Computer Security Symposium 2019
21 - 24 October 2019

無線LAN機器に対するDoS攻撃の実装と評価

窪田 恵人[1,a)]　五十部 孝典[2]　森井 昌克[1]

概要：2018 年に無線 LAN の新たなセキュリティプロトコルである WPA3 が発表された．WPA3 では認証パケットの改ざんを防ぐ Protected Management Frames（PMF）の必須化，認証手続きでの DoS 攻撃への対策など安全性に関わる多くの仕様が組み込まれている．しかし，2019 年に Dragonblood と呼ばれる WPA3 に対する攻撃が提案された．これは WPA3 の特定のプロトコルの脆弱性を利用した攻撃であり，DoS 攻撃やサイドチャネル攻撃などが提案されている．幸い WPA3 に対応する製品は少なく大きな影響はなかったが，今後も攻撃が提案される可能性が高く，対応機器が普及する前にその安全性を評価することが不可欠である．本稿では WPA3 の安全性評価のために無線 LAN のチャネル（周波数）切り替えに利用するパケットを用いた無線 LAN 機器に対する新たな DoS 攻撃を提案し，評価した．攻撃を実装したところ，PMF が有効となっている WPA3 に対応した端末であっても通信不可能となり，接続が切断されたことが確認できた．既存の DoS 攻撃と比較して実行が容易である点からも提案攻撃は注意が必要である．さらに，本稿では攻撃で利用した実装の問題点を整理し，攻撃への対策案についての考察も行った．

キーワード：無線 LAN，DoS 攻撃，WPA3

Evaluating Denial-of-Service Attacks against WPA3

Keito Kubota[1,a)]　Takanori Isobe[2]　Masakatu Morii[1]

Abstract: WPA3, a new wireless LAN security protocol, was announced in 2018. WPA3 incorporates many safety-related specifications such as the requirement of Protected Management Frames (PMF) to prevent forging of authentication packets and countermeasures against DoS attacks in authentication procedures. However, an attack against WPA3 called Dragonblood was proposed in 2019. This is an attack that exploits the vulnerability of specific protocols of WPA3. Fortunately, there are few products that support WPA3 and there was no significant impact, but there is a high possibility that other attacks will be proposed in the future, and it is essential to evaluate the safety of WPA3. In this paper, we proposed a DoS attack on wireless LAN devices using packets used for channel switching. As a result of implementing the attack, it was confirmed that even clients supporting WPA3 were unable to communicate. Furthermore, we organize the problems and consider the countermeasures against the attack.

Keywords: Wireless LAN，Denial-of-Service Attack，WPA3

1. はじめに

ホテルやカフェなどの商業施設，図書館や空港といった公共施設などで，無線 LAN を利用する機会が増えている．データの送受信に電波を使用する無線 LAN は盗聴が容易であり，安全なデータのやり取りには通信の暗号化が必要不可欠である．現在，無線 LAN のセキュリティプロトコル（暗号化方式）として広く使用されているのが WPA2 である．しかし WPA2 には KRACKs（Key Reinstallation AttaCKs） [1] と呼ばれる脆弱性が発見されており，より安全な方式の制定が求められていた．

2018 年に WPA2 の後継として WPA3 と呼ばれる新た

[1] 神戸大学
Kobe University
[2] 兵庫県立大学
University of Hyogo
[a)] kubota@stu.kobe-u.ac.jp

なセキュリティプロトコルが発表された．WPA3 では KRACKs で問題となっていた Management Frame の偽装を防ぐ Protected Management Frames（PMF）が標準採用された．また，パスワードの特定を防ぐために鍵生成の前に事前共有鍵から一時的なマスター鍵を生成する SAE ハンドシェイクが採用された．

WPA3 は WPA2 の後継としてさらに安全なプロトコルであると考えられていた．しかし，2019 年に Vanhoef らによって WPA3 に対する攻撃である Dragonblood が提案された [2]．Dragonblood は WPA3 の実装における脆弱性を利用した攻撃であり，サイドチャネル攻撃，ダウングレード攻撃および DoS 攻撃が提案されている．

WPA3 は発表されてから日が浅く，WPA2 から大きく使用が変更されている関係で広く普及はしていない．そのため Dragonblood を利用した被害は報告されていない．しかし，発表から 1 年以内に脆弱性が発見されたということは今後も脆弱性が見つかる可能性は高い．したがって攻撃者が脆弱性を発見して悪用する前に WPA3 の各仕様についてその安全性を正しく評価することが求められる．

