www.czasopisma.pan.pl PAN www.journals.pan.pl

jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2023, VOL. 69, NO. 2, PP. 293–299
Manuscript received December 23, 2022; revised April, 2023. DOI: 10.24425/ijet.2023.144364

# An IEEE 802.11 MAC Layer Covert Channel Based On Supported Rates

Geovani Teca, and Marek Natkaniec

***Abstract*—Wireless Local Area Networks present several vulnerabilities that are exploited, and as a result, numerous attacks have been developed and used against them. Although countermeasures to detect and eliminate such threats have been created throughout the years, few methods exist to prevent the attacks. IEEE 802.11 covert channels could be considered a candidate to prevent Wi-Fi attacks since they allow secret communication between the client station and the access point without establishing an association. They can be implemented in frames that attackers do not target. This paper presents a new covert channel that prevents Wi-Fi attacks. We also describe metrics, and discuss the performance results of the proposed solution. We show that the new protocol is able to achieve high efficiency of operation.**

***Keywords*—steganography; covert channel; IEEE 802.11 networks; performance evaluation**

## I. Introduction

IEEE 802.11 is the standard for Wireless Local Area Networks (WLANs), commercially known as Wi-Fi. The constant growth in the production of mobile devices transformed IEEE 802.11 wireless networks [1], [2] into a primary system to provide Internet connectivity to those devices. The IEEE 802.11 networks offer multiple benefits: simple to set up and maintain, grant users freedom of mobility, and extend their range with less cost. Those are the main features that led to the fast adoption and popularity of the IEEE 802.11 networks.

Devices in the IEEE 802.11 network send data through electromagnetic waves propagating over the air, which means that no data transmission occurs in secret. Any device working on the same wireless channel can notice the transmission whenever a device sends data. During communication, the data is exposed and vulnerable to threats and attacks. There is a risk of sensitive data being intercepted and decrypted by third parties.

In the IEEE 802.11 networks, traffic analysis is one of the potential security risks that attackers can exploit. Anyone with a monitoring capability can secretly listen to the communications over the wireless channel, capture the frames, and modify them [3], [4]. In addition, there are well-known wireless attacks, such as the rogue access point (rogue AP), reply attack, and deauthentication attack. Although countermeasures against wireless attacks have been developed [5], [6] with the advance of information technology, the attacks have become more sophisticated.

Due to the frame's content and purpose, in IEEE 802.11, some frames are the most targeted of attacks, as is the case of data frames, and other frames are used to initiate an attack, such as deauthentication or association request. The type of frame exchanged between the STA and AP depends on which state STA is in. In the initial state, when STA is unauthenticated and unassociated with the AP, the scope of frames it is allowed to send is limited. In the initial state, some frames draw less attention from the attackers and still allow the STA to execute routine operations, such as scanning for available networks.

The frames STA sends for routine operations can carry secret data to the AP even without any authentication or association through a technique known as steganography. Steganography conceals a secret message inside an explicit message, achieved through covert channels. Therefore, a covert channel based on IEEE 802.11 frames can be a suitable mechanism to prevent wireless attacks.

This paper presents the concept and implementation of a covert channel to prevent IEEE 802.11 STA from attacks by remaining in the scanning phase and simultaneously allowing STA to send secret information without being authenticated or associated with the AP. From the observer's point of view, STA is neither associated with the AP nor attempting to do so. Thus, that cautious behavior reduces the probability of STA becoming a potential target for the attackers.

The paper is organized as follows: Section II presents the state-of-the-art research on IEEE 802.11 MAC layer covert channels that allow communication between STA and AP without association. In section III, we provide the preliminary knowledge and the concepts that are the foundation for the proposed covert channels. The fourth section describes the IEEE 802.11 most predominant attacks and the respective countermeasures. Section V explains the covert channel concept, design, and operation. Section VI presents the covert channel implementation, describing the simulation environment, the simulation scenarios, the covert channel metrics, and results. The conclusions are presented in section VII, which summarizes achievement and final observations.

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

G. Teca and M. Natkaniec are with Faculty of Computer Science, Electronics and Telecommunications, Institute of Telecommunications, AGH University of Science and Technology, Al. Mickiewicza 30, 30-059 Krakow, Poland (e-mail: teca@agh.edu.pl, natkanie@agh.edu.pl).

## II. State of The Art

Covert channels create a hidden and secure communication channel to conceal information between two endpoints without disturbing the regular network operation. This section describes the covert channels implemented in the MAC layer using IEEE 802.11 frames.

The paper [7] describes a unidirectional covert channel based on the Probe Request frame. The secret message is introduced in the Service Set Identifier (SSID) field and sent in the Probe Request while scanning for available networks.

