社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－DPS－126（10）
2006－CSEC－32（10）
2006／3／16

Stealth-LIN6：匿名性のあるIPv6モビリティ通信

市川隆浩[†]　坂野あゆみ[††]　寺岡文男[†,††]

本論文では，IPv6 通信において匿名性を実現するモビリティプロトコル Stealth-LIN6 (SLIN6) を提案する．Stealth-LIN6 はモビリティプロトコル LIN6 をベースとしており，通信毎に IP レイヤにおいて動的に生成されたアドレスを用いることによってノードの匿名性を実現する．また，SLIN6 は特有のプロキシを用いることによってノードの位置秘匿性を実現する．SLIN6 を FreeBSD に実装した．測定の結果，データ通信における SLIN6 のオーバヘッドは無視できる程度であることが分かった．

Stealth-Lin6 : Anonymizing IPv6 mobility communication

Takahiro Ichikawa,[†] Ayumi Banno[††] and Fumio Teraoka[†,††]

This paper proposes a protocol called Stealth-LIN6 (SLIN6) which provides mobility and anonymity in IPv6. SLIN6 is based on LIN6, a mobility protocol in IPv6. It achieves anonymity of node's identity in the IP layer by dynamically generating addresses at each transmission and also achieves anonymity of node's location by introducing proxies specific to SLIN6. SLIN6 was implemented on FreeBSD. The measured results show that SLIN6 has negligible overhead in communication.

1. はじめに

インターネット環境の普及により，あらゆる機器があらゆる場所で通信が行えるようになった．また，携帯通信機器の普及により，移動先からもインターネットへの接続が活発に行われるようになった．そこで移動中も通信が途切れない移動透過性が保証されている通信が必要と考えられ，ノードの移動透過性を実現するモビリティプロトコルである Mobile IPv6[1] や LIN6[2] が提案された．しかし，既存のモビリティプロトコルのパケットヘッダには，通信を行っているノードが接続するサブネットを示す位置指示子と，ノードを一意に識別可能にするノード識別子が格納される．そのため，一般に移動を前提としたモビリティプロトコルを用いた通信には

- 受信者による送信者の情報の悪用
- 盗聴者による通信者の特定
- 盗聴者によるノード移動履歴の追跡

といった脅威が存在する．これらの脅威に対抗するためには，通信するノードの位置秘匿性や匿名性の実現が必要になる．一つ目の脅威に対しては，受信者に送信者のノード識別子を知られないこと必要である．二つ目の脅威に対しては，通信の盗聴者に通信者の位置指示子やノード識別子を知られないことが必要である．三つ目の脅威に対しては，盗聴者にノードが移動したことを知られないことが必要である．しかし，Mixes[3]，Crowds[4]，Aerie[5] といった既存の匿名通信技術をモビリティプロトコルに適用させることはルーティング，帯域，遅延，オーバヘッドを考慮すると望ましくない．本論文ではモビリティプロトコル LIN6 をベースとした位置秘匿性と匿名性のあるモビリティプロコル *Stealth-LIN6 (SLIN6)* を提案する．

SLIN6 のパケット配送機構は既存の IPv6 のインフラストラクチャを使用し，匿名性のある通信と既存の通信を明示的に使い分ける機能を備える．SLIN6 では，トランスポートレイヤ以上では SLIN6 汎用識別子と呼ばれる仮想的な IPv6 アドレスによってノード間にコネクションを生成し，ネットワークレイヤでは SLIN6 アドレスと呼ばれる動的に生成される IPv6 インターフェースアドレスがパケット配送に利用される．この SLIN6 汎用識別子と SLIN6 アドレスとの関係を通信毎に動的に変更することでノードの匿名性を実現

† 慶應義塾大学 理工学部 情報工学科
Department of Information and Computer Science, Faculty of Science and Technology, Keio University
†† 慶應義塾大学 大学院 理工学研究科
Graduate School of Science and Technology, Keio University

する．また，SLIN6 では SLIN6 プロキシと呼ばれる中間ホストを導入し，SLIN6 プロキシがパケットを中継することでノードの位置秘匿性を実現する．さらにノード，プロキシ間の情報交換の機構により，SLIN6 における制御メッセージの保護を実現する．SLIN6 はネットワークレイヤに実装され，上位，下位レイヤに対する変更はない．

