無線LAN環境におけるパケット認証を用いた通信効率の改善手法

岡山聖彦† 谷渕陽祐†† 山井成良† 木澤政雄‡ 岡本卓爾‡‡

†岡山大学総合情報基盤センター ††岡山理科大学大学院工学研究科
‡岡山大学大学院自然科学研究科 ‡‡岡山理科大学工学部

††{okayama,yamai}@cc.okayama-u.ac.jp, †ytyt9050@hotmail.com,
‡kizawa@dist.cne.okayama-u.ac.jp, ‡‡okamoto@ee.ous.ac.jp

概 要

現在最も普及している無線LANの規格であるIEEE802.11aやIEEE802.11gでは，通信内容の漏洩やネットワークの不正利用を防ぐためにWEP(Wire Equivarent Privacy)やWPA(Wi-Fi Protected Access)が用いられている．しかし，これらとend-to-endの暗号化とを併用する場合には，無線区間が二重に暗号化されることになるため，通信効率が必要以上に低下するという問題がある．この問題点を解決するため，本稿ではend-to-end暗号化の有無に応じて，無線区間ではパケット全体の暗号化とパケット認証を切り替えることができるような手法を提案する．end-to-endの暗号化が行われている場合には，無線区間では暗号化の代わりにパケット認証のみを適用することにより，二重暗号化の回避による通信効率の改善が期待できる．

A Method for Improvement of Communicative Efficiency with Packet Authentication on Wireless LAN Environment

Kiyohiko Okayama†, Yousuke Tanibuchi††, Nariyoshi Yamai†,
Masao Kizawa‡, Takuji Okamoto‡‡

†Information Technology Center, Okayama University
††Graduate School of Engineering, Okayama University of Science
‡Graduate School of Natural Science and Technology, Okayama University
‡‡Faculty of Engineering, Okayama University of Science

†{okayama,yamai}@cc.okayama-u.ac.jp, ††ytyt9050@hotmail.com,
‡kizawa@dist.cne.okayama-u.ac.jp, ‡‡okamoto@ee.ous.ac.jp

Abstract

On IEEE 802.11a and 802.11g, that are the most popular standards of wireless LAN networks, encryption functions called WEP (Wire Equivarent Privacy) or WPA (Wi-Fi Protected Access) are used for preventing both eavesdropping and unauthorized access. However, along with end-to-end encription, WEP and WPA have large overhead due to duplicated encryption. In this paper, we propose a method to reduce these drawbacks. On this method, a wireless client can choose packet encryption or packet authentication in its wireless LAN automatically according as end-to-end encryption is performed or not. With packet authentication in case that end-to-end encryption is performed, we can improve the communication speed on the wireless environment.

1 はじめに

無線LANは，電波の届く範囲であれば容易にネットワークへのアクセスが可能であるという利便性の面から，近年注目されている．最近では，無線LAN製品の低価格化や無線LAN内蔵端末(ノートPC等)の普及に伴い，利用者の端末から無線LANを利用してネットワークにアクセスできるような環境が多くの組織で提供されるようになってきた．

しかし，無線LANは有線LANと比較すると通信速度およびセキュリティの面で問題がある．

まず，通信速度の面では，無線LANは比較的低速である点が問題である．現在では，IEEE802.11b[1]よりも高速な規格であるIEEE802.11a[2]や802.11g[3]が普及しており，規格上の最大通信速度は54Mbpsである．しかし，無線LANは有線LANと比較するとオーバヘッドが大きく，実質的な通信速度は高々二十数Mbps程度しかない．

次に，セキュリティの面では，第三者への通信内容の漏洩や利用資格がない者によるネットワークの不正利用が挙げられる．この対策のため，従来はWEP(Wire Equivalent Privacy)[4]と呼ばれる暗号化技法が用いられてきたが，脆弱性を有することが知られており[5, 6]，最近ではWPA(Wi-Fi Protected Access)[7]が急速に普及している．しかし，これらはいずれも無線区間，すなわち，無線LAN端末とアクセスポイント間のセキュリティを確保するための技術であるため，無線LAN端末がアクセスポイントよりも先のネットワーク上にあるサーバなどとセキュアな通信を行うためには，SSLやSSHによるend-to-endの暗号化が併用されることが多い．

