

IEEE 802.11b 環境におけるセキュリティ及び通信効率の改善手法

玉井 正人[†] 金出 地友治^{††} 山井 成良^{††} 岡山 聖彦^{†††}

[†] 岡山大学大学院自然科学研究科

^{††} 岡山大学総合情報処理センター

^{†††} 岡山大学工学部

[†]tamai@net.cne.okayama-u.ac.jp, ^{††}{kanadeti,yamai}@cc.okayama-u.ac.jp,

^{†††}okayama@cne.okayama-u.ac.jp

概 要

現在最も普及している無線 LAN の規格である IEEE 802.11b 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 Equivalent Privacy) が用いられている。しかし、これは脆弱性を有し、また特に end-to-end の暗号化と併用する場合には二重暗号化により通信効率が低下するなどの問題があった。この問題点を解決するため、本稿では WEP よりも安全な暗号方式を用い、end-to-end 暗号化の有無によってパケット全体を暗号化したりあるいはパケット認証のみを行ったりする手法を提案する。これにより、従来の IEEE 802.11b 環境と比較してセキュリティを強化しながらかつ二重暗号化によるオーバーヘッドを軽減して通信効率を改善する効果が期待される。

A Method for Enhanced Network Security and Efficient Communication on IEEE 802.11b Environment

Masato Tamai[†], Yuji Kanadechi^{††}, Nariyoshi Yamai^{††}, Kiyohiko Okayama^{†††}

[†]Graduate School of Natural Science and Technology, Okayama University

^{††}Computer Center, Okayama University, Okayama University

^{†††}Faculty of Engineering, Okayama University

[†]tamai@net.cne.okayama-u.ac.jp, ^{††}{kanadeti,yamai}@cc.okayama-u.ac.jp,

^{†††}okayama@cne.okayama-u.ac.jp

Abstract

On IEEE 802.11b, that is the most popular standard of wireless LAN networks, an encryption function called WEP (Wire Equivalent Privacy) is used for preventing both eavesdropping and unauthorized access. However, WEP is known to have some drawbacks that it is easy to break and, especially along with end-to-end encryption, it has large overhead due to duplicated encryption. In this paper, we propose a method to reduce these drawbacks. On this method, a packet is only authenticated when end-to-end encryption is applied, or otherwise encrypted by a stronger cipher algorithm. By virtue of this method, we can improve the communication speed as well as the the network security on the IEEE 802.11b 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 内蔵の端末の普及に伴い、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、現在普及している無線 LAN は比較的低速である点が問題である。IEEE 802.11a[1], 802.11g[2] など、最大通信速度が 54Mbps のより高速な規格も存在するが、まだ広く普及するまでには至っておらず、現在最も普及していると思われる IEEE802.11b[3] では規格上の最大通信速度は 11Mbps しかない。さらに無線 LAN は有線 LAN と比較するとオーバーヘッドが大きく、例えば IEEE 802.11b では実質的な通信速度は高々 5Mbps 程度しかない。

一方、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、IEEE 802.11b では WEP(Wire Equivalent Privacy) と呼ばれる暗号化技法が用いられている。しかし、WEP は脆弱性を有することが知られており [4, 5]、この脆弱性を利用した解読ツール [6] も公開されている。このようなことから現在では、WEP に代わる新しいセキュリティ規格 IEEE 802.11i[7] の標準化が進められてきているが、大多数の IEEE 802.11b の利用者にとっては脆弱性を抱えたままの状態での利用が強いられることになる。そのため、利用者側でも無線 LAN 部分を含めた end-to-end でのセキュリティを確保するため、SSL や SSH 等による上位レイヤによる暗号化が通常併用されている。

ところが、暗号化を行うと、オーバーヘッドの増加により実質的な通信速度がさらに低下することが懸念される。特に無線 LAN 自身の暗号化と end-to-end の暗号化を併用した場合、無線 LAN 部分の packets が二重に暗号化されるため無駄が多いと考え

られる。そこで本稿では特に IEEE 802.11b の利用環境を対象として、WEP よりも強力な暗号方式を用い、end-to-end 暗号化の有無によって packets 全体を暗号化したりあるいは packets 認証のみを行ったりする手法を提案する。これにより、従来の IEEE 802.11b 環境と比較してセキュリティを強化しながらかつ二重暗号化によるオーバーヘッドを軽減して通信効率を改善する効果が期待される。また、本手法ではすべてソフトウェアによる実現が可能であるため、導入が容易である。