2. モビリティプロトコル LIN6 の概要

LIN6 は，移動透過性を保証するネットワークアーキテクチャである LINA[6] を IPv6 環境へ適用したモビリティプロトコルである．LIN6 は位置指示子とノード識別子を分離するという概念を導入しており，ノード識別子は接続しているサブネットにかかわらず一意に定められる．ネットワークレイヤよりも上位のレイヤにおいては位置に依存しないノード識別子を用いてコネクションを確立し，ネットワークレイヤでは位置指示子を用いて経路制御を行うことによって移動透過性を実現する．現在，IPv6 の通信で主に使用されている Aggregatable Global Unicast Address (AGUA)[7] は，上位 64bits がネットワークプレフィックス，下位 64bits がインタフェース ID を示す．LIN6 のアドレスモデルは，この AGUA 構造全体の 128bits を位置指示子とし，位置指示子の下位 64bits にノード識別子を埋め込む．LIN6 では，ネットワークレイヤより上位レイヤにおいて LIN6 汎用識別子を用い，ネットワークレイヤにおいて LIN6 アドレスを用いる．LIN6 汎用識別子の上位 64bits は LIN6 Prefix と呼ばれる位置に依存しない固定値であり，下位 64bits は LIN6ID と呼ばれるノード識別子である．LIN6 アドレスの上位 64bits は現在接続しているサブネットのネットワークプレフィックスであり，下位 64bits は LIN6ID である．

LIN6 において，LIN6ID と現在のネットワークプレフィックスとの対応づけをマッピングと呼び，このマッピングを管理する機構として *Mapping Agent (MA)* を用いる．LIN6 では，通信を開始する際に MA を用いて通信相手に対するマッピングを取得する．LIN6 ノードはこのマッピングをレイヤ間のアドレス変換に利用して通信を行う．

3. SLIN6 の設計

3.1 SLIN6 の概要

SLIN6 はモビリティプロトコル LIN6 をベースとしており，LIN6 の移動透過性を維持しながらノードの位置秘匿性や匿名性を実現している．

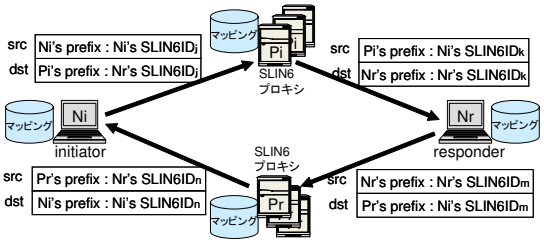

図 1 SLIN6 の動作概要

SLIN6 では，あるノード間で通信を開始する場合，通信要求を行うノードを initiator と呼び，通信要求を受けるノードを responder と呼び，ノードに役割の違いを設けている．initiator にとって responder の LIN6ID は通信したい相手の識別子を示し，responder にとって initiator の LIN6ID はパケットを返す相手を示す．すなわち，responder は initiator がどのノードであるか分からなくてもよい．SLIN6 では，通信毎に initiator と responder 間で動的に LIN6ID を生成し，一時的にパケット配送に利用する．このノードと関連性のない LIN6ID を *SLIN6ID* と呼ぶ．この SLIN6ID は initiator と responder 間のみで解決できればよいので，initiator，responder ともに SLIN6ID を管理する MA を必要としない．また，IPv6 において 1 つのインタフェースは複数の IPv6 アドレスを持つことが可能であることを利用し，各ノードは複数の SLIN6ID を持つことができる．通信中はこの複数の SLIN6ID を始点アドレスとしてランダムに選択して使用する．

位置指示子の隠蔽は，SLIN6 プロキシと呼ばれる中間ホストの導入によって実現する．SLIN6 において，SLIN6 プロキシがノード間のすべてのメッセージを中継し，通信開始時に生成したマッピングを基にパケットのアドレスを書き換え転送する．ノードは使用できる SLIN6 プロキシを複数持つが，すべての SLIN6 プロキシに対して信頼関係があるとする．ノードは通信時に SLIN6 プロキシをランダムに選択することができる．

SLIN6 の動作概要を図 1 に示す．以下，initiator を N_i，responder を N_r，initiator が使用する SLIN6 プロキシを P_i，responder が使用する SLIN6 プロキシを P_r とする． SLIN6 の通信において，パケットヘッダのアドレス部分は図 1 のような 4 種類となる．ここで，盗聴者はインターネット上の一箇所でしか同時に盗聴できないことを前提とする．図 1 のように，SLIN6 プロキシはマッピングを基にアドレスの SLIN6ID 部分を $SLIN6ID_j$ から $SLIN6ID_k$ に，$SLIN6ID_m$ から $SLIN6ID_n$ に変えて転送できる．したがって，

