KSTiT 2022

MULTIKONFERENCJA
ŚRODOWISKA
TELE- I RADIOKOMUNIKACYJNEGO

KKRRiT 2022

PARADOKS PODŁĄCZONY CHOCIAŻ ODŁĄCZONY: SKRYTY KANAŁ STANDARDU IEEE 802.11 ZAPOBIEGAJĄCY ATAKOM NA SIECI WI-FI

CONNECTED WHILE DISCONNECTED PARADOX: AN IEEE 802.11 COVERT CHANNEL TO PREVENT WI-FI ATTACKS

Geovani Teca[1]; Marek Natkaniec[2];

[1] AGH University of Science and Technology, Cracow, teca@agh.edu.pl
[2] AGH University of Science and Technology, Cracow, natkanie@agh.edu.pl

Streszczenie: **Rosnące zapotrzebowanie mobilnych urządzeń na nieprzerwaną łączność z Internetem w dowolnym miejscu i czasie sprawiają, że sieci bezprzewodowe standardu IEEE 802.11 stają się jednym z głównych sposobów zaspokojenia tego zapotrzebowania. Sieć Wi-Fi zapewnia łączność z internetem, ale także otwiera drzwi dla zagrożeń i ataków. W tym artykule przedstawiamy koncepcję skrytego kanału, który ma zapobiegać atakom na sieci Wi-Fi, zapewniając jednocześnie niezawodną i bezpieczną komunikację między stacją a punktem dostępowym.**

Abstract: **The growing demand from mobile devices for uninterrupted internet connectivity from everywhere and anytime transform the IEEE 802.11 wireless networks into one of the primary solutions to meet the demand. A Wi-Fi network is a means to provide internet connectivity to the devices, at the same time opening the door to threats and attacks. This paper presents a covert channel to prevent Wi-Fi attacks while assuring reliable and secure communication between the Wi-Fi station and the access point.**

Słowa kluczowe: **IEEE 802.11 sieci bezprzewodowe, Skryty kanał, Steganografia, Wi-Fi ataki.**

Keywords: **Covert channel, IEEE 802.11 wireless networks, Steganography, Wi-Fi attacks.**

1. INTRODUCTION

The overall development and deployment of electronic devices (e.g.: smartphones, laptops, smart-watches, IoT devices) transformed IEEE 802.11 wireless networks [1] into one of the primary means to assure internet connectivity to those devices. IEEE 802.11 is the standard for Wireless Local Area Network (WLAN), well-known as a Wi-Fi network. Wi-Fi network offers many commodities as it is simple to set up, grants users freedom of mobility, and has the possibility to extend its range without the concern about the physical space or length of cables. Those are the main features that led to the fast adoption and popularity of the IEEE 802.11 wireless networks.

The IEEE 802.11 wireless networks in one way provides Internet connectivity to wireless devices, and in the other way, it exposes the devices to threats and attacks, rising security concerns. During the authentication phase, the device exchanges keys, and during the data transmission, the device might send sensitive data, such as credit card or personal identification number. Both authentication keys or sensitive data can be under attack due to the nature of data transmission in IEEE 802.11 networks. The data in the IEEE 802.11 wireless networks is sent through electromagnetic waves propagating over the air, which means that no data transmission occurs in secret, exposing the data to threats and making it vulnerable to attacks [2], [3]. There is a high risk of sensitive data being intercepted, decrypted, and falling into malicious hands.

Among the most popular attacks in IEEE 802.11 network are: Rogue Access Point (RAP), an Access Point (AP) added to the network without consent, acting as an impostor, and impersonates the functions of the original AP that connects a Client Station (STA) to the internet. Packet sniffing, and capture attacks occur when a network device scans the wireless channel and collects the traffic for further analysis in order to find a security breach in the network. Replay attacks occur when a third-party listen to the ongoing communication in the wireless channel, intercepts it, modifies the data content, and replies as if it were the original sender, luring the receiver to engage in a data exchange with this third-party. Additionally, we mention the deauthentication attack, when the attacker clones the Media Access Control Address (MAC address) of the STA or AP and sends deauthentication request frame, forcing the STA to reauthenticate to the network, and during the reauthentication process, the STA might fall into many traps, such as associating with a RAP.

