1ZA-8

Mobile IPv6 におけるロケーションプライバシーの向上

高橋　弘行†　　蓑原　隆‡
拓殖大学大学院工学研究科†　　拓殖大学工学部‡

1. 研究の背景と目的

移動端末がネットワークを移動しても通信相手とコネクションを維持する技術として MobileIP がある．この MobileIP[1,2]では，パケットのなりすまし，盗聴，改ざんなどを防ぐために IPsec[3]等の暗号化技術が使用される．しかし，暗号化によって通信内容の隠ぺいや，改ざんを防ぐことはできるが，アドレス情報は隠すことができない．このため，移動の前後のパケットを何らかの情報を用いて関連付けることにより，本来関係性を見いだせないはずの，移動端末の移動前のアドレスと移動後のアドレスを関連付けられ，移動履歴を第三者に知られてしまうというロケーションプライバシーの問題がある．したがって移動の前後でのパケットは互いに関連付けられないようにする必要がある．

MobileIP で IPsec を用いてパケットの暗号化を行うとき，パケットの復号化を行うためにパケットに付与される値である Security Parameter Index(SPI)はネットワークを移動しても変化しない．よって，SPI によるパケットの関連付けを防ぐ必要がある．本研究では，移動時に SPI を変化させることでワンタイム化させ，ネットワークを移動しても，パケットに関連性を見いだせないようにする方法を提案する．なお，本研究は Mobile IP を IPv6 で実現した Mobile IPv6[1]を対象としている．

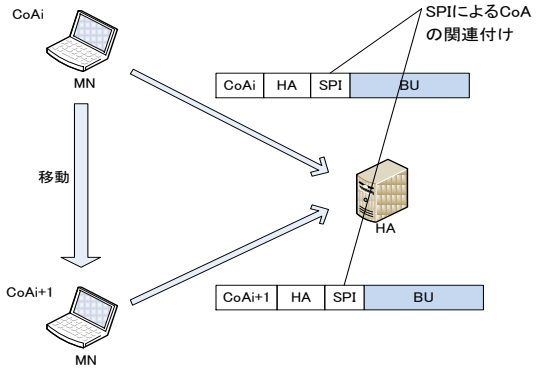

図 1　SPI を用いた移動状況追跡

Enhancing Location Privacy on MobileIPv6
†Hiroyuki TAKAHASHI ,Graduate School of Engineering, Takushoku University
‡Takashi MINOHARA,Department of computer Science, Takushoku University

2. ワンタイム SPI による関連付けの回避

SPI を変化させる方法として，Mobile Node(MN)がネットワークを移動するたびに Internet Key Exchange(IKE)を行い，Security Association(SA)を変更することによって SPI を変更する方法が考えられる．しかし，IKE では通信が発生するため，MobileIP 通信が使用可能になるまでの時間が大きく増加する可能性がある．そこで，本研究では通信を行わずに SPI を変化させることにする．このとき，MN と Home Agent(HA)では互いに同じ SPI 値に変化させる必要がある．また，第三者に変化した SPI 値がわからないようにする必要がある．よって，SPI の系列を一方向性関数を使用し計算で求め，計算に使用するパラメータに秘密鍵を使用することにした．なお，本研究ではこれをワンタイム SPI と呼ぶ．

ワンタイム SPI を用いて通信を行う時の動作を図 2 に示す．まず，HA と MN で一方向性関数によってワンタイム SPI を生成し，SPI と対応づける．MN はパケットを暗号化して送信するとき，パケットの SPI 値を SPI に対応付けられたワンタイム SPI に変更する．その後，パケットを受信した HA はパケットの SPI 値をワンタイム SPI に対応付けられた SPI に変更し，パケットを復号化する．HA から MN へパケットを送信する場合の動作も同様である．

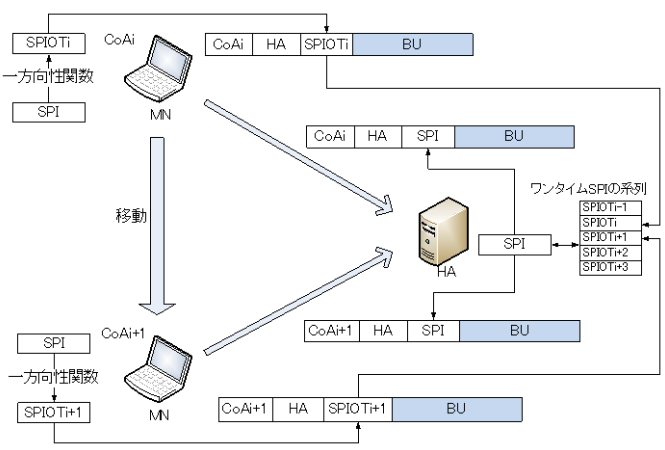

図 2　ワンタイム SPI の概要

3. ワンタイム SPI の問題点

ワンタイム SPI を使用したときの問題点として，パケットロスが発生するとワンタイム SPI の同期が乱れる，ワンタイム SPI の重複が発生すると復号化に失敗するということが考えられる．