我々は以前 CSA（Channel Switch Announcement）と呼ばれる信号を利用した無線 LAN に対する中間者攻撃を実装した [3]．CSA はアクセスポイントがチャネルを切り替える際にクライアントに送信する信号であり，CSA を受信したクライアントは指定されたチャネルに切り替える．この CSA を挿入した偽装ビーコンを送信しクライアントのチャネルを切り替えさせることで中間者になることに成功した．

本稿ではこの CSA を利用した DoS 攻撃を提案する．前述の通り CSA はクライアントのチャネルを強制的に切り替えさせることができる．この性質を利用してクライアントのチャネルを切り替えさせ続けることで通信が切断されることを狙う．実際に攻撃するツールを作成したうえでいくつかの無線 LAN 端末に対して攻撃可能かを調べたところ，今回実験に用いたクライアントのうち 5GHz 帯に対応するすべての端末で攻撃に成功した．攻撃者は標的となるアクセスポイントのビーコンを受信することができれば攻撃可能となる．すなわち提案攻撃は攻撃のハードルが低く容易に実行可能な攻撃であるといえる．さらに，本稿では攻撃を受けた際のログから実装上の問題点を調べた．そして問題点をもとにして攻撃の対策方法について考察した．

2. 予備知識

本章ではまず初めに無線 LAN 機器における通信開始までの手続きとセキュリティプロトコルについて述べる．その後，既存の DoS 攻撃として Deauthentication 攻撃と WPA3 の脆弱性として提案された Dragonblood について述べる．最後に本稿で提案する DoS 攻撃で利用した Channel Switch Announcement（CSA）について述べる．

2.1 アクセスポイントへの接続

クライアントが無線 LAN を利用して通信を開始するためには接続手順に従ってアクセスポイントと接続しなければならない．接続手順は 3 つの手続きからなる．本節ではこれら 3 つの手続きについて説明する．また，本稿で提案する DoS 攻撃では 1 つ目の手続きで用いられるビーコンを利用するため，それについても説明する．

まず最初の手続きとして，クライアントがアクセスポイントと接続するためには通信可能なアクセスポイントを見つける必要がある．これには静的スキャンと動的スキャンの 2 種類の方法がある．アクセスポイントは通信の混雑を避けるために 2.4GHz 帯/5GHz 帯ともにいくつかのチャネル（周波数）に分かれて通信を行っている．また，アクセスポイントは自分の存在を周辺のクライアントに知らせるために自分が使用しているチャネルでビーコンと呼ばれるパケットを定期的に送信している．ビーコンにはアクセスポイントの SSID（Service Set IDentifier）や暗号化方式などの情報が含まれている．静的スキャンでは，クライアントは様々なチャネルでビーコンを受信していくことでアクセスポイントを見つける．動的スキャンではクライアントはプローブ要求と呼ばれる呼びかけをブロードキャストで送信する．プローブ要求を受信したアクセスポイントはそのクライアントに対してプローブ応答を送信する．プローブ応答にはビーコンと同じような情報が含まれており，これによってクライアントはアクセスポイントの存在を認知する．

次にクライアントは見つけたアクセスポイントの中から接続したいアクセスポイントを選択し認証手続きに入る．現在では認証手続きは形だけのもので特に情報などは交換されない．ただし，クライアントが WPA3 を用いて通信する際は認証手続きの前に SAE ハンドシェイクによって事前共有鍵から一時的なマスター鍵を生成する．

その後，アソシエーション手続きに入る．ここでもビーコンやプローブ応答と同じような情報やさらに詳細な通信方式の情報などがアクセスポイントからクライアントに送られる．接続しようとしているアクセスポイントが WPA2 や WPA3 などのセキュリティプロトコルを利用している場合はアソシエーション手続きの後に 4 ウェイハンドシェイクと呼ばれる鍵生成・共有プロトコルによって暗号鍵の生成および共有を行うことで接続が完了する．そうでない場合はアソシエーション手続きによって接続が完了する．