This paper presents the concept and implementation of a covert channel to prevent Wi-Fi attacks, by sending secret data without being connected to the AP. The secret data is inserted in the Most Significant Bit (MSB) of each value that represents the supported rate field of the probe request frame. The secret data is acknowledged by a probe response frame from the AP.

This research paper is structured as follows: Section 2 presents existing measures against IEEE 802.11 wireless networks attacks and existing IEEE 802.11 covert channels that could be deployed to prevent the attacks. Section 3 provides background knowledge regarding IEEE 802.11 wireless networks states and operations, the frame, and the field on which the covert channel is based. Section 4 describes the covert channel concept and operation. The achieved results are presented in section 5. As the last, section 6 is a brief conclusion of this work.

2. RELATED RESEARCHES

2.1. IEEE 802.11 wireless networks attacks

RAP detection by analyzing network traffic characteristics is presented in [4]. The technique consists of analyzing the AP behavior when the end-user generates traffic that demands a reaction from AP. A review of a variety of traffic sniffing attacks and countermeasures in [5] describes the different attacks that the STA could face, after network data traffic is collected, and several strategies against replay attacks are presented in [6]. To prevent deauthentication attack, a mechanism based on hashing the association ID value is described in [7].

2.2. IEEE 802.11 wireless networks covert channels

Covert channels can be considered as one of the mechanisms to prevent IEEE 802.11 wireless networks attacks. They allow sending secret data without previous association with the AP, making the data transfer go undetected through the wireless channel being targeted or monitored. The paper [8] presents a covert channel that is based on the field SSID of the probe request frame. Two methods to send secret data are presented in [9], based on the sequence number and the initialization vector field using regular IEEE 802.11 frames. The paper [10] presents a covert channel based on the 2-bit field protocol version of the IEEE 802.11 frame header.

3. BACKGROUND

In contrast to wired networks, where in most cases, plugging the ethernet cable into the device grants full access to the network, in IEEE 802.11 wireless networks, a device has to exchange information with the AP prior to having full network access. As described in figure 1, in the very first state, the STA is unauthenticated and unassociated (State 1). In this state, STA starts the network discovery process through passive or active scanning. In passive scanning, STA listens to beacon frames from AP that advertise the wireless network's existence. In active scanning, STA sends a probe request frame, searching for the available wireless network and providing its own information. When the probe request is received by the AP, it determines, if the information in the probe request matches the required parameters to associate with the network, and if the information matches, the AP issues a probe response, providing information regarding the wireless network. After discovering the existence of the wireless network, the STA issues 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). In order to have full network access to the network, STA issues an association request, the AP grants the association assigning an association ID to the connection, then STA passes to the last state: authenticated and associated (State 3).

In IEEE 802.11 wireless networks, the STA is exposed to attacks from the moment it announces its presence in the network. In-state 1, when using active scanning the STA can specify in the probe request the Service Set Identifier (SSID) which is the network name. From that moment the STA draws attention and could be a victim of a RAP attack. If state 1 draws attention to the STA, states 2 and 3 open the door for the intruders to attack, because during the authentication phase, the encryption key is exchanged, and after the association the data exchange takes place. A wireless channel compromised from the beginning could lead to the encryption key being captured, which would allow access to unauthorized devices to the network and the exchanged data between STA and AP can be intercepted and decrypted.