Two methods to send secret data are demonstrated in [8]. The first is based on the Sequence Control (SC) field. The SC consists of two subfields: Sequence Number (12 bits), incremented by one in each new frame, and Fragment Number (4 bits), likewise incremented by one in each frame's fragment. The first proposed covert channel inserts the secret message in the eight MSB of the SC. The second covert channel is created in a MAC frame encrypted with Wired Equivalent Privacy (WEP) protocol [9]. When using WEP, a 32-bit Initialization Vector (IV) is added between the IEEE 802.11 frame header and body. The IV header consists of fields: IV (24 bits), Pad (6 bits), and Key ID (2 bits). The IV is a randomly generated value and is used to carry the secret message.

The research [10] proposes a covert channel based on the Protocol Version (PV) field. The IEEE 802.11 MAC header's first field is the Frame Control, consisting of subfields containing details about the frame. The first subfield is the PV (2 bits) which allows specifying the 802.11 standard version. According to the authors, the PV is expected to be zero (00). Therefore, the three remaining combinations (01, 10, 11) are used to encode the secret message.

The paper [11] presents a covert channel using the Beacon frame. The secret information is encoded in the Timestamp field. The Timestamp (64 bits) represents the time elapsed since AP radio was enabled. The authors proposed two covert channel variants. In the first variant, the AP calculates the Timestamp and replaces the four LSB for the secret information. In the second variant, the secret information is encoded by altering the intervals between subsequent Beacon frames.

A similar approach that uses the Beacon frame to create a unidirectional covert channel is proposed in [12]. AP broadcasts Beacon frames periodically to announce the existence of the network and its parameters. The constant interval between consecutive Beacons is indicated in the field Beacon Interval. The proposed covert channel encodes the secret message by either adding a delta value to the Beacon Interval or subtracting a delta value from it.

As presented, the existing covert channels implemented in the IEEE 802.11 MAC layer enable the transmission of secret information in the network or are used as authentication mechanisms between STA and AP. Therefore, a covert channel that allows STA to communicate with the AP without being associated is a suitable mechanism to prevent Wi-Fi attacks.

## III. Preliminary

This section describes the following notions: the IEEE 802.11 state diagram, Probe Request frame, Supported Rates, and Extended Supported Rates fields. The concepts constitute the foundation for creating the covert channel.

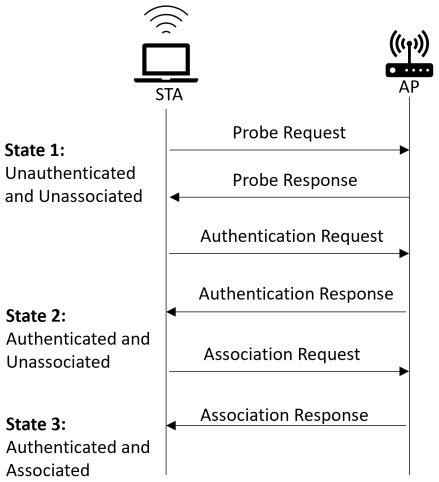


Fig. 1. IEEE 802.11 State diagram

### A. IEEE 802.11 State Diagram

In contrast to Local Area Networks, where in most cases, plugging the Ethernet cable into the network device grants full network access, in IEEE 802.11, the STA has to be associated with the AP. The STA goes through different states to establish the association with the AP.

As depicted in Fig. 1, in the first state, the STA is unauthenticated and unassociated (State 1). In state 1, the STA starts the network scanning process to discover available networks through passive or active scanning. In passive scanning, STA listens to Beacon frames in the wireless channels, and in active scanning, STA broadcasts Probe Request frames over the wireless channel. Upon receiving the Probe Request, the AP replies with a Probe Response containing the relevant network information.

After discovering the wireless network's existence and deciding which AP to establish the association, the STA sends an authentication request, providing its credentials. If the credentials match, the AP replies with an authentication response with a code indicating success. The STA passes to the authenticated and unassociated state (State 2). During the authentication, an attacker could monitor the channel and attempt to decrypt the frames to acquire the STA credentials [13]. Even after authentication, the STA becomes a potential target of a deauthentication attack [14].

To have complete access to the network, STA issues an association request. The AP grants the association assigning an association ID to the connection, and then STA moves to the last state: authenticated and associated (State 3). In state 3, the confidentiality and integrity of the exchanged data frames between STA and AP become a target for the attackers.

