Vol.2019-IOT-44 No.42
2019/3/8

WPA2-Enterpriseモードの APに対する フレーム注入を用いた負荷試験手法

竹田 智洋[1,a)]　大平 健司[2,b)]

概要：大学や企業などの組織において，WPA2-Enterprise モードの無線 LAN アクセスポイント (以下，AP) が設置され，多数の無線 LAN クライアント（以下，端末）が接続されている．無線 LAN の帯域や AP の性能限界から無線 LAN 環境の更新が求められた際，既存環境や新環境に対し負荷試験を行い，性能を評価する必要が生じる．提案手法では IEEE 802.11 Frame Injection を用い，複数の端末の接続処理をエミュレートすることにより，複数の端末が一斉に特定の AP に対し接続を試みた際の，認証時の負荷を再現した．また評価実験では，提案手法による負荷と実際に複数端末を接続した際の負荷を比較・評価した．

キーワード：無線 LAN，負荷試験，フレームインジェクション，WPA2 エンタープライズ

A Frame Injection-based Stress Test Method to an AP in WPA2-Enterprise Mode

Abstract: There are many APs in WPA2-Enterprise mode in organizations, and many Wi-Fi clients are connected. When updating Wi-Fi environment because of a shortage of Wi-Fi bandwidth and a performance limit of the AP, we need to perform a stress test on the existing Wi-Fi environment and the new one. By using IEEE 802.11 frame injection, our proposed method emulates the connection processing of multiple clients. Therefore it generates the load like when many clients try to connect to the AP all at once. In the evaluation, we compared the load by the proposed method and the load when actually connecting many clients.

Keywords: IEEE 802.11，Stress test，IEEE 802.11 Frame Injection，WPA2-Enterprise

1. はじめに

ノートパソコンやスマートフォン，タブレット PC 等の持ち運び可能なコンピュータの普及により，無線によるデータ通信が一般的となっている．これらの機器は，企業や大学等の組織内で使用する際，組織が設置した無線 LAN アクセスポイント (以下，AP) を経由して，組織内のネットワークと通信する．デジタルコンテンツの多様化・高品質化により，コンピュータが行う通信は年々増加している．結果として，組織内において無線 LAN の帯域や各種ネットワーク機器のリソースが逼迫しており，無線 LAN 環境を増強する必要に迫られている．無線 LAN の帯域や AP の性能限界から，無線 LAN 環境の更新が求められた際，既存環境や新たな環境に対し, 様々な負荷試験を行い，多様な視点で性能を評価する必要が生じる．

本研究では，無線 LAN 環境として，WPA2 に対応し暗号化プロトコルとして CCMP を用いる AP を想定する．また，AP は Enterprise モードで使用され，認証に PEAP を用いるものを想定する．

本研究では，認証時の通信に着目する．認証時の通信は，無線 LAN 環境に対し，バックエンドの認証サーバを含めて通信を行う．それゆえ，多数の無線 LAN クライアント（以下，端末）を用いて，AP に対し接続と切断を繰り返すことにより，認証サーバを含めた無線 LAN 環境に負荷を

[1] 徳島大学大学院先端技術科学教育部
Guraduate School of Advanced Technology and Science, Tokushima University
[2] 徳島大学情報センター
Center for Administration of Information Technology, Tokushima University
[a)] takeda@na3alf6.info
[b)] ohira@tokushima-u.ac.jp

掛けることが可能である．この負荷試験は，多数の端末を必要があり，費用面で高コストであるといったデメリットが存在する．このデメリットを解決する使用端末数の削減を本研究の目的とする．

したがって，2 章では様々な負荷試験と本研究が対象とする無線 LAN 環境・負荷試験について述べる．3 章では使用端末数の削減のため，無線 LAN インターフェイスの仮想化に関する先行研究・関連技術を述べる．4 章では IEEE 802.11 Frame Injection（以下，フレーム注入）[1] を用いた負荷試験手法を提案する．5 章では提案手法を用いて構築した負荷試験システムと，そのシステムを用いて行った評価実験について述べ，6 章で結論を述べる．

2. 無線 LAN 環境に対する負荷試験

2.1 負荷試験の分類

無線 LAN 環境に対する負荷試験は，負荷をかける対象により複数の手法が存在する．無線 LAN の帯域や，AP からネットワーク上流に負荷を掛ける場合は，端末が大量の通信を行うスループットテストが行われる [2]．端末が行う通信は，無線 LAN フレームでラップされるため，通信内容は問われない．よってスループットテストは，iPerf 等のネイティブアプリケーションから，スピードテストサイト [3] のようなウェブアプリケーションまで，様々な種類のアプリケーションが存在する．