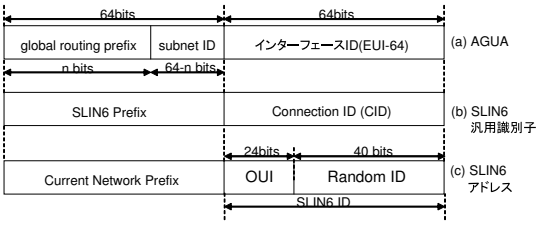

図 2 SLIN6 のアドレスモデル

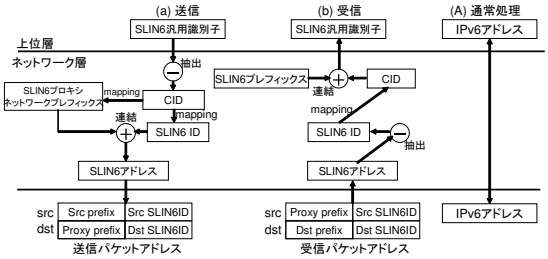

図 3 SLIN6 ノードにおける送受信処理

このどの部分を盗聴されても，直接通信を行っているノード間の関連性がアドレスから特定できない．このように，SLIN6 では SLIN6ID の使用によりノードの匿名性を実現し，SLIN6 プロキシによるアドレス書き換えによりノードの位置秘匿性を実現する．

3.2 SLIN6 のアドレスモデル

SLIN6 のアドレスモデルを図 2 に示す．SLIN6 では，ネットワークレイヤより上位のレイヤにおいて，LIN6ID と同じ働きを持つものとして 64bits の *Connection ID (CID)* を用いてホストを識別する．SLIN6 汎用識別子は上位 64bits が SLIN6 prefix とよばれる固定値であり，下位 64bits は CID である．ネットワークレイヤでは，現在のネットワークプレフィックスと SLIN6ID によって SLIN6 アドレスが生成され，これを使用する．これによって移動透過性を実現する．SLIN6ID の上位 24bits は SLIN6 に割り当てられた OUI (Organizationally Unique Identifier) であり，SLIN6 アドレスか否かはここを見れば判断できる．

3.3 SLIN6 の動作

3.3.1 SLIN6 ノード

SLIN6 ノードにおける送信時の処理を図 3(a) に示す．N_i の CID を CID_N_i，N_r の CID を CID_N_r と表す．対象となる SLIN6 汎用識別子の下位 64bit から CID_N_r を得る．次に，CID_N_r を鍵としてマッピングテーブルを検索する．その結果，その通信で使われているマッピングエントリを発見することが可能であり，N_i と N_r の SLIN6ID とネットワークプレフィックスと使用プロキシのアドレスが求められる．もしマッピングにある SLIN6ID，または使用プロキシが複数ある場合はその中からランダムに選ぶ．この N_i の SLIN6 アドレスを始点アドレス，使用プロキシのネットワークプレフィックスと N_r の SLIN6ID を連結させた SLIN6 アドレスを終点アドレスとしてパケットを配送する．

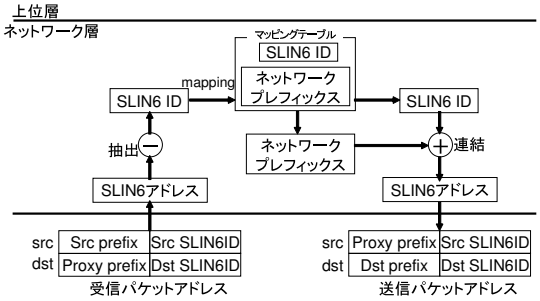

図 4 SLIN6 プロキシにおける送受信処理

SLIN6 ノードにおける受信時の処理を図 3(b) に示す．対象となる LIN6 アドレスから LIN6ID 部分を抽出し，OUI により SLIN6ID または既存の LIN6ID かを判断する．SLIN6ID であった場合，この SLIN6ID を鍵にマッピングテーブルを検索し，対応した SLIN6 汎用識別子を得る．また，既存の LIN6ID であった場合，既存の LIN6 の処理を行う．

