

IEEE802.11ad ミリ波無線 LAN における マルチセクタ AP 接続時の FILS の適用効果

櫛田 裕樹^{1,a)} 真野 浩² 高井 峰生³ 劉 志¹ 石原 進^{1,b)}

概要：ミリ波を用いる無線 LAN 標準規格である IEEE802.11ad は、広い周波数帯域を利用することで高速かつ大容量の通信が可能である。しかしながら、ミリ波は伝搬損失が大きく伝送距離が短いため指向性アンテナを用いる必要がありセルサイズが小さくなる。そのため、移動しながらの利用には単一セルの滞在時間が短くなるためハンドオーバー時のオーバーヘッドが相対的に大きくなる。そこで、IEEE802.11ad として標準化されている FILS (Fast Initial Link Setup) を用いることを検討する。FILS を用いることで、初期接続時間の短縮化を図り、セル滞在中のデータ通信時間をできるだけ長く確保する。これまでに筆者らは、FILS と従来型の無線 LAN 認証方式 WPA2 エンタープライズに関して、シミュレーションによって AP がシングルセクタの IEEE802.11ad における初期接続処理での FILS の効果を調べた。本稿では、AP が複数のセクタを持つ指向性アンテナを搭載している場合の初期接続処理についてこれまでと同様のシミュレーションを行い、複数のセクタを使用することにより発生するアンテナ制御処理が初期接続処理に与える影響と、その時の FILS の適用効果について調べた。

KUSHIDA HIROKI^{1,a)} MANO HIROSHI² TAKAI MINEO³ ZHI LIU¹ ISHIHARA SUSUMU^{1,b)}

1. はじめに

スマートフォンなどの無線 LAN を使用する機器の爆発的な普及により、無線 LAN 通信の総トラフィック量は大きく増加している [1]。そのため、Wi-Fi 及びセルラーネットワークにおいて既存の 10GHz 帯以下の周波数の使用状況は逼迫しており、これ以上の大容量化は困難である。この課題に対し、60GHz 帯のミリ波を無線 LAN に使用することが解決策の一つとして考えられており、今後の開発が注目されている [3]。IEEE802.11ad は、60GHz 帯の周波数を使用する無線 LAN の標準規格である [2]。IEEE802.11ad では、1 チャンネルあたり 2.16GHz もの広い帯域を利用できるため、チャンネルボンディングや MIMO などの技術を利用

しなくても非常に高速（最大約 7Gbps）な通信が可能である。しかしながら、ミリ波は伝搬損失と遮蔽損失が大きいため、一台のアクセスポイント（AP）ごとの実用的な通信可能範囲は狭くなる。IEEE802.11ad では指向性アンテナやビームフォーミング技術を使用することで通信可能範囲を確保している。その上で IEEE802.11ad の想定利用距離は 10m 程度となっている [2]。

ミリ波無線 LAN のカバレッジの狭さにより、ユーザが移動しながら利用する際に生ずる課題として、単一セルに滞在する時間が短くなるためデータ通信可能な時間が短いこと、ハンドオーバーの頻度が高くなることの 2 点が挙げられる。IEEE802.11 無線 LAN では、ある AP と端末が無線 LAN 通信を行う際に初期接続の処理として、基地局検索、暗号化通信路の確立、IP 通信のための設定（IP アドレス、DNS サーバの IP アドレス、デフォルトルータの通知など）のための十数回のパケット交換が必要となる。初期接続処理の手法には様々なものがあるが、現在最も広く用いられているの一つに Wi-Fi Protected Access 2 (WPA2) エンタープライズがある。WPA2 エンタープライズはセ

¹ 静岡大学

Shizuoka University

² コーデンテクノインフォ

KODEN TECHNO & INFO

³ スペースタイムエンジニアリング

Space-time engineering

a) kushida@ishilab.net

b) ishihara@ishilab.net

セキュリティは高いが、必要なパケット交換の回数が多く、ハンドオーバーの度に初期接続処理が行われることでデータ通信の時間が減ってしまう。

これら 2 点の課題に対する解決策の一つに Fast Initial Link Setup (FILS) がある [4]。FILS は IEEE802.11ai で提供される機能で、認証に必要なパケット交換回数を大幅に削減できるため、単一セル滞在中の通信時間の確保と高頻度なハンドオーバーによる通信時間のロスを抑えることが可能である。FILS の初期接続時間の短縮効果について、従来の無線 LAN においては、市販機器を (2.4GHz, IEEE802.11g) を使用した測定実験によって既に確かめられている [5]。しかしながら、IEEE802.11ad ミリ波無線 LAN における FILS の効果は確認されていなかった。IEEE802.11ad は、既存の 2.4GHz, 5GHz の帯域を用いる無線 LAN と比べて様々な点で異なっている。例えば、通信速度が非常に高速であることや、指向性アンテナのビーム方向の調整のために、AP と端末間で従来無線 LAN より多くの制御フレームを交換する必要があることなどが挙げられる。そのため、[5] で確かめられた FILS の効果は IEEE802.11ad 無線 LAN において異なる可能性が高い。

