Effective DoS Attacks against Wireless LAN Devices and Countermeasures

Keito Kubota[1,a)] Yoshiaki Shiraishi[1] Masakatu Morii[1]

Abstract: With the spread of mobile devices and IoT devices and the promotion of remote working in recent years, the importance of wireless communication is increasing day by day. In today's society, countermeasures against DoS attacks are essential to prevent communication availability. We have already proposed a DoS attack that is effective for many wireless LAN devices by exploiting vulnerabilities in the wireless LAN protocol. This method is more serious than previous DoS attacks because it is easier to execute and more widely applicable. We also propose a method to slow down the communication speed of some devices by refining this attack. In this paper, we perform more detailed evaluation experiments of these attacks to reveal the vulnerable devices and their behavior. We also consider the access point-based countermeasure and the countermeasure using a repeater that can be used at the user level, in addition to a client-based countermeasure.

Keywords: Wireless LAN, Denial-of-Service Attack, IEEE802.11

1. INTRODUCTION

There are more and more opportunities to use wireless LANs in commercial facilities such as hotels and cafes, and public facilities such as libraries and airports. Especially in recent years, with the promotion of work style reform, the demand for remote work has been increasing. In addition to these daily life usage, wireless LANs are also used in places where real-time capability is important, such as monitoring systems and sensor networks due to the spread of IoT. Even though there is no damage such as information leakage, DoS attacks interfere with the availability of the system, and therefore, it is necessary to take countermeasures.

Wireless LANs that use radio waves for data transmission and reception are easy to be tapped, and encryption is also essential for safe data exchange. Currently, WPA2 is widely used as a security protocol for wireless LANs. However, WPA2 has been found to be vulnerable [1] [2], and a new security protocol called WPA3 was announced in 2018. In 2019, Dragonblood, an attack against WPA3, was proposed by Vanhoef et al [3]. Dragonblood is an attack that takes advantage of a vulnerability in the implementation of WPA3, and side channel attacks, downgrade attacks and DoS attacks have been proposed. Dragonblood can only attack clients using WPA3, and due to its high difficulty of execution and strict conditions, it has not had a significant impact. However, there is a high probability that vulnerabilities will continue to be found in the future, and it is necessary to evaluate the security of not only WPA3 but also each specification of wireless LANs before an attacker exploits the vulnerability.

We previously proposed a different approach to DoS attacks than Dragonblood, which uses a signal called Channel Switch Announcement (CSA) [4]. The CSA is a signal that an access point sends to the client when it switches channels [5]. We succeeded in disconnecting the client's communication by continuously sending the tampering beacon with this CSA inserted. The proposed attack is more serious than Dragonblood because it is easier to realize and more widely applicable. We also propose a refined version of this DoS attack that allows some clients to stay connected to the access point and significantly slow down the communication speed [6]. These attacks are more serious than previous DoS attacks because they allow the attackers to attack the devices regardless of the security protocol, except for some devices, by cutting off the communication or slowing down the communication speed.

In this paper, we investigate these attacks in more detail using more clients, including the latest operating systems, and investigate the vulnerability and behavior of each client. As a result, we found that it is possible to attack on Raspberry Pi, the latest Ubuntu, iPhone, etc., in addition to the clients that have been attacked before. Thus, our proposed attack is still very effective as a DoS attack on wireless LANs, and countermeasures are necessary.

In addition to the client-based countermeasures proposed in the previous work, we also propose a countermeasure on the access point side and a countermeasure that can be implemented at the user level using a repeater.

[1] Kobe University
[a)] kubota@stu.kobe-u.ac.jp

2. BACKGROUND

In this section, we first describe the procedures of wireless LAN devices to start communication and wireless LAN security protocols. Then, the Channel Switch Announcement (CSA) used in this paper is described. Finally, we describe the existing DoS attacks and a method using Channel Switching by Könings et al.

2.1 Connecting to an access point

In order for a client to initiate communication over a wireless LAN, it must connect to an access point according to the connection procedure. The connection procedure consists of three steps. In this section, these three procedures are explained.

The first procedure is to find a communicative access point in order for the client to connect with the access point. There are two ways to do this: static scanning and dynamic scanning. In this section, we mainly describe static scanning. Access points communicate in several channels (frequencies) in both the 2.4GHz and 5GHz bands to avoid communication congestion. In addition, the access point periodically sends packets called beacons on the channels he uses to inform the surrounding clients of his presence. The beacon contains information such as the SSID (Service Set IDentifier) of the access point and the encryption method. In static scanning, the client finds the access point by receiving beacons on various channels.

