無線 LAN 暗号化方式 WPA-TKIP の脆弱性とそれを用いた攻撃方法の提案

小澤 勇騎 †　　大東 俊博 ††　　森井 昌克 ‡

† 神戸大学工学部
〒 657-8501 神戸市灘区六甲台町 1–1

†† 広島大学情報メディア教育研究センター
〒 739–8511 広島県東広島市鏡山 1–4–2

‡ 神戸大学大学院工学研究科
〒 657-8501 神戸市灘区六甲台町 1–1

あらまし 2008 年に Beck と Tews によって WPA-TKIP に対するメッセージ改ざん攻撃が提案された．彼らの攻撃 (Beck-Tews 攻撃) は 12〜15 分の実行時間で MIC 鍵の復元および ARP パケットのような短い暗号化パケットを改ざんできる．しかしながら，Beck-Tews 攻撃は IEEE802.11e をサポートした無線 LAN 機器に対してのみ実行可能な限定的な攻撃であった．JWIS2009 において，我々は IEEE802.11e をサポートしない無線 LAN 機器に対しても実行可能な中間者攻撃に基づくメッセージ改ざん攻撃を提案している．さらに，メッセージ改ざん方法を工夫することによって攻撃実行時間が 1 分程度まで減少することを示した．しかしながら，この実行時間は大きく見積もった値であり，実際には実行時間は更に短いと予想される．本稿では，無線 LAN 機器を利用した攻撃実験によって JWIS2009 の攻撃の実行時間を評価し，実際の実行時間は平均で 10 秒程度であることを示す．

Weaknesses on WPA-TKIP and Application to the Message Falsification Attack

Yuki Ozawa†　　Toshihiro Ohigashi ††　　Masakatu Morii‡

†Faculty of Engineering, Kobe University
1–1 Rokkodai-cho, Nada-ku, Kobe 657–8501 Japan

††Information Media Center, Hiroshima University
1–4–2 Kagamiyama, Higashi-Hiroshima, Hiroshima 739–8511 Japan

‡Graduate School of Engineering, Kobe University
1–1 Rokkodai-cho, Nada-ku, Kobe 657–8501 Japan

Abstract In 2008, Beck and Tews have proposed a message falsification attack on WPA-TKIP. Their attack (called the Beck-Tews attack) works for only wireless LAN products that support IEEE802.11e QoS features. The Beck-Tews attack can recover a MIC key and falsify an encrypted short packet (for example, an ARP packet) with 12-15 minutes. In JWIS2009, we have proposed a new message falsification attack based on the man-in-the-middle attack, and this attack attack can work for any WPA implementations. Additionally, we reduce the execution time of the attack to about 1 minute in the best case. However, the execution time written in JWIS2009 has been obtained from the rough theoretical estimation. In this paper, we evaluate the execution time of our attack by the experiment in a realistic environment. As a result, we demonstrate that the average execution time of our attack is about 10 seconds in the best case.

1　まえがき

WPA(Wi-Fi Protected Access) [1] は無線 LAN 通信の機密性や完全性を保護するセキュリティプロトコルであり，従来から使われてきた WEP(Wired Equivalent Privacy) [2] の脆弱性 [3, 4, 5] を取り除く仕組みを導入している．WPA-TKIP の安全性は多くの研究者によって議論されているが，辞書攻撃 [6] が可能なパスフレーズを使っているなど特定の条件を除いては現実的な攻撃は知られていなかった．

2008 年に Beck と Tews は 12〜15 分で WPA-TKIP の改ざん検出用鍵 (MIC 鍵) を復元でき，ARP パケットなどの短い暗号化パケットの偽造できる攻撃 (Beck-Tews 攻撃) を提案した [7]．Beck-Tews 攻撃では，chopchop 攻撃 [5] と呼ばれる WEP に対するリプレイ攻撃を IEEE802.11e をサポートしているという条件で WPA-TKIP に適用する．WPA-TKIP では暗号化パケットを受理する毎に増加する TSC カウ