そこで筆者らは、IEEE802.11ad に FILS を適用した場合の初期接続所要時間の短縮効果を確認するため、IEEE802.11ad 上で、WPA2 エンタープライズと FILS の 2 つの認証手法を使用して複数端末の同一 AP に対する初期接続をシミュレーションし、その所要時間と成功率を比較評価した [6]。さらに、端末の初期接続完了後のデータ通信が他の端末の初期接続処理に及ぼす影響について確認するため、1 台の AP と複数の端末の間でトラフィックが大量に流れている環境下において、[6] と同様の 2 手法を使用し 1 台の端末が新規に行う初期接続をシミュレーションし、その所要時間と、流れているトラフィックが初期接続処理と干渉することで発生する処理遅延の大きさを比較評価した [7]。本稿では、[6] 及び [7] ではシナリオに含めていなかった AP が複数のセクタを持ち、それを切り替えながら通信する場合についてシミュレーションを行い、そのセクタ切替処理が初期接続に与える影響について評価した。7 つのアンテナセクタを持つ AP を使用して、それ以外の条件をこれまでに行ったものと揃えたシミュレーションを行い、AP が単一のセクタのみ使用する場合と比較し評価した。

以下、2 章で IEEE802.11ad と既存の無線 LAN 認証方式について概要を述べる。3 章で、IEEE802.11ai で標準化されている FILS について記述する。4 章で、シミュレーションに用いた WPA2 エンタープライズと FILS の認証処理のモデルについて記述する。5 章で、シミュレーション評価について記述し、以前に行った評価に加え、マルチセクタの切り替えを考慮した IEEE802.11ad における FILS の初期接続処理の所要時間短縮効果と、通信トラフィック

による認証処理に対する干渉の影響を軽減する効果について議論する。6 章で本稿をまとめる。

2. IEEE802.11ad と無線 LAN 認証規格

本章では、本稿のシミュレーションで用いたミリ波無線 LAN 標準規格である IEEE802.11ad の概要と、FILS に関する説明の準備として、本稿で FILS との比較に使用した無線 LAN 認証の既存方式について概要を述べる。

2.1 IEEE802.11ad

IEEE802.11ad は、60GHz 帯のミリ波を用いる無線 LAN の標準規格である [2]。1 チャンネルあたり 2.16GHz もの広帯域を利用でき高速かつ大容量の通信が可能だが、伝搬損失及び遮蔽損失が大きく単一 AP あたりのカバーレージが狭くなる。そのため、指向性アンテナやビームフォーミング技術は必須とされている。この点が従来無線 LAN と大きく異なる点で、MAC プロトコルやセキュリティプロトコル等に関しては従来無線 LAN と同等のものが使用される。これらの技術を使用した上で、利用可能範囲は 10m 程度とされている [2]。

IEEE802.11ad のチャンネルアクセスは、Beacon Interval (BIs) 単位で管理される。図 1 に、BI 内部の構成について示す。BI は、主に以下に示す 4 つの要素で構成される。

Beacon Transmission Interval (BTI) AP はセクタを切り替えつつ、自身の持つ全てのセクタから同じ Directional Multi-Gigabit (DMG) Beacon を送信する。

Association-Beamforming Training (A-BFT)

DMG-Beacon を受信した端末は、その AP とアンテナ制御用フレームを数回交換し、AP はその端末と通信するために最も適した (信号強度の高い) セクタを判別する。

Announcement Transmission Interval (ATI) これまでに判明した最適なセクタを使用して、AP と端末間で初期接続処理フレーム及びチャンネルアクセススケジュールの同期用の管理フレームが交換される。

Data Transmission Interval (DTI) AP と端末間でデータフレームの送受信が行われる。DTI は Contention Based Access Periods (CBAPs) と、Scheduled Service Periods (SPs) の 2 要素で構成される。CBAP では、従来の無線 LAN 規格と同じ Distributed Coordination Function (DCF) や Hybrid Coordination Function (HCF) に従うコンテンション方式のデータ送信が行われる。

通信対象へ向けてのアンテナ制御は、Sector-Level Sweep (SLS) と Beam Refinement Protocol (BRP) の 2 段階に分けて行われる。1 段階目の SLS では、Series of sector sweep (SSW) フレームが AP と端末間で交換される。このフレー

ムは AP に搭載された指向性アンテナの複数のセクターから送信され、通信対象である端末からのフィードバックを元に最も信号強度の高いセクターを選択する(図 2)。その後 BRP で、選択したセクターで同様に AP と端末が制御フレームを送受信することで更に微調整を行う。SLS は Beacon 送信後の一定期間の間に行うことが規定されており、BRP については SLS の後でさえあれば必要に応じて実施される。