### B. Supported Rates and Extended Supported Rates

The Probe Request frame format is demonstrated in Fig. 2. The frame consists of a header and a body. The header is a

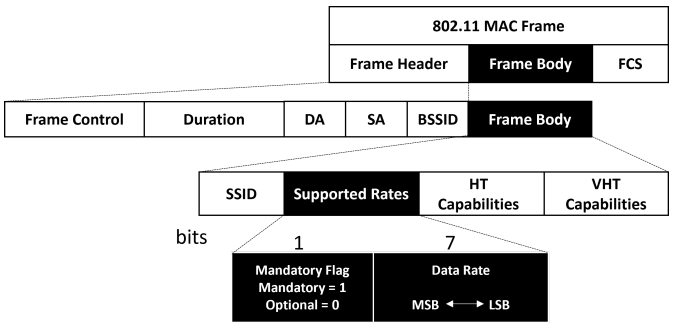


Fig. 2. IEEE 802.11 Probe Request frame format with the location of the Supported Rates field highlighted in the black background

```
IEEE 802.11 Probe Request, Flags: ........
IEEE 802.11 Wireless Management
    Tagged parameters (205 bytes)
        Tag: SSID parameter set: Wildcard SSID
        Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
            Tag Number: Supported Rates (1)
            Tag length: 8
            Supported Rates: 1 (0x02)
            Supported Rates: 2 (0x04)
            Supported Rates: 5.5 (0x0b)
            Supported Rates: 11 (0x16)
            Supported Rates: 6 (0x0c)
            Supported Rates: 9 (0x12)
            Supported Rates: 12 (0x18)
            Supported Rates: 18 (0x24)
        Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
            Tag Number: Extended Supported Rates (50)
            Tag length: 4
            Extended Supported Rates: 24 (0x30)
            Extended Supported Rates: 36 (0x48)
            Extended Supported Rates: 48 (0x60)
            Extended Supported Rates: 54 (0x6c)
```

Fig. 3. Probe Request frame captured from a real Wi-Fi network using Wireshark

regular IEEE 802.11 header for management frames. The body contains SSID, Supported Rates, HT - High Throughput, and VHT - Very High Throughput capabilities.

The Supported Rates field, highlighted in Fig. 2 with a black background, lists the data rates supported by the STA to communicate with the AP. Each data rate value is 8 bits. Seven bits represent the data rate value (from the bit in position 0 through 6), and the last bit (the bit in position 7), the MSB indicates whether the supported rate is mandatory (basic rate) or optional.

The Supported Rates field is up to eight data rates. If STA supports more than eight data rates, it can list them by adding the optional field Extended Supported Rates. Fig. 3 presents a Probe Request captured from a real Wi-Fi network using Wireshark software tool. As demonstrated, the STA supports a total of twelve data rates. The first eight data rates are inserted in the Supported Rates, and for the remaining, the STA lists them in the Extended Supported Rates.

The optional Extended Supported Rates is an extension of the Supported Rates, which is omitted from the Fig. 2.

## IV. IEEE 802.11 Attacks and Countermeasures

The current section introduces the most popular wireless network attacks and the existing countermeasures to detect and eliminate those attacks.

The rogue AP is an AP connected to the network without consent, acting as an impostor and impersonating the legitim AP by sending frames with identical properties to the authentic AP. A rogue AP is challenging to detect for regular network users since it can be intentionally placed closer to the victim, providing better signal strength than the original AP. Additionally, in wireless networks, users can connect to an AP without knowing its location or who is responsible for the network administration [15], [16].

Article [17] presents an excellent overview of the rogue AP problem. It lists prevention techniques and offers a taxonomical classification for rogue AP detection: client-side, server-side, and hybrid approach.

There are several mechanisms to detect rogue AP. Research paper [18] proposes rogue AP detection by analyzing the network traffic characteristics. The method analyzes the AP behavior when the end-user generates traffic that demands a reaction from the AP. Another interesting method to detect rogue AP is presented in [19]. In the proposed method, from two APs configured with the same parameters, the STA acquires the SSID, Basic Service Set Identifier (BSSID), IP, and Round Trip Time (RTT). In essence, the proposed method uses a decision tree. In each step, STA compares the new AP parameters against the previously collected ones. A proposed framework for rogue AP detection is presented [20]. The framework combines existing detection methods with a different approach from the authors. The framework is an open-source application that runs on Linux Operating System.

Packet sniffing attacks consist of using network traffic analyzers such as Wireshark and tcpdump to monitor and collect the network traffic for late decrypting the content of the frames. Packet sniffing detection is challenging because network traffic analyzers run in passive mode, making it hard to locate or realize their presence in the network.

The article [21] describes a comprehensive review of sniffing attacks and provides the respective countermeasures to mitigate the attacks. An innovative method to detect sniffing attacks using traffic probing and machine learning is proposed in [22]. The technique consists in continuously sending traffic to the suspicious machine and analyzing its response time to determine if the target host interface is in monitoring mode.