These days, IEEE 802.11 wireless networks have become popular, anyone with a wireless network device, when turning on the Wi-Fi icon, can discover a considerable number of Wi-Fi networks to connect to. Few networks are open and do not require a password, this implies that no data encryption is guaranteed and even for the networks that require a password, there is no total certainty regarding the legitimacy of the AP with which the STA establishes the connection. Indeed, many users connect to a Wi-Fi network without even seeing where the AP is or knowing who brought the Wi-Fi network into existence, putting themselves in dangerous situations. Data security and privacy are the main concerns to be addressed when establishing a Wi-Fi connection in an untrusted environment. Turns out that network steganography addresses the data security and privacy issues in the Wi-Fi network. Steganography is a mechanism for concealing a secret message within another explicit message. Network steganography is achieved using covert channels. In order to prevent data from being exposed to attacks in an untrusted environment, STA abstains from sending explicit data frames, instead, it sends the data as a secret message inside a regular non-data frame, without raising the awareness of the secret data exchange between STA and AP is taking place.

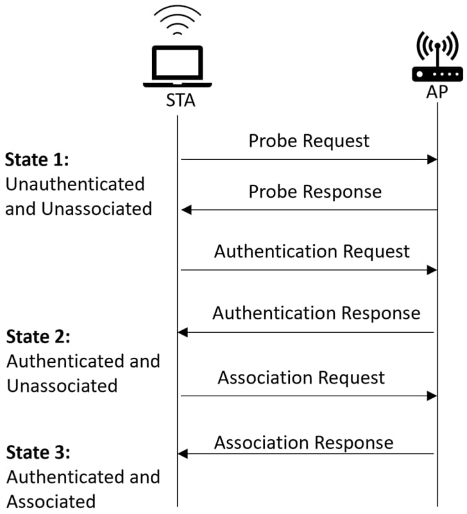
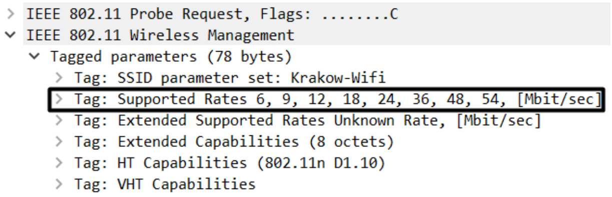


Fig. 1. IEEE 802.11 wireless networks state machine

As a regular non-data frame, the probe request is the frame broadcasted by STA to discover available wireless networks in the vicinities. The IEEE 802.11 probe request frame structure is presented in figure 2, the frame is a typical IEEE 802.11 header, and the body contains the following fields such as the SSID to indicate the network name STA is searching (Empty SSID means, all available networks), field supported rate to indicate data rate which STA supports in Mbps.

In the supported rate field the STA can insert up to 8 values, each value represents the data rate and is 8 bits longer. The bits 0 through 6 represent the data rate value in decimal, the bit 7 (MSB) is to indicate whether the supported data rate is mandatory (set to 1) or optional (set to 0). When AP receives the probe request, among the parameters, that it takes into consideration are the supported data rates. In order to receive a probe response at least one mandatory data rate value in the probe request shall be the same mandatory data rate in the AP.



```
> IEEE 802.11 Probe Request, Flags: ........C
v IEEE 802.11 Wireless Management
  v Tagged parameters (78 bytes)
    > Tag: SSID parameter set: Krakow-Wifi
    > Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    > Tag: Extended Supported Rates Unknown Rate, [Mbit/sec]
    > Tag: Extended Capabilities (8 octets)
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: VHT Capabilities
```

Fig. 2. Probe request frame format with supported rate field highlighted

The possibility to specify whether a data rate value is mandatory or optional using the MSB, opens a window to create a covert channel that conceals the data into a secret message using the MSB of each data rate value. Having the covert channel created in an untrusted environment, the STA remains in state 1 and sends secret data to the AP with no concerns regarding data security and privacy, avoiding the threats and attacks that occur in states 2 and 3.

4. COVERT CHANNEL CONCEPT

We observe that the most popular Wi-Fi attacks take place when STA is in state 2 or 3. It is the attempt to connect to the network that exposes it to threats and makes it vulnerable to attacks. The concept presented in this paper is a covert channel that allows STA to send secret data to AP without performing authentication or association in untrusted environments. The secret message is inserted in the MSB of the values in the supported rate field carried in probe request frames while scanning the network. For each probe request, STA sets to 1 or 0 the MSB of the data rate value in the supported rate field. Each data rate value allows transmitting one bit of covert information. The scheme is presented in figure 3, demonstrating the scheme to encode a secret message as sequence **10101000**. STA sends a probe request setting the 6, 12, and 24 Mbps as mandatory data rate and the remainder data rate as optional.