2.2 WPA2 エンタープライズモード (PEAP) での認証処理

WPA2 は IEEE802.11i として標準化されている IEEE802.11 無線 LAN で広く利用されている無線 LAN のセキュリティプロトコルである [8]。WPA2 には 2 つのモードがあり、1 つは主に家庭内 LAN などで利用される WPA2 パーソナルモードで、もう 1 つは、企業や公共機関などで利用される WPA2 エンタープライズモードである。本稿では WPA2 エンタープライズモードを扱う。WPA2 エンタープライズモードは IEEE802.1X という認証規格を使用するモードである。

IEEE802.1X は、有線 LAN と無線 LAN の両方で使用されるユーザ認証の規格である。企業や大学など多数の AP によって構成される大規模なネットワークで最も広く使用されており、高いセキュリティを得られる。端末は AP を介して認証サーバと Extensible Authentication Protocol (EAP) により認証処理を行う [9]。EAP は拡張可能な認証プロトコルで、EAP 上で動く認証プロトコルは様々なものが存在する。本稿では、Protected-Extensible-Authentication-Protocol (PEAP) を使用する [11]。PEAP は最も広く使われている認証方式の 1 つである。

PEAP は、IEEE802.1X 認証において現在最も広く用いられている認証方式の一つである [11]。PEAP の一般的な認証手順を図 3 に示す。AP が送信する Beacon を受け取った端末は、AuthenticationRequest/Response フレームと AssociationRequest/Response フレームを AP と交換する。

その後、サブリカントと呼ばれる IEEE802.1X 認証を行うアプリケーションが動作し、認証処理が開始される。認証手法に PEAP を使用する場合、ユーザ認証を行う前に認証用パケット交換のための暗号化回線が生成される。この暗号化回線生成には TLS という暗号化プロトコルが用いられ、ここで生成された暗号化回線は TLS トンネルと呼ばれる [13]。TLS トンネル内でユーザ認証用パケットが交換される。

認証が成功すると、データ通信の暗号化に用いる鍵情報が認証サーバから端末へ渡される。その鍵情報を元に、4WayHandshake と呼ばれる手順で暗号化鍵が AP と端末間で生成、共有される。その後、Dynamic Host Configu-

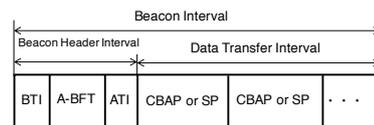


図 1 Beacon interval の内部構成

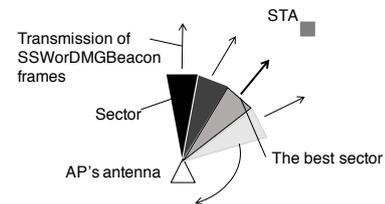


図 2 Sector-Level Sweep (SLS) の動作図

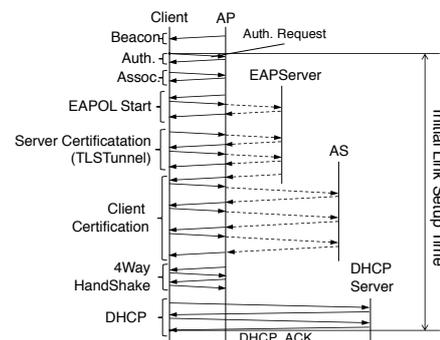


図 3 一般的な WPA2 エンタープライズ (PEAP) の認証手順

ration Protocol (DHCP) を用いて IP 通信のための設定がされ、データ通信が可能となる。

3. IEEE802.11ai (FILS)

IEEE802.11ai は、端末と AP の初期接続の効率化、高速化を目的とした無線 LAN 規格である。FILS とは、IEEE802.11ai の主要な機能の総称である。今回のシミュレーションに使用した FILS の機能は、Extensible Authentication Protocol -Re-authentication Protocol (EAP-RP) のみである。EAP-RP は、認証に必要なフレームの数を大きく減らすことが可能な認証手法である。以下、FILS の重要な機能について概要を述べる。

3.1 チャンネルスキャンの高速化

IEEE802.11 無線 LAN において、通常 AP は 100ms の間隔で Beacon フレームを送信する。FILS は、FILSDiscovery フレームと呼ばれる通常の Beacon フレームより含める情報を絞ったフレームを通常の Beacon フレーム間隔の間に送信することで、チャンネルスキャンを早めることができる。FILSDiscovery フレームに最低限含めなくてはならない情報は AP の SSID のみと定められている。

3.2 アクティブスキャンの効率化

アクティブスキャンとは、端末が AP へ ProbeRequest を

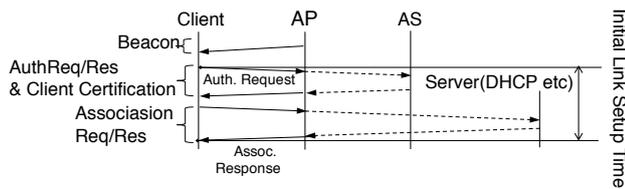


図 4 一般的な FILS (EAP-RP) の認証手順

送信することで認証要求をすることである。端末 A が AP へ ProbeRequest を送信する際、他の端末 B の ProbeRequest 送信を監視する。端末 B の ProbeRequest 送信が確認できた場合、端末 B の ProbeRequest に対する AP の ProbeResponse が返送されるので、端末 A は ProbeRequest を送信せず、AP が端末 B 向けに送信した ProbeResponse を利用する。また、IEEE802.11ai では ProbeRequest に ProbeResponse を待ち受ける制限時間を含める。制限時間内に ProbeResponse を受け取れなければ、端末は別のチャンネルをスキャンする。AP 側が制限時間を過ぎた Request を受信したら ProbeResponse を返送しない。さらに、AP は ProbeResponse を送信する際、同一 Extended Service Set (ESS) 内の他の AP の情報も含める。これらのしくみによって、ProbeRequest 及び ProbeResponse の総数は減り、帯域使用量を抑えることができ、スキャンの効率改善が見込める。

