2008－CSEC－42（42）
2008 / 7 / 25

IEEE802.11i 4 Way Handshake プロトコルを DoS 攻撃から保護する整合フィルタを用いた符号化方式

西 竜三† 堀 良彰‡ 櫻井 幸一‡

†パナソニックコミュニケーションズ㈱ 〒812-8531 福岡市博多区美野島 4-1-62
‡九州大学 〒819-0395 福岡市西区元岡 744

E-mail: †nishi.ryuzou@jp.panasonic.com ‡{hori, sakurai}@csce.kyushu-u.ac.jp

あらまし 無線 LAN のセキュリティ仕様 IEEE802.11i では、鍵を更新する為のプロトコルとして 4-Way Handshake が定義されている．しかしながら、4-Way Handshake においては DoS 攻撃への脆弱性が指摘されている．本稿では、4-Way Handshake におけるメッセージの配送に整合フィルタを用いる符号化方式を提案する．DoS 攻撃への従来の対策例では、DoS 攻撃の頻度が多くなるに応じて、必要とするメモリーや計算能力のリソースをより多く具備する必要があった．提案方式では、DoS 攻撃の頻度に関わらず、一定の処理能力で DoS 攻撃への耐性を効率的に改善することを示す．

キーワード ネットワークセキュリティ、鍵配送、DoS 攻撃、無線 LAN

A Coding Scheme using Matched Filter to protect IEEE802.11i 4-Way Handshake against DoS attack

Ryuzou NISHI† Yoshiaki HORI‡ and Kouichi SAKURAI‡

† Panasonic Communications Co.,Ltd 4-1-62 Minoshima, Hakata-ku, Fukuoka, 812-8531 Japan
‡ Kyushu University 744 Motooka, Nishi-ku, Fukuoka, 819-0395 Japan

E-mail: †nishi.ryuzou@jp.panasonic.com ‡{hori, sakurai}@csce.kyushu-u.ac.jp

Abstract Wireless LAN security standard IEEE802.11i specify 4-way handshake as a re-key protocol. However, some researchers found the vulnerabilities of 4-way handshake against Dos attack. In this paper, we propose a coding scheme for key distribution using matched filter. In the previous countermeasures against DoS attack, the more frequency of DoS attack is, the more required resource (e.g. memory, calculation power) becomes. We show that if our proposal is applied to 4-way handshake, it can reduce the effect of DoS attack and its required power does not depend on the frequency of DoS attack.

Keyword Network security, Key distribution, DoS attack, Wireless LAN

1. まえがき

1.1. 背景

無線 LAN[1]は既に、一般家庭のみならず、駅や空港、レストラン等の公衆でも広く普及している．そして、今後も、更に高速化を図ったシステムが登場しつつあり、ますます無線 LAN の利便性は高まりつつある．しかしながら、無線を使った通信の本質的な課題として、ある範囲内においては無線伝送路がオープンであり、その範囲内にある無線通信機器はそれを受信したり、逆に相手に対して送信したりすることが可能である．従って、無線通信においてはセキュリティの確保が非常に重要である．

IEEE802.11 では、このような無線通信でのセキュリティを確保すべく、無線伝送路上で伝送される信号を暗号化する為に、the Wired Equivalent Privacy (WEP) というプロトコルを提案した．しかしながら、WEP には、鍵管理の仕組みが十分でない等さまざまなセキュリティ上の脆弱性が指摘されている[2]．そこで、IEEE では、よりセキュリティを強化した仕様 IEEE802.11i[3]を 2004 年に承認した．IEEE802.11i では、4-way handshake のような鍵更新プロトコルの追加をはじめ、さまざまな改善がなされている．しかしながら、IEEE802.11i についても、例えば 4-way handshake に対する DoS(Denial-of-Service)攻撃の課題が指摘されている[4,5]．

1.2. 動機

鍵更新に失敗すれば、その後の暗号通信が出来なくなる．また、鍵更新の失敗時に、再度鍵更新を行う場合には、特にネットワークに接続する機器の数が多い場合には、通信のオーバーヘッドが大きくなり、サービス品質の低下を招く恐れがある．従って、DoS 攻撃があっても、鍵更新が停止することなく最後まで処理されることは非常に重要である．本稿では、DoS 攻撃に耐性を有する 4-way handshake の処理時のメッセージ配送時の符号化について提案する．

