Computer Security Symposium 2017
23 - 25 October 2017

無線 LAN の DoS 攻撃に対する電波伝搬特性を利用した認証方式

広瀬 幸[†1]　猪俣 敦夫[†1]

概要：攻撃者が正規のアクセスポイントに大量のトラフィックを送信する DoS 攻撃（Denial of Service attack）に対して，電波強度を基に攻撃が疑われる端末およびアクセスポイントを検知する無線 IDS（Intrusion Detection System）を設置する対策方法が使用されている．これは，ネットワーク層における対策技術である．電波強度を利用した物理層セキュリティとして電波伝搬の可逆性と場所依存性を生かした無線秘密鍵共有技術が検討されている．そこで伝送特性を考慮した秘密鍵生成法および DoS 攻撃検知を含めた認証方式を提案する．

キーワード：無線システム，電波伝搬，認証

An Authentication Scheme Based on the Channel Characteristics Against to Wireless DoS Attack

Miyuki Hirose[†1]　and　Atsuo Inomata[†1]

Abstract: To protect the network from attacks like wireless denial of service (DoS) attacks, a wireless intrusion detection system (IDS) is designed to compromise a network security. Most conventional IDSs do not go below the IP layer to detect anomalous behaviours and are largely ineffective at securing the lower layers needed to protect wireless networks. Key transmission schemes in multipath environments were proposed. In this paper, we proposed an authentication scheme based on the propagation and transmission characteristics against to wireless DoS attacks.

Keywords: Wireless systems, radio propagation, Authentication scheme

1. はじめに

無線 LAN （Local area networks）の普及に伴い，通信の秘匿性に対する需要は大きい．無線 LAN のアクセスポイントに対する DDoS 攻撃（Distributed Denial of Service attack）は様々な種類がある．このような攻撃に対して無線 IDS (Intrusion Detection System) を設置するなどが挙げられるが，既存の対策はネットワーク層以上で検知している．無線 LAN の代表的な規格である Wi-Fi のセキュリティ規格として，WPA (Wi-Fi Protected Access)/WPA2-TKIP が採用されているが，これらに対する脆弱性が報告され，既に攻撃ツールが公開されている[1]-[2]．これは WEP（Wired Equivalent Privacy）に対する鍵回復攻撃である．さらに弱い事前共有鍵（PSK; Pre-Shared Key）が使用されているときに，辞書攻撃を使用することで WPA のセキュリティ保護された無線ネットワークに対する実際の攻撃が報告されている．攻撃が成功した場合，WEP だけでなく TKIP 暗号プロトコルを用いた通信についても，一部のネットワークパケットの偽造が可能となる．

電波強度を利用した物理層における多重波環境の特性を生かした無線通信のセキュリティを実現する秘密情報伝送・共有技術が検討されている [3]-[5]．複数アンテナの指向性（アンテナ重み）を時間変化させ，相関情報となる受信信号系列の時変化を人工的に生成する方式も提案されている[6]．無線 LAN 規格である IEEE802.11 では 11n より MIMO（Multiple-Input Multiple-Output）技術が使用されている．さらに近年 11ac が登場し，MU-MIMO（Multi user MIMO）技術が採用されている．そこで複数ユーザが想定される無線 LAN 環境において，電波伝搬特性および伝送特性を利用した秘密鍵方式を提案し，さらに DoS 攻撃耐性をもつ認証方式を提案する．

2. 電波伝搬特性を利用した秘密鍵暗号方式

2.1 多重波環境と OFDM 技術

オフィス空間のような屋内電波伝搬では反射や回折による到来波が極めて多数存在する多重波環境となる．このような環境において，あらゆる方向からの到来波が相互に干渉することにより，受信信号強度（RSSI; Received Signal Strength Indication）が変動するマルチパスフェージングが生じる．このようなフェージング対策の 1 つとして ODFM（Orthogonal Frequency Division Multiplexing; 直交周波数分割多重方式）技術が挙げられ，IEEE802.11a/g/n/ac で採用さ