Next, the client selects the access point it wants to connect to from among the access points it finds and goes through the authentication process. Nowadays, the authentication procedure is only a formality and no information is exchanged. However, when a client communicates using WPA3, a temporary master key is generated from the preshared key by an SAE handshake before the authentication procedure.

After that, they enter the association procedure. Here again, the access point sends the same information as in the scan and more detailed information about the communication method to the client. Then, the key generation protocol for each security protocol is used to share the encryption key for communication, and the connection is completed.

2.2 Wireless LAN security protocols

Wireless LAN uses radio waves and is therefore easy to wiretap. To prevent information from being leaked to an attacker, encryption of communication is essential. In wireless LANs, there are several security protocols that define the encryption of communication. Currently, WPA2 (Wi-Fi Protected Access 2) is mainly used for this purpose. WPA2 uses a 4-way handshake to generate and share encryption keys. In general, AES encryption is used to encrypt the communication. WPA2 has been widely used as a secure protocol since its release. However, in 2017, an attack was proposed to exploit a 4-way handshake vulnerability called KRACKs [1].

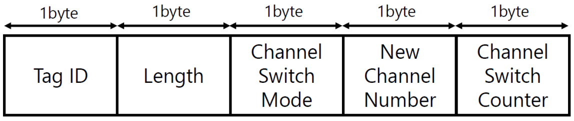

Fig. 1 CSA Format

In 2018, the Wi-Fi Alliance announced WPA3, the successor to WPA2. WPA3 adopts a key generation protocol called SAE handshake before the authentication procedure, and is said to have solved the problem pointed out in KRACKs and improved security by using a temporary key as the key used in the 4-way handshake. In addition, WPA3 adopts Protected Managed Frames (PMF) as a standard feature to authenticate packets used in association procedures and 4-way handshaking to protect against existing attacks. Furthermore, cookie-based authentication is used as a countermeasure against DoS attacks that exploit the computationally costly process in the SAE handshake.

2.3 Channel Switch Announcement

A CSA (Channel Switch Announcement) is a signal that an access point uses to notify a client of a change in the channel, as defined in IEEE802.11h [5].

When an access point receives radio waves, such as satellite communications, on the channel it is using to communicate in the 5 GHz band, it must move to another channel. In this case, the access point sends a CSA to notify the change of the channel without interrupting communication.

When the client receives the CSA, it selects whether to continue communication by changing the channel or to connect to another access point, and if it continues communication, it switches the channel as soon as the channel of the access point changes and resumes communication. In this case, it is not necessary to perform the connection procedure as described in Section 2.1, and communication is immediately resumed on the destination channel.

CSA can be added to some packets, such as beacons. In beacons, the CSA is added to the option area and does not perform encryption or tamper detection.

The format of CSA is shown in Figure 1. Tag IDs are used to identify option information, which is 37 in CSA. Length is the length of the part containing CSA information, which is 3 in CSA. The Channel Switch Mode specifies whether to continue communication after receiving a CSA until the channel is moved. When "1" is set, the client stops communication until the channel is moved. If 0 is set, the communication continues until the channel is moved. New Channel Number shows the new channel to be moved to. The Channel Switch Counter shows the number of beacons sent to the destination channel. Each time a beacon is sent, it is decremented, and when it reaches 0, the channel is moved.

2.4 DoS Attacks on Wireless LAN

Many kinds of DoS attacks against wireless LANs have been proposed since the enactment of IEEE802.11. One of the most famous attacks is the Deauthentication attack [7]. The Deauthentication attack is an attack using disassociation packets, one of the management frames of a wireless LAN. Disassociation packets are used to disconnect the communication when the authentication procedure fails. The Deauthentication attack disguises a disassociation frame and sends it to the target client and the access point, thereby disconnecting the client from the access point. However, the WPA3-based devices are not affected by this attack because PMF is adopted as a standard feature. However, a DoS attack against WPA3-based terminals has been proposed as one of the Dragonblood attacks [3]. Dragonblood is a generic term for the WPA3 vulnerability and the attacks that exploit it, announced by Vanhoef et al. in 2019. Dragonblood can be divided into three main types of attacks. One of them is a DoS attack on access points using the SAE handshake process. The SAE handshake is a protocol that uses elliptic curves to generate a temporary master key from a pre-shared key. This key generation is known to be a very computationally expensive process. As described in section **??**, WPA3 uses cookies to prevent attackers from deliberately repeating key generation by spoofing packets. However, the cookie is based on a falsifiable MAC address, so an attacker can create a cookie simply by spoofing the MAC address. Therefore, the attacker can use spoofed packets to repeatedly generate keys and increase the CPU utilization of the access point to enable a DoS attack.