AP に複数の端末が接続される状況を想定し，複数の端末で大量の通信を行うスループットテストも存在する．クロアチアの公的機関である CARNet (Croatian Academic and Research Network) が 2015 年に行ったスループットテストでは，端末の台数を 13 台，23 台，36 台，60 台と変化させる．最後に 36 台の端末を分散させて設置する．それぞれのケースで TCP のスループットを測定し，性能評価を行っている [4]．

WPA/WPA2 の Enterprise モードを用いる無線 LAN 環境では，認証サーバである RADIUS サーバが存在する．認証時，サプリカントである無線 LAN クライアントからの要求に応じ，オーセンティケータである AP は RADIUS サーバと通信を行い接続の可否を決定する (図 1)．

RADIUS サーバに負荷を掛ける場合は，Apache JMeter[*1]に Radius Jmeter Plugin[*2]を組み合わせる手法や，Apache JMeter に Radius プロトコルを実装する手法 [5] が用いられる．これらは，オーセンティケータの認証サーバに対する通信をエミュレートしている．

2.2 想定する無線 LAN 環境

本研究では，WPA2-Enterprise に対応した無線 LAN 環境を想定する．暗号化プロトコルは WPA2 で標準の CCMP を，認証プロトコルとして PEAP を用いるものを想定する．

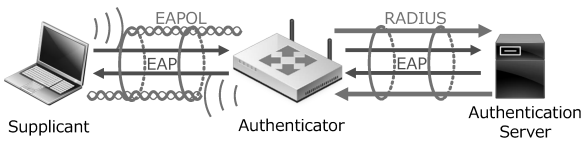

図 1　WPA/WPA2-Enterprise における IEEE 802.1X 認証

PEAP は RFC や仕様書が存在せず，インターネットドラフトがデファクトスタンダードとなっている．複数のバージョンが存在しているが，主に PEAPv0 と PEAPv1 が使用されている．PEAPv0 は Windows XP SP1 以降の Windows に搭載されており [6]，draft-kamath-pppext-peapv0-00[7] で定義されている．また，PEAPv1 は draft-josefsson-pppext-eap-tls-eap[8] のバージョン 0 から 5 を元に定義されている．これらは PEAP の外部認証の仕様であり，TLS 通信の確立後に行われる内部認証の仕様は規定されていない．内部認証は複数種類存在するため，PEAP のバージョンと内部認証により，多数の認証方式が存在する．Wi-Fi Alliance は WPA/WPA2 それぞれに対し，PEAPv0/EAP-MSCHAPv2，PEAPv1/EAP-GTC の組み合わせを認定している．本研究ではより普及している PEAPv0/EAP-MSCHAPv2 が使用される環境を想定する．

2.3 本研究が対象とする負荷試験

PEAP 等の IEEE 802.1X 認証を用いる無線 LAN 環境において，接続完了後の通信と認証時の通信は，異なる経路で通信される．前者は，端末から AP を経由し通信先のサーバと通信が行われるため，無線 LAN の帯域や AP，ネットワーク上流への経路に対して負荷を掛ける．一方で後者は，バックエンドの認証サーバに対して通信が行われるため，認証サーバを含めた無線 LAN 環境に負荷を掛ける．

Enterprise モードで使用される AP は，鍵生成・鍵交換 [9] 後，Personal モードで使用される AP と同様に，やり取りされた鍵を用いて通信の暗号化・復号処理を行う．よって，接続完了後の通信を負荷試験に用いた場合，Personal モードで使用される AP に対する負荷試験と同等のものになる．

そこで，本研究では認証時の通信に着目する．多数の端末を用いて AP に対し接続と切断を繰り返すことにより，認証時の通信を並行して大量に生成し，認証サーバを含めた無線 LAN 環境に負荷を掛ける．認証時の負荷は，CCMP の暗号化・復号と異なり，ハードウェアアクセラレーションが効きづらい処理である．組織内において，始業直後や講義開始時の AP に対する一斉接続によるバーストトラヒックに対する一定の評価基準になると考えられる．

しかしながら，多数の端末を使用するこの負荷試験は，端末を用意する費用の面で高コストである．この問題に対

[*1] https://jmeter.apache.org/
[*2] https://sourceforge.net/projects/radiusjmeterplugin/

