HLIN6の位置登録における認証機構

田中康之[†1] 國司光宣[†2] 石山政浩[†3] 河野通宗[†4] 寺岡文男[†1]
[†1] 慶應義塾大学理工学部情報工学科 [†2] 慶應義塾大学大学院理工学研究科
[†3] 東芝研究開発センター通信プラットホームラボラトリー [†4] ソニーコンピュータサイエンス研究所

1 はじめに

現在HLIN6[5]やFast Handovers for Mobile IPv6 [1]、Hierarchical Mobile IPv6[3]といった高速ハンドオーバープロトコルが提案されている。それぞれのプロトコルでは、特殊な中間ルータを持ち、このルータが高速ハンドオーバープロトコルを実現している。移動ノードはこの中間ルータへ位置情報を登録するが、この際、攻撃者が移動ノードになりすますことを防ぐために、移動ノードの認証が必要不可欠となる。しかし、現段階では各プロトコルで中間ルータと移動ノード間の認証について、具体的な方法は提案されていない。

一方、インターネット上でのノードの認証は、IPsecを利用して行うことが一般的である。しかし、移動ノードと不特定多数のノード間でIPsecの利用を前提とすると、PKI (Public Key Infrastructure)の整備が必要であると共に、鍵交換が非常に複雑となるため、現在のPKIの普及状態では現実的な方法ではないと考えられる。

本稿ではHLIN6における中間ルータと移動ノード間の認証機構を提案する。提案手法では、現在のPKIの状況からIPsecを使用せず、鍵交換を必要としないcookie方式を採用する。そして、提案手法が実用上問題の無い頑強性を持つことを目標として、設計し実装する。最後に、実験ネットワークで提案手法の処理時間を測定し、既存のHLIN6との比較を行う。

2 HLIN6の概要

HLIN6(Hierarchical LIN6)はLIN6[2]を基にした高速ハンドオーバープロトコルである。図1にHLIN6のモデル図を示す。HLIN6はLIN6へdomainという概念を導入し、domain内の移動をdomain外に対し透過にすることにより高速ハンドオーバーを可能にしている。domainとバックボーンの境界にはRegional Root router (RR)と呼ばれる中間ルータが置かれる。移動ノード(MN)はRegional Locator (RLoc)とLocal Locator (LLoc)の二つの位置情報を持つ。RLocはdomainを表すlocatorであり、LLocはAccess Router (AR)のサブネット上のlocatorである。

MNの認証は位置登録をする際に必要となる。認証がない場合、悪意の第三者によるMNのなりすましが可能となってしまうためである。MNの認証には

1. MNとMA間の認証(Mapping Registrationの時)
2. RRとMA間の認証(Regional Mapping Registrationの時)
3. CNとMN間の認証(mapping updateの時)

がある。それぞれの場合においてMNが認証された時にのみ、MNの位置情報に関する変更を行うべきである。認証方法は、1についてはMAとMN間であらかじめ共有鍵を保持していることが可能であるため、IPsecの利用が可能である。3に関しては不特定他数のCNとMNで通信の度に共有鍵を交換することは現実的では無いという考えから、LIN6で提案された簡易認証機構[4]によるMNの認証が考えられている。2についての認証方式はまだ提案されていない。よって、HLIN6におけるMNの認証は不完全であり、HLIN6の抱える問題点の一つとして挙げられる。

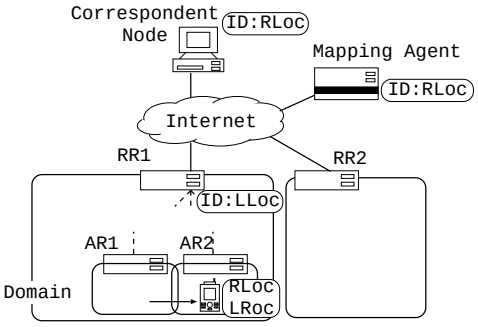

図1: HLIN6のモデル図

3 提案方式

本稿ではRRとMN間の認証について考える。RRとMN間でIPsecを利用した認証を行うためには、PKI (Public Key Infrastructuer)整備が必要であり、鍵交換が複雑となるため、現在のPKIの普及状態では現実的な方法では無い。そこで、本稿では鍵交換を必要としないcookieによる認証方式を提案する。本提案方式では、実用上問題のない強度を持つことを目標としている。

