有線及び無線リンク経由の通信における IPsec 適用手法の一検討

A Study of a Method to Apply IPsec for Communications through Wired and Wireless Links

鎌田　美緒 †　　小口　正人 †
Mio Kamata　　Masato Oguchi

1. はじめに

近年，無線通信技術が急速に普及し，企業だけでなく家庭や公共施設でも広く使われるようになってきた．ネットワークインフラとして無線通信の存在は大きくなり，無線 LAN のホットスポットサービスなどに見られるように有線と無線にまたがった通信環境も多く存在する．しかし有線リンクと比べ無線リンクは通信が傍受されやすく，暗号化によりデータを守ることが必須となる．

ネットワークにおける通信プロトコルは階層構造を持つことが一般的であるが，暗号化技術も各階層に様々な方式が存在し，異なるセキュリティ技術を設定することが可能である [1]．また，一階層の暗号化方式だけでは不十分な場合，他の階層と組み合わせて使用することで，より安全性を高めることができる．しかしセキュリティとパフォーマンスはトレードオフの関係にあると考えられるため，性質の異なるリンクごとに適切な暗号化方式の設定が望まれる．

2. 本研究の目的

現在無線 LAN の暗号化技術としては，データリンク層で暗号化を行う WEP(Wired Equivalent Privacy) が標準的に用いられているが，いくつかの脆弱性が指摘されている．IEEE802.11i など無線 LAN のセキュリティを強化する規格も進められているが，本研究では無線リンクを含む異種リンク間通信の安全性をさらに高めるため，ネットワーク層で暗号化・復号化を行う IPsec(IP Security)[2] の使用を検討した．しかしソフトウェア処理による IPsec は一般に，ノードへ高い負荷をかけスループットを著しく低下させることが知られており，リンクごとの最適な適用手法を検討する必要がある．本研究では，まず有線および無線の各リンクにおいて暗号化処理がパフォーマンスに与える影響を評価する．その結果をもとに，例えばホットスポット周辺のように有線と無線のリンク間をまたがる通信において，セキュリティ要求レベルとパフォーマンスのバランスを考慮した最適なセキュリティ手法の適用モデルを検討する．

3. 暗号化方式適用の評価実験

3.1 有線と無線にまたがるネットワークの構築

図 1 および表 1 に示すようにスペックの異なる 3 台のマシンを全て IEEE802.11b 無線 LAN で接続し，そのうち 2 台を Fast Ethernet でも接続することで複数のリンクを持つネットワーク環境を実現した．暗号化方式としては WEP と IPsec を使用し，IPsec の Linux 実装として FreeS/WAN を用いた．また無線環境において WEP は常時使用の状態である．

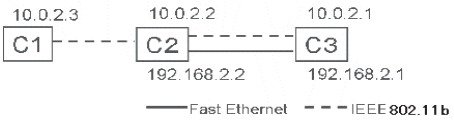

図 1: 実験環境

表 1: 使用計算機

C1	Linux2.4.7-10,Intel PentiumIII 800MHz,256MB
C2	Linux2.4.20-8,Intel PentiumM 1.3GHz,256MB
C3	Linux2.4.7-10,Intel PentiumIII 1GHz,512MB

3.2 単独リンクにおける実験

基礎実験として有線と無線のリンク各々について，IPsec を用いた場合と用いない場合における各マシンのスループットと CPU 使用率を測定した．本実験はマシン C2 と C3 の有線および無線リンクを用いて行った．結果を図 2、図 3 に示す．

有線においては IPsec を用いるとスループットが 55 %減，CPU 使用率が約 70 %増加とどちらも大幅な変化が見られ，IPsec によってマシンの通信性能とアプリケーション実行性能が相対的に大幅低下していることが分かる．有線は無線と比べ本来の通信速度が速いため，IPsec の暗号化・復号化処理により CPU の負荷が大幅に増加することが，スループット低下の原因となっている．一方無線においてはスループットの差は 3 %，CPU 使用率は 7 %程度と変化は微少であった．無線は有線と比べ元々の通信速度が低いため，この速度においては IPsec の影響は少ない．逆に有線リンクにおいては，もし CPU が十分に速く，図 3 に示されたように IPsec 適用時に 100 %使い切ってしまうことがなければ，IPsec を用いてもスループットの低下はわずかで済み，無線リンクにおけるスループット低下率から換算して平均 89Mbps 程度を出せる可能性があると考えられる．