して本研究では，無線 LAN インターフェイスの仮想化を用いて，使用する物理無線 LAN モジュールを削減することにより解決する．

3. 無線 LAN インターフェイス仮想化手法

無線 LAN インターフェイスの仮想化手法は，大別して以下の 3 種類の手法が存在する．

- ソフトウェア面からの解決手法
- ハードウェア面からの解決手法
- 両面からの解決手法

3.1 ソフトウェア面からの解決手法

ソフトウェアにより実現する無線 LAN インターフェイスの仮想化は，OS やデバイスドライバ，VMM (Virtual Machine Monitor) 等により, デバイスモデル (図 2) を作成することにより実現される．ソフトウェア面からの仮想化の代表例として，mac80211 サブシステムに実装されている，Virtual Interfaces[10] と呼ばれる機能が存在する．この機能は PHY device と呼ばれる物理層でのインターフェイス上で，仮想的に複数のインターフェイスを作成する．Virtual Interfaces は，使用する無線 LAN モジュールにより大きく制限がかかる可能性がある．無線 LAN モジュールに搭載されるアンテナ数分しか仮想インターフェイスを作成できない場合や，作成してもサプリカントとして動作出来ない場合，Ad-Hoc モードでしか利用できない場合が存在する．SDN との連携を視野に，無線 LAN 接続のシミュレータも開発されている．Mininet-WiFi[11] は端末と AP の双方の動作をシミュレートする OSS であり，無線 LAN と SDN の組み合わせを実現している．商用では EstiNet[12] が，無線 LAN 対応の OpenFlow エミュレータ兼シミュレータとして販売されている．

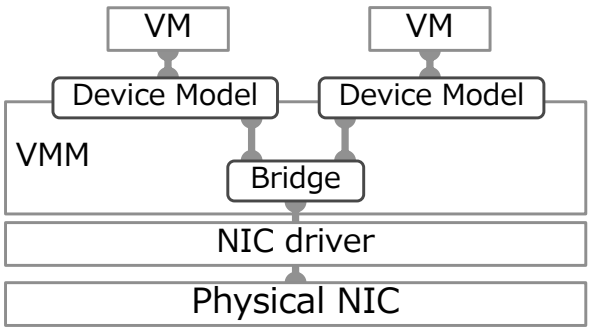

図 2 ソフトウェア面からの無線 LAN 接続仮想化に関する概念図

3.2 ハードウェア面からの解決手法

ハードウェアにより実現する無線 LAN インターフェイスの仮想化は，特殊なハードウェアを使用することにより実現される．ハードウェア面からの無線 LAN インターフェイスの仮想化の代表例として，SR-IOV (Single root I/O virtualization)[13] が存在する．SR-IOV は，PCI Express の拡張であり，PCI Express で接続されるデバイスへのアクセスを分離する (図 3) ことが可能である．SR-IOV は，ソフトウェア面からの仮想化に対するオフロードとして開発された規格であり，主に HPC (High Performance Computing) 用途に使用される．よって，高パフォーマンスではあるが，導入費用が高額になるといったデメリットが存在する．

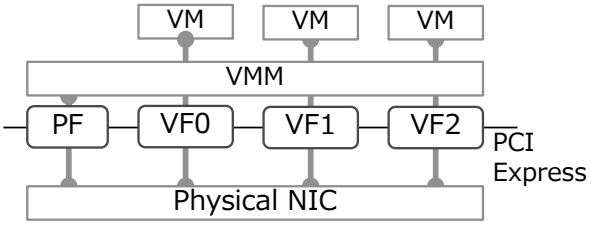

図 3 SR-IOV の概念図

3.3 両面からの解決手法

ソフトウェア面とハードウェア面の，両面から実現した無線 LAN インターフェイスの仮想化手法について述べる．Virtual WiFi[14] では，ハードウェアによるメモリのリマッピングと拡張されたドライバにより，KVM 上の仮想マシンに対し，無線 LAN インターフェイスを提供する (図 4)．これは有線仮想ネットワークの延長による無線 LAN インターフェイスの仮想化である．よって，本研究が対象とする負荷試験に対して用いるためには，仮想マシンの作成と KVM のオーバーヘッドにより，大量のコンピュータリソースが必要となる．

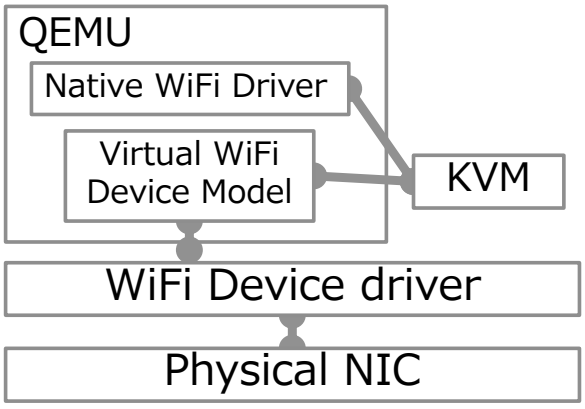

図 4 Virtual WiFi の概念図

Atheros 製の無線 LAN モジュールに関し，ソフトウェア面からの解決手法で述べた Virtual Interfaces と組み合わせることにより，多数の仮想無線 LAN インターフェイスを作成し，AP と接続する手法 [15] が存在する．この手