ところが，無線区間の暗号化とend-to-endの暗号化を併用すると，無線区間では二重に暗号化が行われることになるため，無線LANの実質的な通信速度がさらに低下するという問題が発生する．この問題を解決するため，我々の研究グループでは，無線LAN区間で暗号化の代わりにパケット認証を行うことにより，無線LANの不正利用を防止しつつ二重暗号化による通信速度低下を回避する手法[8]を提案している．ただし，文献[8]では，無線LAN区間で暗号化とパケット認証を使い分けるための基本的なアイデアを示したのみであり，その有効性を見積もるための性能評価実験も，現在では古い規格となりつつあるIEEE802.11bの無線LAN環境で行われたものであった．

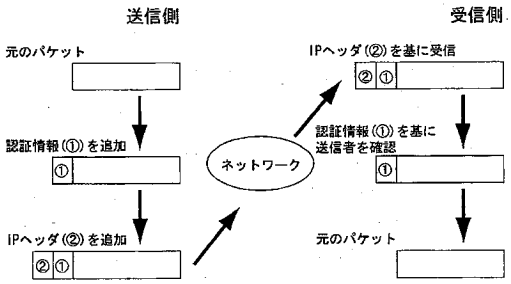

図1: パケット認証の処理手順

そこで本稿では，end-to-entの暗号化の有無に応じて無線区間の暗号化とパケット認証を切り替えるためのシステム設計を示すと共に，現在普及している最新の無線LAN規格を用いて性能評価実験を行うことにより，提案手法の有効性を検証する．以下，パケット認証による通信効率の改善手法について述べた後，提案手法の設計と，その有効性を見積もるために実施した性能評価実験について述べる．

2 パケット認証による通信効率の改善手法

無線LAN経由で利用されるネットワーク環境において，end-to-endの暗号化機能は付与するが，無線LAN部分での暗号化通信機能は付与しないものとすると，二重化による通信速度低下はなくなり，無線区間における通信内容の漏洩も防止できるが，WEPやWPAで実現される不正アクセスが防止できなくなってしまう．そこで，不正アクセス防止機能を付与するために，WEPやWPAに代わる機能としてパケット認証を導入し，上述したend-to-endの暗号化機能と併用して，通信性能低下を回避する．

パケット認証は，不正アクセスの防止と通信データの改竄を検出する機能である．具体的には，図1に示すように，送信側でパケットの内容に応じた認証情報を付加し，それを受信側で検証することにより，発信者が正規利用者であると確認できる．認証情報は発信者が持つ秘密情報に基づいて計算されるため，第三者が認証情報を偽造することは困難であり，ネットワークの不正利用を防止することができる．すなわち，WEPやWPAのように通信データ全体を暗号化処理によって書き換えるといったことがなく，比較的小さな認証情報を付加するだけで済む．

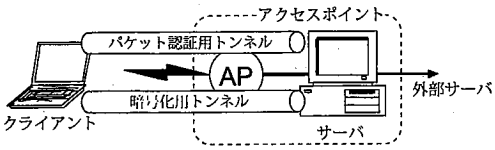

図 2: システム構成

このため，end-to-end の暗号化が行われている場合には，WEP や WPA の代わりにパケット認証機能を付与することで，通信性能の改善が期待できる．

3 提案手法の設計

3.1 システム構成

提案手法のシステム構成を図 2 に示す．図中の “AP” は無線 LAN のアクセスポイントである．提案手法を実現するにあたり，既存の無線 LAN アクセスポイント機器にパケット認証機能を実装するのは困難であるため，有線 LAN を用いて AP にサーバ PC を直結し，AP とサーバ PC をまとめて仮想的なアクセスポイントとみなす．

