複数のホームエージェントによるMobileIPのプライバシー拡張

河島 佑樹† 蓑原 隆‡
拓殖大学大学院工学研究科† 拓殖大学工学部‡

1. はじめに

近年,移動体端末の普及と移動体端末を取り巻く通信環境の発展に伴い,移動体通信の環境と移動先からの安全な通信が重要になってきている.移動体通信の環境ではMobileIPv4/v6がIETFで標準化されており,同じくIETFにて標準化されているIPSecを用いることでIP層での認証と暗号化が可能となる.これらを組み合わせることにより,移動体端末への移動透過的かつ安全な通信を可能としている.

一方プライバシーの観点からするとアドレス情報を用いて,複数の通信を関連付けることで新しい情報が引き出せるという問題が存在する.このような情報はノードの性質を特定することや行動の追跡を容易にしてしまう可能性があるため,アドレスは固定のアドレスを使い続けるのではなく,適宜変更しUnlinkability(非関連性)を持たせることが重要である.IPv6では通信を開始する発信ノードの送信元アドレスをランダムに変更することで,プライバシーを確保する技術が標準で実装されている.また,通信を受け入れる着信ノードに関してはノードを指定するインターフェースID部を適宜変更させながら通信を可能とするワンタイムアドレス[1]が提案されている.しかし,ネットワークを指定するネットワークプレフィックス部をランダムに変更させるとルーティングが困難になるため,着信側のプライバシー確保が制限されるという問題がある.

MobileIP通信では,移動ノードは接続ネットワークが変化する度に新たなIPアドレス(移動先アドレス)を取得し,自身が所属するネットワークに設置した管理サーバ(ホームエージェント)に通知(位置登録)する.ホームエージェントは移動ノードの所属するネットワークでのアドレス(ホームアドレス)と移動先アドレスの組み合わせを位置登録リストとして管理し,移動ノード宛の通信を受信すると移動先アドレスへ中継することで移動ノードの移動透過的な通信を実現している.このMobileIP通信において,位置登付けされると移動ノードの追跡等に繋がると考えられる.そこで本研究はMobileIP通信において現在位置通知の宛先アドレスのネットワークプレフィックス部が固定による通信の関連付けの防止を目的とする.

2. 提案手法

ホームエージェントの着信アドレスのネットワークプレフィックス部を変化させるためにホームエージェントを複数用意し異なるネットワークに設置する.移動ノードはランダムにホームエージェントを選択し位置登録を行うことにより安全な移動体通信を実現する.

移動ノードに対して通信を行おうとするノード(以下対応ノードと呼ぶ)は最新の移動先を知っているホームエージェントを知らないので,ランダムにホームエージェントを選んで送信を行う.対応ノードから通信を受けたホームエージェントは,移動ノードの最新の移動先を知るホームエージェントを検索し,最新の移動先アドレスを取得することが必要となる.そのため,位置登録リストの管理,中継処理を各ホームエージェントが協調して動作できるホームエージェント網を構築する.本手法の概要図を図1に示す.各ホームエージェントが持つ移動ノードの情報のうち新しい情報を判断するために,移動ノードは位置登録情報にカウンタを付与し,ホームエージェント間では,これを参照することで最新の情報を判別するものとする.

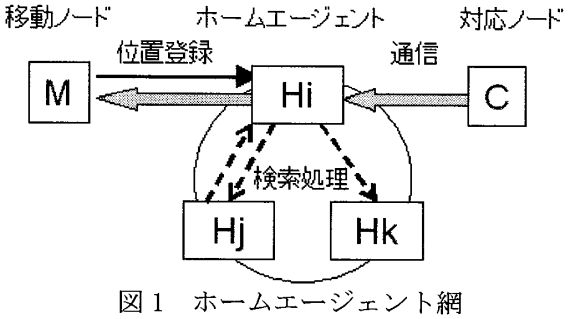

図1 ホームエージェント網

3つのホームエージェントを用いた検索,中継処理の通信例を図2に示す.ホームエージェント網を用いた通信の流れを以下に示す.