†1 東京電機大学
Institute of Industrial Science, The University of Tokyo

れている. また次世代無線通信規格である 11ad でもオプションとして採用されている．IEEE802.11 の通信規格を表 1 にまとめる．OFDM 技術は無線通信でデータを送信する際の伝送方式の 1 つで，占有周波数を複数のチャネルに分割し，信号を送る技術である．詳細は付録 A に記述する．

2.2 電波伝搬特性および場所依存性を利用した秘密鍵共有方式

多重波環境の特性を生かした秘密情報伝送・共有技術は通信路の可逆性に基づいている．秘密鍵共有方式であることから簡易な回路で実現可能であり，鍵配送などの鍵管理を必要としないので十分な安全性が実現できるという特徴がある．無線局の移動により伝搬路特性が変化した場合，基地局 A, B（以降 BS_A, BS_B）における受信信号は反射波や回析などによりフェージングの影響を受ける. ここで，BS_A からの送信と BS_B から同じ周波数で同じ時間に送信すれば，両方の基地局における受信時のフェージング，つまり伝搬特性は，同一特性となる．この伝搬特性をもとにしてデジタル系列などを生成することにより，暗号鍵などの共通する情報を両局で共有することができる．それに対して，異なる地点に位置する他局は異なるフェージング特性を受けることになるため，同じ伝搬路情報を得ることができず，最終的に秘密通信を解読するための暗号鍵を推定することができない．フェージングの影響によりアンテナをわずか数センチ移動させるだけで電波の強さが大きく変動する様子を図 1 に示す．図 1 は周波数 2 GHz で 50 cm × 50cm の範囲における伝搬利得の測定結果である．これが，電波伝搬特性を活用した秘密情報の伝送・共有技術の基本原理となる.

このような方法では，あらかじめ鍵を設定する従来方法とは異なり，秘密鍵共有を任意の時点で随時行うことも可能であり，鍵の更新によりセキュリティを更に向上させることができる．また，伝搬路特性から生成した秘密情報をより複雑な暗号や他の情報秘匿技術の鍵として使用することにより更に高度なセキュリティを実現することも可能である．しかしながら，フェージング環境における無線信号は高速かつ大きく特性が変動し，また雑音の影響も大きいと予想される．したがって，このような秘密情報の伝送・共有を実現するためには，フェージングや雑音に対する対策技術が必要となる.

表 1　IEEE802.11 の通信規格

	周波数帯 [GHz]	伝送方式	変調方式	チャネル幅 [MHz]	最大伝送速度
11b	2.4 GHz	DSSS	DBPSK DQPSK CCK	20	11 Mbps
11a	5 GHz	OFDM	BPSK 16QAM QPSK 64QAM		54 Mbps
11g	2.4 GHz				
11n	5 GHz /2.4 GHz	OFDM/ MIMO		20/ 40	100 Mbps 以上 600 Mbps (MIMO)
11ac	5 GHz		BPSK 16QAM 256 QAM QPSK 64QAM	40 / 80/ 160	256QAM: 433 Mbps, 6.93 Gbps (8×8MIMO)
11ad	60 GHz	シングルキャリア / OFDM	π/2-BPSK π/2-QPSK π/2-16QAM	最大 9 GHz	最大 7 Gbps

DSSS: Direct Sequence Spread Spectrum
DBPSK: Differential Binary Phase Shift Keying
DQPSK: Differential Quadrature Phase Shift Keying
CCK: Complementary Code Keying

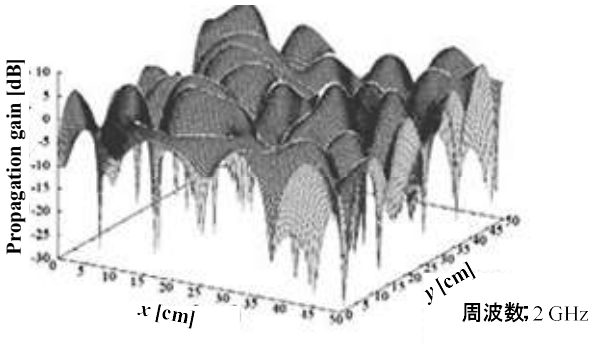

図 1　周波数 2 GHz 帯における伝搬利得の変動.