ンタと呼ばれる値を保持しており，TSC カウンタより小さな値に対応する暗号化パケットを破棄することでリプレイ攻撃を防いでいる．IEEE802.11e では通信に複数のチャネルを利用し，かつ各チャネルで独立して TSC カウンタを管理することから，TSC カウンタが小さなチャネルに対するリプレイ攻撃を実行できる．また，Beck-Tews 攻撃は ARP ポイズニングや DNS ポイズニングを実行することで現実的な被害が生じさせることから注目が集まった．

Beck-Tews 攻撃は IEEE802.11e をサポートした無線 LAN 機器に対してのみ実行可能な限定的な攻撃であり，しかも 11 分以上の時間を攻撃に要する．そこで，我々は JWIS2009 において IEEE802.11e をサポートしない無線 LAN 機器にも適用可能で，かつ大幅に攻撃時間を短縮する方法を提案している [8]．我々の攻撃は中間者攻撃に基づいている．中間者攻撃とは攻撃者がアクセスポイントとクライアントの中間に入り，送受信者間の直接の通信を遮断させた状態で攻撃を行う方法である．我々は攻撃対象として，直接通信が行えない距離にあるアクセスポイントとクライアントを仮定している．送受信者が直接通信が行えない状況においては受信者の TSC カウンタの値が増加しないため，リプレイ攻撃である chopchop 攻撃が実行可能となる．またメッセージ改ざん方法を工夫することによって，1 分程度で攻撃が成功することを示している．しかしながら，文献 [8] で示した 1 分という実行時間は大きく見積もった値であり，実際にはさらに短くなる可能性がある．そこで本稿では，実際の無線 LAN 機器を用いた攻撃実験によって我々の攻撃の実行時間を評価し，実際の実行時間は平均で 10 秒程度であることを示す．

2 Wi-Fi Protected Access

WPA-TKIP ではクライアントとアクセスポイント間でマスタ鍵 (128 ビット) を共有し，マスタ鍵から 64 ビットの MIC 鍵および 128 ビットの暗号鍵を生成する．MIC 鍵はメッセージ完全性符号 (MIC) を生成するために用いられ，暗号鍵はパケットの暗号化に用いられる．

2.1 送信側の処理

初めに，送信者は送信データである MSDU(MAC Service Data Unit) に改ざんチェック用の MIC を付加する．MIC は MIC 鍵 K^* と MSDU から計算される 64 ビットの値であり，受信者は計算で得られた MIC と付加された MIC の値を比較して改ざんの有無を検査する．MIC 生成アルゴリズムは Micheal を使っており，このアルゴリズムを $micheal()$ としたとき MIC の付加の処理は以下のように表わされる．

$$MSDU||micheal(K^*, MSDU) \tag{1}$$

ここで，|| はビットの連結である．

次に，MIC を付加された MSDU は一定のサイズ毎に MPDU(MAC Protocol Data Unit) にフラグメント化される．さらに，フラグメント化された