In IEEE 802.11, both AP and STA can issue Deauthentication frames. Exploring that fact, the attacker can copy the MAC address of AP or STA and send the Deauthentication on behalf of one of them, which is considered a deauthentication attack [23]. The attacker can repeatedly undermine the victims' connections, or during the re-authentication process, the STA might fall into many traps, such as associating with a rogue AP. Several methods have been developed to mitigate deauthentication attacks. The paper [24] proposes a straightforward approach using python automation script. The script enables the interface in monitoring mode and analyzes the frequency of the deauthentication frames sent to a particular AP. The research [25] presents a strategy against deauthentication attacks based on hashes. STA generates a hash#1 and sends it to AP in the Association Request, and AP generates hash#2 and sends it to STA in the Association Response. If one of them wants to issue a Deauthentication, it includes the hash in the Deauthentication to confirm its identity. The research [26] makes use of Supervised Learning to detect deauthentication

attacks. The model collects the network traffic and focuses on three indicators: Frame Interval, Received Signal Strength Indicator (RSSI), and Sequence Number. After learning those parameters from the data set, the model is trained to detect forged Authentication Requests.

Replay attacks occur when a third party listens to the ongoing communication in the wireless channel, intercepts it, modifies the data content, and replies as if it were the original sender. A practical example of a replay attack is the copycat attack [27]. The attacker copies the frame, modifies the header, and forwards it to the router. The article also proposed a mechanism to mitigate replay attacks, which consists in digitally signing the frame using a private key.

While the mentioned countermeasures aim to mitigate the attacks, only some solutions aim to prevent them. We also observe that most attacks occur when STA is in state 2 or 3 according to the diagram presented in Fig. 1. State 1 can be considered the safest among the three states. The STA can hide its presence by switching to passive scanning or announce its presence in active scanning but not engage in any meaningful data exchange with the AP.

## V. Proposed Covert Channel

### A. Covert Channel Design

The concept presented in this paper is a covert channel that allows STA to send secret data to AP without performing authentication or association. The core idea in the proposed covert channel is based on the possibility of specifying whether a data rate is mandatory or optional in the Supported Rates field using the MSB.

For each data rate, the STA sets the MSB to zero or one according to the message it intends to transmit. The scheme is presented in Fig. 4, demonstrating the procedure to encode up to 12 bits represented as binary string 101010000110. For the illustrated case, the STA sends a Probe Request listing 1, 5.5, 9, 36, and 48 Mbps as basic data rates and 2, 6, 11, 12, 18, 24, and 54 Mbps as optional.

The covert channel is difficult to detect because it exploits the open topics in the IEEE 802.11 standards: there is no limit to how long an STA stays in state one and no regulation on which data rates are mandatory or optional for a specific STA. The data rates can be listed in any order, and for the covert channel, the most important thing is the order of the MSB in each data rate of the list.

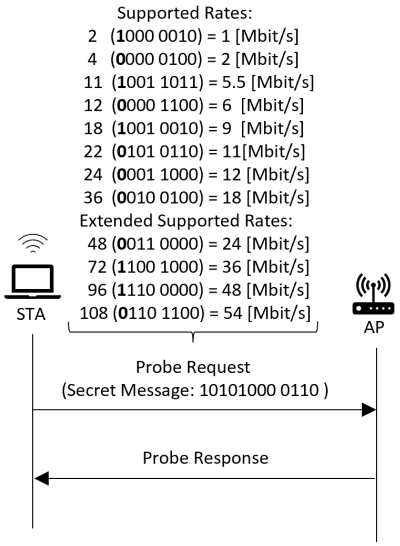


Fig. 4. Practical example how STA sends the covert message 101010000110 using the Probe Request

