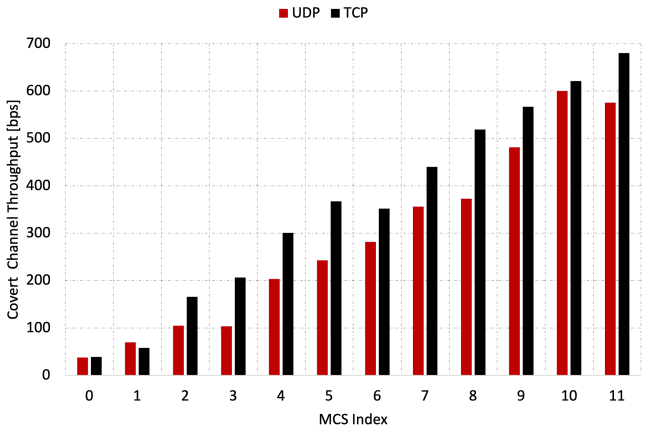
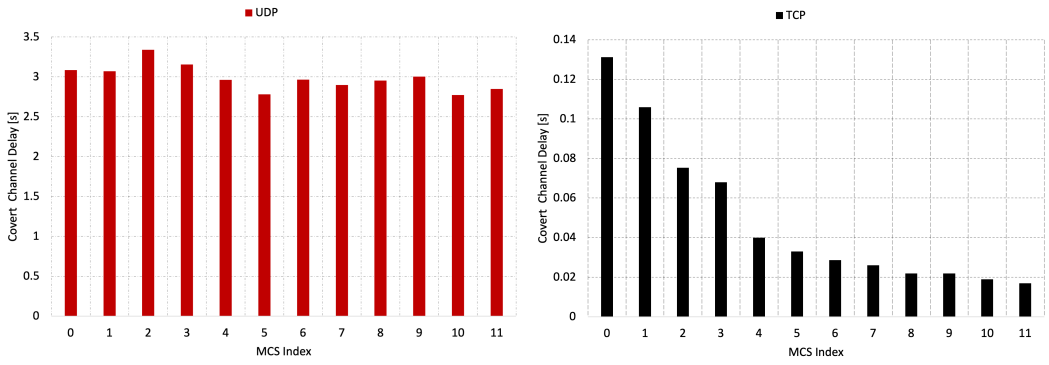


Figure 8. Throughput of the covert channel in relation to the MCS Index.

The MCS index change also causes a change in the delay pattern. As observed in Figure 9a,b, with UDP the covert station saturates the channel in a way that changing the MCS index causes a small variation in the delay around the value of 3 s while using TCP we can observe that changing the MCS index has the opposite effect on the delay, as the MCS increases the delay decreases, because the channel is able available bandwidth expands, more symbols can be sent which translates into more data over a short interval of time.



(**a**) (**b**)

Figure 9. Delay of the covert channel in relation to the MCS Index. (**a**) UDP Traffic; (**b**) TCP Traffic.

6.4. Increasing the Stations Offered Load

In this scenario, we incrementally raise the network's density. The covert STA maintains a consistent frame size of 1024 bytes while delivering a load of 200 Mbps. The objective of the experiment is to examine the impact of augmented traffic generated by additional stations on the covert channel's performance. This evaluation encompasses aspects such as throughput, delay, jitter, and frame efficiency—the latter being defined as the percentage ratio of received frames to sent frames.

The simulation results in Figure 10 show the impact of adding 1, 5, 10, 15, and 20 more stations to the network. It is noted that when external traffic is low, at 1 Mbps, the covert channel remains unaffected, consistently achieving approximately 19 kbps throughput across all five experiments. This can be attributed to the fact that the covert station generates much higher traffic (200 Mbps) than 1 Mbps and, thus, does not face significant interference. However, with a rise in the offered load, the influence of external traffic becomes evident, leading to a decline in covert throughput. This decrease can be ascribed to heightened contention for channel access, resulting from the increased data transmission from external stations. Furthermore, the observation reveals that following the addition of 15 stations, the throughput values become closely aligned. This suggests that beyond this point, incorporating more stations will exert minimal impact on the already diminished network throughput.