The other method of DoS attacks against wireless LANs is proposed by Könings et al at 2009 [8]. It's uses CSA forgery First, we explain the attack method. The attacker has received a beacon of the target access point in advance. The attacker creates a tampered beacon with a CSA inserted into the received beacon that moves it to a non-existent channel. Set the Channel Switch Mode of the CSA to 1 and set the Channel Switch Counter to the maximum value of 255. In this way, the client that receives the tampered beacon stops communicating while the beacon is sent 255 times (about 25 seconds). The client then switches channels, but since there is no access point in the destination channel, a communication error occurs and the client returns to the original channel and resumes communication. As a result, the client would theoretically be unable to communicate for about 30 seconds by receiving a tampered beacon. This attack takes advantage of the fact that the CSA can be easily forged, that it can be switched to a non-existent channel, and that there is no upper limit on the Channel Switch Counter. When Könings et al. proposed this attack, some clients had taken measures such as limiting the value of the Channel Switch Counter to 1 or less. In this case, even if the attacker sends a tampered beacon, the communication does not stop until the Channel Switch Counter drops below 1. Therefore, the DoS state lasts only a few seconds. In fact, when this attack was implemented, many clients did not stop communication when the Channel Switch Counter was large. Therefore, we believe that the impact of DoS by this attack is lessened nowadays.

Table 1 Devices

WPA2	Laptop A(built-in NIC)
	Laptop A（Wi-Fi adapter A）
	Laptop B(built-in NIC)
	Laptop B（Wi-Fi adapter A）
	Raspberry Pi 3B(built-in NIC)
	Raspberry Pi 3B（Wi-Fi adapter A）
	Android Smartphone（Android10）
	iPhone7（iOS13.1）
	iPhone11 Pro（iOS13.4）
WPA3	Laptop A(built-in NIC)
	Laptop A（Wi-Fi adapter A）
	Android Smartphone（Android10）
	iPhone7（iOS13.1）
	iPhone11 Pro（iOS13.4）

3. Continuous DoS Attacks

In this chapter, we describe a DoS attack using CSA and its verification experiments. In section 3.1, we describe our previously proposed method, which is an improvement of the method by Konings et al [6]. In section 3.2, we test the effectiveness of the DoS attacks described in section 3.1 with new clients in addition to the experimental data presented in our previous work [6]. In section 3.3, we explain the behavior of a client when it is attacked.

3.1 Attack Method

First, the attacker receives a beacon of the targeted access point, similar to the method of Könings et al. and generates a tampered beacon by inserting a CSA. Here, unlike the method of Könings et al, the Channel Switch Counter of the inserted CSA is set to 0. In this way, as soon as the client receives the beacon, it tries to switch to the specified channel to continue the communication. The attacker sends the generated tampered beacons at the same interval as the normal beacons. As a result, the client that receives the tampered beacon immediately switches the channel and a communication error occurs, and even if the client returns to the original channel, the tampered beacon is sent periodically, so the client repeatedly switches the channel immediately and cannot communicate and enters a DoS state.

This attack differs from the method by Könings et al. in that the Channel Switch Counter is set to 0, thus invalidating the counter-value limiting measure described in Section 2.3. Furthermore, the DoS state can be continued for a long time by continuously sending a beacon and switching channels.

3.2 Experiment

3.2.1 Experimental Method

An empirical experiment was conducted to investigate the feasibility of the proposed attack. For the experiment, we have created a tool to perform the attack using the proce-

Table 2 Results（WPA2，Windows10）

Client	Connection
Laptop A（built-in NIC）	disconnected
Laptop A（Wi-Fi adapter A）	continued
Laptop B（built-in NIC）	continued
Laptop B（Wi-Fi adapter A）	continued

Table 3 Results（WPA2，others）

Client	Connection
Ubuntu18.04（built-in NIC）	disconnected
Ubuntu18.04（Wi-Fi adapter A）	disconnected
Ubuntu20.04（built-in NIC）	disconnected
Ubuntu20.04（Wi-Fi adapter A）	disconnected
Raspberry Pi 3B（built-in NIC）	disconnected
Raspberry Pi 3B（Wi-Fi adapter A）	disconnected
Android Smartphone	disconnected
iPhone7	disconnected
iPhone11 Pro	disconnected

dure in section 3.1. This tool can be run on the Xubuntu command line.