3. 無線 LAN 認証方式

3.1 Wi-Fi 認証方式

Wi-Fi の接続までの概要は以下のようになる.

1. アクセスポイントは，ビーコンと呼ばれる信号を定期的（100 ミリ秒間隔）にネットワーク内のすべてのクライアントにブロードキャスト送信する.
2. アクセスポイントは，ビーコンと呼ばれる信号を定期的（100 ミリ秒間隔）にネットワーク内のすべてのクライアントにブロードキャスト送信する.
3. 無線端末（クライアント）は，まず電波を自動スキャンし，アクセスポイントが使っている周波数を検知し，

利用できる周波数帯域からビーコンを受信する

4. Probe Request（プローブ要求）
   – クライアントはビーコンを受信すると，自身が設定している ESS-ID（Extended Service Set Identifier）かどうかをアクセスポイントに対して問い合わせ，確認する．クライアントは自分の ESS-ID を使って，同じ ESS-ID を持つアクセスポイントに接続しようとする．
5. Probe Response（プローブ応答）
   – クライアントからの問い合わせで，同じ ESS-ID であれば，アクセスポイントは返事する．
   – 応答があればクライアントは，その無線 LAN に物理的に繋がった状態になる．
6. Authentication
   – 接続を許可して良いかどうかの判断をする．
   – 事前にクライアントとアクセスポイントが設定していた認証方式を使って認証する．
7. Association Request
   – 正しいクライアントだと判断されると，クライアントからアクセスポイントに接続要求する．
8. Association Response
   – Association Request に対してアクセスポイントが許可する．
   – 接続が完了し通信を行うことが可能となる．

しかしながら，様々な脆弱性があり以下のような問題が報告されている．

– SSID（Service Set Identifier）を取得することで，その SSID に対する request-prove を大量に発行することでアクセスポイントの機能を不可にする．
– MAC アドレスのなりすまし．
– 大量のトラフィックを送りつけることでアクセスポイントの機能を不可にする．

また MAC 認証手順の不便さも挙げられる．そこで物理層におけるセキュリティ対策を考える．

3.2 提案する認証方式

図 2 のような認証前に DoS 攻撃を検知システム導入した電波伝搬および伝送特性を利用した秘密鍵による認証方式を提案する．この秘密鍵には電波伝搬特性による場所依存性が含まれていることから，MAC アドレスなりすましも防ぐことが可能である．

3.3 電波伝搬特性および伝送特性を用いた秘密鍵生成方法

DoS 攻撃検知アルゴリズムにも暗号鍵を利用するので，まず秘密鍵生成方法について記述する．通信路の可逆性および場所依存性を基にしている電波伝搬特性を利用した秘密鍵生成方式[3]に無線 LAN で採用されている OFDM 技術を考慮した新たな秘密鍵共有方式を考える．OFDM 技術を利用した鍵生成については，文献[7]で提案されているがこれは 802.11a を想定している．そこで複数アンテナである MIMO システムおよびチャネル幅を考慮した鍵生成を提案する．

表 2　IEEE802.11 における OFDM のサブキャリア数

チャネル幅 [MHz]	FFT サイズ	データ サブキャリア数	パイロット サブキャリア数
20	64	52	4
40	128	108	6
80	256	234	8
160	512	468	16