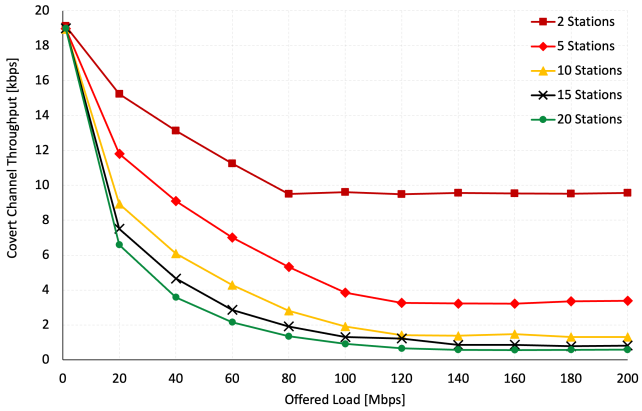


Figure 10. Covert channel throughput vs. regular stations offered load.

Figure 11 depicts how external stations impact the delay of the covert channel. The findings indicate that the delay rises in correlation with the offered load from the regular stations. As the offered load increases, the delay expands due to congestion. Elevated traffic levels lead to more collisions, and the receiving queue at the Access Point (AP) grows, inducing processing delays. Consequently, the delay encountered by the covert channel is directly proportional to the magnitude of the offered load. In the worst-case scenario, with 20 stations generating 200 Mbps of traffic, the covert channel delay remains below 3.5 ms, which is considered an excellent outcome.

As shown in Figure 12, a correlation between the offered load and frame jitter is similar to the relationship with delay. Initially, even with varying numbers of stations in the network, a minimal jitter (around 0.1 ms) is observed, indicating that low traffic has an insignificant impact on the covert channel. Even with a significant traffic load of 60 Mbps, the jitter remains below 1 ms, which is considered acceptable. Only in the scenario with 20 stations and from 160 Mbps of traffic does the jitter exceed the threshold of 2 ms. These findings indicate that the covert channel sustains acceptable jitter levels across various scenarios.

The efficiency of the covert channel is highly dependent on the offered load, as demonstrated by the results presented in Figure 13. This figure illustrates the percentage of frames successfully delivered to the Access Point (AP) and the corresponding percentage of losses based on the number of stations. The covert channel's efficiency demonstrates an inverse

relationship with the offered load, as observed. At a low offered load of 1 Mbps, over 80% of frames are successfully delivered. However, as the traffic volume escalates, there is a substantial decline in efficiency. For instance, in scenarios involving 10, 15, and 20 stations, the efficiency dips below 40% when the offered load reaches 20 Mbps. With the increase in offered load, the occurrence of frame collisions becomes more pronounced. This decrease in efficiency is mainly due to the increase in frame collisions, which is intensified by the number of stations.

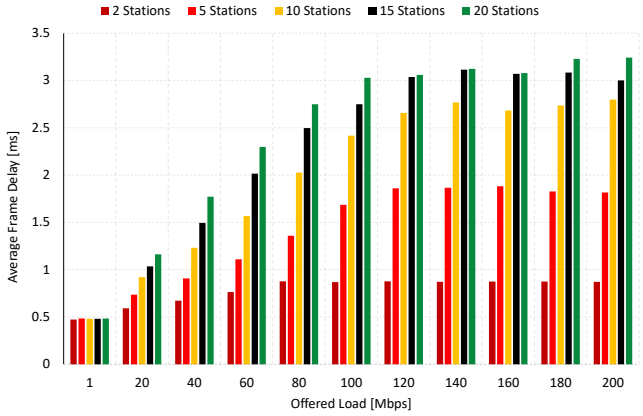


Figure 11. Covert channel delay vs. regular stations offered load.

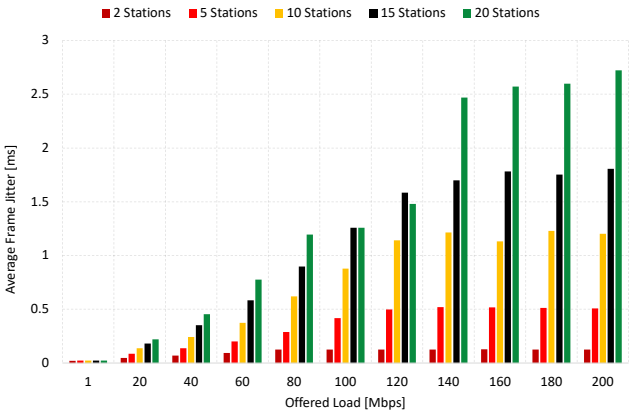


Figure 12. Covert channel average jitter vs. regular stations offered load.