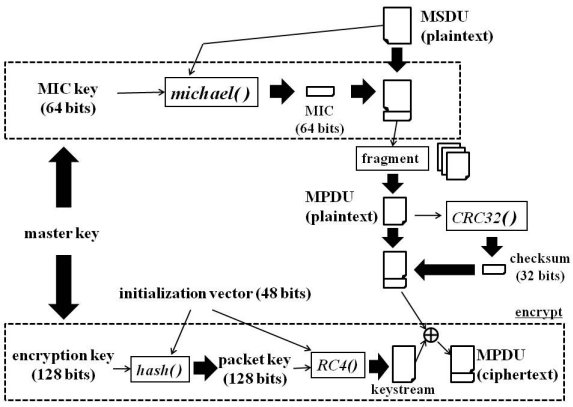

図 1: 送信側の処理

MPDU から CRC-32 を用いて 32 ビットのチェックサムを計算し，以下のように付加する．

$$MPDU||CRC32(MPDU) \tag{2}$$

ここで，$CRC32(MPDU)$ はチェックサムである．

チェックサムを付加された MPDU は，128 ビットの暗号鍵と 48 ビットの初期化ベクトル (IV: Initialization Vector) を用いて暗号化される．WPA-TKIP の IV は暗号化処理毎に 1 ずつ増加する公開値である．暗号化処理では，暗号鍵と IV を独自のハッシュ関数 $hash()$ を使って混合し，パケット毎に異なる鍵であるパケット鍵 PK を生成する．暗号化アルゴリズムはストリーム暗号である RC4 [9] を用い，パケット鍵と IV を種として生成する擬似乱数系列 (キーストリーム) $\{Z_1, Z_2, \ldots, Z_L\}$ と平文 $\{P_1, P_2, \ldots, P_L\}$ の排他的論理和 (XOR) をとることで以下のように暗号文 $C_1, C_2, \ldots, C_L$ を得る．

$$C_i = P_i \oplus Z_i (i = 1, 2, \ldots, L) \tag{3}$$

ここで，C_i, P_i, Z_i はそれぞれ 1 バイトの変数であり，L は平文長である．

最後に，暗号文に IV を平文の状態で付加して受信者に送信する．図 1 に WPA-TKIP の送信側の処理を示している．

2.2 受信側の処理

受信者は IV と暗号文を受け取ると，IV の値と TSC カウンタの値を比較する．TSC カウンタは過去に受理したパケットを用いたリプレイ攻撃を防ぐために用いられる．具体的には TSC カウンタには過去に受理した MPDU の暗号化の中で最も大きな IV の値が代入されており，送られてきた IV が TSC カウンタより大きくなければ過去に送られた暗号化パケットとみなして棄却する．なお，MSDU が受理されたときに初めて，それを構成している MPDU の暗号化パケットが受理されたとみなす．

復号処理では，マスタ鍵と受信した IV から送信者と同一のパケット鍵 PK を生成する．そのパケッ

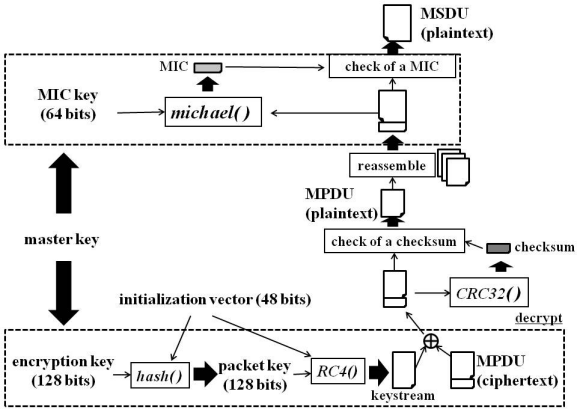

図 2: 受信側の処理

ト鍵を RC4 に入力することで送信側と同じキーストリーム Z を生成し，以下のように平文 P を得る．

$$P_i = P_i \oplus Z_i \oplus Z_i = C_i \oplus Z_i \quad (i = 1, 2, \ldots, L) \quad (4)$$

復号された MPDU は CRC-32 によってチェックサムが計算され，受信したチェックサムと比較される．チェックサムが異なる場合，通信のエラーが発生したとみなし，受信したパケットを破棄する．

すべての MPDU が得られたとき，それらから MSDU 及び MIC が復元される．受信者はマスタ鍵から送信者と同一の MIC 鍵を生成し，Micheal を使って受信した MSDU から MIC を計算する．計算された MIC は付加された MIC と比較され，値が異なれば MSDU が改ざんされたとして関連する全ての MPDU のパケットを破棄し，送信者に MIC エラーメッセージを返す．WPA-TKIP にはカウンタメジャーと呼ばれる方法が実装されており，もし MIC エラーが 1 分間に 2 回以上起きたときには通信を 1 分間閉鎖した後，MIC 鍵を変更して新しいセッションを開始する．したがって，攻撃者は MIC エラーが 1 分間に 2 回以上生じる攻撃の実行が困難となる．MIC エラーが生じずに MSDU が受理されたとき，関連する MPDU の中で最も大きな IV の値を TSC カウンタの値に更新する．図 2 に WPA-TKIP の受信側の処理を示している．

