無線 LAN 高速認証 FILS(Fast Initial Link Setup)の実装及び多重アクセス評価

真野 浩[†1][†2] 森岡 仁志[†1] 上原 哲太郎[†3]

現在の IEEE802.11 無線 LAN は，接続にあたり行なわれる，基地局検索，認証，鍵交換，IP アドレス等上位層情報設定に，数十回のパケット交換を要するため，移動しながらの利用，同時大量のアクセスには適していない． 今後，スマートフォン等の普及により同時に接続する端末が増加し，伝送速度の高速化によりセルサイズがより小さくなる環境では，この初期の接続時間を短縮することが重要な課題となっている．そこで，FILS(Fast Initial Link Setup)方式が，筆者の提案により IEEE802.11TGai として，国際標準化が進められている． この FILS の基本概念のうち，認証，鍵交換，IP アドレス等上位層情報交換を１回のパケット交換にて行なう手法を，商用アクセスポイント，及び端末に実装し，実証実験による評価を行なった． 具体的には，従来接続（WPA2）と高速接続（FILS）について，歩行者が遠方より基地局に接近する状況において，初期に接続が行なわれるまでの距離の比較を，端末が疎な場合，密な場合について測定比較を行なった． この結果，FILS 方式では，従来方式に比べ大幅に接続までの距離（時間）が短縮されることを確認した．また，この FILS の特長を活かし，歩行者が個人 ID 及び接続基地局毎に異なるサービスをうける事が可能であることを，二つの基地局を用いて実証した．

Experimental trial of Wireless LAN FILS (Fast Initial Link Setup)

HIROSHI MANO[†1][†2] HITOSHI MORIOKA[†1] TETSUTARO UEHARA[†3]

1. はじめに

現在の IEEE802.11 無線 LAN は，接続にあたり行なわれる，基地局検索，認証，鍵交換，IP アドレス等上位層情報設定に，数十回のパケット交換を要するため，移動しながらの利用，同時大量のアクセスには適していない． 今後，スマートフォン等の普及により同時に接続する端末が増加し，伝送速度の高速化によりセルサイズがより小さくなる環境では，この初期の接続時間を短縮することが重要な課題となっている．そこで，FILS(Fast Initial Link Setup)方式が，筆者の提案により IEEE802.11TGai[1] として，国際標準化が進められている． この FILS の基本概念のうち，認証，鍵交換，IP アドレス等上位層情報交換を１回のパケット交換にて行なう手法を，商用アクセスポイント，及び端末に実装し，実証実験による評価を行なった．具体的には，従来接続（WPA2）と高速接続（FILS 方式）について，歩行者が遠方より基地局に接近する状況において，初期に接続が行なわれるまでの距離の比較を，端末が疎な場合，密な場合について測定比較を行なった．この結果，FILS 方式では，従来方式に比べ大幅に接続までの距離（時間）が短縮されることを確認した．また，FILS 方式では端末数が増加しても結果に大きな影響が出ない事が確認された．また，この FILS の特長を活かし，歩行者が，個人 ID 及び接続基地局毎に異なるコンテンツをダウンロードする実証を行なった結果，WPA2 方式ではコンテンツ取得に失敗する端末が発生するが，FILS 方式では正しくコンテンツ取得が可能となる事が確認できた．

本稿では，IEEE802.11ai の概要と，本研究で行なった実装を第２章で，実証試験の試験方法と結果を第３章で解説し，実証のまとめと今後の課題を第４章で述べる．

2. IEEE802.11ai と FILS の実装

2.1 IEEE802.11ai の概要

IEEE802.11ai の PAR(Project Authorization Request)[２]では，IEEE802.11 端末が新たな ESS(Extended Service Set)に接続する時に，以下の効率改善が目的とされている．

- 同時に一つの ESS に初期接続する端末数を増やす
- 初期接続に要する接続時間を最小化する
- 初期接続時のセキュリティを確保する

また，この目的を達成するにあたり以下の初期接続に関わる各シーケンスを最適化することが示されている．

- 基地局，ネットワーク検索
- 相互認証
- 鍵交換
- IP アドレス設定などの上位層情報の交換

なお，これらの標準改訂によってもたらされる利便性とその主な利用シーンは，IEEE802.11Use Case Reference List for TGai[3]にまとめられているが，ここでは特に移動端末の密集する地下鉄やスタジアムなどでの利用，路・車間通信利用などが示されている．これらの利用シーンでの要求を満足させるための具体的な技術目標が，