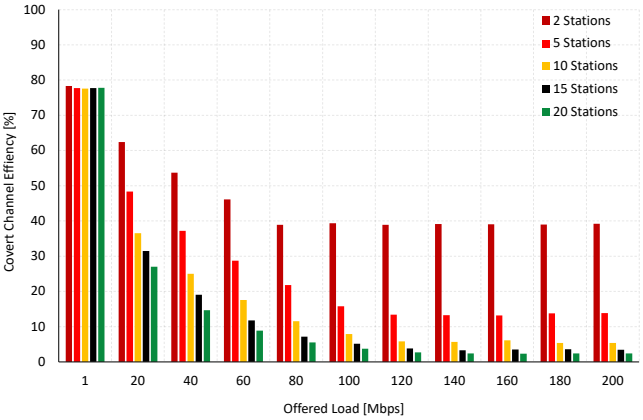


Figure 13. Covert channel efficiency vs. regular stations offered load.

6.5. Increasing the Covert Sender Offered Load

This experiment is designed to analyze the behavior of the covert channel under varying throughput conditions of the covert sender. The throughput is incrementally increased,

starting from 1 Mbps and gradually reaching 200 Mbps, representing the saturation point of the network. The experiment maintains a constant number of regular stations, specifically 20, consistently generating traffic at maximum capacity, while the covert station competes for channel access. The primary objective is to assess the covert channel's response and determine optimal offered load values that can be adapted or adjusted based on network conditions. Our focus is on observing alterations in covert channel throughput, and delay considering both transport protocols employed in the simulation.

In the context of a predetermined number of stations with varying offered loads, the covert channel throughput is depicted in Figure 14 for UDP and Figure 15 for TCP. Initially, in a scenario where the covert channel competes solely against a single station, the covert channel using UDP exhibits a slower approach to saturation. However, as the offered load is increased, a significant drop in throughput is observed in the presence of 5 stations. This behavior persists as more stations join the network. From a station count of 5, it becomes apparent that a 20 Mbps offered load is sufficient for the network to reach saturation.

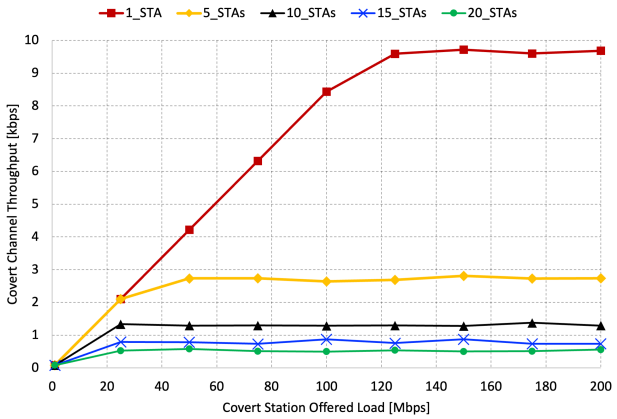


Figure 14. Throughput of the covert channel for UDP Traffic.

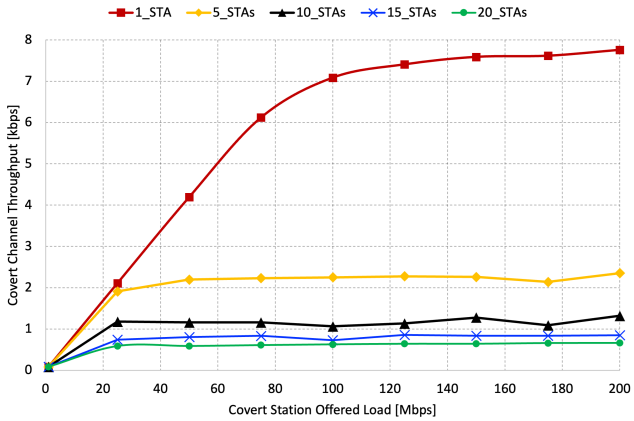


Figure 15. Throughput of the covert channel for TCP Traffic.