3 従来研究

3.1 chopchop 攻撃

chopchop 攻撃は WEP に対する攻撃であり，暗号文から平文の情報が得られる．WEP では IV のチェックを行わないため，過去に取得した暗号化パケットから改ざんパケットを作り受理させるリプレイ攻撃が可能である．またパケットの改ざんチェックはチェックサムでしか行われず，チェックサムが一致しなかった場合には送信者に対してチェックサムのエラーメッセージを返す．

chopchop 攻撃は CRC-32 の性質に注目して平文を復元する．MPDU にチェックサムが付加された平文を P，P の最下位バイトを R，P から R を取り除いた平文を $P^{'}$ とする．WEP では下位 4 バイトの値をチェックサムと判断されて処理され，$P^{'}$ のチェックサムの比較では高確率で一致せずにエラーが出力される．CRC-32 を用いる場合，R から計算されたデータ $f(R)$ を P' に XOR してデータを修正したとき，そのデータはチェックサムが正しい値になることが示されている [7]．関数 $f()$ については紙面の都合で割愛する．上記の性質を利用すれば R が未知の場合に正しい R を推測することができる．攻撃者が R を知りたいとき，攻撃者は 256 通りの R の候補 R^* に対して $f(R^*)$ を計算し，それを使って $P^{'}$ を修正する．修正されたデータをアクセスポイントもしくはクライアントに対して送信し，チェックサムのエラーメッセージの有無を確認する．R^* が誤っている場合にはチェックサムのエラーが送信され，R^* が正しい場合はエラーメッセージは送信されない．したがって，最大 256 回のパケットを送信してエラーメッセージを観測することで正しい R を復元できる．ストリーム暗号を利用している WEP では上記の攻撃シナリオを暗号化パケット C に対しても実行可能である．また，この攻撃を再帰的に x 回実行すれば平文 P の下位 x バイトを復元可能である．

3.2 Beck-Tews 攻撃

Beck-Tews 攻撃とは chopchop 攻撃を WPA-TKIP へ適用したものである．WPA-TKIP では TSC カウンタによって IV の値がチェックされるため，過去に破棄されたパケットを攻撃に使用できない．そこで Beck と Tews は IEEE802.11e(QoS 制御) に注目し，この問題を解決した．IEEE802.11e とは 8 つのチャネルに対して異なるデータを流すことが可能であり，それぞれのチャネルは独自の TSC カウンタを有している．それぞれのチャネルの TSC カウンタにはバラつきがあることから，あるチャネルでキャプチャした IV=x の暗号化パケットを TSC カウンタが $x-1$ 以下のチャネルを探して送信することができ，chopchop 攻撃のようなリプレイ攻撃を成立させられる．また，WPA-TKIP では chopchop 攻撃で平文が復元できたときに MIC の比較まで処理が進むことから，MIC のエラーメッセージの送信の有無を監視することで正しい平文の値を得ることができる．

さらに彼らは，サイズが小さく未知のバイト数が少ない ARP パケットに注目した．彼らは，ARP パケットのデータ部分で，送信者および受信者の IP アドレスの最下位バイト (2 バイト) が未知である場合を想定した．これは無線 LAN 機器を工場出荷時の状態で利用するユーザを考えた場合，妥当な仮定だと考えられる．この場合，MIC とチェックサムを合わせた計 14 バイトが未知となる．Beck-Tews 攻撃では暗号化された ARP パケットから平文の復元を行う．攻撃者は chopchop 攻撃を 12 回行うことにより，MIC とチェックサムを復元する．MIC のエラーメッセージは 1 分間に 2 回以上送らないようにすべきであるため，MIC エラー間には少なくとも 1 分の待ち時間が必要となる．したがって，chopchop

