情報処理学会論文誌 Vol. 51 No. 9 1499–1506 (Sep. 2010)

無線通信における物理レイヤ/MACレイヤへのDoS攻撃に耐性を有する整合フィルタを用いた符号化方式

西 竜三[†1] 堀 良彰[†2] 櫻井幸一[†2]

無線通信においては本質的なセキュリティ上の課題がある．それは，電波の届く範囲内で無線通信チャネルが第三者にオープンであることである．これは，無線通信が物理レイヤおよびMACレイヤへのDoS攻撃に脆弱であることを意味している．このような課題に対する対策として，MACレイヤで整合フィルタを用いるアプローチを提案する．整合フィルタのメッセージ配送鍵として乱数を用いる．正規でないメッセージを受信する確率，および正規のメッセージを受信できない確率を求めると，両者ともにホームネットワークのような環境下では10^{-9}以下となった．これは提案方式が物理レイヤおよびMACレイヤへのDoS攻撃の影響を有線LAN（Ethernet）の雑音以下のレベルまで低減できることを意味しており，提案方式の有効性を確認することができた．

A Coding Scheme Using Matched Filter Resistant against DoS Attack to PHY/MAC Layer in Wireless Communications

Ryuzou Nishi,[†1] Yoshiaki Hori[†2] and Kouichi Sakurai[†2]

In a wireless communication, there is an essential issue. The issue is that wireless communication channel is open in the range where the radio signal can reach. This means that wireless communication is sensitive against DoS attack in PHY/MAC layer. We propose the approach using matched filter in MAC layer as a countermeasure against DoS attack to PHY/MAC layer. We use a random number as a message distribution key of matched filter. We analyzed the probability of receiving the forged message, and the probability of missing the legitimate message. As result, in home network, we have found the two probabilities are less than 10^{-9}. This means that our proposal mitigates the effect of DoS attack to PHY/MAC layer to the level of a wired channel (Ethernet).

1. はじめに

1.1 背景

現在世界的に普及している無線LANにおいては本質的な課題がある．それは，電波の届く範囲内で，無線通信チャネルが第三者にオープンであるということである[1)]．これは，無線通信信号が盗聴される可能性があること，また，無線通信が物理レイヤおよびMACレイヤへのDoS攻撃に対して本質的に脆弱であることを意味している．実際，標準的な無線LAN規格IEEE802.11が物理レイヤおよびMACレイヤでのDoS攻撃に脆弱であることが従来の研究[9),11)]ですでに指摘されている．しかしながら，DoS攻撃環境下にあっても，有線LANと同等の通信品質を無線LANにおいても確保できることが望まれる．無線LANのセキュリティ標準仕様IEEE802.11iにおいては，盗聴対策の記載はあるが，DoS攻撃への対策として認証コード以外の記載はない．そこで，今回は，DoS攻撃への対策に着目した．

このような課題に対する対策例として整合フィルタを用いた対策がある[2),3)]．特に，軍用通信においては，物理レイヤへのDoS攻撃であるジャミングに対する効果的対策として，整合フィルタを用いたスペクトル拡散通信が使用されてきた[2)–6)]．すでに普及している無線LAN IEEE802.11bにおいてもスペクトル拡散通信方式が採用されている．整合フィルタにおいては，メッセージ配送鍵と呼ばれる送受信が共有する情報が送信信号に含まれて実装可能となるが，スペクトル拡散通信のDoS攻撃への有効性は，整合フィルタのメッセージ配送鍵に相当する拡散符号が第3者に知られていないことに基づいている．しかしながら，無線LAN IEEE802.11bでは，相互接続性が要求されることから，拡散符号が公開されている．つまり，相互接続性が要求される無線通信システムにおいては，物理レイヤにおけるDoS攻撃への対策を施すことは困難であり，上位レイヤでのDoS攻撃に対する対策が必要であると考えられる．

†1 パナソニックシステムネットワークス株式会社
Panasonic Communications Co., Ltd.
†2 九州大学
Kyushu University

1.2 動　　機

無線 LAN のような，相互接続性が前提とされている無線通信システムでは，一般にその仕様は公開されている．DoS 攻撃への対策を含むセキュリティ上の対策はそのような公開された仕様のなかで行われる必要がある．