For both UDP and TCP scenarios, the network's behavior is consistent and repeatable. As more stations join, leading to an increased probability of collisions, the network attains saturation more rapidly, resulting in a drop in throughput. Nevertheless, even when confronted with a substantial volume of traffic (e.g., 20 stations and 200 Mbps), the covert channel consistently delivers above 500 bps per second. This achievement is considered satisfactory for a covert channel. Notably, in this case, UDP outperforms TCP to a slight extent.

In the context of delay analysis within this scenario, Figure 16 illustrates the delay for UDP, while Figure 17 presents the delay for TCP. Interestingly, we observed that the

delay patterns for both protocols are quite similar. For UDP traffic, initially, with a low amount of data, the delay for both UDP and TCP is negligible (the values for UDP are so small that they are virtually imperceptible on the scale, especially when compared to the ones from 25 Mbps). As the load increases, indicating more packets in the queue and an escalating collision probability due to the competition for channel access, the delay starts to rise. However, it stabilizes, indicating the point at which the covert channel network reaches its saturation.

Furthermore, concerning the delay, we continue to observe longer delays with UDP and shorter delays with TCP. This discrepancy is attributable to the inherent features of TCP, such as reliability and a congestion control mechanism, which contribute to a more efficient and controlled transmission process.

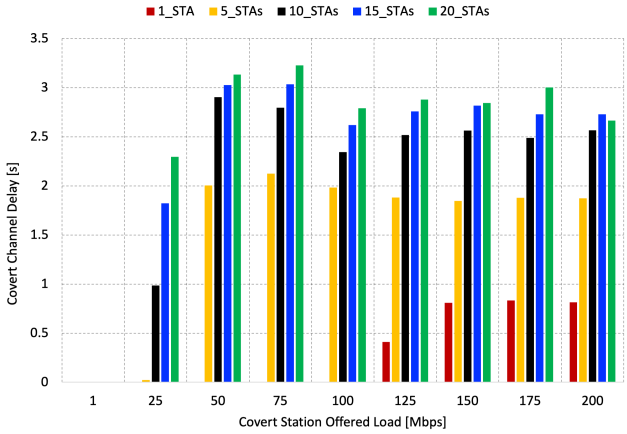


Figure 16. Delay of the covert channel for UDP Traffic.

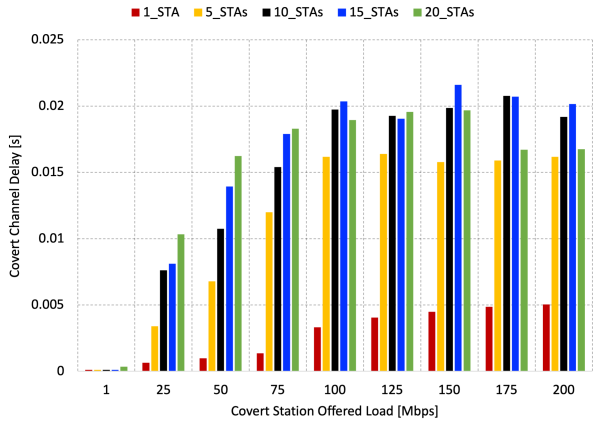


Figure 17. Delay of the covert channel for TCP Traffic.

7. Discussion

In the previous section, we delve into the examination of the parameters affecting the proposed covert channel. To offer a comprehensive overview for quantifying the obtained results, we present the outcomes achieved in a denser environment involving 20 stations during the simulation. We consider this quantity of stations to be reasonable for a typical home network, given the prevalence of connected devices to Wi-Fi in contemporary networks.

In Table 3, in a dynamic scenario with a gradual increase in the number of stations, TCP traffic outperforms UDP in terms of throughput, efficiency, and delay when RTS/CTS is not employed. However, when RTS/CTS is enabled, UDP traffic surpasses TCP throughput, taking into account the additional overhead introduced by RTS/CTS to a reliable protocol like TCP. In Table 4, the UDP traffic exhibits moderate throughput, efficiency, and delay,

while The TCP traffic shows higher throughput and efficiency compared to UDP. The nearly 100% performance indicates that TCP is utilizing the channel efficiently with minimal delay. Similar to the Table 4, for the highest offered load of 200 Mbps, as presented in Table 5, the TCP outperforms UDP in terms of throughput and efficiency even with the increased offered loaded up to 200 Mbps.

Table 3. Summary of the second scenario—Increasing Station Density.