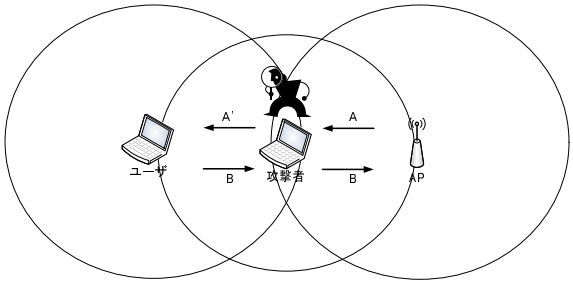

図 3: 中間者攻撃のモデル

攻撃を 12 回実行するとき，少なくとも 11 分の待ち時間が生じる．送信者および受信者の IP アドレスの最下位バイト (2 バイト) の復元は，時間がかかる chopchop 攻撃を利用せず，チェックサムとの比較によって実現する．まず，2 バイト分，すなわち 2^{16} 通りの ARP パケットの候補を作り，それらと復元した MIC を用いて 2^{16} 通りのチェックサムを計算する．次に計算されたチェックサムと chopchop 攻撃によって得られている正しいチェックサムのデータを比較し，チェックサムが一致する ARP パケットの候補を得る．得られた候補数が 1 通りである場合，その候補が正しい ARP パケットとして推定される．Beck-Tews 攻撃の場合，ほとんどの場合で 1 通りに絞り込むことができる．以上により，暗号化された ARP パケットからすべての平文情報が復元でき，平文と暗号文を XOR することで対応するキーストリームも復元できる．また Micheal が可逆な関数であることから，ARP パケットおよび MIC から MIC 鍵を容易に復元できる．MIC 鍵と IV に対応するキーストリームが得られたことにより，キーストリームのサイズまでの暗号化パケットなら自由に偽造できるようになる．

Beck と Tews は MIC 鍵が得られている場合に Beck-Tews 攻撃の実行時間を短縮させられることを示した．これは，MIC 鍵が更新されていない期間に再度攻撃をする場合に有効に働く．MIC 鍵が得られているとき，chopchop 攻撃で得る必要があった MIC は ARP パケットと MIC 鍵から計算できるようになる．したがって，2^{16} 通りの ARP パケットの候補からチェックサムの候補を計算する際に 8 回の chopchop 攻撃の実行を短縮できる．すなわち，攻撃者は chopchop 攻撃を 4 回実行してチェックサムの正しい値を復元し，計算で得られたチェックサムの候補と比較することで平文情報を得ることができる．更に平文情報から対応するキーストリームの復元およびパケットの改ざんが可能になる．この攻撃では MIC エラーによる待ち時間は 3 分であり，攻撃全体の実行時間は 4 分程度となる．

4 提案攻撃

4.1 中間者攻撃のモデル

Beck-Tews 攻撃は IEEE802.11e をサポートした無線 LAN 機器のみ実行可能な攻撃である．これを一般の無線 LAN 機器で拡張することを考えたとき，中間者攻撃のモデルが適している．中間者攻撃は攻撃者がアクセスポイントとクライアントの中間に入り，送受信者間の直接の通信を遮断させた状態で攻撃を行う．我々の場合は，直接通信が行えない距離にあるアクセスポイントとクライアントを攻撃対象とする．送受信者が直接通信が行えない状況においては受信者の TSC カウンタの値が増加しないため，Beck-Tews 攻撃のようなリプレイ攻撃が可能になる．図 3 に我々の提案する中間者攻撃のモデルを示す．我々の攻撃では，中間者攻撃を行う際に以下の 3 つのモードを使用している．

リピータモード: SSID ビーコンを含めた送受信間の全てのパケットをリレーし，送受信者の通信を確保させるためのモードである．このモードは攻撃者が攻撃を行わないときに用いられ，利用者に攻撃の事実を気付かれにくくできる．