3.1 提案方式の概要

提案方式では、MN は RR に対して cookie を持つ。cookie は一つの RR に対し複数持つことができ、cookie index によって一つの cookie を特定することができるものとする。MN と RR はこの cookie と cookie index を利用してハッシュ値を求め、RR 側ではこの値を署名として利用することで MN の認証を行う。図 2 に提案方式の基本となるモデルを示す。モデルでは MN から RR へ位置情報を登録する際の

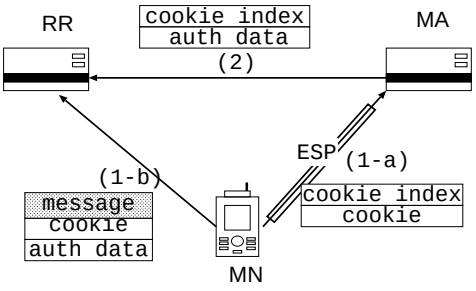

図 2: 提案方式の基本モデル

各メッセージパケットを示している。図 2(1-a) では MN から MA へ cookie と cookie index を通知する。この通知では MA と MN の間で IPsec の ESP を利用して行う。図 2(1-b) では MN から RR へ対して message と共に cookie を通知している。MN の認証は piggyback された署名 (auth data) によって行われる。図 2(1-b) の署名は MN において、cookie index を利用して計算されたハッシュ値となっている。図 2(2) では MA から RR へ cookie index が通知されている。この場合には cookie を利用して MA において計算されたハッシュ値を piggyback する。図 2(1-b) と図 2(2) の 2 つのメッセージを受信した RR は、まず MN から得た cookie を利用してハッシュ値を再計算し、MA の認証を行う。MA の認証がされると、次に MA から得た cookie index を利用して再計算されたハッシュ値によって MN の認証を行う。ここで MN が正しい MN であると認証されると、図 2(1-b) で得られた message が受理されるのである。

実装ではこのモデルが domain 間移動時の位置登録の際に適用される。提案方式適用後の位置登録について domain 間移動と domain 内移動に分けて説明する。

3.2 domain 間移動

domain 間移動の位置登録の様子を図 3 に示す。表 1 には図 3 内のメッセージ番号に対応するメッセージの内容をまとめた。表 2 はメッセージ番号とそれに対応するメッセージタイプを示している。表 1 中の ESP() というのは括弧内の内容を IPsec の ESP で暗号化したものであることを示している。また、H() は括弧内の内容を使用して計算したハッシュ値であることを示している。●はそのメッセージ全体を表している。Ck_ma は cookie を表し、Ck_i は cookie index を表している。

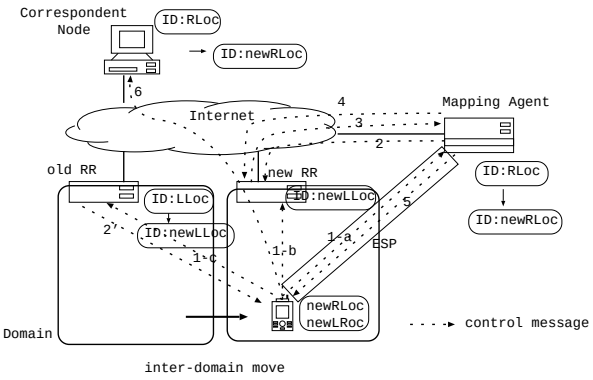

図 3: domain 間移動

表 1: 位置登録時のメッセージ

番号	内容
1-a	ESP(newRLoc, newLLoc, Ck_i, Ck_ma)
1-b	newLLoc, Ck_ma, H(Ck_i, ●)
1-c	newLLoc, H(Ck_i, ●)
2	Ck_i, H(Ck_ma, Ck_i, ●)
2'	位置登録に対する ACK
3	random number
4	random number(3 の数字と同じもの)
5	位置登録に対する ACK
6	mapping update

表 2: メッセージ番号とメッセージタイプの対応

番号	メッセージタイプ
1-a	MA Mapping Registration
1-b	RRnew Mapping Registration
1-c	RRold Mapping Registration
2	Cookie Index Notification
2'	RR Mapping Registration ACK
3	MA Confirmation
4	MA Confirmation ACK
5	Mapping Registration ACK

図 3 の (1-a)、(1-b)、(2) のメッセージは図 2 の (1-a)、(1-b)、(2) のメッセージに対応しており、基本モデルが domain 間移動の際の位置登録に適用されていることがわかる。図 3(1-a) には RLoc が含まれ

ており、図 3(1-a) を受信した MA は MN の RLoc を Mapping Table に登録する。RR が (1-a) のメッセージを受理し、MN の LLoc を Mapping Table に登録し終わると、図 3(3) を MA へ送信し、LLoc の登録完了を通知する。このメッセージを MA が受信すると MN に対して位置登録要求に対する ACK を通知 (図 3(5)) し、domain 間移動時の処理が完了する。