Num. of STAs	Protocol	RTS/CTS	Throughput [kbps]	Frame Efficiency [%]	Delay [s]
20 STAs	UDP	disabled	0.51	2.01	2.92
20 STAs	TCP	disabled	0.65	99.95	0.018
20 STAs	UDP	enabled	0.88	3.5	2.76
20 STAs	TCP	enabled	0.82	99.92	0.010

Table 4. Summary of the third scenario—MCS Index 11 (The index with the highest performance).

Num. of STAs	Protocol	RTS/CTS	Throughput [kbps]	Frame Efficiency [%]	Delay [ms]
20 STAs	UDP	disabled	0.575	2.27	2.84
20 STAs	TCP	disabled	0.68	99.93	0.016

Table 5. Summary of the fifth scenario—Increasing the covert sender offered load up to 200 Mbps (The offered load with the highest performance).

Num. of STAs	Protocol	RTS/CTS	Throughput [kbps]	Frame Efficiency [%]	Delay [ms]
20 STAs	UDP	disabled	0.561	3.32	2.66
20 STAs	TCP	disabled	0.660	99.98	0.016

After examining the simulation results and relating them to real-world applications in smart grids, it is evident that while UDP traffic exhibits lower efficiency, both protocols demonstrate commendable throughput. The selection between UDP and TCP should be contingent on factors such as the nature of the traffic and the desired throughput. Notably, in our simulations, the offered load values from regular and covert stations may be conservative compared to real-world scenarios, suggesting significant potential for the covert channel to achieve even higher values than those observed in this study. Hence, the covert channel offers sufficient throughput to serve as an authentication mechanism, ensuring timely authentication, or as a reliable means for the transfer of confidential data.

In Table 6 , we present a comprehensive comparison with previously developed covert channels, emphasizing the innovative and adaptable nature of our covert channel, particularly tailored for smart grids and beyond. Its deployment can seamlessly integrate into various communication systems based on Wi-Fi, addressing concerns related to authentication and security. In terms of performance, our covert channel introduces a dynamic aspect, offering variable performance and adaptability. Unlike constant throughput implementations, our covert channel can be adapted to diverse environmental conditions and desired data rates (i.e., by adjusting the frame size, MCS index, or enabling RTS/CTS). Our proposed covert channel can be implemented in either a simulator or a network card using the latest IEEE 802.11ax standard with the high offered load. It requires only an 802.11-compliant device as the source, with any 802.11-capable device monitoring the channel serving as the receiver. Distinguishing from similar channels, our covert channel is not tied to any specific IEEE 802.11 frame type. This unique feature allows for using any payload to convey covert bits, seamlessly embedded within the transmission. Regarding security, our proposed covert channel exhibits high resistance to steganalysis, attributed to two key factors. Firstly, it avoids altering any frame parameter, which is considered a suspicious activity by observers. Secondly, it relies on random backoff, an integral part of the IEEE 802.11 standard.

Table 6. Covert Channels comparison with StegoBackoff.

Ref.	Covert data	Performance	Constraints	Covertness
Stego-Backoff	The parity of the backoff slot following the DIFS just before the initiation of transmission.	140,000 bps	The performance relies on how many other devices are sharing the channel, frame length and their offered load which can cause collisions and affect the number of transmissions after DIFS.	High—Random backoff procedure is an integral part of IEEE 802.11 standard.
[18]	Random MAC Address in Probe Request	4770 bps	The method only works when the device is scanning and cannot be used when the device is associated with the access point.	High—MAC address randomization is a recommended practice although it can be detected [42].
[19]	The MSB of each supported rate value in Probe Request	319.43 bps	The method only works when the device is actively scanning using probe requests.	Medium—Altering one of the basic supported rates, might appear deliberate and raise suspicion from observers because most STAs support them.
[22]	2 bits of IEEE 802.11 Protocol Version (PV) field	127.4 bps	There is a risk of a frame being dropped if the receiver assumes that a frame with PV set to non-zero is corrupted during processing.	Low—The default protocol version in iEEE 802.11 standard is 0, and the remaining values are reserved.
[43]	The sum of the intervals between two consecutive transmissions	1800 bps	The method requires a strong understanding of statistical logic to accurately reproduce the backoff slot distribution and mimic the time distribution in IEEE 802.11.	High—The method introduces gaps in how time intervals are spread in the covert channel, making it stand out from the usual pattern in the wireless network.
[23]	The order in which frames are transmitted	9.76 bps	The method requires a minimum of two stations to create the covert channel.	High—The sequence in which stations access the channel can be influenced by different factors, such as the amount of data to send or the DCF backoff values.
[25]	Each DCF backoff slot	46 bps	It adjusts the backoff values directly and relies on a sharing dictionary, mapping the backoff intervals with a secret message.	Medium—The channel's security depends on a third party gaining knowledge of the shared dictionary, where backoffs are mapped to message symbols.
[21]	Adding or subtracting a delta from beacon interval (constant value)	2.79 bps	It relies on the beacon frame.	Medium—Even though the standard does not explicitly specify, most devices commonly use a default beacon interval of 100 milliseconds. Making frequent changes to this interval might signal covert activities.