1.3. 4-way handshake

PTK (Pairwise Transient Key)は PMK (Pairwise Master Key)の他、アクセスポイント(AP)と端末(STA)が各々生成するノンスと各々の MAC アドレスから生成される．4-way handshake では以下の 4 つのメッセージの交換により、互いが生成したノンスを共有することで PTK を更新する．

- メッセージ 1 (AP→STA)
  AP の生成したノンス(ANonce)が配送される．暗号化されていない．
- メッセージ 2 (STA→AP)
  STA の生成したノンス(SNonce)が配送される．PTK で計算した MIC(Message Integrity Code)が付加される．暗号化されない．
- メッセージ 3 (AP→STA)
  グループ鍵を使う場合、更新されたグループ鍵が暗号化されて配送される．MIC が付加される．
- メッセージ 4 (STA→AP)
  メッセージ 3 に対する応答通知

1.4. 4-way handshake の課題

認証後の最初の 4-way handshake におけるメッセージ 1 は暗号化されておらず、偽造が可能である．また、劣悪な伝送路に起因するメッセージの損失がある環境下で 4-way handshake を最後まで処理するには、SAT はメッセージ 1 を全て受信して処理する必要がある．従って、正規の AP がメッセージ 1 を送信後に、攻撃者がメッセージ 1 を大量に偽造して、これらを STA に送信すれば、STA はメモリーを全て消費して 4-way handshake が停止する可能性がある[4,5]．

1.5. 従来の対策例

[5]において、以下の 3 つの対策が提案されている．

a. 受信メッセージを出来るだけ多くメモリーに格納する．
b. AP と STA が既に共有している PMK から一時的な鍵を導出して、これを使って、メッセージ 1 に MIC を付加する．
c. STA は 4-way handshake において受信したノンスや計算した PTK をメモリーに格納せず、メッセージを送信する際には毎回 PTK を計算する．この際、STA が生成するノンスは 4-way handshake が終了するまで更新しない．

1.6. 取り組み課題と本論文の貢献

従来対策例では、DoS 攻撃の規模、すなはち受信する偽造メッセージの量に比例して、より多くの所要メモリーやより多くの計算量を必要とした．本論文では、DoS 攻撃の規模に関わらず一定の処理量で、DoS 攻撃の影響を通常の伝送路環境と同程度まで低減する、鍵更新メッセージ配送時の符号化方式を提案する．

2. 提案方式

2.1. 提案方式の概要

受信信号の SNR (Signal to Noise Ratio) を最大にする整合フィルタを使うことで、耐雑音特性を改善する他、攻撃者からの偽造信号を受信信号の復号時に自動的に除去する．全体的な構成を図 1 に示す．送信系において、事前処理として、送信信号中に予め既知信号情報(テンプレート)を含ませておいて、受信時に、受信信号とテンプレートとの相関をとることで整合フィルタ[6]を実現出来る．

なお、提案方式は 4-Way Handshake の課題に取組むものであるが、4-Way Handshake のプロトコル自身に修正を加えるものではない。4-Way Handshake の DoS 攻撃への耐性を改善する為に、メッセージの配送時の符号化復号化に独自のアイデアを加えたものであり 4-Way Handshake のプロトコルとは基本的に独立なものである。

2.2. 提案鍵配送符号化方式(送信系)

図 2 は、提案鍵配送方式における送信系のブロック図を示す．図 3 は、図 2 のブロック図における各信号間の時間的関係を示すタイミングチャートである．これらの図において、鍵更新メッセージは、提案方式が適用されない場合に配送されるべき元々の鍵更新メッセージである．図 3 に示すように、この鍵更新メッセージ 1 ビットの長さをリサンプリング処理部において、N ビットの長さ ($a_1, a_2, \ldots a_N$ の合計の長さが元の鍵更新メッセージ 1 ビットの長さに相当．$a_i = +1$ or -1 とする．) まで拡張する．ここで、元々の鍵更新メッセージ 1 ビットの長さが鍵配送鍵 1 ビットの長さに等しい．そして、リサンプリング処理部の出力と鍵配送鍵とを乗算する．ここでの乗算とは排他的論理和を意味する．この乗算出力が配送されることになる．

2.3. 提案鍵配送復号化方式(受信系)