3.3 domain 内移動

domain 内移動では図 3 の (1-c) と (2') のやりとりのみを行う。domain 内移動の時点では、MN がもつ cookie と cookie index の対を RR は保持しているため, 改めて cookie や cookie index の通知をする必要が無い。

4 実装

本稿では提案方式を NetBSD 1.6K 上に実装した。実装はすべてユーザ空間で行った。また、ハッシュ値の計算には HMAC を使用した。図 4 に domain 間移動時の、図 5 に domain 内移動時の位置登録処理のメッセージフローを示す。実際には domain 間移動時には移動前に存在した domain の RR へも位置登録をするのだが、今回測定する処理時間には影響しないため図 4 では省略する。

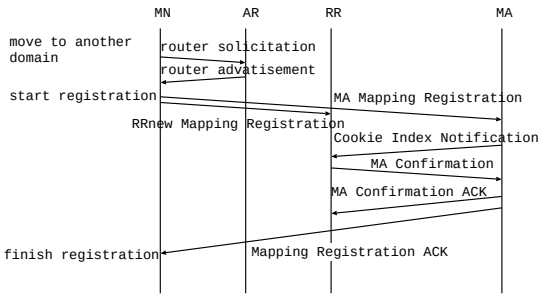

図 4: domain 間移動時のメッセージフロー

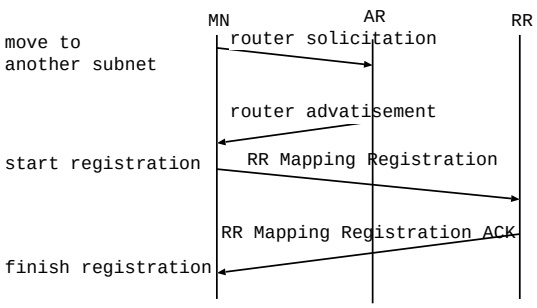

図 5: domain 内移動時のメッセージフロー

5 評価と考察

5.1 定性的な評価

本研究の提案手法では、攻撃者が MN になりすますためには cookie と cookie index の両方を同時に盗聴する必要がある。MN から RR への cookie と cookie index の通知が行われるのは domain 間移動時の登録処理なので、攻撃者が MN のなりすましをするためには、domain 間移動時の登録処理で盗聴をしなければならないと考えられる。

MA と MN の間の通信は IPsec によって暗号化されるので、domain 間移動時に攻撃者が cookie と cookie index を得るためには MA と RR の間 (図 6 の矢印 A) と RR と MN の間 (図 6 の矢印 B) で盗聴をしなければならない。矢印 B での盗聴を考えると、

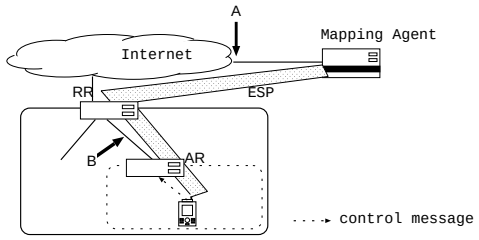

図 6: 攻撃者による盗聴の可能性

AR と MN 間は無線を想定しているため、cookie の盗聴は比較的容易にできてしまうことが考えられる。また、AR と RR 間の経路も静的であることが予想されるため、AR と RR 間の経路上で盗聴することも可能である。しかし、実用された場合、domain を管理する会社が存在するが考えられ、その domain 内のネットワークへ攻撃者が接続することは困難である。一方、矢印 A での盗聴は MA と RR 間の経路は動的であることが一般的なので、経路を予測して cookie index を盗聴することは難しいと思われる。よって、攻撃者は MA が接続しているネットワークか、RR が接続しているネットワークにオンリンクで接続しないと cookie index の盗聴は容易ではない。しかし、たとえ攻撃者が RR と同一ネットワークに接続していたとしてもスイッチが介している場合、盗聴は難しい。MN のなりすましを成功させるためには矢印 A、矢印 B での盗聴を同時にやらなければならないことを考えると、提案方式の頑強性は実用に問題のない強さを持っていると考えられる。