†1 株式会社アライドテレシス開発センター
†2 山梨大学大学院医学工学総合教育部
†3 立命館大学

IEEE802.11 TGai Requirements Document[4]で，以下のように設定されている．

- Link Set-Up Time

セキュアな初期接続時間が 100mSec 以下であること．

- Scalability

１秒間に 100 局の端末が，一つの ESS に入った場合の接続に対応できること．
50%程度の帯域消費状況においても接続が可能であること．
さらに，重要な点として，既に IEEE802.11 において規定されている RSNA(Robust Security Network Association)と同程度以上のセキュリティが確保されていることが求められている．

2.2 本研究における要求要件

本研究では，IEEE802.11ai が現時点で策定過程であり，最終的な仕様が決定していないことから，以下の要件のもとに，そのコンセプトの有効性を実証する事を目的とした．

2.2.1 市販無線 LAN を利用

既に市販されている無線 LAN 機器を利用し，現行の電波法等の規制範囲にて可能な実証実験を行なうこと．
具体的には，送信電力や変復調方式等の変更は行なわず，技術基準適合証明の証明要件を逸脱しないこと．
従って，ハードウェアの変更は行わないこと．

2.2.2 既存の IEEE802.11 標準との互換性

原則，既存の IEEE802.11 標準で規定されているフレームフォーマットの互換性の範囲で実証実験を行なうこと．

2.2.3 定量的なデータ取得

実証実験により，定量的に FILS の効果を確認できること．

2.3 実装

本研究では，2.2 にしめした要求要件を加味し，IEEE802.11ai が検討する最適化のうちセキュアな認証，IP アドレス設定などの上位層情報の交換について，実装を行ない評価した．

2.3.1 前提条件

実装においては，以下の前提のもとに行なった．

- 実験に用いる基地局は，FILS 対応，WPA2 双方に対応したもので同一とし，端末側は，FILS 対応，WPA2 の二種類の実装を用意した．
- 基地局，端末(Android)は，それぞれ市販されている製品を利用した．
- 無線 LAN は，IEEE802.11g(2.4GHz ch13)を利用した．
- 基地局 および STA に，pre-shared user-ID(NAI)/PSK のペアを事前に設定した．
- GTK は，暗号化しないこととした．
- PTK は，動的に変更しないこととした．
- FILS で使用するマネージメントフレームのうち上位層情報は，暗号化しないこととした．

2.3.2 プロトコルシーケンス

本実装では，図 1 FILS 方式の実装プロトコルシーケンスに示すように IEEE802.11 のフレームのうち，Beacon, ProbeReq/Res, Association Req/Resp の各フレームに必要な Vendor Specific IE(Information Element)として実装した．この Vendor Specific IE 内に FILS で使用する情報を以下に述べる sub-IE として格納した．

これらのフレーム交換の中で，相互認証及び PTK/GTK の設定，端末の IPv4 アドレス，ネットマスク，ゲートウェィＩＰアドレス, DNS サーバーのＩＰアドレスの設定を行なえるようにした．

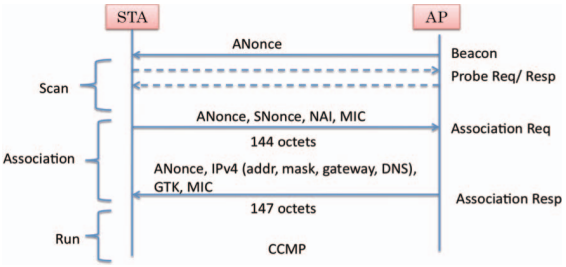

図 1 FILS 方式の実装プロトコルシーケンス

(1) Beacon 及び Probe response の拡張

基地局が FILS 方式に対応していることを示す Capability sub-IE と Timestamp sub-IE を追加した．

(2) Association Reqt の拡張

端末が FILS 方式での接続を要求する事を示す, Capability sub-IE，端末からの認証情報を送る，NAI sub-IE，MIC sub-IE，Nonce sub-IE 及び Timestamp sub-IE を追加した．