MIC 鍵復元モード: MIC 鍵を復元する際に用いられるモードであり，MIC 鍵がない場合の Beck-Tews 攻撃と同様の手順で chopchop 攻撃と平文の復元を行うため 12 分程度の実行時間が必要となる．このモードでは受信者の TSC カウンタの値が増加させないため，送受信者間のパケットをリレーできず通信が途絶する．したがって，通信頻度が低いタイミングを利用してこのモードを実行する必要がある．

メッセージ改ざんモード: MIC 鍵が得られているという条件で暗号化されたパケットの平文を解読及び改ざんを高速に実行するモードである．一度 MIC 鍵が復元されれば送受信者間の MIC 鍵が変更されるまでこのモードは使用できる．この際にも，送受信者間の通信の途絶は生じるが実行時間を極力短くすることで通信頻度が高い場合でもパケットを改ざんできるようになる．Beck-Tews 攻撃と同様の方法では実行時間は 4 分程度になるため，提案攻撃では 4.2 節の方法によって実行時間を 1 分程度まで短縮している．

4.2 攻撃実行時間の短縮手法

Beck-Tews 攻撃を利用する場合，MIC 鍵が得られている条件でのメッセージ改ざんモードの実行時間は 4 分程度となる．4 分の通信途絶時間が生じることは改ざん攻撃を困難にすると考えられるため，本節では MIC 鍵復元モードで得られる情報や確率的な方法によって攻撃実行時間を短縮する．

MIC 鍵復元モードで MIC 鍵を復元するとき，同時に平文の情報からアクセスポイントの IP アドレスも得られる．通常はアクセスポイントの IP アドレスは固定するため，それ以後の攻撃では ARP パケットの未知の情報はクライアントの IP アドレスの最下位バイト (1 バイト) だけになる．したがって，攻撃者は MIC 鍵を用いて 1 バイト分 (256 通り) の ARP パケットに対するチェックサムを計算し，chopchop 攻撃で得られたチェックサムと比較すれば良い．絞り込む候補数が 2^{16} から 2^8 まで減少するため，候補を 1 個に絞り込みやすくなり攻撃成功確率は上昇する．

次に，攻撃実行時間を短縮するために，チェックサムの比較を 4 バイト全てではなく最下位バイトだけで行うように変更する．この場合，chopchop 攻撃の実行回数が 1 回まで減少し，MIC エラーによる待ち時間が生じないため Beck-Tews 攻撃と比べて少なくとも実行時間は 3 分短くなる．したがって，1 分程度で平文の復元およびパケットの改ざんを実行できる．

攻撃が成功する，すなわちチェックサムの最下位バイトの比較で 2^8 の候補を 1 個に絞り込める確率を示す．この確率は，誤った $2^8 - 1$ 個の候補から計算されたチェックサムの最下位バイトが全て正しい値と一致しない確率から以下のように計算できる．

$$\left(\frac{2^8 - 1}{2^8}\right)^{2^8 - 1} \sim 0.369 \tag{5}$$

したがって，約 37%の ARP パケットが 1 分程度で復元できることが分かる．

5 評価実験

4.2 節の提案攻撃の実行時間は大きく見積もった値であり，実際には chopchop 攻撃を 1 回に要する時間は 1 分より短いと予想される．そこで我々は実環境において提案攻撃の成功確率と実行時間の測定を行う．

本実験では，中間者攻撃のモデルによる測定ではなく，Beck-Tews 攻撃のモデルつまり IEEE802.11e をサポートする無線 LAN 機器を用いて測定を行った．Beck-Tews 攻撃のモデルでは IEEE802.11e の機器を用いることにより，任意のチャネルに改ざんパケットを送信することで TSC カウンタのチェックを回避できる．一方，中間者攻撃のモデルでは受信者にパケットを受け取らせないことにより，TSC カウンタの増加を防ぎ，TSC カウンタのチェックを回避する．しかしながら，両者の攻撃方法において chopchop 攻撃を用いて平文の復元を行い，パケットの改ざんを行う手段は同一のものが利用でき，両者で実行時間は変わらない．そこで，測定環境の構築および実装の容易さから，Beck-Tews 攻撃用のツールである tkiptun-ng に 4.2 節の攻撃を実装し，攻撃の実行時間および成功確率を評価した．