図 2 の構成において，無線区間の暗号化およびパケット認証は，クライアント-AP 間ではなくクライアント-サーバ間で行う．したがって，AP はクライアントに対してデータリンク層レベルの接続を提供するのみであり，WEP や WPA といった暗号化機能は一切利用しない．

一方，サーバがクライアントに対して暗号化機能およびパケット認証機能を提供するため，クライアント-サーバ間ではあらかじめ 2 つのトンネル用コネクションを確立するものとする．クライアントはこれらのコネクションをトンネルとして利用することにより，外部のサーバにアクセスすることができる．このとき，一方のトンネルではパケット認証のみを行い，他方のトンネルではパケットの暗号化とパケット認証を行うものとする．クライアントは，end-to-end の暗号化を行う場合や，通信内容を秘匿する必要がない場合にはパケット認証用トンネル，それ以外の通信には暗号化用トンネルを経由することにより，二重暗号化を回避することが可能になる．また，これらのトンネルを確立する際に利用者認証を行うことにより，アクセスポイントの不正利用防止だけでなく，ユーザ単位のアクセス制御も実現できる．

なお，上述した 2 つのトンネルは，VPN ソフトウェアの 1 つである OpenVPN[9] が提供する SSL コネクションを利用して実現する．OpenVPN では，トンネル用コネクションに適用する暗号化通信方式およびパケット認証方式の有無とその種類を指定できるため，上述した 2 つのトンネルが容易に実現できると考えられる．さらに，OpenVPN クライアントでは，各トンネルのエンドポイントは仮想インタフェースとして実現されるため，次節で述べるトンネルの使い分けが容易であるという利点もある．

3.2 無線区間におけるパケット認証と暗号化の選択

前節で述べた 2 つのトンネルを用いることにより，クライアントは無線区間においてパケット認証と暗号化のいずれかを選択することが可能であるが，どの通信に対してどのトンネルを経由させるかが重要となる．厳密には，end-to-end での暗号化通信に関するネゴシエーションを監視して，その結果に応じて適切なトンネル用コネクションを選択する必要があるが，より簡便な方法として，提案手法では宛先ポート番号に基づいた選択を行う．

例えば，SSH(ポート番号 22) や HTTPS(同 443) のように，end-to-end の暗号化通信を前提とするサービスや，DNS(同 53) のように通信内容の秘匿があまり重要視されないサービスの場合には，パケット認証用トンネルを経由させることにより，二重暗号化を回避することができる．一方，それ以外のサービスについては，暗号化用トンネルを経由させることにより，無線区間における通信内容の秘匿を実現できる．

OpenVPN を利用してトンネルを構築する場合，クライアントでは，暗号化用トンネルに対応する仮想インタフェースをデフォルト経路として指定する．一方，パケット認証用トンネルを経由するサービスについては，FreeBSD の divert[10] のような機能を用いて，宛先ポート番号に基づいてパケット認証用トンネルに対応する仮想インタフェースに通信データを転送すればよいと考えられる．

なお，一般に end-to-end の暗号化はパケットのペイロードに適用されるため，OpenVPN の SSL コネクションをパケット認証用トンネルとして利用す

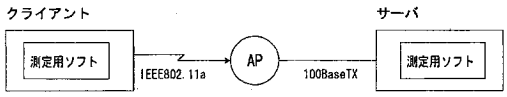

図 3: 実験環境

る場合，カプセル化前のパケットヘッダ部分は平文のままトンネルを流れることになる．このため，通信先となるサーバの IP アドレスまで秘匿したい場合は，暗号化用トンネルを通す必要がある．ただし，上述したポート番号に基づくトンネル選択では，同一の宛先ポート番号を持つトラヒックに対して異なるトンネルを適用することは困難であるため，クライアントのユーザが使用するトンネルを選択できるような方法を検討する必要がある．

4 性能評価

前章で述べたシステムは現在実装中であるため，総合的な性能評価は現時点では行えない．そこで，無線区間における暗号化と，SSL によるパケット認証および暗号化のオーバヘッドを見積もるための予備実験を行った．