(1)移動ノード宛の対応ノードからの通信をホー

† Yuki Kawashima, Graduate School of Engineering, Takushoku University
‡ Takashi Minohara, Department of computer Science, Takushoku University

ムエージェントが代理受信する.
(2)代理受信したホームエージェントは自信の保持する移動先アドレスへ中継を行う.
(3)(2)の処理と同時に他のホームエージェントに移動先アドレスを要求する検索要求を送信する.検索要求には要求元のカウンタを付与する.
(4)検索要求を受信受信したホームエージェントは付与されているカウンタと自信のカウンタを比較し,自信のカウンタが新しい場合のみ検索応答を返信する.検索応答には移動先アドレスとカウンタが付与される.
(5)検索応答を受信したホームエージェントは付与されているカウンタと自信のカウンタを比較し,付与されたカウンタが新しい場合は自信のカウンタと移動先アドレスを検索応答の情報で更新する.更新された移動先アドレス宛に対応ノードからの通信を中継する.
(6) 中継を行った通信のうち,既にその移動先アドレスに移動ノードが存在しなかった場合は,宛先ネットワークに存在するルータによってエラーが返信される.
(7) 中継した通信の中で最新の移動先のみが移動ノードへと到達する.

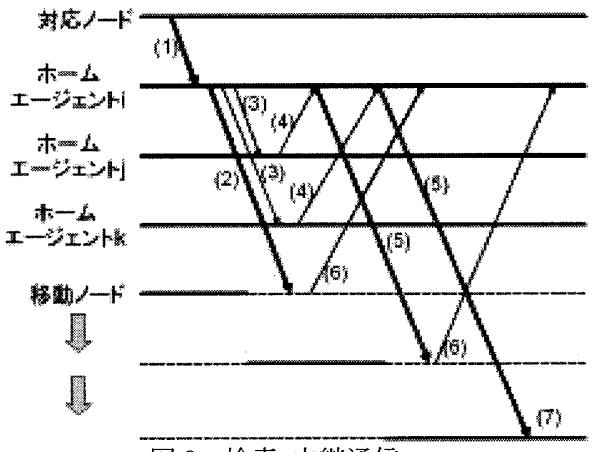

図2 検索-中継通信

3. 検索処理による遅延

対応ノードからの通信をホームエージェントが代理受信して移動ノードへ中継される時間について考察する.本提案手法で複数のホームエージェントを用いると,通常の MobileIP と比較して対応ノードからの通信を中継する際に行う検索処理時間分の遅延時間が生じるという問題が考えられる.

本提案手法で3つのホームエージェント i,j,k を用いて運用した場合について述べる.ここで対応ノードからの通信を受信したホームエージェントを i とすると,i が最新の移動先アドレスを知っていた場合,検索処理と同時に自身の保持する移動先アドレスへと通信を中継しているため遅延時間は発生しない.j または k が最新の移動先を知っている場合,検索要求,検索応答にかかる時間が遅延時間となる.また,遅延時間は i-j,i-k 間の距離(通信時間)によって異なる.

ここで,各ホームエージェント,移動ノード,対応ノードの距離は全て等しく 1 と仮定する.図 3 に提案手法,通常 MobileIP における対応ノードの通信が移動ノードへ届けられるまでの経路を示す.対応ノードから移動ノードまでの距離は通常 MobileIP では 4 となり,提案手法では 6 となっている.これより本仮定において、提案手法は通常 MobileIP の 1.5 倍の通信時間がかかることがわかる.対応ノードからの 2 回目以降の通信では,対応ノードから初回の通信を受信したホームエージェントは,検索処理により対象移動ノードの最新の移動先アドレスを取得している.そのため 2 回目以降の通信では直接の中継が成功するため遅延時間は発生しない.

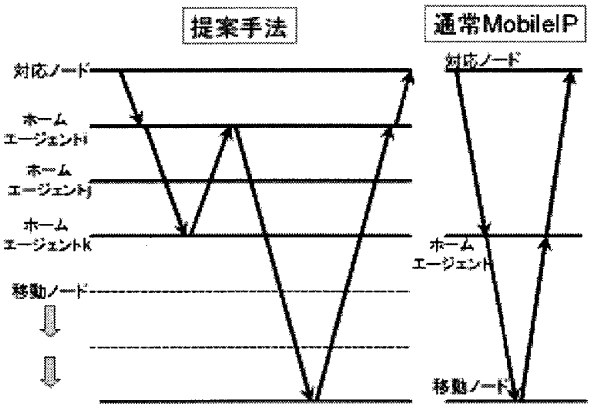

図3 通信経路の比較

4. まとめ

本稿では MobileIP 通信において現在位置を通知する際の宛先アドレスが固定により通信が関連付けられる問題を述べた.また,その解決手法として協調して動作するホームエージェント網を提案し,本提案手法の問題点とする検索処理による遅延について述べた.

参考文献

[1]Sakurai, A., Minohara, T., Sato, R. and Mizutani, K., ``One-Time Receiver Address in IPv6 for Protecting Unlinkability'' Proc. ASIAN 2007, pp. 240-246.