SLIN6 ノードにおける通常の IPv6 アドレスの送受信処理を図 3(A) に示す．パケット送信時にトランスポートレイヤで指定された IPv6 アドレスが SLIN6 汎用識別子または LIN6 汎用識別子でない場合，通常の IPv6 アドレスとして処理される．また，パケット受信時にネットワークレイヤでの IPv6 アドレスが SLIN6 アドレスまたは LIN6 アドレスでない場合，通常の IPv6 アドレスとして処理される．

3.3.2 SLIN6 プロキシ

SLIN6 プロキシにおける転送時の処理を図 4 に示す．SLIN6 プロキシは受信パケットの終点アドレスから LIN6ID 部分を抽出し，OUI により SLIN6ID か否かを判断する．SLIN6ID であった場合，この SLIN6ID を鍵にマッピングテーブルを検索し，対応したネットワークプレフィックスと SLIN6ID を得る．もし SLIN6ID が複数あった場合，その中からランダムに選択する．そしてパケットの始点アドレス，終点アドレスを図 4 のように書き換えて送信する．

3.4 SLIN6 の通信開始手順

SLIN6 の通信開始手順を図 5 に示す．これによって，通信に必要なマッピングが各ノード，プロキシに登録される．N_r のマッピングを管理する MA を MA_{N_r}，N_i の SLIN6 プロキシを P_i，N_r の SLIN6 プロキシを P_r とする． SLIN6 は図 5 の (0) から (7) の手順

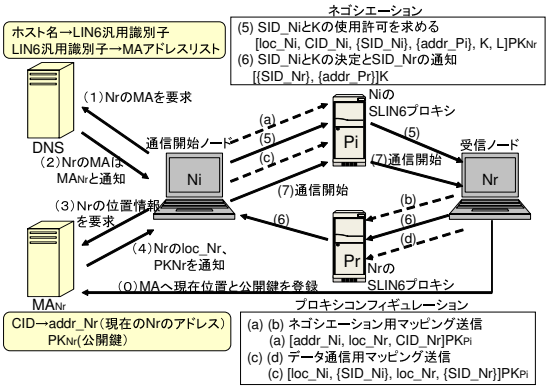

図 5 SLIN6 の通信開始手順

によって匿名通信を開始する．

N_r は responder 機能を持つので，N_r のマッピングを管理する MA_{N_r} へ CID_N_r，現在の IPv6 アドレス $addr\_N_r$，N_r の現在の公開鍵 PK_{N_r} を登録する (図 5(0))．一定時間が経過した時または N_r が他のサブネットに移動しネットワークプレフィクスが変更された時に，N_r はこの現在位置の登録を再び行う．

N_i が N_r と SLIN6 を利用した通信を行う場合，N_i はまず DNS へ N_r のマッピングを管理する MA_{N_r} の IPv6 アドレスを問い合わせる (図 5(1))．DNS は CID_N_r と対応する MA_{N_r} の IPv6 アドレスを通知する (図 5(2))．

次に，N_i は MA_{N_r} へ N_r の位置情報を要求する (図 5(3))．MA_{N_r} は N_i に N_r の現在の IPv6 アドレス $addr\_N_r$ と公開鍵 PK_{N_r} を通知する (図 5(4))．このように，N_i は $addr\_N_r$ と PK_{N_r} を取得することができる．