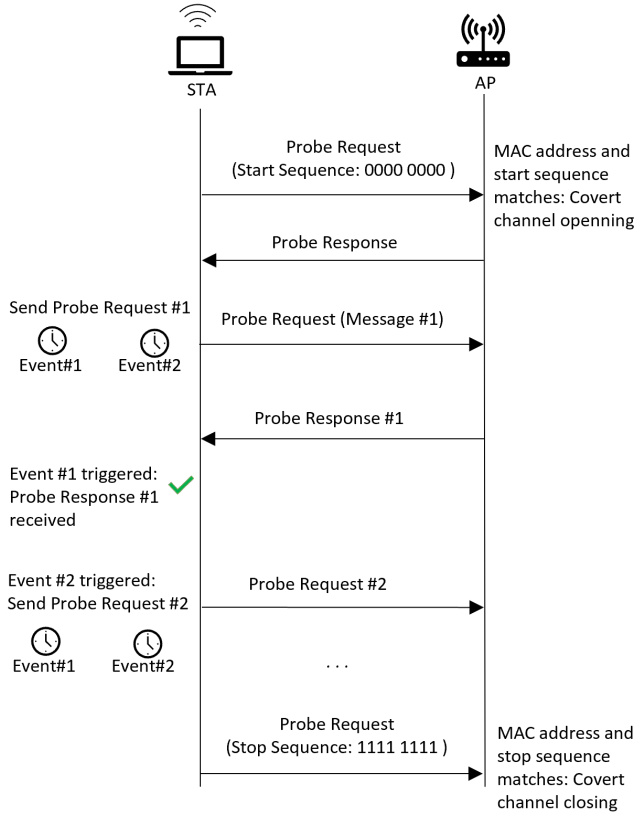


Fig. 5. Covert Channel Operation

### B. Covert Channel Operation

Before starting the secret communication, STA and AP share two values, and each value is 8 bits longer. The first value is the designated Start Sequence to signal the opening of the covert channel, and the second value is the designated Stop Sequence to signal the termination. Additionally, the covert channel is implemented, assuming that AP knows the covert STA MAC address to differentiate its Probe Request from the others.

As illustrated in Fig. 5, when STA intends to open the covert channel, it sends a Probe Request containing eight data rates. The group of MSB in data rates are arranged so that when read are equal to the Start Sequence. When it receives the Probe Request, the AP replies with a Probe Response to indicate its readiness to receive the secret messages. From now on, each Probe Request sent by STA is considered covert data.

Each Probe Request sent schedules two periodic events. When triggered, the first event, STA verifies if a Probe Response was received (Probe Response #1). If a Probe

Response is not received, the STA immediately retransmits it. The second event causes the STA to send the subsequent Probe Request (Probe Request #2), and the procedure repeats till the end of the operation.

To close the cover channel, STA sends a Probe Request with the Stop Sequence as a secret message. When receiving the Probe Request, the AP issues a Probe Response and considers subsequent Probe Request frames from STA as regular frames.

## VI. Covert Channel Implementation

### A. NS-3 Simulator

The wireless network was simulated in NS-3 version 3.35 [28]. NS-3 is an open-source network simulator that supports several network models written in C++ and Python. NS-3 provides the necessary APIs to create STA and AP nodes and add to them the TCP/IP protocol stack. The simulator provides the following helper classes to build the network: WifiHelper and WifiMacHelper for defining the PHY and MAC layer, InternetStackHelper and Ipv4AddressHelper to configure the Internet layer, UdpServerHelper and UdpClientHelper to configure UDP protocol in STA and AP nodes and ApplicationContainer for generating traffic.

We introduce modifications in the simulator source code to meet the covert channel requirements. The Supported Rates field is represented by the class SupportedRates, which shares public methods that allow adding data rates and setting the MSB as a basic data rate or optional. The class also has a friend class ExtendedSupportedRatesIE, representing the Extended Supported Rates field. The class Simulator has publicly available the Schedule method to schedule periodic events.

We repeated the simulations several times, and calculated the average values for each metric. In all figures, the error of each simulation point for the 95% confidence interval did not exceed ± 5%.

### B. Simulation Scenarios

The research was carried out for two scenarios. The secret message is transmitted only using the Supported Rates frame in the first scenario. The Extended Supported Rates field is added in the second scenario to improve the covert channel throughput. In the first scenario, we conducted six experiments. The first experiment is an environment with no external traffic. In the subsequent experiments, more STAs join the network: 10, 20, 30, 40, and 50 STAs. Each added STA runs a UDP client application that sends data to the AP, causing its traffic to interfere with the covert STA. In all the experiments, the covert STA remains in the scanning state throughout the simulation and sends Probe Requests to the AP at regular intervals. The probe request interval varies, starting from 10ms to 100ms, with 10ms as a step.

In the second scenario, we add four additional data rates in the optional Extended Supported Rates field to improve the covert channel throughput. Table I presents the essential parameters set during the simulations.

TABLE I
Simulation Parameters

| Parameter | Value |
|---|---|
| IEEE 802.11 Standard | 802.11ac |
| Channel width [MHz] | 20 |
| Wi-Fi channel model | Yet Another Network Simulator |
| TX and Rx Antennas per Node | 1 |
| Regular STA active probing | False |
| Beacon interval [ms] | 100 |
| Transport protocol | UDP |
| Offered load [Mbps] | 100 |
| Frame size [Bytes] | 1000 |

### C. Performance Metrics

Establishing metrics in the communication channel to provide an orientation about the covert channel's performance is paramount. The metrics are an insight into how the channel performs under certain conditions and what might be improved to optimize its operation. We have selected throughput, latency, and transmission efficiency as metrics.

- *Throughput*: the number of secret bits successfully acknowledged by the AP divided by the simulation time, expressed in bps.
- *Latency*: the time passed between sending a probe request with covert data and receiving the probe response in milliseconds.
- *Transmission efficiency*: the total number of Probe Responses received divided by the number of sent Probe Requests containing covert data, expressed in percentage. The metric provides the percentage of acknowledged covert messages.