(3) Association Resp の拡張

基地局が端末認証し接続許可をする場合，MIC sub-IE, Timestamp sub-IE,GTK sub-IE 及び，上位層情報を通知する IPv4 config sub-IE,IPv4 MAC sub-IE,IPv6 config sub-IE,IPv6 MAC sub-IE を追加した．

2.3.3 基地局の動作

基地局は，定常状態では，前述の拡張された Beacon を一定間隔で送信する．また，基地局は，Probe Req を受信した場合は，拡張された Probe Resp を送信する．
基地局が，拡張された Association Req を受信した場合，そこに含まれている NAI，Timestamp，MIC を評価し，これらが全て有効であった場合，拡張された Association Resp を送信する．
もし，これらが無効であった場合は，deauth を送信する．
なお，基地局は WPA2 端末から Authentication を受信した場合は，通常の Authentication を返信し，WPA2 の手順に対応する．

2.3.4 FILS 端末の動作

端末は，パッシブスキャンにおいて拡張された Beacon を受信した場合，またはアクティブスキャンにおいて自らの送信した Probe Req に対して，拡張された Probe Resp を

受信した場合には，拡張された Association Req を送信する．

端末は，基地局から拡張された Association Resp を受信した場合，そこに含まれる鍵情報及び上位層情報を取り出し，以後これを用いて通信を行なう．

2.3.5 WPA2 端末の動作

WPA2 端末は，パッシブスキャンにおいて拡張された Beacon を受信した場合，またはアクティブスキャンにおいて自らの送信した Probe Req に対して，拡張された Probe Resp を受信した場合，拡張により付加された IE を理解できないため，通常の Authentication を送信し，以後 WPA2 による接続手順を行なう．

2.3.6 アプリケーション

評価のため，以下の機能を有するアプリケーション及びインターネット上のテストサーバーを用意した．

(1) 端末が基地局に接続すると，自動的に指定されたサイトに接続した基地局 BSSID(Basic Service Set ID)と端末の ID を付加して，http クエリーを送信する．

(2) サーバーは，上記クエリーを受信すると，http コンテンツ(109K byte GIF イメージ)を返信する．

(3) 端末は，受信したイメージを画面に表示する．

その他，接続時のステータスや接続履歴，接続時間などを表示する機能を実装した．

3. 実証実験

3.1 実験ネットワーク

図 2 実証実験構成に本研究で行なった実証実験の環境構成を示す．

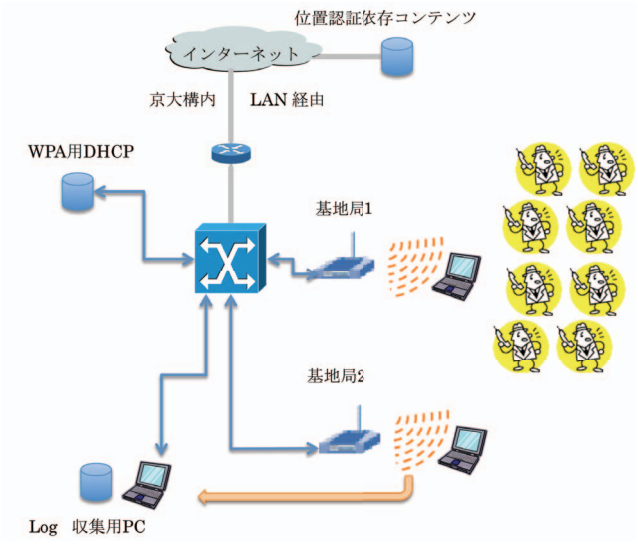

図 2 実証実験構成

ここで，認証サーバーは，基地局に搭載されている簡易 Radius を用いた．

IP アドレスは，FILS では基地局内に保持した IP アドレスプールを用い，WPA2 端末に対しては，基地局と同一ネットワーク上に設置された DHCP サーバーを用いた．