図 4 は、提案鍵配送方式における受信系のブロック図を示す．図 5 は、図 4 のブロック図における各信号間の時間的関係を示すタイミングチャートである．これらの図における受信メッセージは、PHY レイヤで鍵

配送信号を受信後にMACレイヤに転送された信号を意味する．受信メッセージは送信系と同じ鍵配送鍵で乗算される．

送信系と同様、ここでの乗算も排他的論理和を意味する．乗算出力は鍵配送鍵Nビットの間（$a_1,a_2,\ldots a_N$の間）で積分される．そして判定処理部において、積分出力の極性が判定される．ここで、鍵更新メッセージや鍵配送鍵の各ビットは＋１又は－１で表されるとする．この場合、鍵配送時にノイズ等の外部影響がなければ、積分出力は＋N又は－Nとなる．そして、この極性は送信系で鍵配送鍵と乗算された鍵更新メッセージの各ビットの極性（＋１又は－１）に等しくなる．そこで、積分後の判定部では、積分出力が$\alpha\times N$より大きい場合には＋１を、一方、積分出力が$-\alpha\times N$より小さい場合には－１を出力する．ここで、αは0より大きく１より小さい値をとる．積分出力が$\alpha\times N$より小さく、且つ、$-\alpha\times N$より大きい場合には、その結果は破棄される．デサンプリング処理部において、判定処理部の出力の各ビットの周期は、送信系における元々の鍵更新メッセージの各ビットの周期まで縮小されて、鍵更新メッセージが復号される．

2.4. 鍵配送鍵

鍵配送鍵が前述の整合フィルタにおける既知情報信号に相当する．鍵配送鍵はSTA毎に異なるものとする．この鍵配送鍵に求まられる特性として以下の特性が上げられる．

a. 異なるSTAの鍵配送鍵間に相関がないこと．これは、攻撃者からの偽造メッセージを自動的に除去する為である．

b. 出来るだけ多くの鍵配送鍵が確保出来ること．これは、鍵配送鍵の数が少ないと、DoS攻撃が容易になる為である．

提案方式では、鍵配送鍵として乱数を用いる．乱数は、その長さが十分長ければ、上記bの特性を有している．乱数が上記aの特性を有していることは３．２節で明らかにする．

認証後の最初の４－way handshakeの最初のメッセージに対しては、マスター鍵と時刻情報とAPとSTAの各々のMACアドレスとから擬似乱数関数を使って計算された鍵配送鍵が使われる．認証後の最初の４－way handshakeの２番目以降のメッセージに対しては、前述のマスター鍵と時刻情報とAPとSTAの各々のMACアドレスに加えて、そのメッセージが搭載する情報の一つのkey informationの最初の５ビットとから擬似乱数関数を使って計算された鍵配送鍵が使われる．認証後の２番目以降の４－way handshakeの各メッセージに対しては、前回の４－way handshakeで共有されたANonceとSNonceに加えて、そのメッセージが搭載する情報の一つのkey informationの最初の５ビットとから擬似乱数関数を使って計算された鍵配送鍵が使われる．このような鍵配送鍵の生成は、４－way handshakeでメッセージが交換される度に、APとSTAが互いに共有している情報を使って新たに更新された鍵配送鍵が使われるようにする為である．なお、鍵配送鍵の長さは、対応するメッセージ長に等しくする．これは、提案方式の安全性の前提である鍵配送鍵の秘密性を確保する為である．

3. 提案方式の安全性

3.1. 安全性の前提

攻撃者は攻撃対象のSTAの鍵配送鍵を知らないものとする．

3.2. DoS攻撃

鍵配送送信系の出力信号S_iは次式で表現される．ここで、Aは鍵更新メッセージの１ビットに相当する．ai(i=1～N)は鍵配送鍵である．ここで、Nは鍵配送鍵の長さを示すものではなく、後述する受信系の整合フィルタでの積分区間の長さを示す。

$$S_i = A \times a_i \qquad (1)$$

この時、鍵配送受信系で受信される信号（受信メッセージ）R_iは次式(3)で表現される．ここで、NSiは伝送路で付加されたノイズであり、S'_iは攻撃者からの信号であり、