3.3 EAP-RP による認証手順短縮

EAP-RP は、初期接続処理に必要なフレームの数を大幅に減らすことが可能な無線 LAN 認証手法である [12]。端末が一度何らかのサービスを提供するサーバに接続したとき、その認証情報がネットワーク上のあるサーバに保存されており、次回接続時にその認証情報を使用することで、初期接続処理を短縮できる。一般的な EAP-RP の認証手順を図 4 に示す。PEAP の場合と異なり、端末が Beacon を受信した後の Authentication フレーム交換において保存された認証情報の照会がなされる。その後 AssociationRequest/Response フレームが交換される。このフレームには IP 通信のための設定など上位層向けの情報も含まれており、AuthenticationResponse 受信をもってデータ通信が可能となる。

4. シミュレーションモデル

本章では、評価に使用した WPA2 エンタープライズと FILS の認証手順のシミュレーションモデルについて記述する。本稿のシミュレーションは各手法における認証に必要なパケット数の違いに注目しているため、これまでに述べた両手法の一般的な認証手順を元に簡略化した。シミュレータはスペースタイムエンジニアリング社の Scenargie を使用した [14]。Scenargie は並列離散事象シミュレータ

ある。詳細なネットワークシミュレーションが可能で、シナリオ設定のための地理情報システム (GIS) データ管理機能をサポートしている。

4.1 WPA2 エンタープライズ (PEAP)

WPA2 エンタープライズ (PEAP) の認証手順のモデルを図 3 に示す。図 3 中の点線で示した AP と各種サーバとのパケット交換はすべて省略し、省略部分の処理遅延は一切無いものとした。実線で示しているパケット交換を行う部分について、各パケット送受信時の処理遅延は無いものとした。この理由は、WPA2 エンタープライズは外部サーバの実装に依存する処理が多く、それらの処理遅延は各パケット送受信よりも大きいため、外部サーバ遅延を考慮するとその遅延が原因で FILS との初期接続所要時間の差が大きくなってしまふからである。今回のシミュレーションでは、認証に必要なパケット数の違いによる差を明確にするため、外部サーバを用いた処理は十分に速い (処理遅延=0) という条件のもとで行った。

4.2 FILS (EAP-RP)

FILS (EAP-RP) の認証手順のモデルを図 4 に示す。図 4 中で点線で示したパケット交換は省略し、処理遅延は一切無いものとした。これは、前節で述べた WPA2 エンタープライズの条件と合わせるための設定である。今回のシミュレーションでは、端末が AP の発する Beacon を受信した後から先の処理を初期接続としてその所要時間を比較するため、FILSDiscovery フレームは使用しない。今回のシミュレーションはパッシブスキャンの場合のみを考慮したため、ProbeRequest/Response の総数を減らす機能は含んでいない。IP アドレスの割り当ては WPA2 エンタープライズとは異なり、端末が AssociationResponse フレームを受信することで完了するものとした。

4.3 シミュレータ上の BHI

シミュレータ上でも 2.1 に示したものと同様に Beacon-Interval は構成されている。しかし、BRP はシミュレータ上では行われぬ。つまり、シミュレーションにおけるアンテナ制御はセクタ切替のみの事を指す。以下にセクタ切替のためのフレーム交換手順について記述する。まず、AP は自身の持つセクタを切り替えて各セクタより DMG-Beacon フレームを送信する。DMG-Beacon フレームを受信した端末は、SSW フレームを AP へ送信する。最後に、その SSW フレームを受信した AP は、端末へ SSW Feedback フレームを送信する。これらのパケット交換は BTI と A-BFT の中で行われる。

5. シミュレーション評価

本章では、IEEE802.11ad における FILS の初期接続時間

を短縮する効果を確認するため、FILS と WPA2 エンタープライズの 2 手法による初期接続の時間（データ通信が可能になるまでの時間）を測定し比較した。本稿では以下の 2 つのシナリオを用いて評価を行った。

- (1) 同一セル内で複数の端末が一斉に同一の AP に対し認証処理を開始するシナリオ。
- (2) 同一セル内で複数の端末が同一の AP とデータ通信を行っている環境に、新規に端末が認証処理を行うシナリオ。