なお、以下では特に断らない限り単に無線 LAN と記せば IEEE 802.11b を指すものとする。

2 無線 LAN 環境におけるセキュリティ対策とその問題点

本節においては、まず、無線 LAN 環境におけるセキュリティ対策について 2 つの観点から述べ、その問題点を明らかにする。

2.1 無線 LAN における認証・暗号化とその脆弱性

一般に無線 LAN では以下の 2 点がセキュリティ上問題となる。

- (1) 利用資格がない者からのネットワークアクセスの防止
- (2) 悪意のある第三者に対する通信内容の秘匿

IEEE 802.11b においては、これらの対策手段として、ESS-ID(Extended Service Set ID) や MAC アドレスによる認証、および WEP による暗号化が利用可能であり、実際に多くの組織ではこれらを組み合わせて用いている。

これらのうち、前者については、ESS-ID や MAC アドレスは、無線 packets が暗号化されていない状況では傍受により容易に第三者が取得可能であり、これらの手段だけでは不正アクセスの防止効果はあまり期待できない。

一方、後者については、WEP では無線パケットを秘密鍵で暗号化して送信するため、秘密鍵を知らない者に対する不正なネットワークアクセスの防止および通信内容の秘匿をとともに実現することが可能である。但し、本来の WEP では秘密鍵はすべての利用者で共有されるため、同一の無線 LAN を用いる利用者間では通信内容を秘匿することはできない。そのため最近では IEEE 802.1x[8] を導入して利用者認証を行いながら利用者毎に異なる秘密鍵を用いる方法も普及しつつある。

ところが、このような方法を用いたとしても、1 章で述べたように WEP 自身が脆弱性を有しており、特に秘密鍵の長さが 64 ビット (24 ビットの初期ベクトル IV を除くと 40 ビット) のものは短時間で解読できることが知られている。したがって、現時点では IEEE 802.1x を導入した上で 128 ビット (同 104 ビット) の秘密鍵を用い、さらにこれを定期的に変更することが望ましいといえる。

2.2 無線 LAN 部分における二重暗号化

前節で述べたように、無線 LAN での暗号化は脆弱性が知られており、その対策は重要であるが、一方最近では有線ネットワークにおいてもパケットの盗聴や成りすましなどの問題が懸念されるようになってきている。そこで、利用者側では無線 LAN 部分を含めたネットワーク全体のセキュリティ確保のため、SSL(Secure Socket Layer)、SSH(Secure SHell) など、上位レイヤでの end-to-end の暗号化を併用することが一般に行われている。

ところが、この場合、図 1 に示すように、無線 LAN 部分では WEP による暗号化と end-to-end の暗号化が重複して行われることになる。これは一般に end-to-end の暗号化が十分強力であることから実用的な意味は殆どなく、暗号化のオーバーヘッドにより通信効率が低下することが問題となり得る。これを回避する方法として、WEP を用いずに end-to-end の暗号化のみを用いる方法が考えられる。しかし、この方法では無線 LAN での第三者による不正アクセスが防止できなくなり、また end-to-end の暗号化を行っていない通信についてはその内容が秘

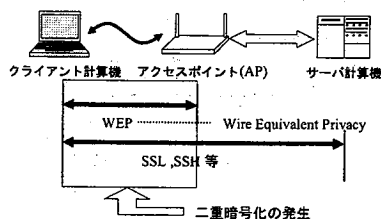


図 1: 無線 LAN 部分における二重暗号化

匿されないなどの問題が生じるため、これを採用することはできない。

3 セキュリティ・通信効率の改善手法

3.1 改善手法の概要

前節で述べたように、WEP には不正アクセスの防止および通信内容の秘匿の両方の役割があるが、そのいずれにも問題がある。すなわち、不正アクセスの防止に関しては end-to-end の暗号化併用時におけるオーバーヘッドが問題となり、また end-to-end の暗号化を用いない場合における通信内容の秘匿に関しては脆弱性を有している。

そこで、本稿では WEP の代わりにパケットレベルでの認証もしくは十分に安全な暗号化を行う機能を導入し、必要に応じてこれらを使い分ける手法を提案する。すなわち、end-to-end の暗号化が行われる場合には、無線 LAN 部分ではオーバーヘッドが大きい暗号化は行わず、代わりにオーバーヘッドの小さいパケット認証を用いて不正アクセスを防止し、また end-to-end の暗号化が行われない場合には、無線 LAN 部分では WEP の代わりにより安全な暗号化を行うようにする。なお、end-to-end の暗号化が行われない場合でも例えば DNS サーバとの問合せ・応答のように通信内容の秘匿よりも通信速度が重視される場合にはパケット認証のみを行うことも可能である。