The proposed mechanism, as well as all other mechanisms, has its drawbacks and limitations. Unfortunately, its performance strictly depends on the number of stations competing for access to the radio channel and also on the total traffic generated by all stations. This means, among other things, that in a dense network environment, its performance may decrease. Its disadvantage is that it allows only one bit of hidden information to be transferred with each transmitted frame. This can be a serious disadvantage for modern multimedia applications, which usually require high bit rates to function properly.

8. Conclusions

WLANs play a pivotal role in the modernization and efficiency of SGs. SGs leverage advanced technologies to monitor, control, and optimize the generation, distribution, and consumption of electrical power. WLANs provide a flexible and scalable communication infrastructure within SG systems, enabling seamless connectivity among various components. This wireless connectivity facilitates real-time data exchange between smart meters, sensors, and other grid devices. By utilizing WLANs, SGs can enhance the reliability and responsiveness of the electricity supply network. Moreover, WLANs allow for dynamic adjustments to power distribution based on real-time conditions. The deployment of WLANs in SGs not only improves operational efficiency, but also supports the development of more resilient and sustainable energy systems.

In this paper, we advocate for the implementation of a novel covert channel designed to augment the data integrity and security of communication within the SG. The proposed covert channel leverages the IEEE 802.11 random backoff procedure, encoding the secret message within the parity of the backoff slot. Its robustness against steganalysis is attributed to its integration into the inherent randomness of the backoff mechanism. The unpredictability of the number of slots, a characteristic of IEEE 802.11, makes the covert channel elusive to regular observers. Furthermore, the covert channel maintains transparency by causing no interference with regular network functionality, allowing it to coexist seamlessly and remain undetected.

We recognize the potential of our solution within the smart grid, specifically within the HAN. In the HAN, where devices under operator control interact with smart meters, our proposed covert channel proves advantageous, providing a discreet method for authentication and ensuring data integrity. Furthermore, in the NAN, designed as a mesh network facilitating data exchange among smart grid devices within a centralized environment, the covert channel plays a crucial role. It ensures the validation of device identities and enables the transmission/encoding of sensitive data in untrusted environments. It can be also used in other applications for SG wherever we want to maintain high confidentiality of transmitted data and, additionally, we do not want other users to know that such data are being transmitted at all.

Our analysis investigated the impact of frame size, offered load, the number of stations, MCS index, RTS/CTS mechanism usage, and transport layer protocol on the covert channel's performance metrics like throughput, delay, jitter, and frame efficiency. Our findings indicate that achieving higher throughput necessitates the use of smaller frame sizes, as larger payloads tend to diminish throughput. Additionally, an escalation in the offered load adversely affects the covert channel's performance, and the number of stations exacerbates this impact, hastening the degradation of network performance.

We emphasize that our experiments were carried out with substantially higher offered loads than those typically encountered in real-life scenarios. Despite these challenging conditions, the covert channel demonstrated satisfactory performance. Drawing from our findings, we confidently assert that, when employed with an appropriate payload size in a moderately congested network, the covert channel emerges as an excellent choice for establishing covert communication. It offers sufficient covert throughput while upholding acceptable levels of delay and jitter.

This work marks the initiation of an innovative mechanism aimed at enhancing data integrity and security in smart grids. As a future research direction to further refine our

covert channel, we propose the development of a secure mechanism for covert sender and receiver recognition. We would also like to increase the throughput of the cover channel with full resistance to existing stegoanalysis methods. It is also worth improving the ability to detect possible transmission errors in the covert channel, thus extending the mechanisms introduced natively by the MAC layer.

