

DDNS サーバからの通知を用いた MIPv6 のハンドオーバー処理方式

友成 貴之[†] 木村 成伴[‡] 海老原 義彦[‡]筑波大学 情報学群情報メディア創成学類[†] 筑波大学 システム情報系情報工学域[‡]

1. はじめに

MIPv6 (Mobile IPv6) [1]では, MN が移動して別のネットワークへ移ると, そのネットワークで使用する CoA (Care of Address)を生成する. その後, MN は HoA (Home Address)と CoA の対応付けを示す BU (Binding Update)を HA (Home Agent)に登録する. そして, MN は通信相手 CN (Correspondent Node)との直接通信を行うために経路最適化を行う. このとき, MN-CN 間のセキュリティ確保のため RRP (Return Routability Procedure)を行う. RRP において, MN は2つのメッセージ HoTI (Home Test Init), CoTI (Care of Test Init)を, 前者は HA 経由で, 後者は CN へ直接送信する. これらを受け取った CN は HoTI に対しては HoT (Home Test), CoTI に対しては CoT (Care of Test)を先ほどと同じ経路で MN へ送信する. 以上で交換した情報を元に, MN と CN は認証情報を生成し, MN は安全に BU を CN へ送ることができる.

しかし, 以上の処理において, HoTI と HoT を交換する処理に HA が必要となるため, HA に障害が発生するとハンドオーバー処理ができなくなる. また, リアルタイム通信などを行っている場合, HA を経由したハンドオーバー処理遅延が通信品質に及ぼす可能性がある. そこで本論文では, DDNS (Dynamic DNS)サーバを用いたハンドオーバー処理方式を提案する.

2. 提案方式

提案方式におけるハンドオーバー処理手順を図1に示す. 提案方式において, MN のホームネットワーク上に DDNS サーバがあり, MN は, あらかじめ, この DDNS サーバに自分の公開鍵を登録しておくとして仮定する. また, CN は, MN と通信を開始する際, MN の HoA を, DNSSEC [2]を用いて, DDNS サーバに問い合わせるものとする. このとき, CN は DDNS サーバのアドレスと公開鍵を取得できる. これらの情報は,

DNS キャッシュサーバを介して問い合わせた場合でも, 取得可能である. 更に, CN の接続するネットワークにファイアウォールがある場合は, ホールパンチングにより, DDNS サーバからのデータを受け取れるようにしておく.

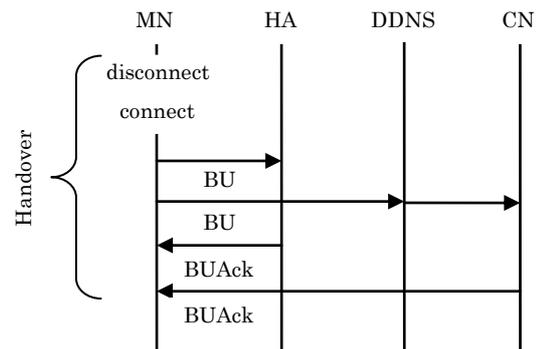


図1 提案方式のハンドオーバー処理手順

さて, MN が移動して別ネットワークに移ると, 従来の MIPv6 との互換性を保つために, HA に対して BU を送ると同時に, MN から CN 宛の BU に MN の秘密鍵で署名をした後, MN から DDNS サーバ宛のヘッダでカプセル化して, これを DDNS サーバに送信する. これを受け取った DDNS サーバはデカプセル化を行った後, MN の公開鍵により署名を検証する. 署名が正しいことが確認できたら, この BU に DDNS サーバの秘密鍵で署名する. そして, BU から CN のアドレスを取得した後, DDNS サーバから CN 宛のヘッダでカプセル化して, これを CN に送信する. CN はデカプセル化を行った後, DDNS サーバの公開鍵により署名を検証し, これが正しいければ, 新たな CoA を用いて MN と通信する.

3. シミュレーション実験

提案方式の有効性を確認するため, 従来の MIPv6 方式と提案方式のハンドオーバー遅延を測定した. ここで, ハンドオーバー遅延は MN が現在の AP (Access Point)との通信が途絶えてから, 移動先の AP へ接続し, HA からの BUAck (BU Acknowledgement), 及び CN からの BUAck を受け取るまでの時間とした.

実験で用いたネットワークトポロジを図2に示す. この図において, MN は IEEE802.11b を用

Handover Process for MIPv6 Using Notification from DDNS Servers

[†] Takayuki Tomonari, College of Media Arts, Science and Technology, School of Informatics, University of Tsukuba[‡] Shigetomo, Kimura and Yoshihiko Ebihara, Faculty of Engineering, Information and Systems, University of Tsukuba

いて通信し，その伝送速度は 11Mbps とする．また，有線経路の伝送速度は 100Mbps とした．AP のセル半径は 200m の同心円であり，隣接するセルの中心の間隔は 100m とした．そして，MN はホームネットワークから外部ネットワーク 1 を経由し，外部ネットワーク 2 まで，直線的に，1m/s で移動する．この間，CN は UDP で CBR (パケットサイズ 1024Byte, ビットレート 1.56Mbps) でデータを伝送する．なお，図の各リンクには伝搬遅延を示しており，通信相手との距離を考慮するために，CN-Router 間の伝搬遅延を変化させ，それぞれ 5 回計測を行ったときの，ハンドオーバー遅延の平均値と，信頼係数が 95% のときの信頼区間を求めた．