2.2 無線 LAN のセキュリティプロトコル

無線 LAN 通信は電波を用いて通信をするため盗聴が容易である．攻撃者によって盗聴され情報が漏れることを防ぐためにも通信の暗号化が不可欠である．無線 LAN では通信の暗号化について定めたセキュリティプロトコルがいくつか存在する．現在，主に用いられているのが 2004

年に発表された WPA2（Wi-Fi Protected Access 2）である．WPA2 では接続手順のアソシエーション手続きの後に 4 ウェイハンドシェイクによって鍵の生成と共有をし，標準では AES 暗号をカウンターモードで利用して通信を暗号化する．WPA2 は発表以来安全なプロトコルとして広く利用されてきた．しかし 2017 年に KRACKs と呼ばれる 4 ウェイハンドシェイクの脆弱性を利用した攻撃が提案された [1]．我々は以前の研究で KRACKs が実環境上で大きな影響を与えることはないということを示した [4]．しかし，脆弱性が存在しているのは確かであり新たなセキュリティプロトコルが求められていた．

2018 年に Wi-Fi Alliance は WPA2 の後継である WPA3 を発表した．WPA3 では認証手続きの前に SAE ハンドシェイクと呼ばれる鍵の生成プロトコルを採用し，4 ウェイハンドシェイクで用いられる鍵を一時鍵にすることで KRACKs で指摘された問題点を解決し，安全性を向上させたといわれている．また，WPA3 ではアソシエーション手続きや 4 ウェイハンドシェイクで利用されるパケットに対して認証をする PMF（Protected Managed Frames）を標準採用し既存の攻撃に対して対策がなされている．さらに，計算コストがかかる SAE ハンドシェイク内の処理を悪用した DoS 攻撃への対策として Cookie を利用した認証がなされている．

2.3 無線 LAN に対する DoS 攻撃

無線 LAN に対する DoS 攻撃は IEEE802.11 の制定以来多くの種類が提案されてきた．なかでも有名な攻撃が Deauthentication 攻撃である [5]．Deauthentication 攻撃は無線 LAN の Management Frame の一つである Deauthentication フレームを利用した攻撃である．Deauthentication フレームは無線 LAN の認証手続きに失敗した場合にクライアントとアクセスポイントが切断するために利用される．Deauthentication フレームは暗号化されておらず偽装可能であった．Deauthentication 攻撃は Deauthentication フレームを偽装して標的のクライアントとアクセスポイントに送信することでクライアントをアクセスポイントから切断させる攻撃である．ただし，WPA3 を利用した端末では PMF が標準採用されているためこの攻撃の影響を受けることはない．しかし，WPA3 を利用した端末に対しても攻撃可能な DoS 攻撃が Dragonblood の一つとして提案された [2]．Dragonblood は 2019 年に Vanhoef らによって発表された WPA3 の脆弱性およびそれを利用した攻撃の総称である．Dragonblood は大きく 3 種類の攻撃に分けることができる．まず SAE ハンドシェイクの処理を利用したアクセスポイントに対する DoS 攻撃．次に Transition-mode の脆弱性を利用したダウングレード攻撃．最後の一つが SAE ハンドシェイクの脆弱性を利用したサイドチャネル攻撃である．本節では DoS 攻撃の概要について述べる．SAE ハンドシェイクは楕円曲線を利用して事前共有鍵から一時的なマスター鍵を生成するプロトコルである．この鍵生成は非常に計算コストのかかる処理であることが知られている．2.2 節で述べたように WPA3 では Cookie を利用することで攻撃者がパケットの偽装によって鍵生成を故意に繰り返させることを防いでいる．しかし，この Cookie は偽装可能な MAC アドレスをもとにして作成されるため攻撃者は MAC アドレスを偽装するだけで Cookie を作成することが可能である．したがって攻撃者は偽装パケットによって鍵生成を繰り返させ，アクセスポイントの CPU 使用率を上昇させることで DoS 攻撃が可能である．