この 2 シナリオにおいて、以下の 2 通りの AP をそれぞれのシナリオで使用した。

- (1) 半値幅 90° のセクタを 1 つのみ持つ AP。
- (2) 半値幅 30° のセクタを 7 つもち、約 120° の受信範囲を確保している AP。

AP(1) は、[6] 及び [7] で使用した AP と同じものである。AP(2) について、マルチセクタを搭載した AP のアンテナパラメータ設定のため、[15] における実験で使用されたものを参考にした。

5.1 シミュレーションシナリオ

5.1.1 端末と AP の配置

AP1 使用時の AP と端末の配置を図 5 に示す。図 5 は、25 台の端末を 1m の高さに 0.5m 間隔で格子状に配置し、1 台の AP を中央の端末の真上 1.5m の位置に配置した。これは、ホールやスタジアムなどの座席に天井から真下へアンテナを向けていることを想定して AP を配置した。図中で AP のアンテナから出ている三角形は指向性アンテナの放射を表している。マルチセクタを搭載した AP を使用したときの AP と端末の配置を図 6 に示す。27 台の端末を 1m の高さに 0.5m 間隔で格子状に配置している。AP は図 5 と同様で中央の端末の真上 1.5m の位置に配置した。この配置は、2 の AP は、自身が持つすべてのセクタによる受信範囲は単一セクタ AP による受信範囲より広いため、その範囲に合わせて端末配置の範囲を少し広げたものである。AP(1) では、指向性アンテナ制御用フレームの交換はされているが、アンテナの向き、ビームパターンは固定されており、変わることはない。AP(2) では、AP は図 6 に示すように 7 つのセクタを持つ半値幅 30° のビームを 15° ずつ左右にずらした形である。

初期接続時間を各手法で以下のように定義した。

FILS

端末が AuthenticationRequest を送信した時刻から、AssociationResponse を受信した時刻まで。

WPA2 エンタープライズ

端末が AuthenticationRequest を送信した時刻から、DHCP ACK を受信した時刻まで。

以上に示した環境で、以下に示す 2 つのシナリオで WPA2 エンタープライズと FILS の各認証手法による初期接続時

表 1 シミュレーションパラメータ

パスロスモデル	Free Space
中心周波数	59.400GHz
チャンネル帯域幅	2,160MHz
通信規格	IEEE 802.ad
送信電力	20dBm
AP(1) のアンテナパターン	半値幅 90 度, 最大利得 8.4dBi
AP(2) のアンテナパターン	半値幅 30 度, 最大利得 8.4dBi
端末のアンテナパターン	Isotropic
Modulation/Coding	MCS4 (Single Carrier, Max. 1.155Mbps)
Beacon 送信間隔	100ms
ChannelScanTimeout	100ms
AuthenticationTimeout	100ms
AssociationTimeout	100ms
UDP パケットサイズ	1,470Bytes
MAC	EDCA

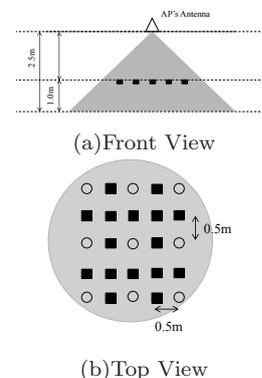


図 5 単一セクタ固定 AP と端末の配置図

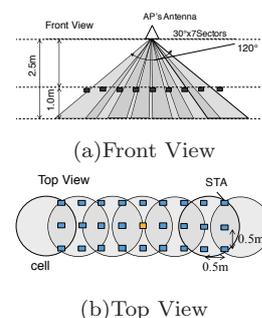


図 6 マルチセクタ AP と端末の配置図

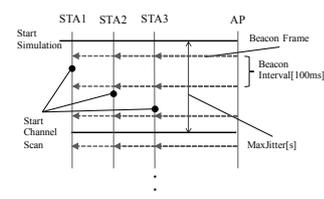


図 7 各端末の Beacon スキャン開始時刻のばらつき

間を測定した。シミュレーションパラメータ表 1 に示す。

5.1.2 シナリオ 1 (複数端末の同時初期接続)

同一セル内で複数の端末が一斉に認証処理を開始した場

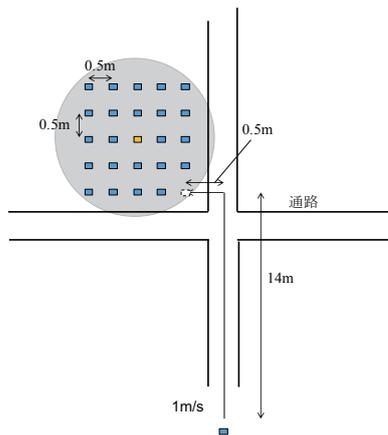


図 8 AP1 と端末の配置図 (シナリオ 2)

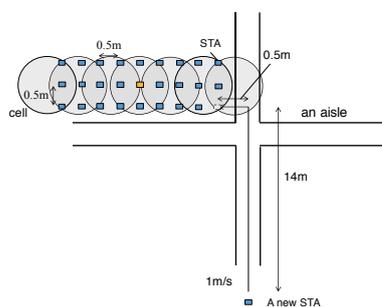


図 9 AP2 と端末の配置図 (シナリオ 2)