3.2 プロトコルの確認及び静的環境での測定

実装した FILS 及び WPA2 における接続時のパケット交換状況をパケットキャプチャにより観測した結果を，表 1 FILS 方式，WPA2 方式のパケット交換時間に示す．この表で，WPA2 では IEEE802.11 Authentication Req から DHCP ACK までに 5.055 Sec を要した．ただし，この測定時には，DHCP OFFER の交換時に，外乱により 6 回のリトライが発生しているため，これに要した時間を減じたとしても，3 秒程度となっている．

これに対して，FILS 方式では，Association Req から Association Resp で，11mSec となっており，IEEE802.11ai の要求要件に満足する範囲で接続が行なわれていることが確認された．

表 1 FILS 方式，WPA2 方式のパケット交換時間

Packet Sequence	WPA2 [Sec]		FILS[Sec]	
	Time	Δ	Time	Δ
Auth Req	11:18:13	0.000		
Auth Resp	11:18:13	0.003		
Assoc Req	11:18:13	0.039	11:25:39	0
Assoc Resp	11:18:13	0.041	11:25:39	0.011
EAP Req (AP->STA)	11:18:13	0.106		
EAP Resp (STA->AP)	11:18:13	0.125		
EAP Req (AP->STA)	not captured			
EAP Resp (STA >AP)	11:18:13	0.146		
EAP Req (AP->STA)	11:18:13	0.162		
EAP Resp (STA->AP)	11:18:13	0.169		
EAP Req (AP->STA)	11:18:14	0.342		
EAP Resp (STA->AP)	11:18:14	0.346		
EAP Req (AP->STA)	11:18:14	0.352		
EAP Resp (STA->AP)	11:18:14	0.361		
EAP Req (AP->STA)	11:18:14	0.368		
EAP Resp (STA->AP)	11:18:14	0.375		
EAP Req (AP->STA)	11:18:14	0.388		
EAP Resp (STA->AP)	11:18:14	0.395		
EAP Req (AP >STA)	11:18:14	0.402		
EAP Resp (STA->AP)	11:18:14	0.416		
EAP Success	not captured			
EAPOL Key 1	11:18:14	0.490		
EAPOL Key 2	11:18:14	0.533		
EAPOL Key 3	not caputred			
EAPOL Key4	11:18:14	0.551		
DHCPDISCOVER	11:18:14	1.019		
DHCPOFFER	11:18:16	3.021		
retry	11:18:16	3.021		
retry	11:18:16	3.022		
retry	11:18:16	3.022		
retry	11:18:16	3.022		
retry	11:18:16	3.023		
retry	11:18:16	3.023		
DHCPDISCOVER	11:18:18	5.046		
DHCPOFFER	11:18:18	5.048		
DHCPREQUEST	11:18:18	5.054		
DHCPACK	11:18:18	5.055		

3.3 接続距離評価

3.3.1 接続距離評価方法

図 3 基地局配置のように，京都大学時計台二階の会議室に基地局を設置し，左遠方より端末を所持した被験者が基地局設置方向に徒歩（時速 4.5km 程度）により近づき，端末が基地局 1 と接続され，http コンテンツがダウンロードされたことを視認したら，被験者は歩行を中止し，その時の基地局からの距離を記録した．