The covert channel allows transmitting up to 8 bits in a single transmission, therefore before the opening of the covert channel, STA and AP must prove each other authenticity, which will allow eliminating the suspicion of the existence of an impostor from both sides. For that purpose, a 4-bit Cyclic Redundancy Check (CRC-4) is used, and STA and AP share three polynomial generators, the opening polynomial generator used to signal the opening, the data polynomial generator one to secret data, and the terminating polynomial generator to signal the covert channel termination. To signal the start of transmission, STA takes a 4-bit sequence and encodes it using the opening polynomial generator, producing an 8-bit sequence. Each bit from the sequence is then inserted in the MSB of each data rate value and sent in the probe request. The AP receives the probe request and decodes using the same starting polynomial and sends back a probe response, signaling that it is also ready to start the communication.

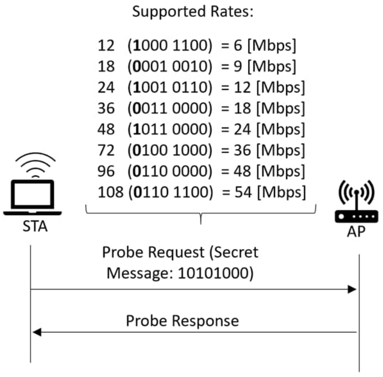

Supported Rates:
12 (1000 1100) = 6 [Mbps]
18 (0001 0010) = 9 [Mbps]
24 (1001 0110) = 12 [Mbps]
36 (0011 0000) = 18 [Mbps]
48 (1011 0000) = 24 [Mbps]
72 (0100 1000) = 36 [Mbps]
96 (0110 0000) = 48 [Mbps]
108 (0110 1100) = 54 [Mbps]
STA
AP
Probe Request (Secret Message: 10101000)
Probe Response

Fig. 3. Pratical example of sending a covert message ***10101000*** *using probe request*

After receiving the probe response that confirms that the covert channel is created, the STA sends the first covert message, as presented in figure 4, the STA after sending each covert message, schedules two periodic events. The first event is to schedule the next transmission and the second is to schedule the verification if a probe response has been received. If STA detects that the probe response has not been received, it retransmits right away the probe request.

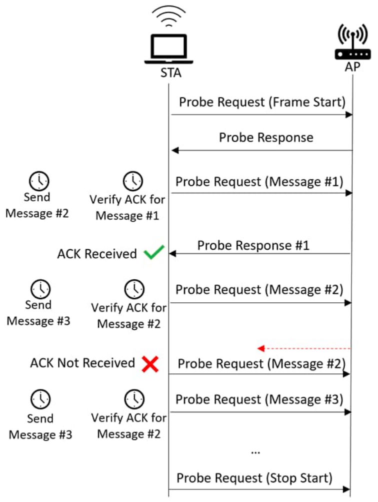

STA
AP
Probe Request (Frame Start)
Probe Response
Send Message #2
Verify ACK for Message #1
Probe Request (Message #1)
ACK Received
Probe Response #1
Send Message #3
Verify ACK for Message #2
Probe Request (Message #2)
ACK Not Received
Probe Request (Message #2)
Send Message #3
Verify ACK for Message #2
Probe Request (Message #3)
...
Probe Request (Stop Start)

Fig. 4. Covert channel concept using probe request frame

In order to terminate the covert channel, the STA performs the same procedure as in opening the covert channel, but using the terminating polynomial, the AP decodes the secret message using the terminating polynomial. In general, the AP takes each MSB from the data rates in the received probe request, forms the 8-bit sequence, runs the CRC against the three polynomial generators to find a match, and determines whether the probe request signals opening, data, or terminating the covert channel.