$$S'_i = A' \times a'_i \qquad (2)$$

とする．

$$R_i = S_i + NS_i + S'_i \qquad (3)$$

この時、鍵配送受信系で復号される信号（鍵更新メッセージ）ISは以下のようになる．

$$IS = \sum_{i=1}^{N} R_i \times a_i$$

$$= \sum_{i=1}^{N} (S_i + NS_i + S'_i) \times a_i$$

$$= (\sum_{i=1}^{N} S_i \times a_i) + (\sum_{i=1}^{N} NS_i \times a_i) + (\sum_{i=1}^{N} S'_i \times a_i)$$

$$= A \times (\sum_{i=1}^{N} a_i \times a_i) + (\sum_{i=1}^{N} NS_i \times a_i)$$

$$+ A' \times (\sum_{i=1}^{N} a'_i \times a_i)$$

$$= A \times N + (\sum_{i=1}^{N} NS_i \times a_i)$$

$$+ A' \times (\sum_{i=1}^{N} a'_i \times a_i) \qquad (4)$$

上式（４）において、第１項は正規の信号に対する復号出力である．第２項はノイズと鍵配送鍵との相関値を示す．ノイズは鍵配送鍵と無相関と考えて良いから第２項のレベルは第１項より十分小さいと考えられる．

第３項は攻撃者からの信号と自身の鍵配送鍵との相関値を示す．ここで、

$$X_i = a'_i \times a_i \qquad (5)$$

とおくと、X_iは互いに無相関な乱数同士の乗算結果であるから、$X_1, X_2, \cdots X_N$は互いに独立で同一の分布に従うと見ることが出来る．この時、$X_i = +1$ or -1 であるから、Nが十分大きい場合には、中心極限定理により、上式(4)の第３項 $(\sum_{i=1}^{N} a'_i \times a_i) = X_1 + X_2 + \cdots + X_N$は平均値がゼロ、標準偏差が$\sqrt{N}$の正規分布で近似出来る．一方、２．３．節で述べたように、積分後の判定部では、積分出力が$\alpha \times N$ より大きい場合には＋１を、一方、積分出力が$-\alpha \times N$より小さい場合には－１を出力する．簡単の為に、$A=A'$とすると、これは、上式(4)の第３項の出力の絶対値が$\alpha \times N$ を超えた場合には、判定部がDoS攻撃によって誤判定することを意味する．$\alpha = 0.8$ とした時の各積分区間の長さに対する誤判定確率についての計算結果を図５に示す．計算結果より、積分区間の長さが少なくとも64を越えれば、誤判定確率は10^{-9}以下となる．

次に、αの具体的な値について考察する．αが１により近い場合には、上記誤判定確率はより小さい値になる．一方、無線のように伝送路誤りの大きい伝送路では、αが１により近い場合には、本来受信すべき希望メッセージを見逃す確率が大きくなる．ここで、積分区間長をN、伝送路のビット誤り率をerrとすると、この見逃し確率Pmは次式のようになる．

$$Pm = 1 - \sum_{i=\alpha N}^{N} {}_N C_i \times (1-err)^i \times err^{N-i} \qquad (6)$$

ここで、劣悪な伝送路を想定して$err = 0.01$とし[8]、$N=64$ として、式(6)を計算した結果を図７に示す．

図７より、$\alpha = 0.8$ の時、見逃し確率は10^{-9}以下となる．

ところで、有線LANのEthernetの規格[7]では、伝送誤り率(BER:Bit Error Rate)として10^{-9}以下と規定されている．これは、我々の提案方式で、誤って希望メッセージ以外の偽造メッセージを復号してしまう確率と希望メッセージの見逃し確率が、有線 LAN の Ethernet の伝送誤り率と同等レベルであることを意味する．つまり、我々の提案方式では、DoS 攻撃の影響を、その規模に関わらず、有線LANのEthernetと同等の伝送品質まで低減出来ることを意味する．

3.3. リプレイ攻撃

攻撃者が攻撃対象のSTAの鍵配送鍵を知らないことが提案方式の安全性の前提である．しかしながら、攻撃者が攻撃対象のSTAの鍵配送鍵を知らなくても、攻撃者が鍵配送時のメッセージを受信して、これを攻撃対象のSTAに送信すれば、そのSTAはそのメッセージを誤って復号してしまう．