5.1 実験環境および攻撃手順

Beck-Tews 攻撃の攻撃ツールを利用するため，測定環境を構築する際に以下の条件を満たす必要がある．攻撃対象となるアクセスポイントとクライアントに使用する無線 LAN 機器は IEEE802.11e をサポートしていなければならない．IEEE802.11e は Wi-Fi Multi-media（WMM）という表記で実装されている．暗号化方式は WPA-TKIP とし，鍵変更間隔は 20 分以上に設定する．また攻撃者が用いる WLAN のチップの型番によっては追加設定を行う必要がある [10]．表 1 に実験の測定環境を示す．

次に攻撃の手順について説明する．tkiptun-ng を使用するにあたり，幾らかの初期設定が必要となる．

表 1: 測定環境

攻撃者プラットホーム	Ubuntu 8.04
攻撃者ツール	tkiptun-ng
アクセスポイント	WHR-HP-G
利用者 WLAN	WLI-UC-AG
攻撃者 WLAN	WLI-UC-AG
攻撃者 WLAN チップ	ZyDAS ZD1211B

まず，攻撃目標となる BSSID，クライアントの MAC アドレス，そして両者が使用しているチャネルを確認する必要がある．これらを実行するためには攻撃に使用する WLAN インタフェースをモニターモードに切り替える必要がある．モニターモードに切り替えることによって，アクセスポイント情報の取得や攻撃に必要なパケットのインジェクトが可能になる．以下にコマンド例を示す．

```
1. # airmon-ng check
2. # airmon-ng start wlan0
3. # airodump-ng mon0
4. # airmon-ng stop mon0
5. # airmon-ng start wlan0 7
6. # tkiptun-ng -a 00:1D:73:4F:9C:80
       -h 00:1D:73:BE:33:C1 mon0
```

1. 現在使用している WLAN インタフェースの確認を行う．
2. モニターモードに移行する．ここで wlan0 は攻撃に使用する WLAN インタフェースである．
3. アクセスポイントの情報を取得する．ここで BSSID，MAC アドレス，チャネル情報が取得できる．また mon0 はモニターモード移行後のインターフェイス名である．
4. チャネルが異なればモニターモードを停止させる．
5. チャネル（ここでは 7）を指定して再度モニターモードに移行する．
6. 必要な情報が取得できたら攻撃を開始する．ここで，00:1D:73:4F:9C:80 はネットワークの BSSID，00:1D:73:BE:33:C1 はクライアントの MAC アドレス，mon0 は WLAN のインタフェースである．

5.2 実験結果

MIC 鍵が得られている条件における攻撃の実行時間および攻撃成功確率を実環境で測定した．攻撃の試行回数は 100 回とし，アクセスポイントの IP アドレスは固定，クライアントの IP アドレスは試行毎に変更した．表 2 に提案攻撃の成功確率，表 3 に提案攻撃および Beck-Tews 攻撃の実行時間の最短時間・最長時間・平均時間を示す．表 2 より，実験によって得られた成功確率 0.35 は式 (5) によって得られた理論値にほぼ近い値になっていることを確認で

表 2: 提案攻撃の成功確率

実験回数	100 回
攻撃成功回数	35 回
攻撃成功確率	0.35

表 3: 攻撃の実行時間

	提案攻撃	Beck-Tews 攻撃
最短時間 (秒)	0.217	205.629
最長時間 (秒)	21.121	246.956
平均時間 (秒)	9.824	221.763