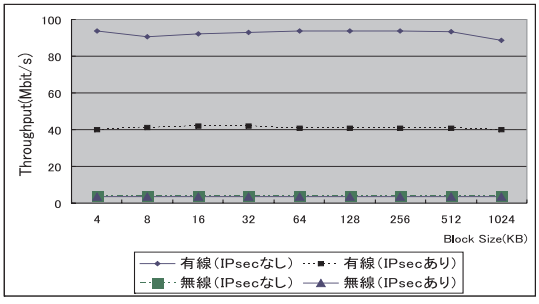

図 2: 有線，無線の各リンクにおけるスループット

†お茶の水女子大学，Ochanomizu University

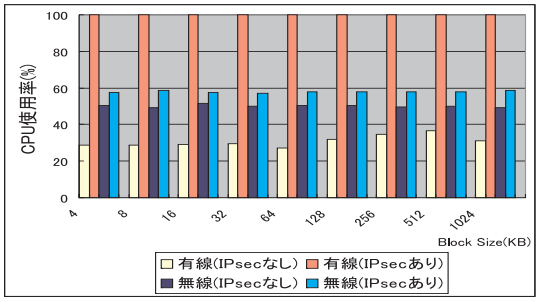

図 3: 有線，無線の各リンクにおける CPU 使用率

3.3 複数のリンクにまたがった環境における実験

構築したネットワークのうち有線と無線の 2 つのインタフェースを持つマシン C2 をゲートウェイとしてリンクをまたがる通信を可能とした．これは Linux の iptables コマンドによりマシン C2 カーネルにおいてパケットフォワード機能を動作させ，さらにマシン C1 と C3 において route コマンドにより経路制御表を書き換えることにより実現している．マシン C2 が，いわばホットスポットのアクセスポイントに相当する．IPsec を適用するか否かの組み合わせにより 4 種の経路を用意し，各マシンのスループットと CPU 使用率を測定した．(図 4)

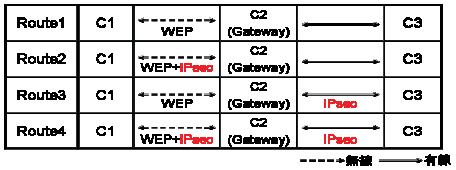

図 4: IPsec の適用モデル

各経路におけるスループットと CPU 使用率は図 5〜図 7 の通りである．

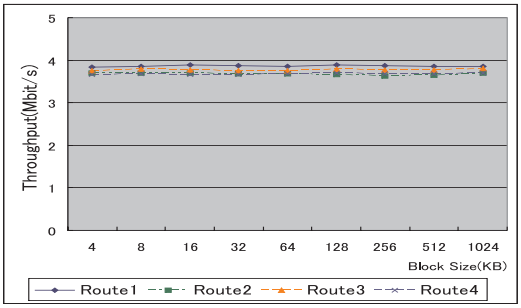

図 5: 各経路におけるスループット

3.4 複数リンクにおける実験結果の考察

スループットはどの経路においても大きな差はなく，無線の単独リンクにおけるスループットと同程度の値になった．C1 における CPU 使用率は，IPsec を C1 で用いた場合 (Route2,Route4) と用いない場合 (Route1,Route3) の差が 10 %程度であった．またゲートウェイである C2 における CPU 使用率は IPsec を全く用いない場合 (Route1) が最も低く，IPsec を用いると，その処理により CPU 使用率が 10〜15 %程度高くなることが分かった．

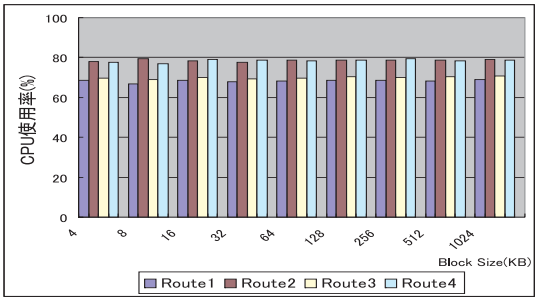

図 6: 各経路における C1 の CPU 使用率

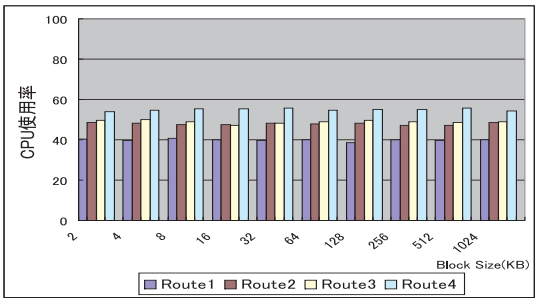

図 7: 各経路における C2(Gateway) の CPU 使用率

単独リンクの場合と比較すると，複数リンクの場合は無線を含むため性能は単独リンクの無線に近いものとなり，この場合も IPsec を使用したことによる影響は少ない．C2(Gateway) をアクセスポイントと考えた場合，その CPU 使用率は接続される相手数により変化するが，IPsec を適用しても C2 における CPU 使用率に大きな差はなく，またホットスポット等における同時アクセスノード数は一般に高々10 台程度以下であることが多い．従って通信のセキュリティを考慮すると，有線におけるセキュリティが保障されている場合には無線のみを IPsec で暗号化する Route2，有線のセキュリティも確保する必要がある場合には無線・有線ともに暗号化を行う Route4 が最適な経路であると言える．

4. まとめと今後の課題

本研究では有線リンクと無線リンクを経由する通信における暗号化手法適用時の定量的評価を行い，各環境における最適な適用モデルの検討を行った．今後はこのような通信環境におけるセキュアなコネクションの設定手法などについて検討したい．

参考文献

[1] 難波誠一，小口正人：インターネット・無線 LAN・放送における暗号化技術，情報処理，vol.45，no.11，pp.1143-1145，2004 年 11 月

[2] 小早川知昭：IPsec 徹底入門，翔泳社

[3] Bruce Potter,Bob Freck 著 根津研介 監訳：802.11 セキュリティ，オライリー・ジャパン