### D. Simulation Results - First Scenario

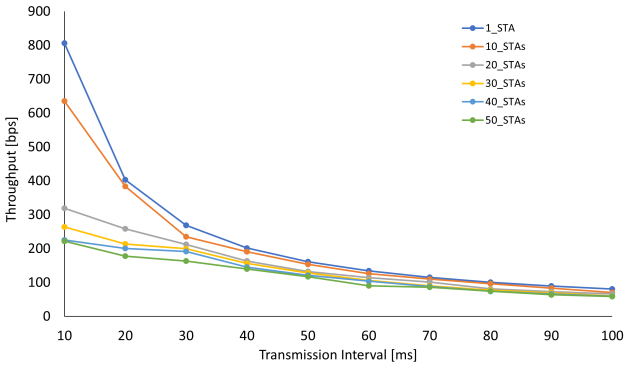


Fig. 6. Covert channel throughput vs. transmission interval for different number of STAs

As shown in Fig. 6, the covert channel achieves its highest throughput of 806 bps in the experiment with no external interference with a transmission interval of 10ms. Analyzing the relation between throughput and transmission interval, we can draw the following conclusions.

The first observation is that when more STAs joined the network and generated traffic slowly, the throughput started to

decrease for the same transmission interval. This is because the covert STA has to compete with every other STA to access the wireless channel. Moreover, the AP has to split its resource to handle requests from multiple STAs.

The second observation is that the channel throughput for each experiment is inverse proportional to the transmission interval. The more the transmission interval is extended, the less the throughput, and regardless of the number of STAs generating UDP traffic, the throughput values start becoming very close.

Analyzing the transmission efficiency as presented in Fig. 7, the covert channel is perfect when there is no external interference and no frame loss registered. We observed the correlation between longer transmission intervals and transmission efficiency in the presence of external traffic. The faster the covert STA sends, the more frames are lost.

Longer transmission intervals improve covert channel efficiency by reducing the frame collision probability in an environment with multiple STAs competing to access the transmission medium. That fact is evident in scenarios where the number of STAs was between 20 and 50. The minimum efficiency value was for an experiment with 50 STAs, and the efficiency was about 27%. However, when the transmission interval was extended for a similar experiment, the efficiency was above 70%.

It is crucial to highlight that the main factor contributing to better channel throughput and efficiency is that the covert channel uses the retransmission mechanism. The retransmission adds to the probability of a frame being successfully delivered.

As presented in Fig. 8, the latency of the covert channel for the scenario with no external traffic interference was below 1 ms. The more external interference, the slower the covert channel gets due to channel occupancy and the AP handling requests from the covert STA and regular STAs.

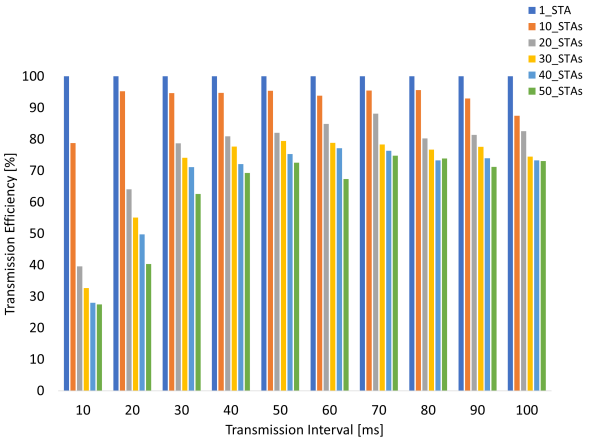


Fig. 7. Covert channel efficiency vs. transmission interval for different number of STAs

### E. Simulation Results - Second Scenario

When the Extended Support Rates field is added, the relation between the network throughput and the transmission interval is expected to remain the same. The Extended

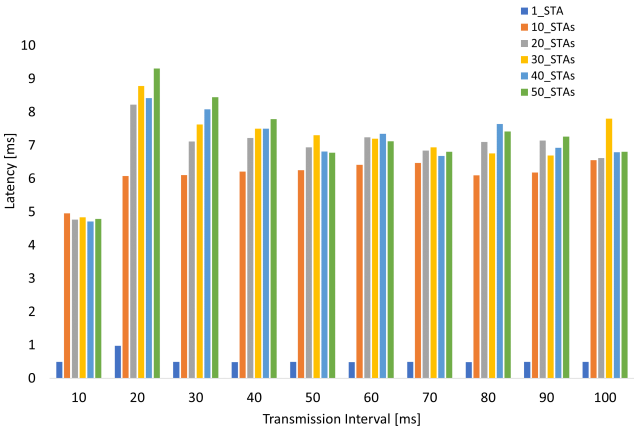


Fig. 8. Covert channel latency vs. transmission interval for different number of STAs

Supported rates only add to the covert channel a few bits sent per frame, increasing the throughput. To avoid presenting a duplicate plot (throughput vs. Probe Request interval), we added the Extended Supported Rates to the Probe Request and conducted simulations to compare the network throughput and latency. For the comparison, we used the shortest transmission interval (10 ms) and repeated all the six experiments.