4.1 実験環境

実験環境を図3に示す．クライアントとサーバの間に AP を配置し，クライアント-AP 間は IEEE802.11a で接続し，AP-サーバ間は 100Base-TX の Ethernet で接続した．クライアント (Pentium4-3.2GHz, メモリ 512MB)，サーバ (Pentium4-3.0GHz，メモリ 1GB) はいずれも WindowsXP 搭載の PC/AT 互換機で，AP は Planex 社製 GW-AP54SAG である．現在普及している高速な無線 LAN 規格には IEEE802.11g もあるが，2.4GHz 帯を使用するため，同じ周波数帯を使用する電子レンジやコードレス電話などからの干渉が考えられる．さらに，実験室の周囲を調査したところ，IEEE802.11g を使用するアクセスポイント製品が多数存在することが判明した．これらの機器による影響をできるだけ排除するため，今回の実験では 5GHz 帯を使用する IEEE802.11a を選択した．

一方，end-to-end での暗号化およびパケット認証を行うため，クライアントおよびサーバには SSL トンネルの構築ソフトウェアである stone[11] を導入した．stone は暗号化とパケット認証の有無 (とその種類) を制御可能であるため，無線区間における暗号化の有無と組み合わせることによりさまざまな場合の通信性能が測定できる．図3の実験環境において，通信のボトルネックになるのは AP-サーバ間ではなくクライアント-AP 間であるため，stone によるパケット認証を無線区間のパケット認証，stone による暗号化を end-to-end の暗号化とみなした．さらに，クライアントおよびサーバにはネットワークのスループット測定ソフトウェアである ttcp[12] を導入した．

4.2 実験方法

二重暗号化による通信性能の低下とパケット認証の有効性を検証するため，無線区間の暗号化とパケット認証，および end-to-end の暗号化を組み合せて ttcp による測定を行った．

実験パラメータとして，無線区間では，

(1) 暗号化なし

(2) 64 ビット WEP(以下，WEP64)

(3) 128 ビット WEP(以下，WEP128)

(4) WPA の AES[14] モード (以下，WPA-AES)

(5) WPA の TKIP モード (以下，WPA-TKIP)

の 5 通りの暗号方式を設けた．一方，stone による SSL トンネルとしては，

(a) 暗号化なし (パケット認証も行わない)

(b) パケット認証のみ

(c) AES 暗号とパケット認証

の 3 通りを設けた．すなわち，15 通りの組み合わせを設けた．本実験では，それぞれの場合において，ttcp クライアントから ttcp サーバに 50MB のデータを 5 回送信し，その平均スループットを算出した．

4.3 実験結果と考察

実験結果を表1に示す．まず，無線区間の暗号化に注目すると，stone によるパケット認証や暗号化

表 1: 実験結果

単位(Mbps)

無線区間 / end-to-end間	暗号化なし	WEP-64	WEP-128	WPA-AES	WPA-TKIP
暗号化なし	19.12	17.97	17.92	18.00	14.60
パケット認証のみ	18.96	17.79	17.74	17.87	14.49
暗号化:AES256 + パケット認証	18.77	17.77	17.75	17.75	14.01

の有無に関わらず，WEP64，WEP128，WPA-AESはいずれもスループットの低下が6%程度であるのに対し，WPA-TKIPの場合は約25%もの低下が見られる．これは，WEPおよびWPA-AESはAPにおける暗号化および復号をハードウェアで処理しているのに対し，WPA-TKIPは既存の機器に対する互換性重視のため，暗号処理の一部をソフトウェアで実現していることが原因であると推測される．

次に，stoneによる暗号化およびパケット認証では，無線区間の暗号化の有無に関わらず，パケット認証のみを行う場合の性能低下は1%未満，AESによる暗号化とパケット認証の両方を行った場合は1〜4%程度の低下となっている．今回の実験で使用したstoneは，その仕様上，暗号化を行う場合にパケット認証を無効にすることができなかったが，パケット認証によるスループット低下は非常に小さいため，AESによる暗号化とパケット認証の両方を行った場合のオーバヘッドは，ほぼ暗号化によるものであると考えられる．