5.2 定量的な評価

実装した提案方式の処理時間を図 7 に示す実験ネットワークで測定した。表 3 に実験に使用したマシンのスペックを示す。

表 4 に提案方式 (aHLIN6) と既存の HLIN6(HLIN6

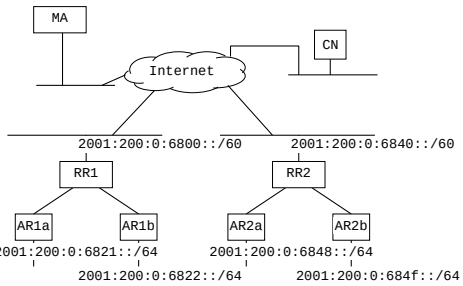

図 7: 実験ネットワーク

表 3: 実験ネットワークの各マシンのスペック

役割	CPU	メモリ
MA	Pentium Pro 551 MHz	256 MB
RR	Pentium Pro 864 MHz	512 MB
AR	Pentium Pro 532 MHz	512 MB
MN	Pentium III 500 MHz	192 MB

とする) の MN での処理時間の測定の結果を示す。Router Solicitation (rtsol) を送信後、位置登録処理完了の ACK メッセージを MA から受信するまでに MN でかかる時間を処理時間として測定した。また、

表 4: 実験ネットワークでの処理時間 ($msec$)

aHLIN6		HLIN6	
domain 間	domain 内	domain 間	domain 内
32.9	23.8	27.9	23.0

aHLIN6 において、MN でかかる処理時間が domain 間移動では式 1、domain 内移動では式 2、の関係を持つことを測定結果より導いた。定数値の単位は $msec$ である。また、$RTT_{A\leftrightarrow B}$ は A と B 間の RTT 値を示す。

$$T_{\text{間}} = 32.0 + (RTT_{MN\leftrightarrow MA} + RTT_{RR\leftrightarrow MA}) \quad (1)$$

$$T_{\text{内}} = 23.1 + RTT_{MA\leftrightarrow RR} \quad (2)$$

表 4 から、aHLIN6 の処理時間は HLIN6 に対し、domain 間移動では 17.9%、domain 内移動では 3.4% 増加していることがわかった。domain 間移動時の処理時間の差の原因は、認証のためにハッシュ値を計算する処理の部分や、位置登録処理全体でパケットの送受信の回数が増えたことによると考えられる。domain 内移動時の処理時間の差が小さくなった原因は、aHLIN6 と HLIN6 の処理の違いがハッシュ値の計算の部分だけで、パケットの送受信回数は等しいためであると考えられる。

本研究の測定で使用した実験ネットワークでは RR と MA が物理的に近く、$RTT_{RR\leftrightarrow MA}$ 値が小さかった (表 5)。しかし、実用の際には $RTT_{RR\leftrightarrow MA}$ 値は大きいことが考えられ、aHLIN6 と HLIN6 の処理時間の差は大きなくることが予想される。

表 5: 実験ネットワークでの RTT 値

	RTT 値 ($msec$)
MN と RR 間	0.25
MN と MA 間	1.03
RR と MA 間	0.20

6 まとめ

本稿では、マイクロモビリティサポートプロトコル HLIN6 において、RR と MN の間の認証機構について設計、実装した。提案手法では鍵交換を必要としない cookie 方式を採用するとともに、cookie と cookie index の 2 つの情報を異なる経路で RR へ通知することにより、頑強性を持たせた。また、実験ネットワークにおいて実装した提案手法の処理時間も測定し、HLIN6 の処理時間との比較を行った。今後の課題としては、より高速なハンドオーバを可能にするため L2 トリガを HLIN6 へ導入、実装することが挙げられる。また、HLIN6 上で VoIP 等のアプリケーションを動作させ、HLIN6 の処理がアプリケーションに与える影響についても評価する必要がある。

参考文献

[1] Rajeev Koodli. Fast Handovers for Mobile IPv6. Internet Draft, *IETF*, Sep 2002. work in progress.

[2] M. Kunishi, M. Ishiyama, K. Uehara, H. Esaki, and F. Teraoka. LIN6: A New Approach to Mobility Support in IPv6. In *The Third International Symposium on Wireless Personal Multimedia Communications*, Nov. 2000.

[3] Hesham Soliman, Karim El-Malki, and Ludovic Bellier. Hierarchical Mobile IPv6 mobility management (HMIPv6). Internet Draft, *IETF*, Oct 2002. work in progress.

[4] 國司光宣, 石山政浩, 寺岡文男. 移動体プロトコル LIN6 の簡易認証機構. DICOMO, 2002.

[5] 原田友紀子, 國司光宣, 寺岡文男. LIN6 のマイクロモビリティサポート. 情報処理学会論文誌, Vol. 43, No. 12, pp. 3878–3888, December 2002.