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

Funding: This research was supported by the National Research Institute, grant number POIR.04.02.00-00-D008/20-01 on "National Laboratory for Advanced 5G Research" (acronym PL-5G) as part of the 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 on request from the corresponding author.

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

Abbreviations

The following abbreviations are used in this manuscript:

AMI	Advanced Metering Infrastructure
AP	Access Point
BSS	Basic Service Set
CTS	Clear to Send
CW	Contention Window
DCF	Distributed Coordination Function
DIFS	DCF Interframe Space
EG	Electric Grid
HAN	Home Area Network
IEEE	Institute of Electrical and Electronics Engineers
IF	Isolation Forest
IoT	Internet of Things
LAN	Local Area Network
LSTM	Long Short-Term Memory
MAC	Medium Access Control
MCS	Modulation Coding Scheme
MSB	Most Significant Bit
NAN	Neighborhood Area Network
PDU	Protocol Data Unit
PG	Power Grid
RTS	Request to Send
SG	Smart Grid
SIFS	Short Interframe Space
SM	Smart Meter
STA	Station
SVM	Support Vector Machine
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network
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. Tutorials* **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. *IEEE 802.11;* 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. NIST. *The Smart Grid Interoperability Standards Roadmap*; Electric Power Research Institute (EPRI) Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2009.
6. Parikh, P.P.; Sidhu, T.S.; Shami, A. A Comprehensive Investigation of Wireless LAN for IEC 61850–Based Smart Distribution Substation Applications. *IEEE Trans. Ind. Inform.* **2013**, *9*, 1466–1476. [CrossRef]
7. Benzaïd, C.; Boulgheraif, A.; Dahmane, F.Z.; Al-Nemrat, A.; Zeraoulia, K. Intelligent Detection of MAC Spoofing Attack in 802.11 Network. In Proceedings of the Proceedings of the 17th International Conference on Distributed Computing and Networking, ICDCN '16, Singapore, 4–7 January 2016.
8. Agarwal, M.; Biswas, S.; Nandi, S. An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks. *Int. J. Wirel. Inf. Netw.* **2018**, *25*, 130–145. [CrossRef]
9. Liu, C.; Yu, J. Rogue Access Point Based DoS Attacks against 802.11 WLANs. In Proceedings of the 2008 Fourth Advanced International Conference on Telecommunications, Athens, Greece, 8–13 June 2008; pp. 271–276. [CrossRef]
10. Juhász, K.; Póser, V.; Kozlovszky, M.; Bánáti, A. WiFi vulnerability caused by SSID forgery in the IEEE 802.11 protocol. In Proceedings of the 2019 IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMI), Herlany, Slovakia, 24–26 January 2019; pp. 333–338. [CrossRef]
11. Farooq, T.; Llewellyn-Jones, D.; Merabti, M. MAC Layer DoS Attacks in IEEE 802.11 Networks. In Proceedings of the 11th Annual Conference on the Convergence of Telecommunications, Networking and Broadcasting (PGNet 2010), Liverpool, UK, 21–22 June 2010.
12. Joshi, D.; Dwivedi, V.V.; Pattani, K. De-Authentication attack on wireless network 802.11 i using Kali Linux. *Int. Res. J. Eng. Technol.* **2017**, *4*, 1666–1669.
13. Alnasser, A.; Rikli, N.E. Design of a Trust Security Model for Smart Meters in an Urban Power Grid Network. In Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Montreal, QC, Canada, 21–26 September 2014.
14. 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]
15. Aloul, F.; Al-Ali, A.; Al-Dalky, R.; Al-Mardini, M.; El-Hajj, W. Smart Grid Security: Threats, Vulnerabilities and Solutions. *Int. J. Smart Grid Clean Energy* **2012**, *1*, 1–6. [CrossRef]
16. Gwiazdowicz, M.; Natkaniec, M. Feature Selection and Model Evaluation for Threat Detection in Smart Grids. *Energies* **2023**, *16*, 4632. [CrossRef]
17. Stryczek, S.; Natkaniec, M. Internet Threat Detection in Smart Grids Based on Network Traffic. *Energies* **2023**, *16*, 329. [CrossRef]
18. Teca, G.; Natkaniec, M. A Novel Covert Channel for IEEE 802.11 Networks Utilizing MAC Address Randomization. *Appl. Sci.* **2023**, *13*, 8000. [CrossRef]
19. 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]
20. 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.
21. 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]
22. 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.
23. Sawicki, K. A Method of Covert Management of Heterogeneous ICT Networks. Ph.D. Thesis, Faculty of Cybernetics (WCY), Wojskowa akademia Techniczna, Warsaw, Poland, 2019.
24. 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.
25. Radhakrishnan, S.V.; Selcuk Uluagac, A.; 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.
26. Simmons, G.J. The prisoners' problem and the subliminal channel. In *Advances in Cryptology: Proceedings of Crypto 83*; Springer: Berlin/Heidelberg, Germany, 1984; pp. 51–67.