The presented covert channel finds its practical use, for data exchanged between STA and AP in untrusted or hostile environments, where the users avoid being exposed to threats or attacks.

5. PERFORMANCE ANALYSIS

5.1. Simulation scenarios

The simulation environment was created using the ns-3 discrete-event network simulator [11]. The network was IEEE 802.11ac with a 20MHz channel with one AP and wireless STAs connected to the same AP. All the nodes were in constant position during the entire simulation. There was only one STA sending covert data (sending probe request all the time) and the remaining STAs generated UDP traffic in saturated conditions. To evaluate the performance of the covert channel, we have created different scenarios with different parameters. The parameters we intended to analyse the covert channel performance are:

- Throughput as the number bits per second sent and successfully acknowledged by the AP.
- Covert channel efficiency as the percentage of successful received frames over transmitted.
- Impact of retransmission mechanism, as a measure of how much the retransmission contributed to the covert channel efficiency.

In the first scenario, there is only one AP and one STA exchanging probe request and response. In the second scenario, we analyse the impact of external traffic on the covert channel by adding 5, 25 and 50 more STAs respectively, generating UDP traffic in saturation conditions. The variable parameter is the probe request interval, which indicates how often the STA generates the covert message in form of probe request. The simulation time was 300 seconds.

5.2. Simulation results

We observed that the covert channel achieves its maximum capacity which is 802 Mbps in isolated scenarios, only having the covert STA and the AP. However, adding four more regular Wi-Fi devices generating UDP traffic still has no big impact on the covert channel performance, as the results are slightly closed. The covert channels suffer degradation as observed when a network transits from small (having five stations) to a medium having 25 stations. The throughput degrades considerably down to more than 50% percent, and the registered throughput was 293 Mbps. Increasing the number of stations to 50 also had only a slight degradation in the covert channel throughput.

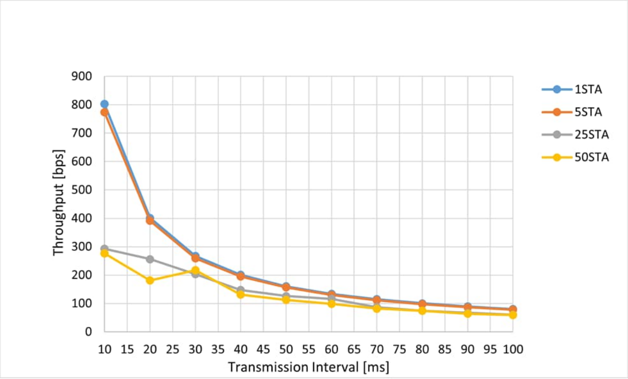


Fig. 5. Covert channel throughput analysis

Figure 6, presents the covert channel efficiency over the transmission interval. In isolated scenarios with only the covert STA and the AP, it was registered 100% efficiency as there was no external traffic to interfere or cause a collision with the covert STA. The same stable efficiency is observed with a network with four more additional stations with an efficiency of around 96%. We also observe that for the medium and larger network (25 and 50 stations respectively), shorter transmission interval leads to more collisions, as consequence the efficiency decreases considerably. The efficiency improves with a larger transmission interval, as the covert STA waits longer to transmit and has more chances to get a response.

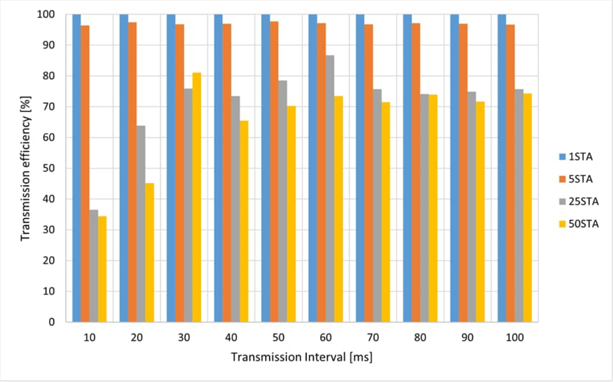


Fig. 6. Covert channel efficiency

The presented covert channel is reliable, providing retransmission in case of failure to receive the probe response and retransmission is a mechanism to improve the covert channel throughput and efficiency. In figure 7, which network size caused more frames to be retransmitted. For isolation, the scenario has previously presented with 100% of efficiency it registered no retransmission, for a small network with four more regular stations about 30% of the frames are retransmitted. The retransmission rate increases as the number of stations in the network also increase with shorter transmission interval.