The equipment used in the experiment is shown in Table 1. The laptop uses a built-in NIC and a USB Wi-Fi adapter A to communicate. Windows 10 (Ver. 1903), Ubuntu 18.04 and Ubuntu 20.04 are used for the laptop A and only Windows 10 is used for the laptop B. Of the clients used in WPA2, laptop A, Android smartphone, iPhone7 and iPhone11 Pro are used as WPA3-compatible clients. For laptop A, we used only the built-in adapter on Windows 10, and the built-in adapter and Wi-Fi adapter A on Ubuntu 18.04 and Ubuntu 20.04 because of the WPA3 support status. The OS of Raspberry Pi 3B is Raspbian (May 2020).

3.2.2 Results

We investigated whether a proposal attack can be performed on each client using the tool we developed.

Tables 2 and 3 show the experimental results with the WPA2 clients. Among the clients used in the experiment, the communication could be disconnected except for the case of using the built-in adapter of laptop B and the Wi-Fi adapter A with USB connection on Windows 10. That is, we found that the DoS attack using CSA was effective on these clients. For Wi-Fi adapter A, the reason for the failure of the attack is that it only supports 2.4GHz band. IEEE802.11h, which is defined for CSA, is a standard for communication in the 5GHz band, and Wi-Fi adapter A, which only supports the 2.4GHz band, does not need to support IEEE802.11h. However, even if the same Wi-Fi adapter A is used, the attack is successful if the OS is Ubuntu. This may be because the Linux driver of Wi-Fi adapter A had CSA enabled. In fact, we checked on the command line and found that Wi-Fi adapter A supports CSA. In addition, it is thought that the CSA is disabled for the adapter built into the main body of the laptop B, because of its behavior during the attack. The detailed behavior of each client during an attack is described in Section 3.2.3.

Table 4 Results（WPA3）

Client	Connection
Windows10（built-in NIC）	disconnected
Ubuntu18.04（built-in NIC）	disconnected
Ubuntu18.04（Wi-Fi adapter A）	disconnected
Ubuntu20.04（built-in NIC）	disconnected
Ubuntu20.04（Wi-Fi adapter A）	disconnected
Android Smartphone	disconnected
iPhone7	disconnected
iPhone11 Pro	disconnected

The results for the WPA3 clients are shown in Table 4. In WPA3, all the clients used in the experiment were disconnected. All the clients used in the WPA3 experiment were also disconnected in WPA2, indicating that they are effective regardless of the security protocol.

From these results, it can be said that our proposed DoS attack using CSA can attack many clients that can use CSA even if you have the latest OS installed. This attack is an effective DoS attack against wireless LANs because an attacker can attack a target client if it can receive a beacon at the access point to which it is connected. Since the results of the experiments show that the success or failure of CSA attacks depends on the effectiveness of the CSA regardless of the OS, it is necessary to implement CSA-related measures.

3.2.3 Client behavior

We used Wireshark to find out what kind of communication each client was doing during the attack. Among the clients that were successfully attacked, we first investigated the behavior of the laptop A (without the adapter), Raspberry Pi 3B, iPhone7 and iPhone 11 Pro. When these clients received a tampered beacon, they switched to the channel indicated by the New Channel Number and started looking for an access point, and after a few seconds they returned to the original channel because they could not find an access point. We repeated the process of receiving the tampered beacon in the original channel again and switching channels for a while, then these clients timed out and disconnected from the access point.

On the other hand, among the devices that were successfully attacked, the Android smartphone could not observe communication on the channel indicated by New Channel Number even though it received a tampered beacon. Upon closer examination, we found that the Android smartphone we tested disconnects communication with the access point upon receiving a tampered beacon. In other words, unlike other clients, Android smartphones can be disconnected without sending a large number of tampered beacons.

In the same way, we observed packets using Wireshark for clients that failed the attack. As a result, we could not observe any channel switching during the attack at those clients. This is due to the fact that the client that failed the attack does not support CSA or that CSA is disabled.