次に N_i は MA_{N_r} から取得した情報を基に $addr\_N_r$ と CID_N_r を利用し，SLIN6ID を決定する処理に入る．N_i は loc_N_i を現在のネットワークプレフィックスとし，N_i の SLIN6ID である SID_N_i を複数ランダムに生成する．また，CID である CID_N_i と，N_i と N_r 間で使う共通鍵 K をランダムに生成し，共通鍵 K のライフタイムを L とする．そして，使用するプロキシ P_i を決定し，プロキシの IPv6 アドレスを $addr\_P_i$ とする．これらのパラメータは N_i 上のマッピングテーブルで保持される．その後，N_i は $[loc\_N_i, \{SID\_N_i\}, CID\_N_i, \{addr\_P_i\}, K, L]PK_{N_r}$ を含むメッセージを N_r にプロキシ P_i を中継させて N_r へ送信する (図 5(5))．ここで $[loc_{N_i}, \{SID\_N_i\}, CID\_N_i, \{addr\_P_i\}, K, L]PK_{N_r}$ とは，loc_{N_i}，$\{SID\_N_i\}$，CID_N_i，$\{addr\_P_i\}$，K，L を PK_{N_r} を用いて暗号化することを意味しており，$\{SID\_N_i\}$ とは，SID_N_i が複数あることを意味している．N_r は N_i からのメッセージを受信すると，秘密鍵 SK_{N_r} でメッセージを復号化し，$\{SID\_N_i\}$ が N_r 上で一意であるかを確認した後，N_r の SLIN6ID である SID_N_r を複数ランダムに生成する．そして，使用するプロキシ P_r を決定し，プロキシの IPv6 アドレスを $addr\_P_r$ とする．これらのパラメータは N_r 上のマッピングテーブルに保持される．次に，N_r は N_i へ $[\{SID\_N_r\}, \{addr\_P_r\}]K$ を含むメッセージをプロキシ P_r を中継させて N_i へ送信する (図 5(6))．メッセージ受信した N_i は $[\{SID\_N_r\}, \{addr\_P_r\}]K$ を共通鍵 K で復号化し，N_i 内のマッピングテーブルを検索する．N_i は，検索により発見されたエントリに $\{SID\_N_r\}$，$\{addr\_P_r\}$ を追加する．SLIN6 では，この一連の処理をネゴシエーションと呼ぶ．ネゴシエーションを行うことによって，通信を行う両ノードがマッピングを持つことができ，SLIN6 アドレスを用いた匿名通信を開始することができる (図 5(7))．

SLIN6 では，パケットを送信する前に必ず SLIN6 プロキシにアドレス書き換え設定を行うためのマッピングを登録する．これをプロキシコンフィギュレーションと呼ぶ．プロキシコンフィギュレーションには二種類あり，一つはネゴシエーションメッセージを送る前のコンフィギュレーション，もう一つは SLIN6 アドレスを用いた通信を行う前のコンフィギュレーションである．N_i は N_r にネゴシエーションメッセージ (図 5(5)) を送信する前に，$addr\_N_i$，loc_N_r，CID_N_r，を含むメッセージ $[addr\_N_i, loc\_N_r, CID\_N_r]PK_{P_i}$ を P_i へ送信する (図 5(a))．ここでの PK_{P_i} とは，P_i の公開鍵のことである．一方，N_r は N_r にネゴシエーションメッセージ (図 5(6)) を送信する前に，$addr\_N_r$，loc_N_i，CID_N_i を含むメッセージ $[addr\_N_r, loc\_N_i, CID\_N_i]PK_{P_r}$ を P_r へ送信する (図 5(b))．これらのプロキシコンフィギュレーションによって，プロキシはネゴシエーションメッセージを転送するためのマッピングを持つことができる．

ネゴシエーションが終わると，N_i は N_r に loc_N_i，$\{SID\_N_i\}$，loc_N_r，$\{SID\_N_r\}$ を含むメッセージ $[loc\_N_i, \{SID\_N_i\}, loc\_N_r, \{SID\_N_r\}]PK_{P_i}$ を P_i へ送信する (図 5(c))．一方，N_r は N_i に loc_N_r，$\{SID\_N_r\}$，loc_N_i，$\{SID\_N_i\}$ を含むメッセージ $[loc\_N_r, \{SID\_N_r\}, loc\_N_i, \{SID\_N_i\}]PK_{P_r}$ を P_r へ送信する (図 5(d))．これらのプロキシコンフィギュレーションによって，プロキシは SLIN6 アドレスを用いたデータパケットを転送するためのマッピングを持つことができる．

3.5 SLIN6 の移動処理

N_i が他のサブネットに移動し，ネットワークプレフィクスが変更された場合，まず P_i を新しいマッピングでプロキシコンフィギュレーションする．そして，N_i は N_r にプロキシ P_i を中継させてマッピングアップデートメッセージを送信する．N_i の新しいネットワークプレフィクスを $loc2\_N_i$ とすると，このマッピングアップデートメッセージは，$\{loc2\_N_i, \{SID\_N_i\}, CID\_N_i, K, L\}K$ となる．このマッピングアップデートメッセージは，移動前に使用していた SLIN6 アドレスを用いて送信する．

N_r は受信したマッピングアップデートメッセージからマッピングテーブルを検索し，取得した共通鍵 K を利用してマッピングアップデートメッセージを復号化した後，マッピングアップデートメッセージ内の共通鍵 K との整合性を確かめる．共通鍵 K が一致したならば，N_r はマッピング登録メッセージを送信した相手が正しい N_i であることを認証できる．この認証後，N_r は自身のマッピングテーブルを更新し，P_r に対して新しいマッピングでプロキシコンフィギュレーションを行った後，N_i に確認応答する．