そこで本稿では，そのような相互接続性が要求される無線通信システムに適用可能な物理レイヤおよび MAC レイヤへの DoS 攻撃への対策を提案する．

1.3 DoS 攻撃

1.3.1 物理レイヤにおける DoS 攻撃

物理レイヤにおける DoS 攻撃として，以下があげられる[2),4)]．

- ジャミング：悪意のあるユーザが，攻撃対象のユーザに妨害電波を放射して，その周波数帯域を使用不能にすることで，攻撃対象のユーザの通信機能を使用不可能にする．

1.1 節でスペクトル拡散通信の課題について述べた，ジャミングによる DoS 攻撃は，悪意のあるユーザの無線機器と攻撃対象のユーザの無線機器とが同じ仕様の場合に脅威となる．

1.3.2 MAC レイヤにおける DoS 攻撃

MAC レイヤにおける DoS 攻撃として，以下があげられる．

- wireless frame flooding[12)]：悪意のあるユーザが，攻撃対象のユーザに大量に妨害信号を送信することで，その受信処理において攻撃対象のユーザの計算リソースやメモリリソースを消耗させることで，攻撃対象のユーザの通信機能を使用不可能にする．
- 偽 deauthntication/disassociation フレームの送信[9),10)]：正規のユーザに代わり，悪意のあるユーザが偽の deauthntication/disassociation フレームを正規のユーザの通信相手に送信することで，正規のユーザの通信を止める．
- 偽 4-way handshake メッセージの送信[9),11)]：無線 LAN のセキュリティ標準 IEEE802.11i におけるセッション鍵の更新プロトコルである 4-way handshake において，偽の 4-way handshake メッセージを正規のユーザに大量に送信することで，4-way handshake を止める．
- 偽 EAPOL-Logoff/Start フレームの送信[12)]：LAN 上における認証プロトコルである EAPOL において，偽の EAPOL-Logoff/Start フレームを，正規のユーザの通信相手に送信することで，EAPOL を止める．
- 偽 EAP-Logoff/Start フレームの送信[12)]：認証プロトコルである EAP において，偽の EAP-Logoff/Start フレームを正規のユーザの通信相手に送信することで，EAP を止める．

（対策）

wireless frame flooding については，攻撃対象のユーザの機器が物理レイヤでいったん受信することが前提となる．この場合，悪意のあるユーザの機器が攻撃対象のユーザの機器と同じ仕様である必要があるため，スペクトル拡散通信は有効でなくなる．

偽 4-way handshake メッセージの送信については，たとえば，メッセージ認証コードのメッセージへの付与である程度対応可能であるが，偽メッセージが大量に送信された場合には，計算リソースやメモリリソースを消耗して，プロトコルが停止してしまう[9),11)]．

偽 EAPOL-Logoff/Start フレームおよび偽 EAP-Logoff/Start フレームの送信については，たとえば，メッセージ認証コードがフレームへ付与されれば，対応可能と考えられる．

以上のことから，悪意のあるユーザが正規ユーザと同じ仕様の無線機器を使った場合のジャミングや，wireless frame flooding，偽 4-way handshake メッセージに対しては，既存の対策では対応困難と考えられる．

1.4 本稿で取り組む技術課題

前述のように，既存の対策では対応困難な無線 LAN に対する，物理レイヤおよび MAC レイヤにおける DoS 攻撃が存在する．無線 LAN セキュリティ標準 IEEE802.11i[8)] では，このような DoS 攻撃に対する対策は記載されていない．しかしながら，たとえば，無線 LAN ベンダにとって，自社の提供する無線 LAN 機器が DoS 攻撃等によって一時的でも使用不可になることは品質問題になる恐れがある．そのような意味でも，無線 LAN に対する DoS 攻撃の影響を有線 LAN 等と同等まで低減させることは可用性の向上につながると考えられる．

1.5 本稿の貢献

提案する符号化方式により，ホームネットワークのような環境では，偽造メッセージを受信する確率は 10^{-9} 以下まで低減させることができることが分かった．さらに，正規のメッセージを見逃す確率も 10^{-9} 以下まで低減させることができることが分かった．有線 LAN においては，ビットエラーレートが 10^{-9} 以下であることが規定されている[7)]．いい換えれば，DoS 攻撃の環境下にあっても，我々の提案方式は，有線 LAN と同等のレベルまで可用性を確保できることが分かった．我々の知る限り，このような議論がなされたのは初めてである．

本稿の構成は，2 章では，関連研究について紹介するとともに，それらの課題および提案方式の関連研究に対する優位性について議論する．3 章では，提案方式の具体的な構成について紹介する．4 章では，提案方式の評価について議論する．具体的には，