法では，使用するチャネルが固定される等の制約が存在するが，同一 AP に対しアンテナ数以上の接続を行うことが可能である．この手法は．無線 LAN モジュール・デバイスドライバ・Linux カーネルの全てが，Virtual Interfaces に対応している必要がある．この手法を用いて，仮想マシンに仮想無線 LAN インターフェイスを提供する研究 [16] も存在する．ハードウェア面からの解決手法と比較し，使用する無線 LAN モジュールはノート PC にも搭載されることもあるため，比較的入手しやすく，安価であるハードウェアではある．しかしながら，この手法は現在 Atheros 製の無線 LAN モジュールのみでしかサポートされておらず，依然としてハードウェア面からの解決手法と同様の，特殊なハードウェアが必要になるといったデメリットが存在する．

3.4 本研究が解決すべき問題点と目的

無線 LAN インターフェースの仮想化に関して，ハードウェア面からの解決手法や，両面からの解決手法では，特殊なハードウェアが必要であるため，強いハードウェア依存が内在する．本研究では，ソフトウェア面からの解決手法を用いて，強いハードウェア依存を可能な限り軽減する手法を提案する．また，2.3 節で述べた負荷試験を行う上で，使用する無線 LAN モジュールの削減を研究目的とする．

4. 提案手法

複数の端末をエミュレートし，認証時の通信を同時に並行して作成し，AP に対し認証サーバを含め負荷を掛ける．接続完了後，接続を切断し再接続を行うことにより，継続的な接続時の負荷を実現する．

ユーザー空間上で実行するマネジメントアプリケーションにて，無線 LAN 接続時の端末の動作をエミュレートし，認証に関する無線 LAN フレームをハンドリングする．提案手法の概略図を図 5 に示す．

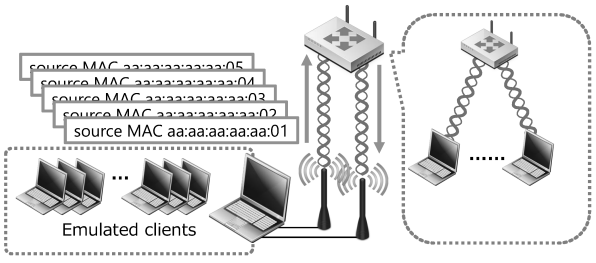

図 5 提案手法の概略図

無線 LAN インターフェースは，提案手法の安定化のため，送信用と受信用を使い分ける．無線 LAN フレームの受信は，monitor モードもしくは promiscuous モードに変更した受信用無線 LAN インターフェイスにて一括して行う．無線 LAN フレームの送信は，monitor モードに変更した送信用無線 LAN インターフェイスにてフレーム注入を用いて行う．

端末の AP に対する接続に関する処理は，wpa_supplicant を使用した場合，nl80211 サブシステムや cfg80211 サブシステムを通して，mac80211 サブシステムにて実行される (図 6 の Normal Process)．フレーム注入は，monitor モードのソケットを RAW で開きデータを書き込む．よって提案手法では，ソケットを通し net_dev から mac80211 サブシステムにアクセスする (図 6 の Proposed method) ことにより，マネジメントアプリケーションから接続に関する処理を行う．

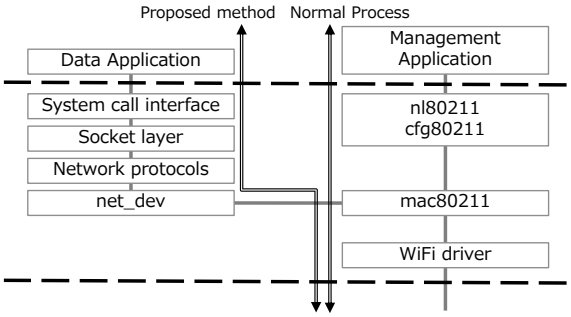

図 6 使用するネットワークスタックの比較

マネジメントアプリケーションでは，エミュレートする端末の台数と同数のスレッドを作成する．一括で受信した無線 LAN フレームは，マネジメントアプリケーションにて送信先 MAC アドレス毎に分離し．対応するスレッドに渡される．データはスレッド毎に処理され，必要に応じてデータの送信が行われる．マネジメントアプリケーションの概念図を図 7 に示す．

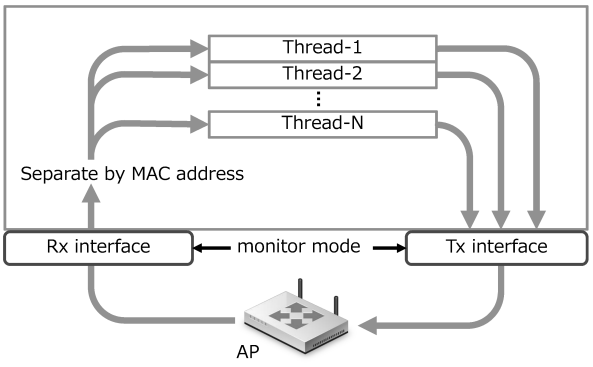

図 7 マネジメントアプリケーションの概念図

5. 評価実験

5.1 実験の概要

2 種類の AP(表 1 の AP-1，AP-2) に対して，以下の 3 種類の手法を用いて接続と切断を繰り返すことにより，認証

時の通信を並行して大量に生成した．

- 既存手法 1　　多数の端末を用いた手法
- 既存手法 2　　Atheros 製無線 LAN モジュールと Virtual Interfaces を用いた手法
- 提案手法　　フレーム注入を用いた手法