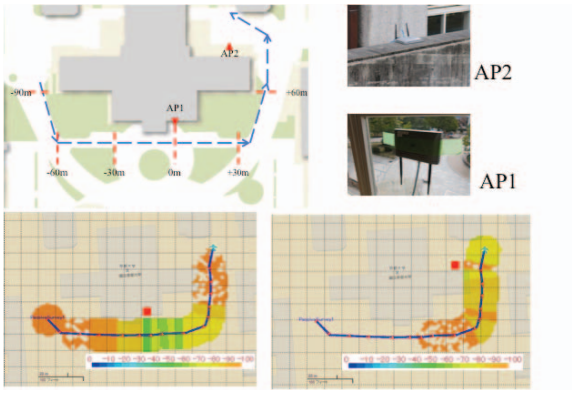

図 3 基地局配置

この実験を．以下の３種類の条件により実施した

(1) **低密度（混在）**

FILS 端末, WPA2 端末をそれぞれ所持した被験者各１名=計２名が並んで歩行する試行を五回繰り返した．

(2) **高密度（混在）**

FILS 端末, WPA2 端末をそれぞれ所持した被験者各 20 名=計 40 名が並んで歩行する試行を行なった．

(3) **高密度（FILS のみ）**

FILS 端末を所持した被験者 41 名が並んで歩行する試行を行なった．

3.3.2 接続距離評価結果

図 4 接続距離（低密度混在）から図 6 接続距離（高密度 FILS）に，各実験の結果を示す．これらの図において，横軸は接続時点の基地局から距離で，中央の破線が基地局の正面位置を示しており，マイナスは基地局正面到達までの距離を，プラスは基地局正面通過後の距離を示している．

また，この時の測定値の集計を表 2 接続距離測定値（高密度混在）及び

表 3 接続距離集計値（高密度 FILS のみ）に示す．この結果より FILS 端末はの接続距離は，単純平均で高密度混在時に−１９m，高密度 FILS のみ時に−１３m であった．このように FILS 端末は高密度時においても，安定して基地局の正面に到達する以前に接続が完了することが確認できた．

これに対して，WPA2 端末は，その多くが基地局正面を通過後に接続完了をしていることが確認できた．

また，FILS 方式では，基地局正面から最大 56m 程度手前でも接続に成功する端末が確認された．これは，FILS 方式では接続開始に要する時間が短いことから，反射伝搬により飛び地的にサービスエリアが形成される場合や，外乱雑音が一時的に低下して所要伝搬品質が短期間に確保された場合も，有効に接続利用可能となっているためと推察する．

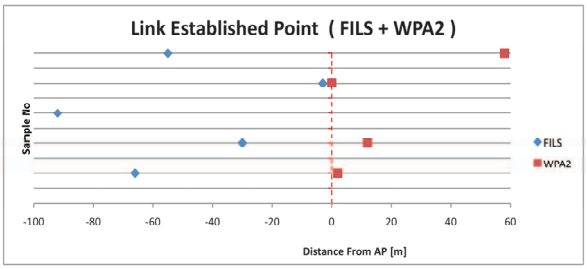

図 4 接続距離（低密度混在）

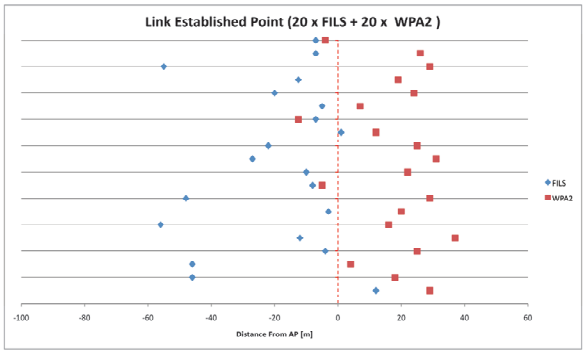

図 5 接続距離（高密度混在）

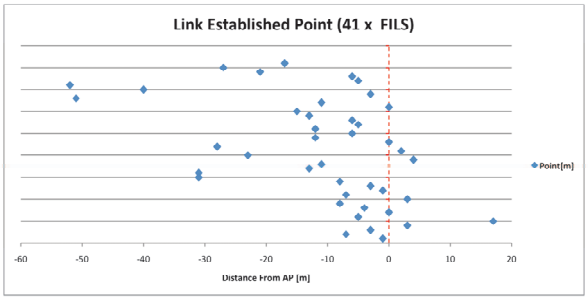

図 6 接続距離（高密度 FILS）

表 2 接続距離測定値（高密度混在）

No	Link Established point [m]	
	FILS	WPA2
1.000	12.000	29.000
2.000	−46.000	18.000
3.000	−46.000	4.000
4.000	−4.000	25.000
5.000	−12.000	37.000
6.000	−56.000	16.000
7.000	−3.000	20.000
8.000	−48.000	29.000
9.000	−8.000	−5.000
10.000	−10.000	22.000
11.000	−27.000	31.000
12.000	−22.000	25.000
13.000	1.000	12.000
14.000	−7.000	−12.500
15.000	−5.000	7.000
16.000	−20.000	24.000
17.000	−12.500	19.000
18.000	−55.000	29.000
19.000	−7.000	26.000
20.000	−7.000	−4.000
Average	−19.125	17.575
σ	20.263	13.394
+3 σ	1.138	30.969
−3 σ	−39.388	4.181
Min	−56.000	−12.500
Max	12.000	37.000