DoS 攻撃とリプレイ攻撃に対する耐性，提案方式の課題としてあげられる通信のオーバヘッドと，それを考慮したアプリケーションについて議論する．最後に 5 章でまとめを行う．

2. 関連研究と提案方式との比較

1.3 節で述べた，偽 4-way handshake メッセージに対する対策として，He ら[9] は，以下の 3 つの対策を提案している．

a. 受信メッセージをできるだけ多くメモリに格納する．これによって DoS 攻撃への対策を図る．
b. アクセスポイントと端末がすでに共有しているマスタ鍵から一時的な鍵を導出し，これを使って，アクセスポイントから端末への最初のメッセージに MIC（Message Integrity Code）を付加する．これによって，DoS 攻撃への対策を図る．
c. 端末は 4-way handshake において受信した乱数や計算したセッション鍵をメモリに格納せず，MIC の計算やメッセージを送信する際には毎回セッション鍵を計算する．この際，端末が生成する乱数は 4-way handshake が終了するまで更新しない．これによって，DoS 攻撃への対策を図る．

上述の対策 a，c の場合，機器に十分なメモリ量もしくは計算能力を必要とし，機器が大変高価なものになるという課題がある．上述の対策 b の場合，物理レイヤにおける DoS 攻撃に対しては効果がないという課題がある．

また，暗号技術を用いた，DoS 攻撃に対する対策例としては，メッセージ完全性コードやメッセージ認証コードを使った例[11] がある．これは秘密鍵を共有する送受信者が，メッセージ完全性コードやメッセージ認証コードに付与された秘密鍵の存在を確認することで，正規のメッセージであることを確認して，第三者からの偽造メッセージ受信を防ぐというものである．この対策については，上述の対策 b と同様，物理レイヤにおける DoS 攻撃に対しては効果がないという課題がある．

一方，提案方式では，物理レイヤにおける DoS 攻撃に対して効果を有するほか，MAC レイヤにおける DoS 攻撃に対しても効果を有する．また，提案方式では，基本的には積和演算のみの処理であるので，大きなメモリや計算能力を必要とすることもない．

なお，提案方式には，乱数との排他的論理和で符号化する点等，One Time Pad 暗号との類似点がある．One Time Pad 暗号も簡単な構成で十分な暗号的強度を有する．提案方式と One Time Pad 暗号の基本的な違いは，One Time Pad 暗号では，伝送時の誤りが許容されないのに対して，提案方式では，しきい値の範囲内であれば，伝送時の誤りが許容される点にある．

3. 提 案 方 式

3.1 整合フィルタ

提案方式では，MAC レイヤにおけるメッセージ符号化に整合フィルタを使う．ここでは，整合フィルタの概要について説明する．

整合フィルタは出力 SNR（Signal to Noise Ratio：信号対雑音比）を最大にするフィルタとして定義される．このことは，BER（Bit Error Rate）を最小にすることを意味する．一般にフィルタの出力信号 $y(t)$ は以下の式で表現される．

$$y(t) = \int_{-\infty}^{\infty} s(\tau)h(t-\tau)\,d\tau \tag{1}$$

ここで，$s(t)$ はフィルタの入力信号，$h(t)$ はフィルタのインパルス応答である．整合フィルタの定義を満足する条件は次式で表現される．

$$s(\tau) = h(t-\tau) \tag{2}$$

式 (2) を式 (1) に代入すると，次式が得られる．

$$y(t) = \int_{-\infty}^{\infty} s(\tau)s(\tau)\,d\tau \tag{3}$$

上式は，整合フィルタは，フィルタの入力信号 $s(t)$ と，受信側で生成した信号 $s'(t)$ $(= s(t))$ との相関をとることによって実装できることを示している．つまり，送受信で共有する信号 $s(t)$ どうしの相関をとることによって実装できることを示している．ここで，$s(t)$ は通常テンプレートとも呼ばれることがあるが，本稿では提案方式におけるテンプレートの使い方を考慮して，$s(t)$ をメッセージ配送鍵と呼ぶことにする．

3.2 提案方式の概要

前節で述べた整合フィルタを使うことで，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，MAC レイヤにおいて送信信号中にあらかじめ既知信号情報（メッセージ配送鍵）を含ませておいて符号化し，受信時に，MAC レイヤにおいて受信信号とメッセージ配送鍵との相関をとることで復号化することで整合フィルタを実現できる．

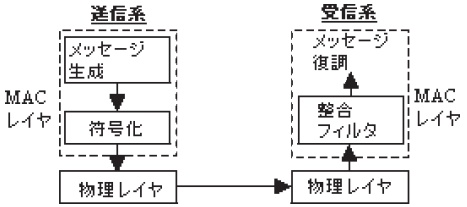

図 1　提案方式概要
Fig. 1　Overview of proposal method.