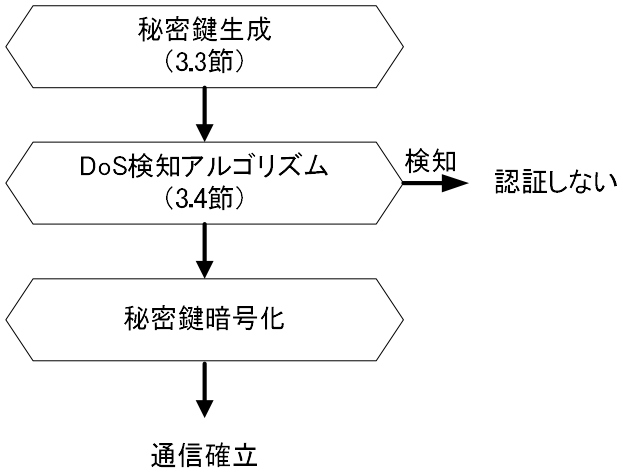

図 2.　提案方式の流れ

OFDM 技術は周波数軸上で搬送波（キャリア）を分割したサブキャリアにより構成される．表 1 より 11n のチャネル幅は 20/40 MHz，11ac は 40/80/160 MHz であり，その時の分割されたキャリア数を表 2 にまとめる．推定した一つの伝送路の周波数特性は，周波数軸に 312.5 kHz 刻みで 108 点（中心周波数を除く）のデータ値で構成される．108 点のデータ値をすべて使用すると，遅延スプレッドが小さい環境においてサブキャリア間の周波数相関が極めて高くなるため，2 値化処理を行った後，0 または 1 が連続的に発生する問題が発生する．このため，データ間の周波数刻みを大きくとることとする．108 点のデータ値に中心周波数（ヌルデータ）を含めた 109 点のデータ値について，周

波数が低い方から 5 点置きにデータ値を選び，20 点の標本値を得る．データ間は 1.875 MHz になるため，周波数相関は小さくなる．また，これら一連の処理を時間軸に 90 ms 刻みで 10 回行い，時間・周波数領域全体で 200 点の標本点を求める．この 200 点の標本点全体の平均値をしきい値とし，これを基準にして 2 値化し，200 ビットのデータを生成する．WPA2 で採用されている AES アルゴリズムを使用することにより 128 ビットもしくは 192 ビット鍵を生成することができる．一度，秘密鍵を共有できたならばその鍵を使い続けることができるため，端末は移動可能である．また，共有鍵の変更を行いたい場合には改めて秘密鍵を生成する．

3.4 場所依存性および電波伝搬特性を利用した DoS 攻撃検知アルゴリズム

前節で提案した秘密鍵を利用して認証前の DoS 攻撃を防ぐ方法を提案する．図 3 のようなネットワーク構成について考える．各ユーザは電波伝搬および伝送特性を利用した暗号鍵を所持しており，鍵の組み合わせはそれぞれ異なる．アクセスポイントは，その鍵に対応した MAC カウンタを用意し，プローブ要求を大量に発行するようなクライアントをネットワークから外す．カウンタ機能はシンプルで複雑なシステムにはならない．ここでプローブ要求は，クライアントが送信する 802.11 管理フレームである．iOS や android のプローブ要求の平均間隔を表 3 に示す[8]．少なくとも平均的なプローブ要求間隔は 1 分以上であることが確認できる．また，Pry-Fi [9]のような攻撃ツールでは 1 分間に 3.3 回以上 100 分連続で攻撃をすることが報告されている．そこで，同じ鍵を持つクライアントからの信号が 1 分間に 2 回以上連続したら承認しないようにする．ここでアクセスポイントのカウンタ機能で防ぐことが可能（つまりアクセスポイントとサーバ間の通信には影響しない）であるから，既に通信が確立している他ユーザの通信には影響しない．未認証の鍵には生存時間および上限を設ける．生成した鍵が生存時間に達するか上限数になったら古い鍵から削除する．

4. 提案する鍵生成方式のシミュレーション

表 1 より IEEE802.11n および 11ac で採用されている変調方式 QPSK（Quadrature Phase Shift Keying）を OFDM で伝送する QPSK-OFDM 伝送を想定して生成した秘密鍵について検討する．この変調方式は 1 シンボル 2 ビット構成で，図 5 のように搬送波の位相を π/2 ラジアンごとに変化させた位相（PSK; Phase Shift Keying）変調方式である．

図 6 に QPSK-OFDM における送受信アンテナ数を変化させた場合の SN 比に対する鍵の不一致率の計算結果を示す．ここでは，レイリーフェージング環境を想定している．図

表 3　Wi-Fi プローブ要求間隔の平均時間 [秒]