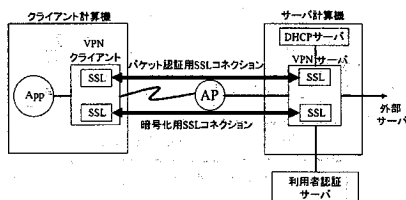


図 2: システムの構成

3.2 システムの構成および通信手順

現時点におけるシステムの構成を図 2 に示す。図に示すように、本システムでは本研究とは別にクライアント計算機における休止・復旧時のコネクション維持などの機能を提供するため、アクセスポイントの他にサーバ計算機を設け、クライアント計算機とサーバ計算機との間で一種の VPN を構築することを予定している。その際、無線 LAN 部分では WEP は用いず、クライアント計算機とサーバ計算機との間には VPN リンクとして 2 本の SSL コネクションを確立し、そのうち 1 本はパケット認証のみを行うため、もう 1 本は暗号化を行うために用いることにより上記の機能を実現する。またクライアント計算機とサーバ計算機上の VPN 用ソフトウェアはパケットの発信元・宛先ポート番号を監視し、2 本の SSL コネクションのうちどちらを用いるかを決定する役割を果たす。更にサーバ計算機では VPN リンクとして用いているいずれかの SSL を経由したパケットのみを外部ネットワークに中継する。これにより不正アクセスの防止を実現する。

通信手順の概要を以下に示す。

- (1) クライアント計算機は DHCP を用いてサーバ計算機から IP アドレスの割当を受ける。
- (2) クライアント計算機はサーバ計算機との間でパケット認証用コネクションと暗号化用コネクションを確立する。
- (3) クライアント計算機は暗号化用コネクションを用いて利用者認証情報を送信する。サーバ計算機はこれを受け取り、利用者認証サーバを用いて認証を行う。

- (4) 認証に成功すると、クライアント計算機はサーバ計算機との間で VPN リンクの設定を行い、外部との通信は 2 種類の SSL コネクションのいずれかを用いて中継するようにする。また、サーバ計算機でもこのクライアント計算機と外部ネットワークとの通信を中継するようにする。

4 性能評価

4.1 実験環境

前章で述べたシステムは現在その詳細を設計中であり、総合的な性能評価は現時点では行えない。そこで、WEP による暗号化、SSL によるパケット認証および暗号化のオーバーヘッドを見積もるために予備実験を行った。

実験環境を図 3 に示す。クライアント計算機、サーバ計算機にはいずれも 2.4GHz の Pentium4 を搭載しており、その OS は Linux である。また、無線 LAN としては、アクセスポイント (AP) には Proxim 社製 ORiNOCO AP-2000 を用い、クライアント計算機にはメルコ社製 Air Station を装着して、両者の間で通信速度 11Mbps の IEEE 802.11b で通信するようにした。アクセスポイント・サーバ計算機間は 100Mbps のファーストイーサネットを用いて接続した。

この環境においてクライアント計算機及びサーバ計算機には自作プログラムを設置し、インタラクティブ型およびバルク型で一定量のデータ通信を行った場合の伝送時間を測定した。その際、802.11b の設定として WEP を用いない場合 (noWEP と表記)、初期ベクトルを含めて 64 ビットの鍵を用いて暗号化した場合 (WEP64 と表記)、同じく 128 ビットの鍵を用いて暗号化した場合 (WEP128 と表記) の 3 通りに変化させ、またクライアント計算機・サーバ計算機間は SSL を用いない場合 (NULL と表記)、SSL を用いてパケット認証のみを行う場合 (SNUL と表記)、SSL を用いて RC4 および AES による暗号化を行った場合 (それぞれ RC4, AES と表記) の 4 通りに変化させ、これらを組み合わせた計 12 通り

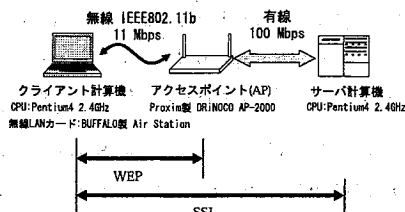


図 3: 実験環境

の環境を用意した。

伝送時間の測定にあたっては、インタラクティブ型データ通信に関しては 1MB のデータを 1 バイト単位で送信した場合の伝送時間を、またバルク型データ通信に関しては 1MB のデータを 1kB 単位で送信した場合の伝送時間を測定し、それぞれ 100 回の測定における平均値を求めた。