きる．また，表 3 より，提案攻撃の実行時間は平均で 10 秒程度，最長でも 20 秒程度であり，Beck-Tews 攻撃はどちらも 4 分前後であることから，提案攻撃は実行時間を大幅に短縮できていることが分かる．また，提案攻撃の実行時間は文献 [8] で見積もっていた 1 分よりも実際は短くなることが分かった．さらに，最短の場合ではわずか 0.2 秒で実行できており，通信頻度が高い場面においても提案攻撃が有効であるといえる．

今回実験に使用した攻撃ツールでは chopchop 攻撃の MIC エラーの検出が確実に行えるとは限らない．本実験では MIC エラーが検出できなかった場合は実験回数に含めず，MIC エラーの検出が確実に行えた場合の結果を示した．ただし本実験中においてはこの現象が起こる頻度は比較的低く，例えば提案攻撃を実行した場合に MIC エラーが検出できなかったのは 100 回のデータを取るまでに 3 回程度とわずかであった．

6 考察

クライアント側の IP アドレスを効果的に推測して攻撃成功確率を向上させる方法について考察する．IP アドレスの 4 オクテット目は 0 や 255 およびアクセスポイントのアドレスを使用することはなく，規模が小さなネットワークでは IP アドレスを全て使用することは稀である．特に DHCP を用いる場合，推測する IP アドレスの範囲を大幅に絞り込むことができる．実験に使用したアクセスポイント WLI-HP-G の初期設定では，第 4 オクテットが 2〜65 のアドレスを DHCP で割り当てる．初期設定で使っているユーザが多数と仮定すると，64 個の候補を推測すれば良いので攻撃成功確率は $((2^8-1)/2^8)^{64-1} \sim 0.778$ まで改善される．さらに 2〜17 を配布範囲にしている製品も存在し，この場合は攻撃成功確率は $((2^8-1)/2^8)^{16-1} \sim 0.943$ まで上昇する．

7 むすび

本稿では，無線 LAN 機器を用いた実験によって提案攻撃の実行時間および成功確率を評価した．成功確率の実験値はおよそ 35% であり理論値とほぼ一致した．さらに，1 分程度と大きく見積もっていたメッセージ改ざんモードの実行時間は，実際には最大 20 秒，平均 10 秒程度のように更に短いことが明らかになった．また，実験中には 0.2 秒というわずかな時間で改ざんできる場合も確認されている．中間者攻撃では通信途絶時間がメッセージの改ざんに要する時間に依存するため，提案攻撃のように短時間で実行方法が有効になると考えられる．今後の課題として，中間者攻撃の攻撃モデルの実装及び評価，攻撃実行時間を更に短縮することが挙げられる．

謝辞

本研究は科研費 (21700018) の助成を受けたものである．

参考文献

[1] Wi-Fi Alliance, “Wi-Fi protected access,” available at http://www.weca.net/opensection/protected_access.asp

[2] IEEE Computer Society, “Wireless lan medium access control (MAC) and physical layer (PHY) specifications,” IEEE Std 802.11, 1999.

[3] E. Tews, R. Weinmann, and A. Pyshkin, “Breaking 104 bit WEP in less than 60 seconds,” Cryptology ePrint, 2007, available at http://eprint.iacr.org/2007/120.pdf

[4] R. Teramura, Y. Asakura, T. Ohigashi, H. Kuwakado, and M. Morii, “Breaking WEP with Any 104-bit Keys –All WEP Keys Can Be Recovered Using IP Packets Only–,” Proc. of SCIS2009, CDROM, 1A2-6, Jan. 2009.

[5] KoreK, “chopchop (Experimental WEP attacks),” 2004, available at http://www.netstumbler.org/showthread.php?t=12489

[6] R. Moskowitz, “Weakness in Passphrase Choice in WPA Interface,” 2003, available at http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html

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

[8] T. Ohigashi and M. Morii, “A practical message falsification attack on WPA,” Proc. JWIS 2009, CDROM, 5A-4, 2009.

[9] B. Schneier, Applied Cryptography, Wiley, New York, 1996.

[10] http://www.aircrack-ng.org/doku.php?id=compatibility_drivers