しかしながら、鍵配送の度に鍵配送鍵は更新されるので、上記リプレイ攻撃は次の鍵配送の前までに限定されてしまう．そこで問題となるのは、次の鍵配送の前までに、リプレイ攻撃によるメッセージが受信された場合である．提案する鍵配送方式は、前述のように雑音に強い耐性を有するので、4-way handshake でのメッセージの再送が必要なケースは非常に少ないと考えられる．そこで、リプレイされたメッセージの受信は、正規のメッセージの受信後であることを考慮して、その最初の、すなわち正規のメッセージの受信後は、一定時間の間だけ次の正規のメッセージを待つことにする．つまり、更新された鍵配送鍵が使われたメッセージを待つことにする．もし、一定時間の間、次の正規のメッセージを受信出来なければ再送要求を行うこととする．このような対策によりリプレイ攻撃を防ぐことが可能であると考えられる．

4. 従来方式との比較

１．５節で紹介した従来対策例のａについては、DoS攻撃の為の偽造メッセージの量に比例して必要なメモリー量が増大する．また、従来対策例のｂとｃについては、DoS攻撃の為の偽造メッセージの量に比例して必要な計算量が増大する．これに対して提案方式では、DoS攻撃の為の偽造メッセージの量に関わらず、DoS攻撃の影響を、その規模に関わらず、有線LANのEthernetと同等の伝送品質まで低減出来る．

DoS攻撃の為のリプレイ攻撃については、例えば、メッセージ１のリプレイメッセージの受信がメッセージ２の送信前であれば、リプレイカウンターの検証の為の計算量の負荷は元々の4-way handshakeと同等である．しかし、これらのリプレイメッセージは、前節で説明したように破棄されるので、4-way handshakeが停止することはない．次に、メッセージ１のリプレイメ

ッセージの受信がメッセージ２の送信後であれば、鍵配送鍵が更新されるので、リプレイメッセージは整合フィルターで自動的に破棄されるので、DoS 攻撃の為のリプレイメッセージの量に関わらず、DoS 攻撃の影響を、有線 LAN の Ethernet と同等の伝送品質まで低減出来る．

ところで、提案方式では、鍵配送時の通信のオーバーヘッドが発生する．積分区間の長さを N とすると、鍵配送時の所要伝送量は従来の N 倍になる．4-way handshake のメッセージは、MAC レイヤが上位レイヤに提供するデータ領域を使って伝送される．この領域の伝送速度（スループット）は通常数 Mbps から約 20Mbps[9]である．ここで、4-way handshake の各メッセージ長は 95 オクテット＝95×8 ビットであり、伝送される速度を最も遅いと想定される 1 Mbps とする．この時、4-way handshake の 4 つのメッセージの伝送に要する時間は、95×8×4×(1/1Mbps)＝約 3msec となる．ディジタル無線通信では一般に、無線伝送路で発生するフェージングの影響低減の為に伝送路符号化や時間インターリーブの処理が行われ、それらの処理にともなう伝送遅延は数 10msec
になっている[10]．このような通常の伝送遅延を考慮すれば、提案方式における通信のオーバーヘッドは許容される範囲内のものと考えられる．

5. まとめ

4-way handshake において指摘されている DoS 攻撃に耐性を有する、メッセージの配送方式（鍵配送方式）を提案した．提案方式は、DoS 攻撃の規模に関わらず、その影響を有線 LAN の Ethernet と同等の伝送品質まで低減出来ることを示した．

提案方式は、通信のオーバーヘッドが大きい為、通常のリアルタイムのデータ伝送に適用することは困難であるが、リアルタイム性の要求されない制御フレーム等の通信にも広く応用可能である．また、提案方式の応用は無線 LAN に限定されるものでもない．例えば、次世代無線通信システムとして期待されているモバイル WiMAX でも、未認証時の制御フレーム等への偽造や DoS 攻撃は無線 LAN 同様に脅威であり、モバイル WiMAX 等にも広く応用可能である。