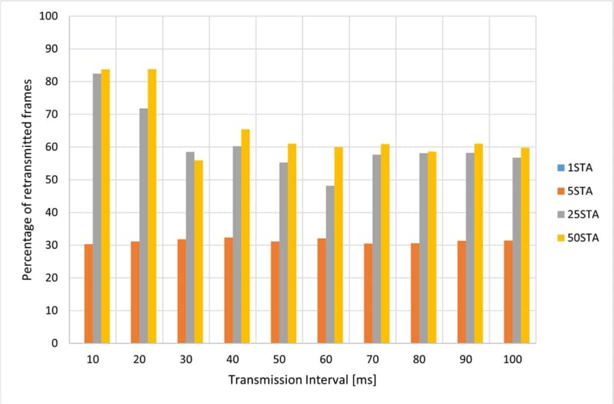


Fig. 7. Effect of retransmition on the covert channel perfomance

6. CONCLUSION

In this paper, we presented the current threats and attacks against IEEE 802.11 wireless networks. We described the popular attacks and threats and the developed countermeasure. We also proposed a covert channel to prevent the attacks avoiding the STA to going to unsaved zone (states 2 and 3) simultaneously allowing STA to send data to AP. The covert channel encodes the secret data in the MSB bit of supported rates values in the probe request with retransmission capabilities. The presented results proved that the covert channel performance stands out providing high values of throughput when compared with existing covert channels, even in dense network.

ACKNOWLEDGEMENTS

This work 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.

REFERENCES

[1] IEEE Standard for Information Technology. 2021. “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. IEEE Std 802.11-2020”. *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*: 1-4379.

[2] Umesh Kumar, Sapna Gambhir. 2014. “A Literature Review of Security Threats to Wireless Networks”. *International Journal of Future Generation Communication and Networking,* 7 (4): 25-34.

[3] Noor Mardiana, Hassan Wan. 2013. “Wireless Networks: Developments, Threats and Countermeasures.” *International Journal of Digital Information and Wireless Communications* 3: 125-140.

[4] Shetty Sachin, Song Min and Ma Liran. 2007. “Rogue Access Point Detection by Analyzing Network Traffic Characteristics.” *MILCOM 2007 - IEEE Military Communications Conference*: 1-7.

[5] Prabadevi. Nagamalai Jeyanthi. 2018. “A Review on Various Sniffing Attacks and its Mitigation Techniques”. *Indonesian Journal of Electrical Engineering and Computer Science,* 12 (3): 1117-1125.

[6] Aura Tuomas. 1997. “Strategies against Replay Attacks”. *Proceedings 10th Computer Security Foundations Workshop:* 59-68.

[7] Arora Ananay. 2018. “Preventing wireless deauthentication attacks over 802.11 Networks”.

[8] Sawicki Krzysztof. 2017. ”Two-way complex steganographic system for authentication and authorization in IEEE 802.11 wireless networks”. *ELEKTRONIKA - KONSTRUKCJE, TECHNOLOGIE, ZASTOSOWANIA*, 1: 24-28.

[9] Frikha Lilia, Trabelsi Trabelsi. El-Hajj Wassim. 2008. “Implementation of a Covert Channel in the 802.11 Header”. *International Wireless Communications and Mobile Computing Conference*: 594-599.

[10] Goncalves Ricardo. Tummala Murali. Mceachen John. 2012. “Analysis of a MAC Layer Covert Channel in 802.11 Networks”. *International Journal on Advances in Telecommunications,* 5 (3 & 4): 131-140.

[11] https://www.nsnam.org