27. Grzesiak, K.; Piotrowski, Z.; Kelner, J.M. A Wireless Covert Channel Based on Dirty Constellation with Phase Drift. *Electronics* **2021**, *10*, 647. [CrossRef]
28. Blume, S.W. *Electric Power System Basics for the Nonelectrical Professional*; John Wiley & Sons: Hoboken, NJ, USA, 2016.
29. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput. Netw.* **2014**, *67*, 74–88. : 10.1016/j.comnet.2014.03.029 [CrossRef]
30. Hafeez, A.; Kandil, N.H.; Al-Omar, B.; Landolsi, T.; Al-Ali, A.R. Smart Home Area Networks Protocols within the Smart Grid Context. *J. Commun.* **2014**, *9*, 665–671. [CrossRef]
31. Meng, W.; Ma, R.; Chen, H.H. Smart grid neighborhood area networks: A survey. *IEEE Netw.* **2014**, *28*, 24–32. [CrossRef]
32. Kim, Y.; Hakak, S.; Ghorbani, A. Smart grid security: Attacks and defence techniques. *IET Smart Grid* **2023**, *6*, 103–123. [CrossRef]
33. Mathas, C.M.; Grammatikakis, K.P.; Vassilakis, C.; Kolokotronis, N.; Bilali, V.G.; Kavallieros, D. Threat landscape for smart grid systems. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual Event Ireland, 25–28 August 2020; pp. 1–7.
34. Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man in the Middle Attacks. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 2027–2051. [CrossRef]
35. Ye, A.; Li, Q.; Zhang, Q.; Cheng, B. Detection of Spoofing Attacks in WLAN-Based Positioning Systems Using WiFi Hotspot Tags. *IEEE Access* **2020**, *8*, 39768–39780. [CrossRef]
36. Feng, Z.; Ning, J.; Broustis, I.; Pelechrinis, K.; Krishnamurthy, S.V.; Faloutsos, M. Coping with packet replay attacks in wireless networks. In Proceedings of the 2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, Salt Lake City, UT, USA, 27–30 June 2011; pp. 368–376.
37. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
38. Bou-Harb, E.; Fachkha, C.; Pourzandi, M.; Debbabi, M.; Assi, C. Communication security for smart grid distribution networks. *IEEE Commun. Mag.* **2013**, *51*, 42–49. [CrossRef]
39. Baig, Z.A.; Amoudi, A.R. An Analysis of Smart Grid Attacks and Countermeasures. *J. Commun.* **2013**, *8*, 473–479. [CrossRef]
40. Natkaniec, M.; Pach, A. An analysis of the backoff mechanism used in IEEE 802.11 networks. In Proceedings of the IEEE Fifth Symposium on Computers and Communications (ISCC), Antibes-Juan Les Pins, France, 3–6 July 2000; pp. 444–449.
41. NS-3 a Discrete-Event Network Simulator. Available online: https://www.nsnam.org/ (accessed on 6 June 2023).
42. Martin, J.; Mayberry, T.; Donahue, C.; Foppe, L.; Brown, L.; Riggins, C.; Rye, E.C.; Brown, D. A Study of MAC Address Randomization in Mobile Devices and When it Fails. *Proc. Priv. Enhancing Technol.* **2017**, *4*, 268–286. [CrossRef]
43. Tahmasbi, F.; Moghim, N.; Mahdavi, M. Adaptive ternary timing covert channel in IEEE 802.11. *Secur. Commun. Netw.* **2016**, *9*, 3388–3400. [CrossRef]