合の FILS の効果を評価する．各端末が AP へ接続を試みるまでの時間にばらつきを与えた．シミュレーション開始時刻から，端末が Beacon のスキャンを開始するまでの時間の最大値を，0s, 0.1s, 0.2s, 0.5s, 1s の 5 通り与えた．各端末は与えられた値以下の時間をランダムに選択し，選択した値の時間だけ Beacon のスキャン開始時間を遅らせる．図 7 に Beacon のスキャン開始にばらつきを与えた場合の各端末の動作について示す．各端末は黒点で Beacon のスキャンを始める．各認証方式で，Beacon のスキャン開始時刻のばらつきの値ごとに 100 回ずつ異なるシード値を用いてシミュレーションを行った．

5.1.3 シナリオ 2 (帯域使用率の高い環境における新規端末の初期接続)

同一セル内で複数の端末が帯域を使用している環境において，新規の端末が認証処理を行うとき，その処理に FILS が与える効果を評価する．図 5 と，図 6 で示す端末のうち，右下の 1 台以外が AP とデータ通信を行っている．そこへ，通路を通過して右下の座席に新規ユーザが着席しに来るというシナリオである (図 8, 図 9)．新規端末は移動中から Beacon をスキャンしており，Beacon を受信でき次第認証処理を開始する．各端末と AP の間で Iperf により上りと下り両方で UDP パケットを送信した．それぞれの場合で，送信側のトラフィック量を送信バッファが空にならない程度に維持させた．

5.2 シミュレーション結果

5.2.1 シナリオ 1 (複数端末の同時初期接続)

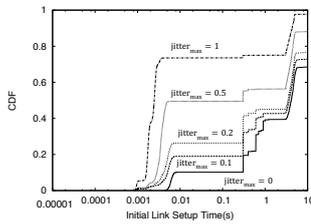
端末を 1 台 (図??の中央の端末) のみ配置した場合の各方式の初期接続所要時間の平均を表 2 に示す．端末は 1 台のみであるので，他のパケットとの衝突は起こらない．さらに，ホスト上の処理遅延は無いものとしているため，両方式の初期接続所要時間の差の原因は，認証処理に必要なパケットの数と，パケット長のみである．表 2 に示すとおり，FILS を使用することで WPA2 エンタープライズを使用した場合と比べて約 10 倍高速化できている．これは，認証に必要なフレーム数が FILS の場合 WPA2 より少ないからである．

配置した端末全てを使用した場合の初期接続所要時間の CDF を図 10, 図 11 に示す．各グラフの横軸は対数軸である．これらの図より，以下のことが観察できる．

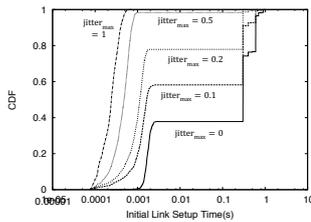
- Beacon スキャン開始時刻のばらつきの値が大きくなるにつれ，両方式とも同じ所要時間での認証成功端末数が増加している．これは，ばらつきの値が大きくなるほど同時に AP に初期接続を試みる端末数が減ることになり，各認証フレームの衝突及び MAC プロトコルによる競合が減るためである．
- 各グラフにおける，CDF が最初に大きく上昇する部分はシミュレーション開始後，初めて受信した Beacon に対し初期接続処理を行い，その処理がタイムアウトすること無く完了した端末群を示している．いずれの場合も FILS を使用した場合のほうが上昇幅が大きく，Beacon スキャン開始時刻のばらつきの値による影響も小さい．
- WPA2 エンタープライズを使用した場合のグラフ中に所要時間が 10s に達しても CDF が 1 に満たない部分がある．これは，認証パケットの交換に失敗し続けたためにサブリカント上でタイムアウトとなったことを表している．一般的な IEEE802.1X 認証におけるサブリカントでのタイムアウト時間は数 10 秒と設定されている．
- CDF の値が伸びずに平坦になっている部分が全てのグラフにおいて存在する．これは，他のパケットとの干渉により一度認証に失敗した端末が，再び Beacon のスキャンを開始するまでの時間を表している．AP 及び端末は，ある認証パケットを規定回数再送しても応答がなかった場合，その認証パケットの最初の送信時刻から 0.1s 後にその処理をタイムアウトによりキャンセルする．その後 Beacon のスキャンを開始するが，端末は混雑を避けるために前回の AP からの Beacon には応答しない．今回のシミュレーションでは AP は 1 台のみ配置しているため，端末は新たに別の AP を見つけることはなく，スキャン開始から 0.1s 後にそのスキャンはタイムアウトによりキャンセルされる．そ

表 2 端末 1 台使用時の各認証方式の初期接続所要時間

	WPA2-Enterprise	FILS
Initial link set up time	0.922ms	0.092ms



(a) WPA2 エンタープライズ (PEAP)