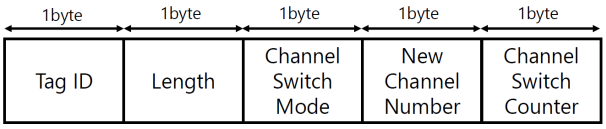

図 1 CSA のフォーマット

2.4 Channel Switch Announcement

CSA（Channel Switch Announcement）はアクセスポイントがクライアントに対して通信に使用するチャネルの変更を通知する信号であり，IEEE802.11h で定義されている [6]．アクセスポイントは 5GHz 帯で通信中に使用しているチャネルで衛星通信などの電波を受信した場合，別のチャネルに移動しなければならない．その際に通信を途切れさせることなくチャネルの変更を行うためにアクセスポイントは CSA を送信しチャネルの変更を通知する．CSA を受け取ったクライアントはチャネルを変えて通信を続けるか別のアクセスポイントに接続するかを選択するかを選択し，通信を続ける場合はアクセスポイントのチャネルが変わり次第チャネルを切り替えて通信を再開する．この際，2.1 節のような接続手順を行う必要はなく移動先のチャネルですぐに通信が再開される．CSA はビーコンなどいくつかのパケットに追加可能である．ビーコンにおいて CSA はオプション領域に追加され，暗号化や改ざん検知は行われない．

CSA のフォーマットを図 1 に示す．Tag ID はオプション情報を識別するための ID であり CSA では 37 になる．Length は CSA の情報が入っている部分の長さであり CSA では 3 になる．Channel Switch Mode は CSA 受信後チャネルが移動するまでに通信を続けるかを指定する．1 がセットされている場合はクライアントはチャネル移動まで通信を停止する．0 がセットされている場合はチャネル移動までも通信を続ける．New Channel Number には移動先の新しいチャネルが記されている．Channel Switch Counter はチャネル移動までに送信されるビーコンの数が記されている．ビーコンを送信するたびにディクリメントされていき，0 になるとチャネルの移動が行われる．

3. CSA を用いた DoS 攻撃

2.3 節で述べたように，無線 LAN に対する DoS 攻撃は様々な手法が提案されている．我々はこれまでに WPA2 で採用されている 4 ウェイハンドシェイクのパケットが偽装できることを利用した DoS 攻撃を提案した．しかし，2.2 節で述べたように WPA3 では PMF が標準採用されており 4 ウェイハンドシェイクの偽装が困難となっている．そこで，本稿では WPA3 でも実行可能な無線 LAN に対する DoS 攻撃として CSA を用いた DoS 攻撃を提案する．3.1 節では提案した攻撃の攻撃手法について述べる．3.2 節では実際に攻撃を実装したうえで，WPA2 対応クライアントと WPA3 対応クライアントのそれぞれに対して攻撃可能であるかを調べた．3.3 節では実験結果を踏まえたうえで既存の DoS 攻撃との比較および評価を行う．

表 1　実験に使用した機器

攻撃者	Xubuntu(VMware) Wi-Fi アダプタ A
アクセスポイント	モバイルルータ（WPA2） 業務用アクセスポイント（WPA3）
クライアント（WPA2）	Windows10（本体内蔵アダプタ） Windows10（Wi-Fi アダプタ B） Ubuntu18.04（本体内蔵アダプタ） Ubuntu18.04（Wi-Fi アダプタ B） Android スマートフォン iPhone7
クライアント（WPA3）	Windows10（本体内蔵アダプタ） Ubuntu18.04（本体内臓アダプタ） Ubuntu18.04（Wi-Fi アダプタ A） Android スマートフォン

3.1　攻撃手法

WPA3 では PMF の標準採用によって通信開始以降のパケット改ざんが難しくなった．しかし，通信開始以前に送信されるビーコンやプローブ要求・応答といったパケットは依然として改ざん可能である．すなわち，WPA3 が採用されていたとしてもビーコン内に含まれている CSA などの信号を改ざんした攻撃を防ぐことはできない．そこで本稿では CSA を挿入したビーコンを偽装することで WPA3 に対しても攻撃可能な DoS 攻撃を提案する．CSA を採用しているクライアントは CSA を受け取った場合，実際に移動先のチャネルにアクセスポイントが存在するかを確かめる前にチャネルを切り替える．チャネルを切り替えた後にアクセスポイントが見つからない場合の動作はクライアントの実装によって異なり，元のチャネルに戻る場合とアクセスポイントとの通信を切断したうえでスキャンからやり直す場合がある．いずれの場合であってもチャネルの切り替えおよびアクセスポイントの探索をしている間は通信が停止する．この仕様を利用し，アクセスポイントの存在しないチャネルに切り替えさせる CSA を挿入したビーコンを送信し続けることで DoS 攻撃が可能となる．なお本攻撃はブロードキャストで送信されるビーコンを偽装するという性質上，攻撃者の偽装ビーコンが届く範囲のすべてのクライアントが影響を受ける．