Android L 5.0.1	Android 4.4.2	iOS 8.1.3
66	72	330

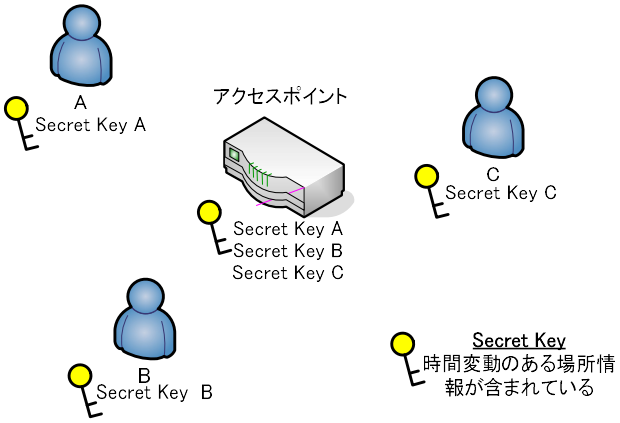

図 3.　ネットワーク構成例.

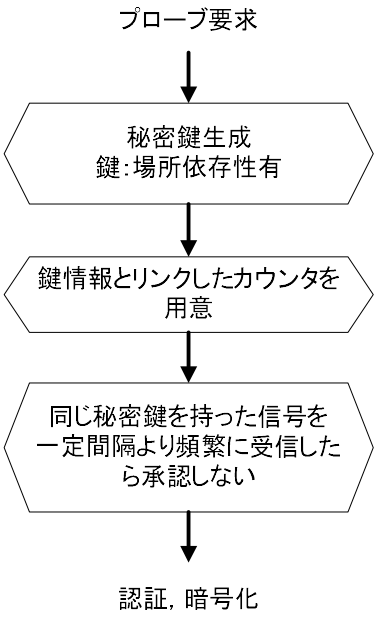

図 4.　DoS 攻撃検知を設けた場合の認証手順

より送信アンテナ 1，受信アンテナ 1 の場合（1×1）より送信アンテナ 2，受信アンテナ 2（2×2）の MIMO 環境の方が，不一致率が小さいことが確認できる．これはアンテナ数が増加することで信号を多重化し，伝送効率伝送効率が上がったためと考えられる．

5. まとめ

無線 LAN における攻撃において，既存のシステムはネットワーク層以上で検知している．そこで既存の電波伝搬特性を利用した秘密鍵の共有技術に，送受信アンテナ数も含めて伝送特性を考慮した秘密鍵生成法を提案しシミュレーションをした．さらに認証前の DoS 攻撃を検知するアルゴリズムも掲示した．ここではプローブ要求を大量発行する DoS 攻撃を対象にしている．今後の課題として提案方式の伝送環境を変化させた場合について検討し，さらに実験を行う．また，無線および有線 LAN には IEEE802.11x 認証が規格化されており，現行認証との比較についても検討する．

参考文献

[1] M. Beck and E. Tews, “Practical attacks against WEP and WPA,” in *Proceedings of the second ACM conference on Wireless network security*, pp. 79-86, 2009.

[2] M. Beck and E. Tews, “Practical attacks against WEP and WPA,” preprint version available at http://dl.aircrack-ng.org/breakingwepandwpa.pdf, 2008.

[3] 岩本 尚希，笹岡 秀一，岩井 誠人,“複数アンテナを用いた秘密鍵共有方式の秘密鍵容量,” 電子情報通信学会論文誌 B, vol. J98-B, no. 7, p. 547-556, 2015.

[4] D. Katselis and P. Papadimitratos, “On secret key generation through multipath for wireless networks,” in 2013 *IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, Athens, Greece, Dec. 2013.

[5] B. Zan, M. Gruteser, and F. Hu, “Key agreement algorithms for vehicular communication networks based on reciprocity and diversity theorems,” *IEEE Trans. Vehicular Tech.*, vol. 62, no. 8, pp.4020-4027, 2013.

[6] 樋口拓己，笹岡秀一，岩井誠人，“伝搬係数の共有とアンテナ重み情報の公開伝送を用いた秘密情報共有の検討,” 信学技報, IEICE-RCS2016 -164, pp.65-70, Oct. 2016.

[7] 北浦 明人，笹岡 秀一,“陸上移動通信における OFDM の伝送路特性に基づく秘密鍵共有方式,” 電子情報通信学会論文誌 A, vol. J87-A, no. 10, p. 1320-1328, 2004.

