経路制御を用いた盗聴防止方式の提案

服部正尚† 水野優良† 柿崎淑郎† 辻秀一‡
東海大学大学院工学研究科† 東海大学電子情報学部‡

1 はじめに

近年、インターネットは爆発的な勢いで普及しつつある。それに伴って個人データの外部への流出が懸念されている。個人情報など重要なデータなどが流出しないために暗号化が主に用いられる。現在、秘密鍵暗号方式で扱う共有鍵を送信先に送る際、公開鍵を使って送るケースが多く、ＣＡ（認証局）の承認が必要などの煩雑な仕組みとなる。

本論文では、共通鍵や平文でのデータを公開鍵暗号方式を使わずに、ネットワークの経路制御によりユーザが意識せずに盗聴を防止する方式を提案する。

2 従来の手法

現在、盗聴の防止方式には暗号化を使うことが一般的である。共通鍵暗号方式では、共通鍵は暗号化も復号化も同じ鍵で行なうため、鍵を安全に運べるかどうかが暗号化の強度になる。一方、公開鍵暗号方式では、鍵のアルゴリズムは素因数分解である。よって、鍵長が長くなれば長くなるほど安全のデータ通信が行うことができる。また信頼できる暗号が行なわれるためには信頼できる認証局に承認をもらうなどの手間もかかる。

3 提案方式

パケットの通る経路を自ルータから見た最適経路だけではなく一度、ルーティングサーバを経由してそこからの最適経路でも目的ノードに到達させることで、一方の経路で待ち伏せされ、パケットを盗聴されても別ルートのパケットは見られないので中のデータを見られることはない。

ユーザ側からすれば、面倒なシステムを使うことは抵抗があるため、セキュリティステムをより有効にするためにはユーザが意識せずに利用できることが望ましいと考える。

また、重要なデータなどの盗聴は社内ＬＡＮなどの閉じられた空間で起きやすいことよりＬＡＮ内での運用を前提としている。

本稿ではユーザが特に意識せずに利用でき、経路制御による安全なパケット送信についての方式の提案をする。

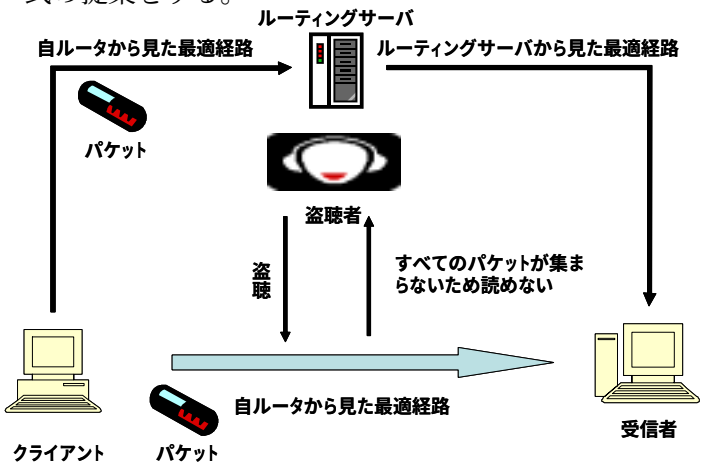

図１提案方式の概要

3．１ システム構成

本システムは、ＩＰヘッダ付加ソフトウェア、ルーティングサーバ、ＩＰヘッダ破棄ソフトウェアから成り立つ。

① ＩＰヘッダ付加ソフトウェア

各クライアントに導入され、送信先の宛先を付与して出来上がったＩＰアドレスを再びアプリケーション層に戻しルーティングサーバ行きのＩＰヘッダを再び付与するソフトウェア。

② ルーティングサーバ

ＡＳ外（ＩＳＰ）などにおいてあると仮定するルーティングサーバでＩＰヘッダ付加ソフトウェアによって作られたヘッダ２の宛先のサーバである。

The Proposal Of The Tapping Prevention System Using The Routing Server

†Masanao Hattori †Masayoshi Mizuno †Yoshio Kakizaki ‡Hidekazu Tsuji
†Graduate School Of Engineering, Tokai University
‡School of Information Technology and Electronics, Tokai University