ここからは具体的な攻撃の流れについて述べる．まず攻撃者は標的となるアクセスポイントのビーコンを受信し保存する．次に攻撃者は保存したビーコンのオプション領域に CSA を挿入する．ここで挿入する CSA は Channel Switch Mode を 1，New Channel Number を実際のアクセスポイントと異なるチャネル，Channel Switch Counter を 0 に設定しておく．Channel Switch Mode を 1 に設定しておくことでクライアントはチャネル切り替えまで通信を停止し，正規チャネルからのパケットを無視する．Channel Switch Counter を 0 に設定しておくことでクライアントは CSA 入りのビーコンを受け取り次第チャネルを切り替える．これら 2 つの動作の組み合わせによってクライアントは CSA 入りのビーコンを受け取った際に正規アクセスポイントからの通信に関わらず即座にチャネルを切り替える．攻撃者は CSA を挿入した偽装ビーコンを通常のビーコンと同じ間隔（一般的には 100ms 間隔）で送信し続けることで DoS 攻撃が可能となる．なお，攻撃者は偽装ビーコンのタイムスタンプも変更する必要がある．

3.2　評価実験

実際に 3.1 の手順で攻撃するツールを作成し攻撃可能であるかを調べる評価実験を行った．攻撃対象は WPA2 と WPA3 のクライアントとし，アクセスポイントも WPA2 と WPA3 に対応するものを用いた．

3.2.1　実験機器

攻撃ツールは我々が以前作成した CSA を用いた中間者攻撃を行うためのツールの一部を書き換えて作成した．このツールは Vanhoef らによって公開されているチャネルベース中間者攻撃を行うツール [7] を改良したものである．チャネルベース中間者攻撃と CSA を用いた中間者攻撃はともにクライアントとアクセスポイントの間に入って通信の仲介をする攻撃である [8] [9]．今回の攻撃ではクライアントに偽装したビーコンを送信するだけでよいため上記ツールのうちクライアントと通信する部分のみ利用する．なお，ツールは Xubuntu のコマンドライン上で実行可能である．

実験で使用した機器は表 1 の通りである．攻撃者は VMware 上で立ち上げた Xubuntu であり，偽装したビーコンを送信するために USB 接続の Wi-Fi アダプタ A を接続する．アクセスポイントは WPA2 に対応するものとして

表 2　実験結果（WPA2）

クライアント	通信可否	再接続
Windows10（本体内蔵アダプタ）	切断	自動
Windows10（Wi-Fi アダプタ B）	可能	-
Ubuntu18.04（本体内蔵アダプタ）	切断	自動
Ubuntu18.04（Wi-Fi アダプタ B）	可能	-
Android スマートフォン	切断	手動
iPhone7	切断	手動

モバイルルータを使用し，WPA3 に対応するものとして業務用アクセスポイントを使用した．なお，業務用アクセスポイントは WPA2 にも対応しているが WPA2 と WPA3 の併用モードでは一部クライアントが接続できなかったため WPA3 のみ使用するモードで実験を行った．WPA2 を利用したクライアントとしては Windows10 のノートパソコン，Ubuntu18.04 のノートパソコン，Android スマートフォン（Android6.0.1），iPhone7（iOS10.2.1）を用いた．ノートパソコンは本体内蔵の Wi-Fi アダプタの他に USB 接続の Wi-Fi アダプタ B も利用した．WPA3 を利用したクライアントとしては Windows10 のノートパソコン，Ubuntu18.04 のノートパソコン，Android スマートフォン（AndroidQ beta4）を用いた．WPA3 では各機器の WPA3 への対応状況から Windows10 のノートパソコンでは本体内蔵アダプタのみ，Ubuntu18.04 では本体内蔵アダプタの他に Wi-Fi アダプタ A も利用した．

3.2.2　実験結果（WPA2）

作成したツールを用いて WPA2 に対応した機器に対して CSA を用いた DoS 攻撃が可能かを調べた．あらかじめ攻撃対象となるクライアントをアクセスポイントに接続させ，ツールを用いて攻撃を実行しネットワークに通信が切断されるかを調べた．さらに通信が切断された場合は自動的に再接続されるかも調べた．