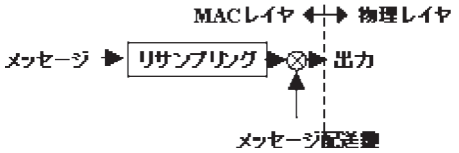

図 2　提案方式送信系ブロック図
Fig. 2　Sender-side block diagram.

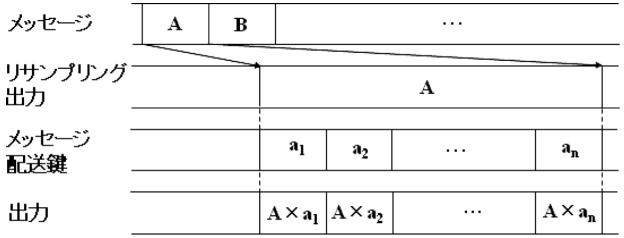

図 3　提案方式送信系タイミングチャート
Fig. 3　Sender-side timing chart.

3.3　メッセージ符号化方式（送信系）

図 2 は，提案符号化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，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メッセージである．メッセージの各ビットは $+1$ または -1 で表される．図 3 に示すように，このメッセージ 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，

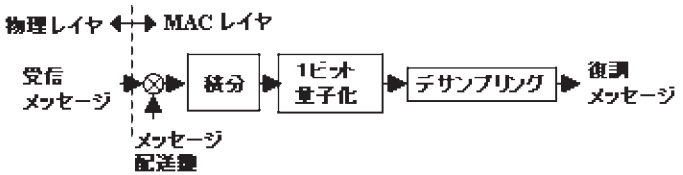

図 4　提案方式受信系ブロック図
Fig. 4　Receiver-side block diagram.

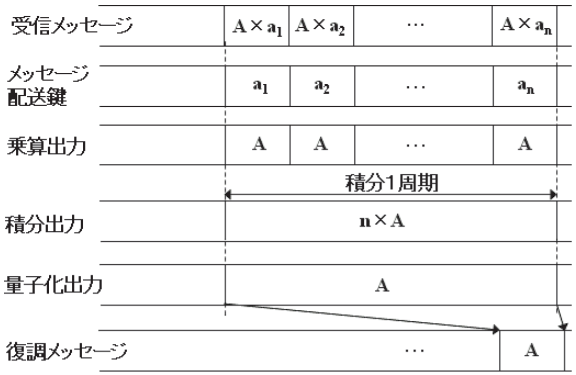

図 5　提案方式受信系タイミングチャート
Fig. 5　Receiver-side timing chart.

元々のメッセージ 1 ビットの長さがメッセージ配送鍵 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メッセージ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．

3.4　メッセージ復号化方式（受信系）

図 4 は，提案符号化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，物理レイヤでメッセージを受信後に 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メッセージ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．乗算出力はメッセージ配送鍵 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，受信メッセージやメッセージ配送鍵の各ビットは $+1$ また

は -1 で表されるとする．この場合，伝送時にノイズ等の外部影響がなければ，積分出力は $+N$ または $-N$ となる．そして，この極性は送信系でメッセージ配送鍵と乗算されたメッセージの各ビットの極性（$+1$ または -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，かつ，$-\alpha \times N$ 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メッセージの各ビットの周期まで縮小されて，メッセージが復号される．

3.5　メッセージ配送鍵

メッセージ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．メッセージ配送鍵は受信機ごとに異なるものとする．このメッセージ配送鍵に求められる特性として以下の特性があげられる．

a.　異なる受信機のメッセージ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ためである．

b.　できるだけ多くのメッセージ配送鍵が確保できること．
　これは，メッセージ配送鍵の数が少ないと，DoS 攻撃が容易になるためである．

提案方式では，メッセージ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次節で明らかにする．

メッセージ配送鍵の生成については，パケット（メッセージ）ごとに異なるセッション鍵のハッシュ値をメッセージ配送鍵とする．ここで，ハッシュ関数を使うのは，セッション鍵の長さを提案方式の受信系の積分の長さに変換するためである．