N_i と N_r が同時に移動した場合，N_i が再び MA_{N_r} へ N_r の現在のネットワークプレフィクスを問い合わせ，再びネゴシエーションを行う．

3.6 SLIN6ID の衝突

通信開始時，または移動時に同一リンク内で同じ SLIN6ID が存在する可能性がある．その際は，Duplicated Address Ditection (DAD) により SLIN6ID の重複を発見する．重複が発見されると，ノードは新たに SLIN6ID を生成し，通信相手ノードにマッピングを送信する．

4. Stealth-LIN6 の実装と評価

SLIN6 は LIN6 の実装を参考に，カーネル空間とユーザ空間に必要な機能を追加した形で実現した．実装したオペレーティングシステムは FreeBSD 5.4-release である．SLIN6 ノードのカーネルはパケットのアドレスの SLIN6 汎用識別子と SLIN6 アドレスの変換処理を行う．SLIN6 プロキシのカーネルはパケットの IP ヘッダ内の SLIN6 アドレスの書き換え，転送処理を行う．また，通信状態の情報をカーネル空間にキャッシュするために，カーネル空間にマッピングテーブルを生成した．また，ユーザ空間には SLIN6 における制御メッセージの送受信やカーネルと情報交換を行うデーモンを実装した．

SLIN6 が実ネットワークにおいて動作することを確認した．そして，従来の IPv6 パケット処理と比べたネットワークレイヤにおける SLIN6 のパケット処理時間のオーバヘッドを測定した．その結果，SLIN6 ノードにおいて送信処理で +12.47%，受信処理で +44.69% となったが，いずれも μsec オーダであり，実ネットワークでの Round Trip Time (RTT) が $msec$ オーダであることを考慮するとこのオーバヘッドは無視できる．また，SLIN6 プロキシにおいて受信からアドレスを書き換えて送信までの処理は時間は $134\mu sec$ であり，μsec オーダであることからこのオーバヘッドも無視できる．

5. 考　　察

5.1 位置秘匿性と匿名性の考察

5.1.1 initiator の responder に対する匿名性

SLIN6 において，responder はパケットに含まれる情報とネゴシエーションにより得られる情報から，initiator に関する情報として loc_A，SID_A，CID_A，$addr\_P_i$ を取得できる．このうち，loc_A は initiator が現在アクセスしているサブネットの位置を示す値である．SID_A と CID_A はネゴシエーション開始時にランダムに生成された値であるため，initiator のノード情報ではない．これらの情報から initiator がネットワーク上のどの場所からアクセスしていて，どの SLIN6 プロキシを使用しているかは判断できるが，どのノードであるか断定することはできない．したがって，initiator は responder に対して匿名性があると言える．

5.1.2 盗聴者に対する送信者と受信者の位置秘匿性と匿名性

SLIN6 において，盗聴の可能性があるパケットのヘッダ情報として，図 1 に示したように 4 種類が考えられる．以降の議論では，盗聴者は同時には 1ヶ所でしか盗聴できないことを前提とする．

SLIN6ID は動的に生成，変更することにより，ノードとの関連性を発見することが困難になる．また，複数の SLIN6ID を用い，さらに SLIN6 プロキシによって SLIN6ID が書き換えられるので相関を得ることも困難になる．また図 1 のどのパケットヘッダの情報を見ても，SLIN6 がパケットを中継しているため始点または終点アドレスのどちらか片方のプレフィックスは必ず SLIN6 プロキシのものとなる．よって，どのサブネット同士が通信を行っているかを判別することは困難となる．したがって，initiator と responder は盗聴者に対して位置秘匿性と匿名性があると言える．

5.1.3 盗聴者の追跡に対する耐性

SLIN6 はマッピングを含む制御メッセージを暗号化しており，SLIN6ID を動的に変更してよいことから SLIN6ID を追跡される可能性は極めて低い．また SLIN6 プロキシにより，SLIN6ID が書き換えられるので SLIN6ID の相関を得ることも困難となる．さらに移動時に使用する SLIN6ID を変更すれば，移動前と移動後の SLIN6ID による追跡は不可能になる．したがって，initiator と responder は盗聴者の追跡に対して耐性があると言える．