実験の結果を表 2 に示す．実験に用いたクライアントのうち本体内蔵アダプタを用いた Windows10, Ubuntu18.04, Android スマートフォン，iPhone7 においては通信の切断が確認できた．特に Android スマートフォンと iPhone7 においては攻撃を止めた後も自動でアクセスポイントに再接続されなかったため設定画面から手動でアクセスポイントを選びなおして再接続する必要があった．Wireshark を用いて通信パケットを観測したところ，いずれのクライアントにおいても攻撃開始後すぐに正規のチャネルと別のチャネルで通信を続けようとしていることが観測された．つまり，攻撃後すぐにチャネルが切り替えられたことがわかる．一方，USB 接続の Wi-Fi アダプタ B を利用した場合は Windows10，Ubuntu18.04 の両方で攻撃に失敗した．これは Wi-Fi アダプタ B が 2.4GHz 帯の通信にしか対応していないことが原因であると考えらえれる．CSA について定めている IEEE802.11h は 5GHz 帯での通信についての規格であり，2.4GHz 帯にしか対応していない Wi-Fi アダプタ B は IEEE80.11h に対応する必要がない．実際にコマンドライン上で Wi-Fi アダプタ B が CSA に対応しているか調べたところ未対応であることが分かった．つまり，WPA2 においてはクライアントが 5GHz 帯に対応している場合は攻撃に成功すると考えられる．近年の無線 LAN 対応端末は 5GHz 帯に対応しているものがほとんどであり，近年発売された端末であればほぼすべての端末で攻撃に成功する．

表 3　実験結果（WPA3）

クライアント	通信可否	再接続
Windows10（本体内蔵アダプタ）	切断	自動
Ubuntu18.04（本体内蔵アダプタ）	切断	自動
Ubuntu18.04（Wi-Fi アダプタ A）	切断	自動
Android スマートフォン	切断	手動

3.2.3　実験結果（WPA3）

WPA3 に対応する端末に対しても作成したツールを用いて同様の実験を行った．実験の結果を表 3 に示す．WPA3 の実験においては WPA2 の場合と異なりすべてのクライアントが 5GH z 帯に対応していいため，すべてのクライアントで攻撃に成功した．つまり，CSA を用いた DoS 攻撃は使用されているセキュリティプロトコルに関わらず実行可能であることがわかった．また Android スマートフォンでは攻撃中止後は 3 分ほど再接続不可能であった．これは Android スマートフォンの Wi-Fi ドライバの使用によると考えられる．さらに Ubuntu18.04 では無線 LAN 接続のために標準で採用されている wpa_supplicant [10] を利用したが，Dragonblood の対策がなされた後の最新バージョン（wpa_supplicant2.8）でも攻撃に成功した．

3.3　既存攻撃との比較

3.2 節の結果を踏まえて 2.3 節で述べた既存攻撃と提案攻撃を比較する．まず，Management Frame を利用する Deauthentication 攻撃や WPA3 に対する Dragonblood といった既存攻撃と提案攻撃との違いは攻撃対象が広いことである．提案攻撃は 5GHz 帯に対応してさえいればほぼすべての端末で実行可能である．しかし，Deauthentication 攻撃は PMF が有効となっている WPA3 対応の端末などでは攻撃不可能であり，Dragonblood は逆に WPA3 に対応していない場合は攻撃不可能である．この点から提案攻撃は既存の DoS 攻撃に比べて多くのクライアントに対して影響があるといえる．

次に，提案攻撃は攻撃実行のハードルが低いことが挙げられる．Dragonblood は WPA3 の SAE ハンドシェイクが行われるタイミングでのみ実行可能であり，任意の端末をアクセスポイントに接続させる必要がある．また，Cookie

の偽装のために通信トラフィックを観察して秘密情報のヒントを得なければならず容易に実行可能であるとは言えない．提案攻撃は 3.1 で述べたようにビーコンの受信と CSA の挿入のみで攻撃可能である．すなわち，Dragonblood に比べて容易に攻撃を実行可能であるといえる．

さらに，提案攻撃はアクセスポイントに接続しているすべての端末の通信が切断されるという点で単体のクライアントを狙う Deauthentication 攻撃と差別化される．