次にメッセージ配送鍵の更新について述べる．メッセージ配送のたびにメッセージ配送鍵は更新されるものとする．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，更新されたメッセージ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できなければ再送要求を行うこととする．このような処理を行うのは，後述するリプレイ攻撃への対策のためである．

4.　提案方式の評価

4.1　安全性の前提

攻撃者は攻撃対象の受信機のメッセージ配送鍵を知らないものとする．

4.2　提案方式の DoS 攻撃への耐性の評価

送信系の出力信号 S_i は次式で表現される．ここで，A はメッセージの 1 ビットに相当する．a_i（$i = 1 \sim N$）はメッセージ配送鍵である．ここで，N はメッセージ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．

$$S_i = A \times a_i \tag{4}$$

このとき，受信される信号（受信メッセージ）R_i は式 (6) で表現される．ここで，S'_i は攻撃者からの信号であり，

$$S'_i = A' \times a'_i \tag{5}$$

とする．

$$R_i = S_i + S'_i \tag{6}$$

このとき，受信系で復号される信号（復号メッセージ）IS は以下のようになる．

$$\begin{aligned} IS &= \sum_{i=1}^{N} R_i \times a_i \\ &= \sum_{i=1}^{N} (S_i + S'_i) \times a_i \\ &= \left(\sum_{i=1}^{N} S_i \times a_i \right) + \left(\sum_{i=1}^{N} S'_i \times a_i \right) \\ &= A \times \left(\sum_{i=1}^{N} a_i \times a_i \right) + A' \times \left(\sum_{i=1}^{N} a'_i \times a_i \right) \\ &= A \times N + A' \times \left(\sum_{i=1}^{N} a'_i \times a_i \right) \end{aligned} \tag{7}$$

上式 (7) 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 項は攻撃者からの信号と自身のメッセージ配送鍵との相関値を示す．ここで，

$$X_i = a'_i \times a_i \tag{8}$$

とおくと，X_i は互いに無相関な乱数どうし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できる．このとき，$X_i = +1$ 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，式 (7) の第 2 項 $\left(\sum_{i=1}^{N} a'_i \times a_i \right) = X_1 + X_2 + \cdots + X_N$ は平均値がゼロ，標準偏差が $\sqrt{N}$ の正規分布で近似できる．一方，3.4 節で述べたように，

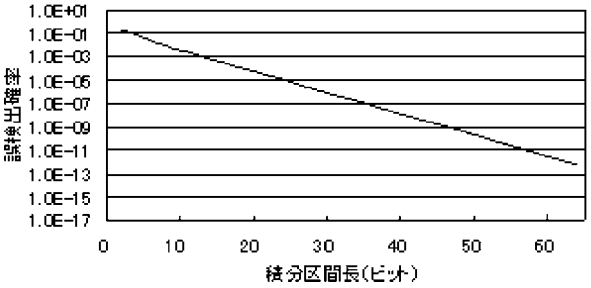

図 6　誤検出確率
Fig. 6　Probability of error detection.

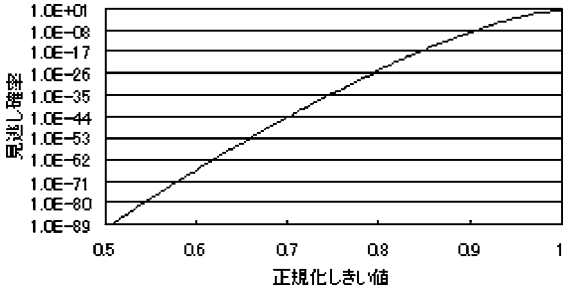

図 7　見逃し確率
Fig. 7　Probability of missing.

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．判定部の判定のためのしきい値は N に依存するが，α は，N を正規化したしきい値である．ここで，$A' = cA$ とする．ここで，c は伝送路の状況で決まる正の定数である．まず，$c = 1$ とすると，これは，式 (7) の第 2 項の括弧内が $\alpha \times N$ を超えた場合には，判定部が DoS 攻撃によって誤検出することを意味する．この誤検出確率 Pe は次式のようになる．