Table 5 Results（Wi-Fi adapter A）

Client	Speed	Connection
Ubuntu18.04	-	disconnected
Ubuntu20.04	slow down	continued
Raspberry Pi 3B	-	disconnected

4. Further Refinement

From the results of the experiments in Chapter 3, it can be said that the proposed attack is an effective DoS attack against wireless LANs because it can reliably terminate communication with CSA-enabled clients. In this chapter, we first introduce an attack we've proposed previously [6]. It slows down the communication speed of some clients by controlling the timing of sending CSA. After that, we perform an experiment to verify the effectiveness of the attack, including the results of previous work [6].

4.1 Methods

From the results of Section 3.2, it was found that the clients used in this experiment, other than Android smartphones, try to return to the original channel several times when they are unable to communicate with the access point on the channel to be switched. However, the longer the attack time, the longer it takes to find the access point and the longer the connection times out, the more likely it is to be disconnected from the access point. Therefore, we propose a method to detect an access point on original channel by sending a CSA that returns the client to the original channel instead of leaving the client on the channel to be switched. This method prevents the client from making communication errors. As a result, it is possible to attack the client by forcing it to communicate only a little at a time, which significantly slows down the communication speed. This attack method can slow down the communication speed and impede the availability of wireless LAN communication, and since communication is uninterrupted, it can be attacked in a more natural state without being disconnected from the access point.

The specific attack methods are as follows.

(1) Let the client switch channels using the method in section 3.1.
(2) After sending a tampering beacon, attacker switches the channel just like the client.
(3) After a certain amount of time, it sends a tampered beacon with a CSA inserted to return to the original channel.
(4) Repetition of steps 1 to 3 keeps the client switching channels, which slows down the communication speed.

4.2 Experiments

In the experiment, we used WPA2 as a security protocol because the results of section 3.2 show that the attack is not dependent on the security protocol. We used a laptop A (OS: Windows 10, Ubuntu 18.04 and Ubuntu 20.04), Raspberry Pi 3B, iPhone7 and iPhone11 Pro as the client. We tested both built-in NIC and Wi-Fi adapter A on Ubuntu 18.04, Ubuntu 20.04 and Raspberry Pi 3B. Android smartphone was not included in this experiment because it disconnected from the access point without switching channels when it received a CSA.

Table 6 Results（built-in NIC）

Client	Speed	Connection
Windows10	slow down	continued
Ubuntu18.04	-	disconnected
Ubuntu20.04	-	disconnected
Raspberry Pi 3B	-	disconnected
iPhone7	slow down	continued
iPhone11 Pro	slow down	continued

The results of the experiment are shown in Table 5 and 6. When we accessed the homepage with a web browser, it took about a minute on Windows 10, Ubuntu20.04 with Wi-Fi adapter A, iPhone7 and iPhone11 Pro to load a little at a time. This may be because the communication speed of the client is reduced by the proposed method. In the case of Ubuntu18.04, Ubuntu20.04 with built-in NIC and Raspberry Pi 3B, the communication was disconnected.

From the above results, we have confirmed that Windows 10, Ubuntu20.04 with Wi-Fi adapter A, iPhone7 and iPhone11 Pro can be significantly slowed down communication speed by the proposed attack. On the other hand, on Ubuntu18.04, Ubuntu20.04 with built-in NIC and Raspberry Pi 3B, only a normal DoS attack was possible because it was disconnected after receiving CSA several times.

5. COUNTERMEASURES

In this chapter, we discuss the countermeasures against the attacks shown in the previous chapters.

5.1 Countermeasure on the Client Side

One of the countermeasures for clients is to disable CSA. However, since CSA itself is also used in normal communication, we need a method of countermeasures with CSA enabled.

The countermeasures are described below.

- To receive a CSA from the access point and resume communication on the original channel when the communication fails, and to ignore the CSA for a certain period of time.
- Limiting channel switching by CSA, for example, up to two times per minute.

By implementing these methods, we can counter the proposed attack.

5.2 Countermeasure on the Access Point Side

First, we discuss the requirements for the success of the proposed attack. There are two possible requirements for a successful attack.

- The client switches to the channel specified in the CSA after receiving the CSA.

- The access point must continue to communicate on the original channel even if the attacker sends a beacon with a CSA inserted.

When these two requirements are satisfied, the client and the access point attempt to communicate on different channels, and the attack succeeds.

Here, the tampering beacon that is sent to switch the channel of the client to be attacked can also be received by the access point in most cases. In such a case, when a tampering beacon is sent, the access point can read the information and switch the channel as the client does, so that the communication can be continued on the new channel.