4. 攻撃への対策

3 節の実験結果および既存攻撃との比較から CSA を用いた DoS 攻撃は無線 LAN に対する DoS 攻撃としては攻撃難易度が低く，影響範囲が広いため対策が不可欠な攻撃であるといえる．そこで，本節では実際に攻撃を行った際のログからクライアントの問題点を指摘し対策案を考える．なお，本節では 3 で用いたクライアントのうち wpa_supplicant を利用した Ubuntu18.04 のログを利用する．4.1 節ではログを参考にクライアントの動作を整理する．4.2 節ではログを参考にして対策案を示す．

4.1 クライアントの動作

まず，Ubuntu における無線 LAN ソフトウェアの構成について述べる．Linux では無線 LAN 接続のためにユーザースペース上では wpa_supplicant と iw，カーネル上では cfg80211 や mac80211 などが動作している．wpa_supplicant は主に認証手続き，アソシエーション手続きや IEEE802.11i で定められたセキュリティプロトコルを用いた認証などアクセスポイントとの接続に関する部分を担当している．また cfg80211 はチャネルなどのハードウェア関連の制御やイベントが起こった際のフラグ管理を行っている．wpa_supplicant はカーネル上のソフトウェアを制御する役割も担っており，cfg80211 と wpa_supplicant は密接に関係している．wpa_supplicant のログを見ることで cfg80211 の動作も確認可能であり無線 LAN 関連の動作を確認することが可能である．そこで，本節では wpa_supplicant のログから攻撃を受けた際のクライアントの動作を調べた．

攻撃が実行された後，CSA が挿入された偽装ビーコンを受信した cfg80211 は CSA のフラグ（NL80211_CMD_CH_SWITCH_NOTIFY）を立てる．また，cfg80211 は受信した CSA の New Channel Number を読み取って移動先のチャネルを調べる．そして cfg80211 はこれらの情報を wpa_supplicant 側に渡す．wpa_supplicant は CTRL-EVENT-CHANNEL-SWITCH と呼ばれるチャネル切り替えの状態に遷移し，カーネル側に対してチャネルの切り替えを命令する．チャネルの切り替え実行後は新たなチャネルで通信の継続を試みる．しかし cfg80211 は新たなチャネルで接続しているアクセスポイントのビーコンを受信できないためビーコンを見失ったフラグ（NL80211_CMD_NOTIFY_CQM）を立てて wpa_supplicant に情報を渡す．wpa_supplicant は cfg80211 からの情報を受けて CTRL-EVENT-BEACON-LOSS と呼ばれる状態に遷移し，待機する．その後一定時間待機したのちにビーコンが受信できなかった場合，cfg80211 は再びフラグを立てて wpa_supplicant に情報を渡す．二度目のフラグを立てた時点で cfg80211 はアクセスポイントと切断するために NL80211_CMD_DEL_STATION および NL80211_CMD_DEAUTHENTICATE のフラグによって wpa_supplicant を切断モードに移行させる．wpa_supplicant は Deauthentication フレームを送信することでアクセスポイントと切断する．ただし，これは内部的な処理であり実際にはチャネルが異なるため Deauthentication フレームは届かずアクセスポイント側は切断を認知しない．

切断後はスキャンモードに移行して接続手順の静的および動的スキャンからやり直す．ここで，クライアントは元のチャネルで接続していたアクセスポイントを再度発見する．wpa_supplicant は自動的に元のチャネルでアクセスポイントとの接続手順を開始し，認証手続きやアソシエーション手続きを行う．しかし接続手順の途中で CSA の処理が割込みし再びチャネルの切り替えが起こり，前述の動作と同じ流れでアクセスポイントと切断される．その後もクライアントはスキャン，接続手順，切断を繰り返してしまい通信ができなくなる．

4.2 対策案

4.1 節で述べた攻撃を受けたクライアントの動作をもとに実装上の問題点と対策案について考察する．クライアントの実装上の問題としてまず挙げられるのは CSA を受信してチャネルを切り替えた後の動作が正確に決められていない点である．現在の仕様では CSA を受信してチャネルを切り替えた後にビーコンを受信できなかった場合は CSA が原因であると判断されない．クライアントは単純に何らかの理由でアクセスポイントが消失してしまったと判断して切断したのちにスキャンからやり直してしまう．また，再接続の際に一度 CSA を受信したクライアントが元のチャネルで通信を行っており再び CSA が挿入されたビーコンを送信してきても素直に CSA に従ってチャネルを切り替えることも問題である．本来であれば CSA を送信したアクセスポイントは必ずチャネルを切り替えるので元のチャネルで通信をしていることはありえない．さらに，そこから再び CSA を送信するということは明らかに通常の動作では考えられない．したがってこのようなアクセスポイントは悪意のあるものだと判断されるべきである．