③　ＩＰヘッダ破棄ソフトウェア

ルーティングサーバに導入され受信されたパケットのヘッダを破棄してもうひとつのヘッダの宛先に再送要求を出すソフトウェアである。

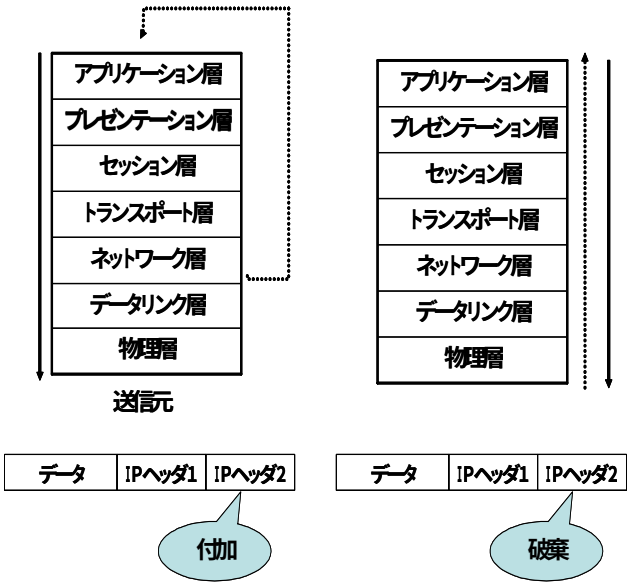

図２ソフトウェア動作図

３．２　システムの基本動作

クライアントからデータを送信元に送る際、生成され、分割されたパケットをいくつかに分け、その中の一部のパケットは通常の経路（受信者までの最適経路）で送信し、残りのパケットはルーティングサーバまで送信され、そこから受信者まで送信される。

以下にシステムの動作について過程ごとに述べる。

３．２．１　各端末、自ルータの動作

情報の漏洩を防ぎたい場合のデータを送信したい場合ＩＰパケット付加ソフトウェアを用いてパケットを生成する。その際、ヘッダ２が付加されるパケットと付加されないパケットの割合はルーティングサーバの台数と送信先端末の数によって変わってくる。

自ルータは受信者までの宛先が入っているヘッダ１のみが付加されているパケットはそのまま最適経路（最短経路）で送信する。また、ルーティングサーバまでの宛先が入っているヘッダ２が付加されているパケットはルーティングサーバまでの最適経路で送信される。

３．２．２　ルーティングサーバの動作

クライアントから送られてきたパケットはルーティングサーバ内のＩＰパケット破棄ソフトウェアによってヘッダ２のみを破棄し、再びヘッダ１をチェックし本来の受信者まで送信する。その際には、ルーティングサーバから見た受信者までの最適経路で送信する。

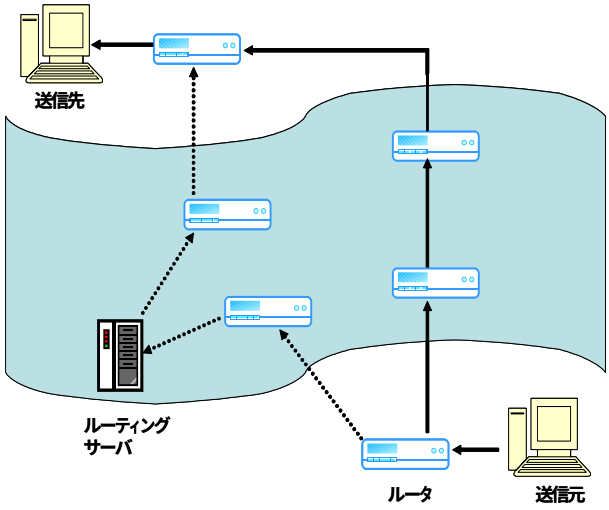

図３システム構成図

４　まとめ

本稿では、ユーザが特に意識せずに利用でき、経路制御による安全なパケット送信についての提案を行った。この方式を用いると、パケットを２種類以上の経路で送信することによりルータ間待ち伏せによる盗聴を防ぐことができる。

問題点としては、送信先や送信元の近い部分でのルータにて待ち伏せをされていたときの安全性の確保や経路でのルータの数が少ないと意味が薄くなってしまうことが挙げられる。

今後、本提案を実験し問題点の解消を行ってみて実装時の環境をシミュレートしてみる。

５　参考文献

[1] 松井佑馬, 江崎浩: ＡＳ内部のネットワークの安定性に関する研究: 情報処理学会第６５回全国大会: 3T9-5: 2003.

[2] 吉田薫, 江崎浩: 大規模ＯＳＰＦネットワークにおけるトラフィックエンジニアリングに関する研究: 情報処理学会第６５回全国大会: 3T9-4: 2003

[3] 堀賢治,吉原貴仁, 堀内浩規: 高信頼自動ルータ設定プロトコルの設定: 情報処理学会第６５回全国大会: 4K-2: 2003

[4]BRUCE SCHNEIER: APPLIED CRYPTOGRAPHY SECOND EDITION: 1996.