[8] J. Freudiger, “Short: How talkative is your mobile device? An experimental study of Wi-Fi probe requests,” in *8th ACM Conf. on Security and Privacy in Wireless and Mobile Networks (WiSec'15)*, NY, USA, June 2015.

[9] http://thehackernews.com/2014/02/chainfire-released-pry-fi-android-app.html

[10] 三瓶政一，“デジタルワイヤレス伝送技術,” ピアソン・エデュケーション, 2002.

付録

付録 A　OFDM 技術について

OFDM は周波数分割多重化の一種で，マルチキャリア変調である．送信信号を複数の副搬送波（サブキャリア）に分け，データ信号を周波数軸上で並列に多重化する方式である [10]．各サブキャリアは BPSK，QPSK などの位相変調方式や QAM（直交振幅変調方式）で一次変調されており，お互いに直交している．OFDM 信号のサブキャリアはお互いに重なり合うように密に配置されているが，フーリエ変換によって各サブキャリア信号を完全に分離することができ，サブキャリア各波が干渉し合うことなく並列伝送できる．サブキャリア毎の変調信号が重なり合っているのに独立して受信可能なのは，図 A-1 のように，各サブキャリアの中心周波数に他のサブキャリア信号のヌル点（信号電力密度がゼロになる周波数）が一致しているためである．例えば IEEE802.11n では，帯域幅 312.5 kHz の 56（うちデータ用は 52）のサブキャリアに分割し，低域の方から Band #1，Band #2 と番号付けを行う．各サブバンドは直交周波数分割多重（Orthogonal Frequency Division Multiplex，OFDM）している．

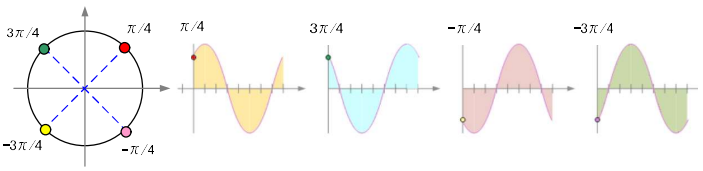

図 5.　QPSK 信号点配置図（位相表示）．

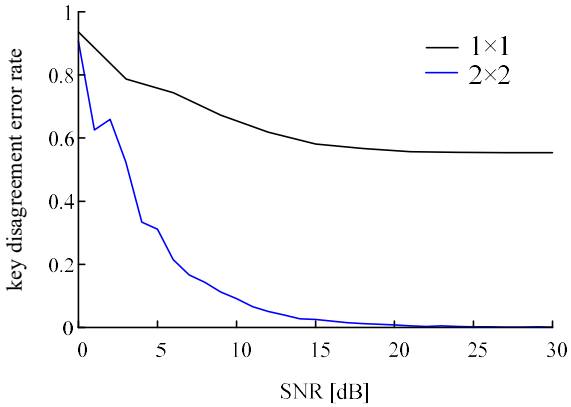

図 6.　QPSK- OFDM における鍵不一致率特性．黒線が送信アンテナ 1，受信アンテナ 1 の場合，青線が送信アンテナ 2，受信アンテナ 2 の場合．

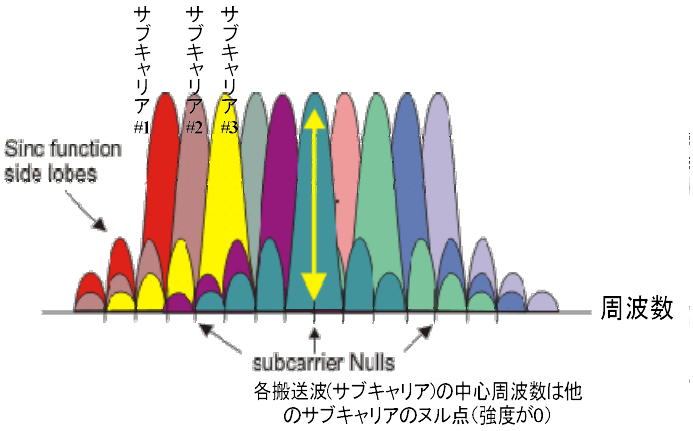

図 A-1.　OFDM 方式のスペクトル配置．