(b) FILS (EAP-RP)

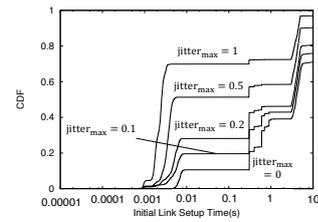
図 10 単一セクタ AP による認証方式ごとの端末 25 台の初期接続所要時間の CDF

の後再びスキャンを開始するが、その際は以前に除外した AP が発する Beacon に対しても応答する。以上で示した、最初のタイムアウトから次回回のビーコン受信までの間隔がグラフの平坦な部分に現れている。

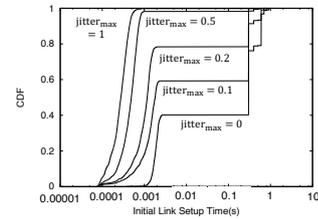
- 単一セクタ AP 使用時とマルチセクタ AP 使用時の CDF はほぼ違いがない。これは、本シミュレーションでは端末は静止しているため、各端末と通信する際に使用するセクタの更新の機会がなく、マルチセクタを使用することによる差異はセクタごとに送信される DMG-Beacon の数の増加する程度にとどまる。そのため、マルチセクタ AP を使用することによるオーバーヘッドは結果が示すように軽微なものになると考えられる。

5.2.2 シナリオ 2 (帯域使用率が高い環境における新規端末の初期接続)

下りトラフィックを発生させた場合と上りトラフィックを発生させた場合の新規端末の初期接続所要時間の CDF を図 12, 図 13 に示す。横軸は対数軸である。トラフィックの方向にかかわらず、WPA2 エンタープライズを使用した場合は認証処理に大きく遅延が生じている。表 2 で示した伝送路に妨げがない環境で端末 1 台が認証処理を行った場合の所要時間 (0.922ms) と比較すると、1ms 以下で認証を完了している端末は存在しない。下りトラフィックを発生させた場合は 8 割、上りトラフィックを発生させた場合はわずか 2 割の端末が 1ms 付近の時間で認証を完了しているが、それ以外の端末は認証完了に 1s 以上かかっている。下りトラフィックを発生させた場合よりも上りトラ



(a) WPA2 エンタープライズ (PEAP)



(b) FILS (EAP-RP)

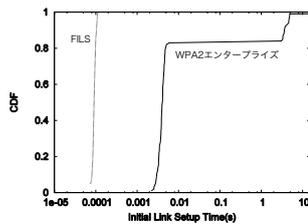
図 11 マルチセクタ AP による認証方式ごとの配置端末 27 台の初期接続所要時間の CDF

フィックを発生させた場合の方が認証処理の遅延が大きい原因は、1 台の AP からそれぞれの端末へ向けてデータが送信される下りトラフィックと違い、上りトラフィックの場合、複数の端末が同じ AP へデータ送信を試みるので、各端末間で MAC プロトコル上の競合が発生するためである。一方 FILS を使用した場合は、表 2 で示した所要時間 (0.092ms) と比較しても、ほぼすべての端末が 0.1ms 以下で認証処理を完了しており、発生させたトラフィックによる認証処理の遅延は見られない。WPA2 エンタープライズでは FILS と比べて認証に必要なパケットの数が多く、さらに DHCP による IP アドレス割り当てに必要な通信が UDP 上で行われるため、発生させたトラフィックとの競合の影響が大きくなると考えられる。

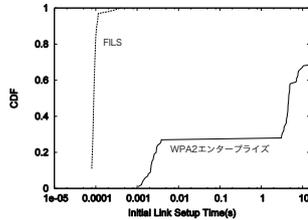
マルチセクタ AP 使用時と比較すると、AP と端末間で初期接続用管理フレームの交換のみだったシナリオ 1 と比較すると、CDF が落ちている部分が存在する。これは、データトラフィックが激しく流れることによって、セクタ切り替えによるオーバーヘッドがシナリオ 1 と比べ大きく現れたためであると考えられる。

6. 結論

筆者らはこれまでに、IEEE802.11ad ミリ波無線 LAN における無線 LAN 高速認証手法である FILS の効果を確認するために、現在最も広く用いられている無線 LAN 認証手法の一つである WPA2-Enterprise を用いた場合と FILS を用いた場合との端末認証の所要時間を、複数の端末が同時に初期接続を行うシナリオと、単一セル内で複数の端末が AP と密にデータ通信を行っている環境に対して新規に端末が初期接続処理を行うシナリオにおいてそれぞれ評価を行った。本稿では、これらの評価に対して、IEEE802.11ad ミリ波無線 LAN 特有の要素であるセクタスイープを考慮するため、単一セクタのみを使用する AP と複数のセク