パケットロスが発生すると，MN ではワンタイム SPI が変化しているが HA ではワンタイム SPI が変化していないというワンタイム SPI の同期が乱れた状態が発生する．同期が乱れると，ワンタイム SPI から SPI への変換が正常に行われなくなるため，パケットロスによる同期の乱れに対応する必要がある．

ワンタイム SPI の重複が発生すると，ワンタイム SPI から正しい SPI を復元できず，復号化が失敗する可能性がある．これは，ワンタイム SPI は計算によって生成され，MN は他の MN が作ったワンタイム SPI を知ることができないことから，重複が起こる可能性があるためである．そのため，ワンタイム SPI の重複を回避する必要がある．

3.1 同期の乱れに対する対策

ワンタイム SPI の同期の乱れを回避する方法として，一定範囲のワンタイム SPI の系列をあらかじめ作成しておき，通信相手から範囲内のワンタイム SPI が送られてきた場合に，それに追従して同期のずれを許容できるようにする．また，作成した範囲よりも多くのパケットロスが発生した場合は，相手に同期の乱れが発生したことを通知し同期を初期化する．

3.2 ワンタイム SPI の重複の回避

ワンタイム SPI の重複を回避する方法として，MN の Home Address(HoA)を使用して，ワンタイム SPI がどの MN に対して使用されているか区別する．具体的には，HoA とワンタイム SPI を対応づけたリストを用意しておき，パケット受信時にパケットのアドレスとリストにある HoA を比較することによってワンタイム SPI の区別を行う．

4. 評価

4.1 実装環境

ワンタイム SPI のオーバーヘッドの測定を行うため，LinuxPC に実装を行った．実装を行った PC のスペックは，Pentium4 3.0GHz である．

4.2 測定結果

ワンタイム SPI では，HoA によってワンタイム SPI の重複を区別しているため，HA が管理する MN の数でワンタイム SPI を検索するための時間が変化することから，MN の数による HA でのオーバーヘッドの変化を測定するために実験を行った．ここで HA のオーバーヘッドのみ考慮している理由として，HA の管理するアドレスは MN よりも多いため，HoA とワンタイム SPI を対応づけたリストの検索にかかるオーバーヘッドは HA のほうが大きくなるためである．また，パケットロス等による同期の乱れを許容するために作る一定範囲のワンタイム SPI の数は，ネットワークでパケットロスが連続して起こる確率を考えると大量に必要ないと考えられるので，余分に作るワンタイム SPI は 5 個として測定を行った．

HA が管理する MN の数を，100，500，1000，10000 とし，HA に送る BU，BA それぞれにワンタイム SPI を使用したときのオーバーヘッドの測定を行った．その結果，図 3 のように BU，BA のオーバーヘッドはほぼ線形に増加することが分かった．また，オーバーヘッドの増加は数 100μ秒以内に収まっていることが分かった．ネットワークの通信にかかる時間は数 10～数 100m秒のため，測定したオーバーヘッドと比べると小さいため，MN，HA 共にワンタイム SPI を使用したことによるオーバーヘッドは無視できると考えられる．

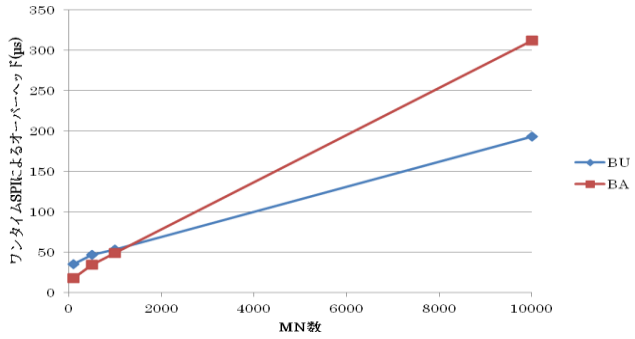

図 3　MN の数によるオーバーヘッドの変化

5. まとめ

MobileIP で IPsec を使用したときにパケットに付与される SPI を用いた移動関連付けについ述べ、その対策法を提案した。そして、その対策について実装を行い、性能評価を行った結果、少ないオーバーヘッドで SPI による移動追跡の対策を実現可能なことを確認した。

参考文献

[1] C. Perkins Ed., “IP Mobility Support for IPv4”, RFC3344, Aug. 2002.

[2] D. Johnson, C. Perkins and J. Arkko, “Mobility Support in IPv6”, RFC3775, Jun. 2004.

[3] S.Kent and K.Seo, “Security Architecture for the Internet Protocol”, RFC4301, Dec. 2005.