4.2 実験結果と考察

インタラクティブ型データ通信、バルク型データ通信における各環境下の平均伝送時間をそれぞれ図 4、図 5 に示す。これらの結果より以下のことが言える。

まず、WEP を用いた場合では、WEP を用いていない場合と比較すると伝送時間は暗号鍵の長さによらずインタラクティブ型の場合には約 15%、バルク型の場合には約 35% 増加しており、WEP のオーバーヘッドはかなり大きいことがわかる。ここで、バルク型のほうがインタラクティブ型と比較してオーバーヘッドが大きいのは、WEP で用いられている暗号方式 RC4 がストリーム型暗号であるためと思われる。一般にバルク型データ通信のほうがインタラクティブ型より高い通信速度が要求されることを考慮すると、特にバルク型データ通信における大きなオーバーヘッドは重要な問題となり得る。

一方、パケット認証によるオーバーヘッドは認証を行わない場合 (NULL) と比較するとインタラクティブ型の場合で約 7%、バルク型の場合で約 1% と十分小さく、無線 LAN 部分での暗号化が不必要である場合には WEP の代わりにパケット認証を用いる

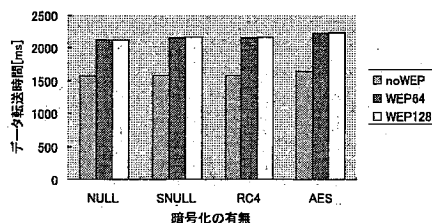


図 4: インタラクティブ型データ通信における伝送時間

と通信効率をかなり改善できると推測できる。

SSL における暗号化を用いた場合では、全体的にパケット認証よりオーバーヘッドが大きいが、RC4 による暗号化はオーバーヘッドが比較的小さくパケット認証とほぼ同じといえる。一方、AES による暗号化のオーバーヘッドはかなり大きく、暗号化しない場合 (NULL) と比較するとインタラクティブ型の場合で 15~20% 程度、バルク型で 5% 程度である。しかし、インタラクティブ型でも WEP を用いずに AES で暗号化する場合 (noWEP と AES) と、AES を用いずに WEP で暗号化する場合 (WEP64 と NULL または WEP128 と NULL) を比較すると同程度の伝送時間であり、AES のほうが WEP よりもかなり安全性が高いことを考慮すると有効であるといえる。また、高い通信速度が要求されるバルク型データ通信では AES による暗号化のオーバーヘッドは WEP よりも十分小さく、安全性と通信効率の両面で AES による暗号化は WEP より優れていると言える。なお、バルク型データ通信において AES による暗号化のオーバーヘッドが比較的小さい理由は、AES がブロック型暗号方式であるためと思われる。

以上のことから、提案手法は従来の IEEE 802.11b における WEP と比較してセキュリティを強化しながらかつ二重暗号化によるオーバーヘッドを軽減して通信効率を改善する効果が十分見込めるといえる。

5 まとめ

本稿では、IEEE 802.11b 環境において用いられる WEP の脆弱性および end-to-end の暗号化との併用

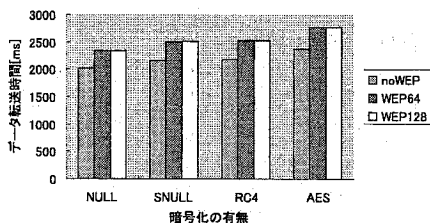


図 5: バルク型データ通信における伝送時間

による通信の非効率性を改善するため、無線 LAN 部分に WEP よりも強力な暗号方式を用い、必要に応じてパケット全体を暗号化したりあるいはパケット認証のみを行ったりする手法を提案した。また予備実験により WEP のオーバーヘッドがかなり大きいことを明らかにし、提案手法により通信効率を改善できる可能性を示した。

本手法は現在詳細設計中であり、VPN のオーバーヘッドを含めた end-to-end での性能評価はまだ行えない。今後の課題としては本手法を実装し、end-to-end での有効性を検証することが挙げられる。

参考文献

- [1] 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 Control (MAC) and Physical Layer (PHY) specifications - Amendment 1: High-speed Physical Layer in the 5 GHz band", IEEE, 1999.
- [2] IEEE: "IEEE 802.11g-2003 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 - Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band", IEEE, 2003.

- [3] IEEE: "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.
- [4] Nikita Borisov, Ian Goldberg, and David Wagner: "Security of the WEP algorithm", <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>, 2001.
- [5] Scott Fluhrer, Itsik Mantin, and Adi Shamir: "Weaknesses in the Key Scheduling Algorithm of RC4", http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf
- [6] The Shmoo Group: "AirSnort Homepage", <http://airsnort.shmoo.com/>.
- [7] IEEE: "IEEE P802.11i/D3.0 Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE, 2003.
- [8] IEEE: "P802.1X, D10, January 2001 DS5886 P802.1X Draft Standards for Local and Metropolitan Area Networks: Standard for Port based Network Access Control", IEEE, 2001.
- [9] The OpenSSL Project: "OpenSSL", <http://www.openssl.org/>.