評価実験のネットワーク図を図 8 に示す．また，使用機器を表 1 に示す．

既存手法 1 では，16 台の端末 (表 1 の Client-1〜16) を使用した．端末の使用台数を変え，それぞれの AP に対して 10 分間の試行を 9 回ずつ行った．端末の使用台数は 1，2，4，6，8，10，12，14，16 台と増加させた．各端末では，wpa_supplicant とそのフロントエンドプログラムである wpa_cli を用いて接続と切断を繰り返した．また，wpa_cli を用いて切断後 PMKSA キャッシュを削除することにより，次回認証時も RASIUS サーバに問い合わせを行うようにした．

既存手法 2 では，Atheros 製の無線 LAN モジュールと mac80211 subsystem に実装されている Virtual Interfaces を使用した．これは，3 章で述べた無線 LAN インターフェイスの仮想化の内，2.3 節で述べた負荷試験に対して，最もコンピュータリソースを大量に必要としない比較的低コストで実現可能な実現可能な手法である．この手法では，端末を増加させる代わりに，仮想無線 LAN インターフェイスを作成した．1 台の端末 (表 1 の Client-17) を使用し，既存手法 1 の端末の使用台数と同数の仮想無線 LAN インターフェイスを作成し，それぞれの仮想無線 LAN インターフェイスで wpa_client と wpa_cli を用いて接続と切断を繰り返す 10 分間の試行を 9 回ずつ行った．

提案手法では，4 章で述べた手法を用いて，複数の端末が AP への接続時に行う通信をエミュレートした．この手法では，端末を増加させる代わりに，エミュレートする端末数を増加させた．1 台の端末 (表 1 の Client-18) を使用し，既存手法 1 の端末の使用台数と同数の端末をエミュレートした．それぞれの AP に対し，作成したシステムにより切断と接続を繰り返す 10 分間の試行を 9 回ずつ行った．

各試行終了後には，RADIUS サーバより試行中のログファイルを回収した．手法・AP 毎に 9 回，合計 54 個のログファイルを回収した．最後に回収したログファイルそれぞれに対して，試行中の 10 分間を抽出し，認証成功回数を集計した．本実験では，性能評価の基準に関して，評価実験にて手法を問わずログを収集することが出来，2.3 節で述べた負荷試験において，通信を行い負荷を掛けたと証明できるものとして，認証成功回数を採用した．

既存手法 1 より，多数の端末を使用した際に，2.3 節で述べた負荷試験により，無線 LAN 環境を評価可能であるかを確認した．既存手法 2 より，既存の無線 LAN インターフェイスの仮想化を用いて，2.3 節で述べた負荷試験で使用する端末数の削減が可能であるかを確認した．提案手法により，端末のエミュレートとフレーム注入を用いて，2.3 節で述べた負荷試験で使用する端末数の削減が可能であるかを確認した．

表 1　評価実験の使用機器
Table 1　Equipment of the evaluation

名前	役割/機器詳細
AP-1	AP
	・Allied Telesis AT-TQ4400
AP-2	AP
	・GIGABYTE GB-BXCE-2955
	・OS : Debian 9
	・CPU : Intel Celeron Processor 2955U
	・RAM : 4 GB
	・WLAN : Planex GW-900D
Client-1〜16	無線 LAN クライアント
	・Fujitsu ESPRIMO K556/M
	・OS : Ubuntu 18.04 LTS
	・CPU : Intel Core i3-6100T
	・RAM : 8 GB
	・WLAN : Planex TL-WN725N
	・OS : Ubuntu 18.04 LTS
Client-17	無線 LAN クライアント
	・OS : Ubuntu 18.04 LTS
	・CPU : Intel Core i5-6400
	・RAM : 8 GB
	・WLAN : Atheros AR5BHB112
Client-18	無線 LAN クライアント
	・OS : Ubuntu 18.04 LTS
	・CPU : Intel Core i5-6400
	・RAM : 8 GB
	・WLAN1 : Planex GW-900D
	・WLAN2 : Planex GW-900D