図 3 に，MN がホームネットワークから外部ネットワーク 1 へ移った際の値を示す．同図より，従来方式は CN-Router 間の伝搬遅延に比例してハンドオーバー遅延が増加しているが，提案方式はほぼ一定であり，従来方式よりも 245~725ms 平均ハンドオーバー遅延が減少した．これは，提案方式のハンドオーバー処理時に，MN が HA と (DDNS 経由で) CN に BU をほぼ同時に送るため，HA から BUAck が返ってくるまでの間に，CN からの BUAck が返ってきているからである．

図 4 に MN が外部ネットワーク 1 から外部ネットワーク 2 へ移った際の値を示す．図 3 と比較すると，従来方式は 1081ms，提案方式は 718~

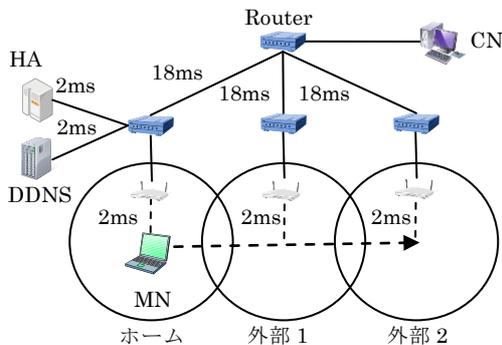


図 2 ネットワークトポロジ

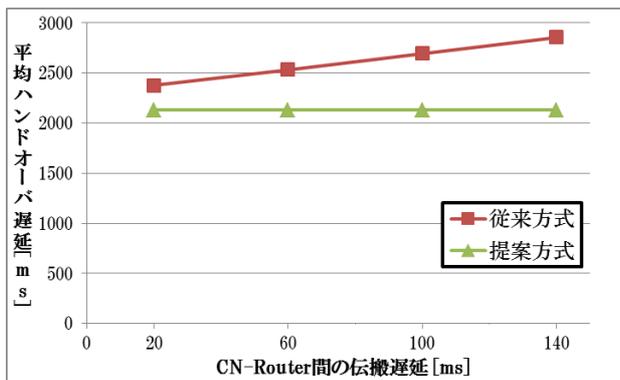


図 3 ホーム-外部 1 間の平均ハンドオーバー遅延

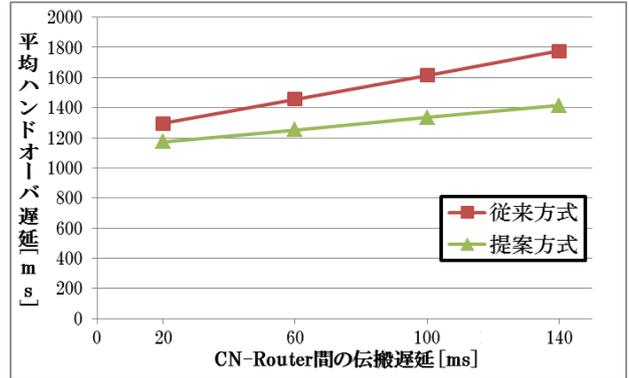


図 4 外部 1-外部 2 間の平均ハンドオーバー遅延

958ms 小さくなった．これは，MN が外部ネットワーク 2 に移動して，HA に BU を送ったとき，外部ネットワーク 1 に移動した際に送った BU のキャッシュが HA に残っており，ホームネットワークで HoA の重複アドレス検出が省略されたため，HA が BUAck を返すまでの遅延 (1000ms 程度) が削減されたためである．さらに，提案方式では，この処理と並行して行っていた CN から BUAck が返ってくるまでの遅延が隠蔽されなくなったため，削減幅が従来方式より小さくなった．また，図 4 における提案方式と従来方式の平均ハンドオーバー遅延の差は 122~362ms に減少した．これは，提案方式で上述の遅延が隠蔽されなかったことに加え，従来方式の RRP において，外部ネットワーク 1 に移動した際に送られた HoT のトークンが期限切れしておらず，HoTI と HoT の交換が行われなかったことによる．しかし，期限切れした場合は，この交換が行われるので，平均ハンドオーバー遅延の差は約 80ms 増加すると考えられる．

4. まとめ

本論文では，DDNS サーバからの通知によって MIPv6 におけるハンドオーバー処理を行う方式を提案した．シミュレーション実験により，提案方式は従来方式よりも平均ハンドオーバー遅延を削減することを示した．今後の課題として，提案方式によるハンドオーバー処理方式が通信中のパケット損失率などにどの程度影響を与えるのかを調べることなどが挙げられる．

参考文献

- [1] C. Perkins, Ed., D. Johnson, and J. Arkko, "Mobility Support in IPv6," RFC6275, 2011.
- [2] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Resource Records for the DNS Security Extensions," RFC4034, 2005.