However, there are some problems with this countermeasure plan. First of all, we cannot communicate with clients that are not affected by the proposed attack. In most of the access points, one channel is used for communication. If an access point switches the channel by the CSA as in the proposed method, the communication may not be possible on the original channel because channel switching does not occur in the client where the CSA is disabled. In addition, if the access points are rewritable by users, such as access points using host_apd, it is easy to implement the countermeasure, but it is not possible to implement the countermeasure for general access points that are commercially available because they cannot be modified by users.

5.3 Countermeasures Using a Repeater

In order to solve the problems of the access point side countermeasures and to counter the proposed attack, a countermeasure using a repeater based on the Channel-Based Man-in-the-Middle (MitM) concept is considered. Channel-Based MitM is a kind of man-in-the-middle attack on wireless LANs in which the client and the access point communicate on different channels and the attacker gets in between them to manipulate the communication. In this attack, an attacker set up a fake access point with the same MAC address but a different channel, and then invite clients to connect to it to become a man in the middle.

The procedure of the proposed countermeasure using this idea is shown below.

(1) Prepare a repeater with the same MAC address as the regular access point (but do not allow any communication to take place when not under a DoS attack).

(2) When a tampering beacon inserted by CSA is detected, the regular access point continues to communicate on the original channel while switching only the repeater to the channel specified by CSA.

(3) Clients with CSA disabled can communicate with the regular access point on the original channel, while clients with CSA enabled can continue to communicate through the repeater, thus disabling the DoS state.

This repeater can be easily created using modwifi, which is a tool of Channel-Based MitM, and is not restricted by the type of access point, so it is easy to introduce. However, the cost will be high since unnecessary repeaters are required in addition to the regular access points.

6. CONCLUSION

In this paper, we investigate DoS attacks using CSA, which is a signal to switch the channel of the client, and its modification, which is an attack to slow down the communication speed, by conducting more detailed verification experiments using many clients including the latest operating systems and investigating the vulnerability of each client and its behavior. The results of our experiments show that for normal DoS attacks, many clients were successfully attacked, except for a few clients where the CSA was considered to be disabled. Since the attack was successful regardless of the security protocol, we cannot feel secure even if we have the latest security protocol, WPA3, in place. As for the attack to slow down the communication speed, we succeeded in attacking about half of the clients used in the experiment. In the case of a client that failed to slow down, the communication was cut off. Although there are some limitations depending on the type of client, it is more difficult for victims to realize that they are being attacked compared to the normal DoS attacks described in the previous chapter, so the impact is the same or greater.

In addition to the proposed countermeasures on the client side, we have proposed a countermeasure on the access point side and a countermeasure that can be implemented at the user level using the repeater. Although these methods have some problems compared to the client-side countermeasure, such as the cost and the inability to support all terminals, they are easier to implement than the client-side countermeasure, and we believe that they are effective countermeasures. In the future, we will evaluate the effectiveness of the proposed countermeasures by implementing them.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number JP20K11810.

References

[1] Vanhoef, M. and Piessens, F.: "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2", *ACM SIGSAC CCS 2017*, ACM, pp. 1313–1328 (2017).

[2] URL: `https://www.eset.com/int/kr00k/`.

[3] Vanhoef, M. and Ronen, E.: "Dragonblood: A Security Analysis of WPA3's SAE Handshake", *IACR Cryptology ePrint Archive*, p. 383 (2019).

[4] Kubota, K., Isobe, T. and Morii, M.: "Evaluating Denial-of-Service Attacks against WPA3", *Computer Security Symposium 2019*, pp. 1079–1085 (2019).

[5] IEEE-SA: "802.11h-2003 - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications".

[6] Kubota, K., Isobe, T. and Morii, M.: "Effective Denial-of-Service Attacks against WPA2 and WPA3", *2020 Symposium on Cryptography and Information Security* (2020).

[7] Bellardo, J. and Savage, S.: "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", *Proceedings of the 12th USENIX Security Symposium, Washington, D.C., USA, August 4-8, 2003* (2003).

[8] Könings, B., Schaub, F., Kargl, F. and Dietzel, S.: "Channel switch and quiet attack: New DoS attacks exploiting the 802.11 standard", *2009 IEEE 34th Conference on Local Computer Networks*, IEEE, pp. 14–21 (2009).