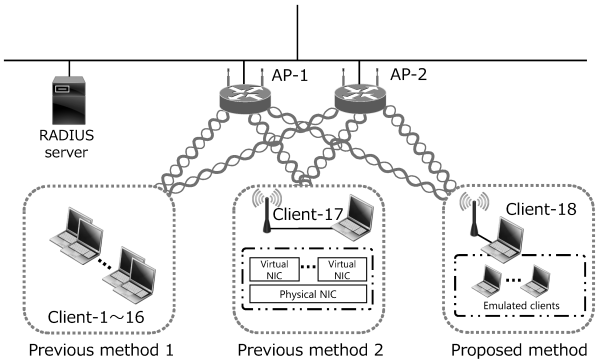

図 8　評価実験ネットワーク図

5.2　提案手法を用いたシステムの実装

本実験で使用する提案手法を用いた手法では，無線 LAN モジュールとして Planex GW-900D を 2 つ使用する．フレーム注入と monitor モードによるデータの受信を併用し

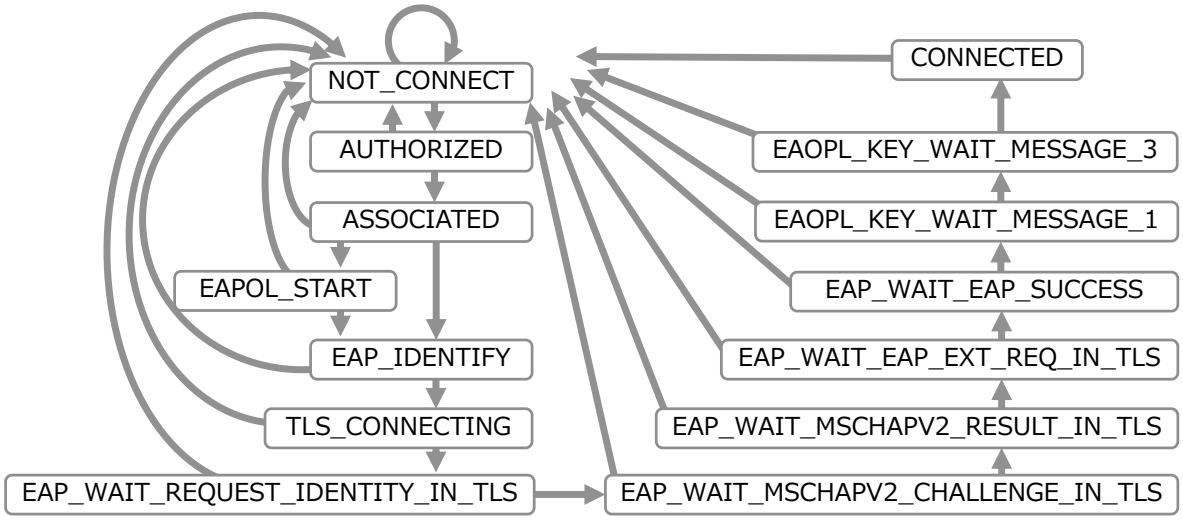

図 9 提案手法を用いたシステムの状態遷移図

た場合，本システムで使用したデバイスドライバ[*3]では動作が不安定になる可能性がある．よって受信用と送信用のモジュールを分け使用する．実験のため作成したシステムに関して，通信のエミュレートには Python を用いる．ネットワークライブラリとして Scapy を使用し，monitor モードに変更した無線 LAN インターフェイスに対して，通信のハンドリングを行う．状態遷移の管理には transitions を用いた．また TLS 通信は tlslite-ng によりハンドリングを行う．暗号化・復号・ハッシュの計算には passlib や cryptography を使用する．これらのソフトウェアバージョンを表 2 に示す．

表 2 提案手法を用いたシステムのソフトウェアバージョン

ソフトウェア	バージョン
デバイスドライバ	5.1.5
Python	3.6.6
Scapy	2.4.0
transitions	0.6.8
tlslite-ng	0.7.5
passlib	1.7.1
cryptography	2.1.4

本システムではエミュレートする端末毎にスレッドを作成し並列処理を行う．受信用インターフェイスがデータを受信した際，フレームの MAC アドレスを確認する．受信者アドレスがスレッドがエミュレートする端末の MAC アドレスと同一であり，送信者アドレスが負荷試験の対象である AP の MAC アドレスと同一であった際，受信したデータの処理を行う．

各スレッドでは端末の状態を保持している．保持された状態に応じて，受信したデータから次に送信するデータを作成し，送信用インターフェイスを通して AP に送信する．本システムの状態遷移図を図 9 に示す．本システムでは状態遷移を簡略化しており，エラーが発生した場合は，エミュレートされた端末の状態を初期化する．

[*3] https://github.com/aircrack-ng/rtl8812au/tree/v5.1.5

5.3 実験結果

10 分間の各試行での，RADIUS サーバに記録された認証成功回数に関し，AP-1 に対する各手法の比較を図 10 に示す．また，AP-2 に対する各手法の比較を図 11 に示す．