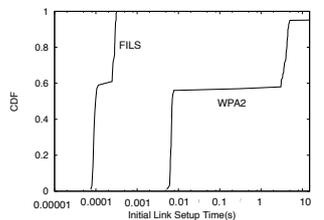


(a) 下りトラフィックを発生させた場合

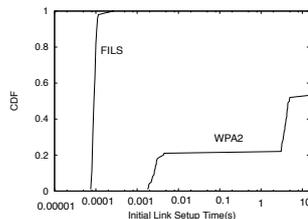


(b) 上りトラフィックを発生させた場合

図 12 単一セクタ AP 使用時の新規端末の初期接続所要時間の CDF



(a) 下りトラフィックを発生させた場合



(b) 上りトラフィックを発生させた場合

図 13 マルチセクタ AP 使用時の新規端末の初期接続所要時間の CDF

タを使用する AP の 2 種類の AP を使用して再度行った。その結果、端末が静止している状態だと、セクタ切り替えによるオーバーヘッドは非常に少ないこと確認できた。また、AP と端末間のトラフィックが激しいと、セクタ切り替えによるオーバーヘッドは大きく現れることを確認した。

今後の考慮すべき課題を 2 点挙げる。

- (1) 今回のシミュレーションでは、ユーザが移動しながら利用することは考慮しなかったため、マルチセクタ AP のセクタ切り替えのオーバーヘッドは軽微であった。しかしながら、ユーザが移動しながら利用すると、セクタ切り替えの頻度は増加し、そのオーバーヘッドも大幅に増加すると予想される。
- (2) 本稿では、AP と各種サーバとのパケット交換はないものとして扱ったが、今後省略したパケット交換もシミュレーションモデルに組み込んだ上で評価を行う予定である。

謝辞

本研究は RAPID-5G の研究チームの協力のもとで行われたものである。ここに記すことで謝意を示す。

参考文献

- [1] CISCO, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021 White Paper, 2017
- [2] IEEE 802.11 Working Group, IEEE 802.11ad, Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band, 2012.
- [3] G. Athanasiou, P.C. Weeraddana, C. Fischione, and L. Tassiulas, Optimizing client association for load balancing and fairness in millimeter-wave wireless networks, IEEE/ACM Trans. Netw. vol.23, no.3, pp.836–850, June 2015.
- [4] IEEE 802.11 Working Group, IEEE 802.11ai-2016, Amendment 1: Fast Initial Link Setup, 2016.
- [5] 真野浩, 他: 無線 LAN 高速認証 FILS (Fast Initial Link Setup) の実装及び多重アクセス制御, マルチメディア, 分散, 協調とモバイル (DICOMO2013) シンポジウム, pp.1634–1639, 2013.
- [6] 榎田裕樹, 真野浩, 高井峰生, 石原進: IEEE802.11ad における Fast Initial Link Setup (FILS) の適用効果, 電子情報通信学会技術研究報告書, vol.116, no.407, pp.59–64, 2017.
- [7] 榎田裕樹, 真野浩, 高井峰生, 石原進: 高密度ユーザ集中環境下での IEEE82.11ad の認証とデータ通信における Fast Initial Link Setup(FILS) の適用効果, 研究報告モバイルコンピューティングとパーベシブシステム (MBL), 2017-MBL-84(18), 1-8 (2017-08-22), 2188–8817.
- [8] IEEE 802.11 Working Group, IEEE 802.11i, Amendment 6: Medium Access Control (MAC) Security, 2012.
- [9] B. Aboba, Microsoft, L. Blunk, Merit Network Inc, J. Vollbrecht, Vollbrecht Consulting LLC, J. Carlson, Sun, H. Levkowitz, Ed., and ipUnplugged, RFC3748: Extensible Authentication Protocol (EAP), <https://tools.ietf.org/html/rfc3748>, 2004
- [10] C. Rigney, S. Willens, Livingston, A. Rubens, Merit, W. Simpson, and Daydreamer, RFC2865: Remote Authentication Dial In User Service (RADIUS), <https://tools.ietf.org/html/rfc2865>, 2000.
- [11] A. Palekar, D. simon, Microsoft Corporation, J. Salowey, H. Zhou, G. Zorn, Cisco Systems, S. Josefsson, and Extundo, Internet-Draft: Protected EAP Protocol (PEAP) Version 2, <https://tools.ietf.org/html/draft-josefsson-ppext-eap-tls-eap-10> 2004.
- [12] V. Narayanan, L. Dondeti, and Quallcomm, Inc., RFC5296: EAP Extensions for EAP Re-authentication Protocol (ERP), <https://tools.ietf.org/html/rfc5296>, 2008.
- [13] R. Khare, 4K Associates / UC Irvine, and S. Lawrence, Agranat Systems, Inc., RFC2817: Upgrading to TLS Within HTTP/1.1, <https://tools.ietf.org/html/rfc2817>, 2000.
- [14] Space-Time Engineering: <https://www.spacetime-eng.com>
- [15] 滝波浩二, 白方享宗, 高橋和晃: IEEE802.11ad/WiGig に対応した 60GHz 帯無線アクセス技術と将来展望, 学術技法, IEICE Technical Report, PN2016-71, EMT2016-100, OPE2016-146, LQE2016-135, EST2016-110, MWP2016-84 (2017-01)