As demonstrated in Table II, adding the Extended Supported Rates field positively influences the covert channel throughput. It is observed that for a small network (10 STAs), the achieved throughput is almost double the throughput when using only the Support Rates option. As more STAs join the network, it is observed that its throughput is still higher compared to the first scenario. Table III indicates that the latency of the covert channel with the Extended Supported Rates option remains on the same level.

TABLE II
THROUGHPUT COMPARISON BETWEEN FIRST AND SECOND SCENARIO

| | $1^{st}$ Scenario Throughput [bps] | $2^{nd}$ Scenario Throughput [bps] |
|---|---|---|
| 1 STA | 806,67 | 1210,0 |
| 10 STAs | 582,67 | 1031,1 |
| 20 STAs | 319,43 | 413,6 |
| 30 STAs | 263,93 | 290,5 |
| 40 STAs | 225,83 | 259,9 |
| 50 STAs | 175,33 | 221,0 |

## VII. CONCLUSIONS

Wireless network attacks have become more sophisticated. 802.11 wireless networks implementation and procedures have vulnerabilities exploited to conduct attacks against the networks. Countermeasures have been developed to detect and eliminate such threats, and only a few methods can prevent the attacks.

This paper presents a novel covert channel based on the IEEE 802.11 standard. The described mechanism prevents

TABLE III
LATENCY COMPARISON BETWEEN FIRST AND SECOND SCENARIO.

| | $1^{st}$ Scenario Latency [ms] | $2^{nd}$ Scenario Latency [ms] |
|---|---|---|
| 1 STA | 0,48 | 0,49 |
| 10 STAs | 4,9 | 4,9 |
| 20 STAs | 4,8 | 4,8 |
| 30 STAs | 4,8 | 4,7 |
| 40 STAs | 4,7 | 4,6 |
| 50 STAs | 4,7 | 4,5 |

wireless STA from becoming a target of attacks and simultaneously allows secrete data transmission between STA and AP. The secret message is hidden in the Supported Rate and Extended Supported Rate fields and sent in the Probe Request frame. The covert channel was implemented and analyzed using the NS-3 network simulator.

The results demonstrated that for the shortest transmission interval, the higher throughput and the lower latency can be obtained. On the other hand, extending the transmission interval decreases the throughput but increases the transmission efficiency. To improve the covert channel performance, the optional Extended Supported Rates field was added to increase the number of covert bits sent per single frame. That possibility allowed the covert channel to increase the achieved throughput. The proposed covert channel has retransmission feature, which assures better data reliability.

The proposed covert channel is characterized by its implementation simplicity, scalability, and data retransmission capability. The covert channel could benefit from one more layer of security improvements. As future research direction, we point to creating a mechanism to verify the authenticity of the AP sending the Probe Responses.

## REFERENCES


[1] "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," pp. 1–7524, 2021.

[2] M. Ergen, "IEEE 802.11 tutorial," https://www.researchgate.net/publication/2533138_IEEE_80211_Tutorial, 2002, online; accessed: 23 December 2022.

[3] K. Umesh and G. Sapna, "A literature review of security threats to wireless networks," *International Journal of Future Generation Communication and Networking*, vol. 7(4), pp. 25–34, 2014.

[4] J. J. Flores and A. Cruz, "A study in wireless attacks and its tools," in *11th Latin American and Caribbean Conference for Engineering and Technology*, 08 2013.

[5] M. M. Noor and W. H. Hassan, "Wireless networks: Developments, threats and countermeasures," *International Journal of Digital Information and Wireless Communications*, vol. 3, no. 1, pp. 125–140, 2013.

[6] M. Aung and K. Thant, "IEEE 802.11 attacks and defenses," in *Proceedings of the 17th International Conference on Computer Application (ICCA)*, 03 2019, pp. 186–191.

[7] K. Sawicki and Z. Piotrowski, "Two-way complex steganographic system for authentication and authorization in ieee 802.11 wireless networks," *ELEKTRONIKA - KONSTRUKCJE, TECHNOLOGIE, ZASTOSOWANIA*, no. 1, pp. 24–28, 2017.

[8] L. Frikha, Z. Trabelsi, and W. El-Hajj, "Implementation of a covert channel in the 802.11 header," in *2008 International Wireless Communications and Mobile Computing Conference*, 2008, pp. 594–599. [Online]. Available: http://doi.org/10.1109/IWCMC.2008.103

[9] S. Vibhuti, "IEEE 802.11 wep (wired equivalent privacy) concepts and vulnerability," in *CS265 Spring*, 2005. [Online]. Available: http://www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf

[10] G. Ricardo, T. Murali, and M. John C., "Analysis of a mac layer covert channel in 802.11 networks," *International Journal on Advances in Telecommunications*, vol. 5, no. 3 & 4, pp. 131–140, 2012.