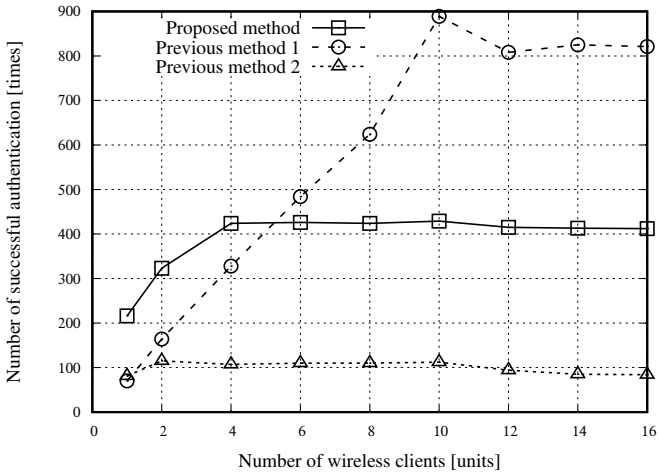

図 10 AP-1 に対する認証成功回数の比較

5.4 実験考察

AP-1 に対する既存手法 1 を用いた実験結果 (図 10 の Previous method 1) では，端末数が 10 台以上の場合，10 分間の認証成功数がおおよそ横這いになった．実験中の端末の挙動から，AP-1 は，認証処理中の端末を並行して 10 台までしか受け付けないことが分かった．AP-1 に対する 10 台までの認証成功回数 (図 10 の Previous method 1) 並びに AP-2 に対する認証成功回数 (図 11 の Previous method

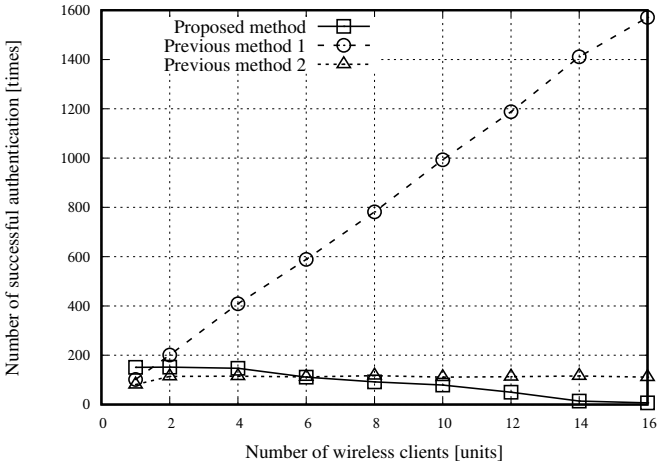

図 11 AP-2 に対する認証成功回数の比較

1) は使用した端末数に対して，おおよそ比例している．この結果から，多数の端末を使用した場合，使用台数に比例して認証に関する通信を増加させることが可能であることを確認した．

既存手法 2 を用いたそれぞれの AP に対する実験結果 (図 10，図 11 の Previous method 2) では，仮想無線 LAN インターフェイスを増加させても，認証成功回数が大きく増加することはなかった．2.3 節で述べた負荷試験に対して，Virtual Interfaces を用いた無線 LAN インターフェイスの仮想化では，負荷を掛けることが出来ないことがわかった．Virtual Interfaces を用いた場合，無線 LAN モジュールが使用可能な無線 LAN 帯域やリソースは，仮想無線 LAN インターフェイス数で等分される．よって，仮想インターフェイスを増加させても，仮想無線 LAN インターフェイス毎のパフォーマンスが低下するため，このような結果になったと考えられる．よって，既存の無線 LAN インターフェイスの仮想化手法の内，コンピュータリソースが少量で済む比較的低コストで実現可能な実現可能な手法では，本研究が対象とする負荷試験は実現不可能であると考えられる．

提案手法を用いた AP-1 に対する実験結果 (図 10 の Proposed method) では，端末のエミュレートが 4 台までは認証成功回数が増加した．4 台以降のエミュレートでは，成功回数が横這いになっている．端末 4 台のエミュレートにより，使用した送信用無線 LAN モジュールの性能限界値に達したため，このような結果になったと考えられる．既存手法 1 で用いる無線 LAN モジュールを N 台とした場合，提案手法では $1 + N/4$ 台程度の無線 LAN モジュールが必要になると考えられる．よって，負荷試験で多数の無線 LAN モジュールを用意する場合，一定のコスト削減に寄与できる．

提案手法を用いた AP-2 に対する実験結果 (図 11 の Proposed method) では，エミュレートする端末の台数を増加させても，認証成功回数が増加することはなかった．提案手法を用いたシステムの挙動を観察したところ，認証中のタイムアウトが頻発していた．AP-2 は市販の無線 LAN モジュールを使用しており，hostapd を用いて AP として機能させている．提案システムを用いたシステムは，状態遷移 (図 9) を簡略化し，タイムアウト等の例外処理が発生した場合，端末の状態を初期化している．既存手法 1 では端末数に比例して増加しているため，無線フレームの再送処理など例外処理を適切に行うことにより，認証成功回数が増加するものと考えられる．