5.2 通信開始時のオーバヘッド

SLIN6 の通信開始時にはネゴシエーション，プロキシコンフィギュレーションといった処理のオーバヘッドが発生する．この通信開始時の処理において，動的に生成した SLIN6 アドレスをインターフェースに付与する際は，DAD 処理によって大きな遅延が発生する．しかし，この遅延は通信開始時のみで通信中は発生しないので，位置秘匿性，匿名性を得ることを考えると許容できると考える．

5.3 送受信時のオーバヘッド

SLIN6 のアドレス書き換え処理によるオーバヘッドは処理時間が非常に小さいため無視できることが分かった．よって，SLIN6 の通信におけるパケット送受信時の遅延は，SLIN6 プロキシがパケットを中継することによってパケットが冗長経路を通ることによる遅延である．しかし，各パケットは 1 つの SLIN6 プロキシのみに中継されればよく，位置秘匿性を得ることを考えるとこのオーバヘッドは最小限である．

5.4 SLIN6ID の衝突検知処理

通信開始時または移動時に，使用する SLIN6ID が同一リンク上で衝突しないか DAD により確かめる必要がある．これはインタフェースに付与するすべての SLIN6 アドレスにおいて行われるので，より多くの SLIN6ID を用いる場合はその SLIN6ID の数だけ DAD を行う必要があり，処理時間のオーバヘッドが増大する．また衝突が検知された場合は，SLIN6ID の再決定をし新しいマッピングを送信しなければならない．しかし，SLIN6ID は 40bits 空間であり既存の IPv4 の 2^8 倍のアドレス空間を保持できるので，SLIN6ID の衝突確率はほぼ無視できる．

5.5 今後の課題

SLIN6 通信において，responder になるすべてのノードは匿名でのアクセスを許可している．実運用を想定した場合，どのようなノードに対して匿名でのアクセスを許可するかポリシを決める必要がある．また，SLIN6 プロキシの使用方法や運用方法の考察と，様々なアプリケーションやトランスポートレイヤに対する適正度を評価する必要がある．

6. 結　　論

SLIN6 は移動透過性を保証するモビリティプロトコル LIN6 に必要な機能を加え，移動透過性を失うことなく以下の 3 つの匿名性や位置秘匿性を実現できた．

- initiator の responder に対する匿名性
- 盗聴者に対する両端ホストの匿名性，位置秘匿性
- 盗聴者による追跡を防ぐ移動ノードの匿名性，位置秘匿性

SLIN6 では，通信開始時にネゴシエーション，プロキシコンフィギュレーションを行うことによって位置秘匿性，匿名性を有する通信を行うことができる．initator は自分が管理される MA を持たなくてもよく，SLIN6 の通信ができるまでのオーバヘッドは大きいが通信中のオーバヘッドは無視できる．SLIN6 の実運用を考えると，SLIN6 プロキシ運用方の決定や匿名通信ポリシの決定などの課題が挙げられる．

参 考 文 献

1) D. Johnson, C. Perkins and J. Arkko. Mobility Support in IPv6. RFC3775, Jun. 2004.
2) Mitsunobu Kunishi, Masahiro Ishiyama, Keisuke Uehara, Hiroshi Esaki and Fumio Teraoka. LIN6 : A New Approach to Mobility Support in IPv6. In *Proceedings of the Third Inernational Sympsium on Wireless Personal Multimedia Communications*, pp. 1079–1084, Nov. 2000.
3) David Chaum. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communications of the ACM*, pp. 84–88, Feb. 1981.
4) Michael K. Reiter and Aviel D. Rubin. Crowds: Anonymity for Web Transaction. *ACM Transactions on Information and System Security*, pp. 1(1):66–92, Nov. 1998.
5) 阿部洋丈, 加藤和彦. Aerie: WWW のための完全分散型匿名プロキシ. 情報処理学会論文誌, Vol. 46, No. SIG3, pp. 51–61, Jan. 2005.
6) Masahiro Ishiyama, Mitsunobu Kunishi, Keisuke Uehara, Hiroshi Esaki, Fumio Teraoka. LINA: A new approach to mobility support in wide area networks. *IEICE Transactions on Communication*, Vol. E84-B, No. 8, pp. 2076–2086, Aug. 2001.
7) R. Hinden, S. Deering and E. Nordmark. IPv6 Global Unicast Address Format. RFC3587, Aug. 2003.