$$Pe = (1/\sqrt{2\pi N}) \int_{\alpha N}^{\infty} \exp(x^2/2N)\, dx \tag{9}$$

$\alpha = 0.8$ としたときの各積分区間の長さに対する誤検出確率についての計算結果を**図 6** に示す．計算結果より，積分区間の長さ N が約 50 以上になれば，誤検出確率は 10^{-9} 以下となる．次に，$c < 1$ の場合，式 (7) の第 2 項の括弧内が $\alpha \times N \div c$ を超えた場合に誤検出することを意味するから，誤検出確率は $A = A'$ の場合よりさらに小さくなる．このような場合は，攻撃者から受信信号の大きさが正規の受信信号の大きさより小さいときを意味している．具体的には，一般には攻撃者が正規の送信者より遠くに存在していることを意味しており，そのような環境として，ホームネットワークのような環境があげられる．逆に，$c > 1$ の場合，誤検出確率は $A = A'$ の場合より大きくなる．このような場合は，攻撃者から受信信号の大きさが正規の受信信号の大きさより大きいときを意味しており，具体的には，一般には攻撃者が正規の送信者より近傍に意味している．しかしながら，たとえば，$c = 2$，すなわち，攻撃者からの受信信号の大きさが正規の受信信号の大きさの 2 倍であっても，誤検出確率は約 6.9×10^{-4} となり，高い DoS 攻撃への耐性を有している．

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，上記誤検出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，本来受信すべき正規メッセージを見逃す確率 Pm 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．

$$Pm = 1 - \sum_{i=\alpha N}^{N} {}_N C_i \times (1 - err)^i \times err^{N-i} \tag{10}$$

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 (10) を計算した結果を**図 7** に示す．図 7 より，α が約 0.87 以下のときには，見逃し確率は 10^{-9} 以下となる．

ここで，$\alpha \times N$ が見逃し判定のしきい値なので，α または N が大きくなると，見逃し確率 Pm は大きくなる．N が小さいと演算量も少なくなり，さらに通信のオーバヘッドも小さくなるが，しきい値も小さくなるため，誤検出確率が大きくなるという面もある．したがって，演算量や通信のオーバヘッド等の実装面やシステム性能に変更を加えることなく，しきい値を変えるには α だけを変更すればよい．

以上の議論より，積分区間長 $N = 64$ で，たとえば正規化しきい値 $\alpha = 0.8$ のときには，誤って正規メッセージ以外の偽造メッセージを復号してしまう誤検出確率と正規メッセージの見逃し確率が，少なくとも，ホームネットワークのような環境下では，ともに 10^{-9} 以下になることが分かる．

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，誤って正規メッセージ以

外の偽造メッセージを復号してしまう確率と正規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，有線 LAN の Ethernet と同等の伝送品質まで低減させることができることを意味する．

式 (7) の第 2 項については，正規の信号と攻撃者からの信号との相関値であり，これらの信号間に相関がないことから上述の結果が導かれている．攻撃者からの信号だけでなく，伝送路上でのジャミングや雑音も正規の信号とは無相関である．したがって，提案方式は，ジャミングや雑音も含めた DoS 攻撃に対して有効であると考えられる．

4.3　提案方式に対するリプレイ攻撃

攻撃者が攻撃対象の受信機のメッセージ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受信機のメッセージ配送鍵を知らなくても，攻撃者がメッセージを受信して，これを攻撃対象の受信機に送信すれば，その受信機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，メッセージ配送のたびにメッセージ配送鍵は更新されるので，上記リプレイ攻撃は次のメッセージ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，次のメッセージ配送の前までに，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．提案するメッセージ符号化方式は，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，更新されたメッセージ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でき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．

4.4　通信のオーバヘッドとアプリケーション

提案方式は，基本的には，MAC レイヤのメッセージ全体について適用可能である．しかしながら，提案方式では通信のオーバヘッドが発生する．たとえば，整合フィルタの積分区間の長さが 64 の場合，元々のメッセージの 63 倍の冗長メッセージが，元々のメッセージに付加されることになる．したがって，通常のメッセージ全体に対して提案方式の符号化を適用すれば，伝送効率の大幅な低下を招くことになる．

したがって，提案方式の適するアプリケーションとしては，メッセージの重要度が大きく，かつ，伝送量の小さいメッセージである．そのようなメッセージとして，秘密鍵更新時の秘密鍵情報を含むメッセージがある．このメッセージが DoS 攻撃で正しく受信できなければ，その後の通信は不可能になるため，そのようなメッセージの可用性を向上させるために適用できる．