6. 結論

本研究では，認証時の通信に着目したフレーム注入と通信のエミュレートによる負荷試験手法を提案した．また評価実験にて，その提案手法に則ったシステムを開発し評価した．その結果，提案手法により 1 つの無線 LAN モジュールに対し 4 台程度の端末であればエミュレート可能であり，負荷試験の台数削減に寄与できることを確認した．

提案手法では，フレーム注入が可能な無線 LAN モジュールが必要になる．この条件は，既存手法の特定ベンダーの無線 LAN モジュールが必要になるという条件と比較し，ハードウェア依存の低い条件である．よって提案手法では，ハードウェア依存低い手法による無線 LAN モジュールの削減を実現した．

評価実験にて作成したシステムでは，エミュレートした端末の状態遷移を大幅に簡略化したため，再送処理やタイムアウトが頻発すると大幅に性能低下が発生することが確認された．実際の負荷試験に用いるためには，wpa_supplicant 等既存のサプリカントの状態遷移を参考にプログラムを作成するか，ダミー無線 LAN インターフェイスとフレーム注入に用いる無線 LAN インターフェイスとの間をバイパスするカーネルモジュールを作成し，既存のサプリカントにより制御を行う必要があると考えられる．

参考文献

[1] How to use packet injection with mac80211 https://www.kernel.org/doc/Documentation/networking/mac80211-injection.txt (2019 年 1 月 31 日参照)
[2] 802.11ac wireless throughput testing and validation guide - Cisco https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212892-802-11ac-wireless-throughput-testing-and.html (2019 年 1 月 31 日参照)
[3] Speedtest by Ookla - The Global Broadband Speed Test http://www.speedtest.net/ (2019 年 1 月 31 日参照)
[4] CARNet Wi-Fi Independent Test Results Access Points Comparison May 2015 http://ruckus-www.s3.amazonaws.com/pdf/other/carnet-wifi-test-results.pdf (2019 年 1 月 31 日参照)
[5] RADIUS Server Load Testing - A Guide — BlazeMeter https://www.blazemeter.com/blog/radius-server-load-testing-a-guide (2019 年 1 月 31 日参照)
[6] Protected EAP (PEAP) Support Added

to Windows XP SP1 and Windows Server 2003 https://support.microsoft.com/en-us/help/325725/protected-eap-peap-support-added-to-windows-xp-sp1-and-windows-server (2019 年 1 月 31 日参照)

[7] Microsoft's PEAP version 0 (Implementation in Windows XP SP1) https://tools.ietf.org/html/draft-kamath-pppext-peapv0-00

[8] draft-josefsson-pppext-eap-tls-eap - Protected EAP Protocol (PEAP) Version 2 https://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap

[9] RFC 3748 - Extensible Authentication Protocol (EAP) https://tools.ietf.org/html/rfc3748

[10] en:users:documentation:iw:vif [Linux Wireless] https://wireless.wiki.kernel.org/en/users/documentation/iw/vif (2019 年 1 月 31 日参照)

[11] Ramon R. Fontes, Samira Afzal, Samuel H. B. Brito, Mateus A. S. Santos, and Christian E. Rothenberg. "Mininet-WiFi: Emulating software-defined wireless networks." In Network and Service Management (CNSM), 2015 11th International Conference on, pp.384–389. IEEE, 2015.

[12] Shie-Yuan Wang, Chih-Liang Chou, and Chun-Ming Yang. "EstiNet openflow network simulator and emulator." IEEE Communications Magazine, vol. 51, no.9, pp.110–117, IEEE, 2013.

[13] Overview of Single Root I/O Virtualization (SR-IOV) — Microsoft Docs https://docs.microsoft.com/en-us/windows-hardware/drivers/network/overview-of-single-root-i-o-virtualization–sr-iov- (2019 年 1 月 31 日参照)

[14] Lei Xia, Sanjay Kumar, Xue Yang, Praveen Gopalakrishnan, York Liu, Sebastian Schoenberg, and Xingang Guo. "Virtual WiFi: bring virtualization from wired to wireless." Proceedings of the 7th ACM SIGPLAN/SIGOPS international conference on Virtual execution environments, vol.46, no.7, pp.181–192, ACM, 2011.

[15] Virtual STA and AP interfaces with ath5k, ath9k and ath10k https://www.candelatech.com/vsta.php (2019 年 1 月 31 日参照)

[16] Ghannam Aljabari and Evren Eren. "Virtual WLAN: Extension of Wireless Networking into Virtualized Environments." International Journal of Computing Research Institute of Intelligent Computer Systems, vol.10, no.4, pp.1–9, 2010.