[11] K. Sawicki and Z. Piotrowski, "The proposal of ieee 802.11 network access point authentication mechanism using a covert channel," in *2012 19th International Conference on Microwaves, Radar & Wireless Communications*, vol. 2, 2012, pp. 656–659. [Online]. Available: http://doi.org/10.1109/MIKON.2012.6233587

[12] H. Seong, I. Kim, Y. Jeon, M.-K. Oh, S. Lee, and D. Choi, "Practical covert wireless unidirectional communication in IEEE 802.11 environment," *IEEE Internet of Things Journal*, pp. 1–1, 2022. [Online]. Available: http://doi.org/10.1109/JIOT.2022.3204987

[13] T. Mekhaznia and A. Zidani, "Wi-fi security analysis," *Procedia Computer Science*, vol. 73, pp. 172–178, 2015.

[14] K. Chintan, B. Dhrumil, B. Ravi, P. Vivek, and D. Deepti, "De-authentication attack on wireless network," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 3S, pp. 881–884, 02 2019.

[15] Y. Song, C. Yang, and G. Gu, "Who is peeping at your passwords at starbucks? — to catch an evil twin access point," in *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, 2010, pp. 323–332. [Online]. Available: http://doi.org/10.1109/DSN.2010.5544302

[16] W. Wu, X. Gu, K. Dong, X. Shi, and M. Yang, "Prapd: A novel received signal strength–based approach for practical rogue access point detection," *International Journal of Distributed Sensor Networks*, vol. 14, no. 8, 08 2018.

[17] A. Abhijit S. Bodhe, "Rogue access point: A threat to wireless society," *IAETSD JOURNAL FOR ADVANCED RESEARCH IN APPLIED SCIENCES*, vol. 4, no. 7, pp. 97–102, 12 2017.

[18] S. Shetty, M. Song, and L. Ma, "Rogue access point detection by analyzing network traffic characteristics," in *MILCOM 2007 - IEEE Military Communications Conference*, 2007, pp. 1–7. [Online]. Available: http://doi.org/10.1109/MILCOM.2007.4455018

[19] V. Modi and C. Parekh, "Detection of rogue access point to prevent evil twin attack in wireless network," *International Journal of Engineering Research & Technology (IJERT)*, vol. 6, no. 4, pp. 23–26, 04 2017.

[20] R. Gonçalves, M. E. Correia, and P. Brandão, "A flexible framework for rogue access point detection," in *15th International Joint Conference on e-Business and Telecommunications (ICETE 2018)*, vol. 2: SECRYPT, 2018, pp. 466–471.

[21] P. B and J. Nagamalai, "A review on various sniffing attacks and its mitigation techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, pp. 1117–1125, 12 2018. [Online]. Available: http://doi.org/10.11591/ijeecs.v12.i3.pp1117-1125

[22] M. Gregorczyk, P. Żórawski, P. Nowakowski, K. Cabaj, and W. Mazurczyk, "Sniffing detection based on network traffic probing and machine learning," *IEEE Access*, vol. 8, pp. 149 255–149 269, 2020.

[23] K. Yogi and Ernastuti, "Analysis of deauthentication attack on ieee 802.11 connectivity based on iot technology using external penetration test," *Communication and Information Technology (CommIT)*, vol. 14, no. 1, pp. 45–51, 2020.

[24] A. H. Noman, M. A. Shahidan, and H. I. Mohammed, "An automated approach to detect deauthentication and disassociation dos attacks on wireless 802.11 networks," *IJCSI International Journal of Computer Science*, vol. 12, no. 4, pp. 107–112, 07 2015.

[25] A. Arora, "Preventing wireless deauthentication attacks over 802.11 networks," *CoRR*, vol. abs/1901.07301, 2019. [Online]. Available: http://arxiv.org/abs/1901.07301

[26] A. Amoordon, V. Deniau, A. Fleury, and C. Gransart, "A single supervised learning model to detect fake access points, frequency sweeping jamming and deauthentication attacks in ieee 802.11 networks," *Machine Learning with Applications*, vol. 10, p. 100389, 12 2022.

[27] Z. Feng, J. Ning, I. Broustis, K. Pelechrinis, S. V. Krishnamurthy, and M. Faloutsos, "Coping with packet replay attacks in wireless networks," in *8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2011, pp. 368–376. [Online]. Available: http://doi.org/10.1109/SAHCN.2011.5984919

[28] "NS-3 network simulator." [Online]. Available: https://www.nsnam.org