無線 LAN のセキュリティ標準仕様 IEEE802.11i[8] では，秘密鍵配送を行うプロトコルとして 4-way handshake が定義されている．公開されているデータ[13] では，4-way handshake の開始から完了までに要する時間は，8 msec 以下となっている．したがって，整合フィルタの積分区間の長さが 64 の場合，通信のオーバヘッドは最大で $8 \times 63 \approx 504$ msec となる．ここで述べるオーバヘッドとは，符号化時に付加される冗長成分の伝送に要する時間のことである．一般に，4-way handshake の周期は数分程度であることを考慮すると，上記オーバヘッドは大きな問題にはならないと考えられる．

5. ま と め

MAC レイヤにおいて，整合フィルタを用いた新たな符号化方式を提案した．この符号化方式を用いれば，DoS 攻撃の影響を有線 LAN における雑音の影響のレベルまで低減させることができることを示した．

MAC レイヤに実装する提案方式は，攻撃者と被攻撃者が同じ仕様の無線機器を使うことを前提にしている．一方，物理レイヤに実装されるスペクトル拡散通信は，攻撃者と被攻撃者が違う仕様の無線機器を使う場合に効果的である．したがって，提案方式とスペクトル拡散通信を併用すれば，DoS 攻撃に対してより効果的になると考えられる．

参 考 文 献

1) Aissi, S., Dabbous, N. and Prasad, A.R.: Security for Mobile Networks and Platforms, *Artech House* (2006).
2) Simon, M.K., Omura, J.K., Scholtz, R.A. and Levitt, B.K.: *Spread Spectrum Communication, Volume 1*, Computer Science Press (1976).
3) Turin, G.L.: An Introduction to digital matched filters, *Proc. IEEE*, Vol.64, pp.1092–1112 (July 1976).
4) Nakagawa, M.: Fundamental and Application of Spread Spectrum Communication Techniques, *TRICEPS* (1987). (in Japanese)
5) Homes, J.K.: *Coherent Spread Spectrum System*, KRIEGER (1982).
6) Scholtz, R.: The Origins of Spread-Spectrum Communications, *IEEE Trans. Communications*, Vol.30, Issue 5, Part 2, pp.822–854 (May 1982).
7) IEEE Std 802.3-2005 Part 3: Carrier sense multiple access with collision detection

(CSMA/CD) access method and physical layer specifications (2005).
8) 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 (2004).
9) He, C. and Mitchel, J.C.: Security Analysis and Improvements for IEEE 802.11i, *the 12th Annual Network and Distributed System Security Symposium* (*NDSS'05*) (Feb. 2005).
10) Lin, G. and Noubir, G.: On link layer denial of service in data wireless LANs, *Journal on Wireless Comm. and Mob. Computing* (Aug. 2004).
11) He, C. and Mitchel, J.C.: Analysis of the 802.11i 4-Way Handshake, *Proc. 2004 ACM Workshop on Wireless Security*, pp.43–50 (2004).
12) Inoue, D., Nomura, R. and Kuroda, M.: Transient MAC address scheme for untraceability and DoS attack resiliency on wireless network, *Wireless Telecommunications Symposium*, pp.15–23 (Apr. 2005).
13) WPA Packet Capture Explained.
http://www.aircrack-ng.org/doku.php?id=wpa_capture

(平成 21 年 11 月 30 日受付)
(平成 22 年 6 月 3 日採録)

西　竜三（正会員）

1986 年広島大学卒業．1986 年三菱電機（株）入社．無線通信システムの開発に従事．1991 年パナソニックコミュニケーションズ（株）入社．無線通信システムの開発に従事．2004 年から 2005 年まで九州システム情報技術研究所（現，九州先端科学技術研究所）に出向して，セキュリティ技術の研究に従事．

堀　良彰（正会員）

1992 年九州工業大学卒業．1994 年九州工業大学大学院前期博士課程修了．2002 年九州工業大学大学院後期博士課程修了．1994 年から 2003 年まで九州芸術工科大学助手．2003 年から 2004 年まで九州大学助手．2004 年から九州大学准教授．セキュリティ技術の研究に従事．

櫻井　幸一（正会員）

1986 年九州大学卒業．1988 年九州大学大学院前期博士課程修了．1993 年九州大学大学院後期博士課程修了．1993 年三菱電機（株）入社．1994 年から九州大学准教授．2002 年から九州大学教授．2004 年から九州先端科学技術研究所情報セキュリティ研究室室長．セキュリティ技術の研究に従事．