表 3 接続距離集計値（高密度 FILS のみ）

	Point [m]
Average	−13.68
Min	−52.00
Max	17.00
σ	16.49
+3 σ	−30.17
−3 σ	2.81

3.4 サービス評価

3.4.1 サービス評価方法

FILS 方式を実環境で用いた場合，期待される利用シーンの一つである位置，認証依存サービスの可能性を確認するため，以下の手順よる試行を行なった．

京都大学時計台教室二階の窓際及び，建物背面に，基地局各一台を各々のカバーエリアがオーバーラップしないように設置した．

この環境で，遠端より FILS 端末，WPA2 端末をそれぞれ所持した被験者各 20 名=計 40 名に順に二つの基地局のサービスエリアを通過させ各々の基地局と連携した http コンテンツが正しくダウンロードされた端末数を記録した．

3.5 サービス評価結果

本評価の結果，FILS 端末は，二つの基地局において，逐次正しいコンテンツをダウンロードすることに成功したが，WPA2 端末は，半数の端末において一つのコンテンツもダウンロード出来なかった．

これは，WPA2 端末では，最初の基地局への接続時間が長く，接続完了後にコンテンツがダウンロード完了する前に，サービスエリアを通過してしまったためである．

さらに，一つ目のサービスエリアの終点近くで接続に成功し場合，そのリンクを一定時間維持するため，切断後に二つ目の基地局に対する検索を開始することが遅れ，結果として一つもコンテンツをダウンロード出来なかっものと推察する．

4. まとめ

本研究では，従来接続（WPA2）と高速接続（FILS）について，歩行者が遠方より基地局に接近する状況において，初期に接続が行なわれるまでの距離の比較を，端末が疎な場合，密な場合について測定比較を行なった．この結果，FILS 方式では，従来方式に比べ大幅に接続までの距離（時間）が短縮されることを確認した．また，FILS 方式では端末数が増加しても大きな影響が出ない事が確認された．

さらに，短時間の接続認証により飛び地的あるいは短時間にサービスエリアが形成される場合にも，有効に無線 LAN が利用できることが確認された．これは，路・車間通信で交差点通過時の通信や，すれ違い通信等の用途における有用性を示すものと考える．

また，この FILS の特長を活かし，歩行者が，個人 ID 及び接続基地局毎に異なるコンテンツをダウンロードする実証を行なった結果，WPA2 方式ではコンテンツ取得に失敗端末が発生するが，FILS 方式では正しくコンテンツ取得が可能となる事が確認できた．

今回の実証実験では，IEEE802.11ai にて策定中の高速認証技術のうち，基地局検索部分については取り入れていない．そこで，今後は標準化の進捗動向に合わせて，これらの機能の評価を行なう必要がある．

また，今後の評価としては，より定量的な評価を大規模な端末数で行なう事を目的として，エミュレータ等による評価を合わせて実施する予定である．

謝辞

本実証実験は，総務省 情報通信国際戦略局通信規格課の支援のもと，Wi-FILS 推進協議会会員と京都大学関係者各位の協力により行なわれた．ここに，実験に参加協力いただいた関係者に対し謝意を表す．

参考文献

1 Status of Project IEEE 802.11ai
http://www.ieee802.org/11/Reports/tgai_update.htm
2 IEEE802.11 TGai PAR(Project Authorization Request)
https://mentor.ieee.org/802.11/dcn/10/11-10-1152-01-0fia-fast-initial-link-set-up-par.doc
3 IEEE802.11Use Case Reference List for TGai
https://mentor.ieee.org/802.11/dcn/11/11-11-0238-19-00ai-use-case-reference-list-for-tgai.docx
4 IEEE802.11 TGai Requirements Document
https://mentor.ieee.org/802.11/dcn/11/11-11-0745-05-00ai-tgai-functional-requirements.docx