これらの問題点をもとに CSA を用いた DoS 攻撃の対策として次の 2 つの方法が考えられる．

(1) 二度目の CTRL-EVENT-BEACON-LOSS の後に

Deauthentication フレームを送信するのではなくチャネルを戻すようにする

(2) 一度 CSA を送信したアクセスポイントからの CSA は一定時間無視する

これら 2 つの方法を組み合わせることでチャネル切り替え後の通信エラーを一定時間で抑えることができ，その後一定時間は通信エラーを引き起こさせないことが可能となる．また，日本においてはベンダーがスループットの上昇のために意図的に CSA を利用している場合など一部の場合を除いて，CSA は利用されないことが多い．そこで一度 CSA を送信したうえで通信が切断されたアクセスポイントをブラックリストに記憶しておき，そのアクセスポイントからの CSA は永久定期に無視するといった対策も考えられる．

5. まとめ

本稿では，クライアントのチャネルを切り替えさせる信号である CSA を利用した DoS 攻撃を提案した．実際に提案手法を用いて DoS 攻撃を行うツールを作成し，攻撃の可否についていくつかのクライアントで調査した．結果として，WPA2 および WPA3 のどちらで通信をしていた場合であってもクライアントが CSA に対応していれば攻撃に成功した．なお 5GH z 帯での通信が可能な場合は基本的に CSA に対応しているため，5GHz 帯に対応する端末が増えた近年では多くの端末で攻撃が可能であるといえる．また，クライアントの実装にもよるが攻撃を停止した後も見かけ上はアクセスポイントに接続しているが通信ができない場合があった．このようなクライアントに対しては手動でアクセスポイントに再接続させる必要があり，より大きな影響を与える．

DoS 攻撃はパスワードを特定したり，通信を復号するような攻撃に比べると影響が小さく軽視されがちである．しかし，DoS 攻撃によって通信を妨害しつつ Evil Twin 攻撃に繋げるなど他の攻撃と組み合わせることで通信データの流出など大きな被害が出る可能性は常に存在する．また本稿で提案した攻撃はアクセスポイントに接続しているすべてのクライアントが通信不可能となる．したがって，攻撃者自身が攻撃の影響を受けないように CSA を無効化した端末を利用することで通信を独占してスループットを上昇させることも可能である．カフェなどの屋外での公衆無線 LAN の利用が増えている現在ではこのように容易にアクセスポイントの通信を不可能にできてしまうことは大きな問題である．以上のように提案攻撃は直接パスワードなどの秘密情報は流出しないが，無線 LAN が普及している現代社会においては影響は大きなものとなるため対策されることが望まれる．

謝辞

本研究にあたり，多くのご助言をいただいた NTT セキュアプラットフォーム研究所の藤堂洋介氏に感謝の意を表する．

参考文献

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

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

[3] 窪田恵人，小家　武，藤堂洋介，五十部孝典，森井昌克：“Wi-Fi 機器に対する中間者攻撃の実装と考察”，暗号と情報セキュリティシンポジウム論文集 (2019).

[4] 窪田恵人，小家　武，船引悠生，藤堂洋介，五十部孝典，森井昌克：“実環境を想定した WPA2 に対する KRACKs の評価実験”，コンピュータセキュリティシンポジウム 2018 論文集，pp. 561–568 (2018).

[5] 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).

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

[7] URL: `https://github.com/vanhoefm/modwifi`.

[8] Vanhoef, M. and Piessens, F.: “Advanced Wi-Fi attacks using commodity hardware”, *ACSAC 2014*, ACM, pp. 256–265 (2014).

[9] Vanhoef, M., Bhandaru, N., Derham, T., Ouzieli, I. and Piessens, F.: “Operating Channel Validation: Preventing Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks”, *ACM Conference on Security & Privacy in Wireless and Mobile Networks, WiSec , 2018*, ACM, pp. 34–39 (2018).

[10] URL: `https://w1.fi/wpa_supplicant/`.