以上のことから，二重暗号化を行った場合のスループット低下は，無線区間でWEPおよびWPA-AESを使用する場合は7〜10%，WPA-TKIPを使用する場合は26〜29%であるとみなすことができる．これに対し，stoneにおいて暗号化とパケット認証を使用した場合のスループット低下は1〜4%に留まっているため，end-to-endで暗号化する場合には，無線区間では暗号化の代わりにパケット認証のみを行うことにより，スループット低下が大きく改善されると言える．

なお，表1のAPでのAES暗号とstone，すなわちサーバPCでのAES暗号のオーバヘッドを比較するとわかるように，AP上でハードウェア処理を行ったとしても，PC上のソフトウェアによる暗号化処理の方が高速であるという結果になっている．最近ではPCも比較的安価になってきているが，一般家庭に普及しているAP製品との価格差は依然として大きいため，提案手法のようにAPとPCを組み合わせて仮想的なAPを構成すると，場合によってはコストの問題が無視できない．このため，今後はAP製品自体にパケット認証機能を組み込む方法も検討したい．

5 まとめ

本稿では，無線LANでの暗号化とend-to-endでの暗号化の併用による通信の非効率性を改善するため，end-to-endにおける暗号化の有無に応じて無線区間での暗号化とパケット認証を切り替えることができるシステムの設計を示した．また，実際の無線LAN環境で性能評価実験を行うことにより，WEPやWPAのオーバヘッドがかなり大きいことを明らかにし，本手法により通信効率を改善できる可能性を示した．

本手法は現在実装中であり，無線区間で利用するVPNのオーバヘッドを含めた性能評価は未実施である．今後の課題として，本手法の実装と，これを用いた有効性を検証が挙げられる．

謝辞 本研究の一部は，総務省・戦略的情報通信研究開発推進制度(特定領域重点型研究開発プログラム，課題番号041108001)の補助を受けている．ここに記して感謝の意を表する．

参考文献

[1] IEEE: "802.11b-1999 Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4GHz band", IEEE, 1999.

[2] IEEE: "IEEE 802.11a-1999 (8802-11:1999/Amd 1:2000(E)), IEEE Standard for information technology - Telecommunications and Information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Contorol (MAC) and Physical Layer (PHY) specifications - Amenndment

1: High-speed Physical Layer in the 5 GHz band", IEEE, 1999

[3] IEEE: "IEEE 802.11g-2003 IEEE Standard for Information technology - Telecommunications and information exchage between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band", IEEE, 2003.

[4] L. M. S. C. of the IEEE Computer Society: "Wireless LAN medium access control(MAC) and physical layer(PHY) specifications", IEEE Std 802.11, 1999.

[5] Nikita Borisov, Ian Goldberg, and David Wagner: "Security of the WEP algorithum", http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, 2001.

[6] Scott Fluhrer, Itsik Mantin, and Adi Shamir: "Weaknesses in the Key Scheduling Algorithm of RC4", http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

[7] IEEE: "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements", IEEE Std 802.11i, 2004.

[8] 玉井正人, 金出地友治, 山井成良, 岡山聖彦: "IEEE802.11b 環境におけるセキュリティ及び通信効率の改善手法", 情報処理学会 分散システム/インターネット運用技術シンポジウム 2004 論文集, pp.19–24, 2004.

[9] J. Yonan: "OpenVPN", http://openvpn.sourceforge.net/index.html

[10] A. Cobbs: "divert - kernel packet diversion mechanism", http://www.FreeBSD.org/cgi/man.cgi

[11] H. Sengoku: "Simple Repeater stone", http://www.gcd.org/sengoku/stone/Welcome.ja.html

[12] PCAUSA Inc.: "Test TCP(TTCP) Benchmarking Tool for Measuring TCP and UDP Performance", http://www.pcausa.com/Utilities/pcattcp.htm

[13] Netscape Corporation: "The SSL Protocol version 3.0", http://wp.netscape.com/eng/ssl3/draft302.txt, 1996.

[14] US National Institute of Standards and Technology, 11Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, 2001.