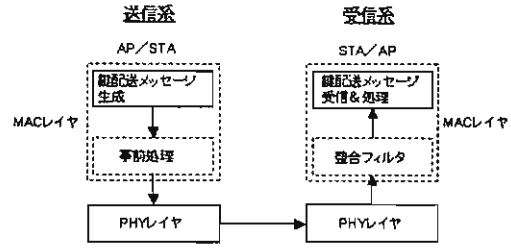

図１　提案方式の基本構成

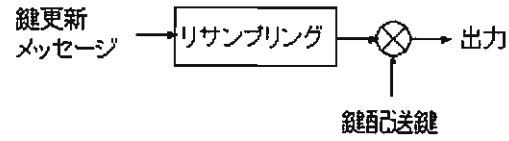

図２　鍵配送送信系ブロック図

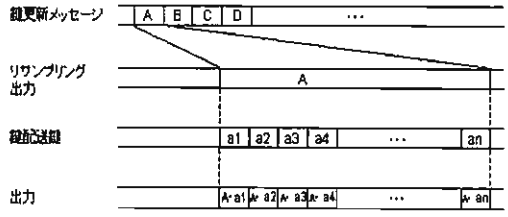

図３　鍵配送送信系タイミングチャート

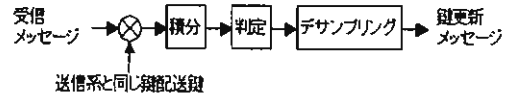

図４　鍵配送受信系ブロック図

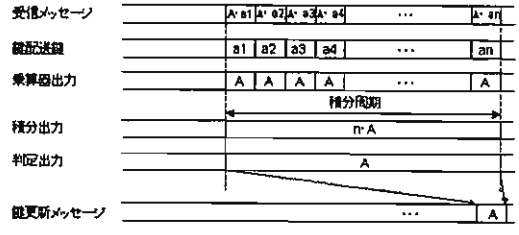

図５　鍵配受信系タイミングチャート

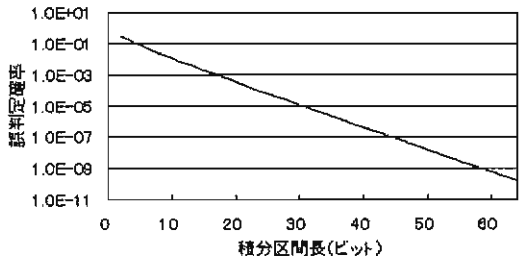

図 6　誤判定確率

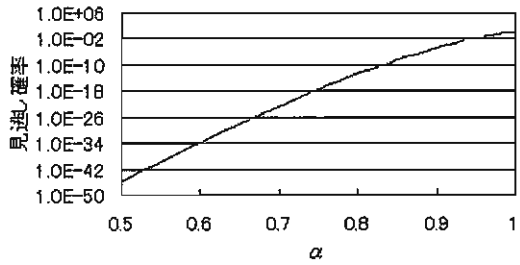

図 7　希望信号の見逃し確率

文　献

[1] IEEE Std 802.11-2007. Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[2] Arbaugh,W.A., Shankar.N., and Wang,J. "Your 802.11 Network has no Clothes". In Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks, pp.131-144, December, 2001.

[3] IEEE Std 802.11i-2004. Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information technology - Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[4] Changhua He, John C. Mitchel "Security Analysis and Improvements for IEEE 802.11i", The 12th Annual Network and Distributed System Security Symposium (NDSS'05), Feb. 2005.

[5] Changhua He, John C. Mitchel" Analysis of the 802.11i 4-Way Handshake", Proceeding of the 2004 ACM workshop on Wireless security pp.43-50

[6] Turin,G.L. "An Introduction to digital matched filters", IEEE Proceedings, vol.64, July 1976, pp.1092-1112.

[7] IEEE Std 802.3-2002. Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

[8] Zwick,T., Demmerle,F., Wiesbeck,W., "Simulation and measurement of bit error rates for a 2FSK-system in indoor environment", Vehicular Technology Conference, Volume 1, Issue 18-21 May 1998, pp.649-652

[9] 守倉正博、久保田周治"改訂三版 802.11 高速無線 LAN 教科書"インプレス R&D 2008 年

[10] 中川 正雄, 大西誠、丸亀剛 "リアルタイム無線通信システムの研究"
http://www.jst.go.jp/shincho/db/seika/2005_s/2005_s_1/2005_s_1_3_ningenshien/2005_s_1_3_ningenshien_1_2.pdf

[11] Taeshik Scon and Wook Choi,"An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions" First International Conference, NBiS 2007, LNCS, Vol.4650, pp.88-97, 2007