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

2007－MBL－40 (8)
2007－UBI－13 (8)
2007／2／22

Mobile IP SHAKEにおけるセキュアなAlliance構築手法の検討

四條 雅博† 石原 進††

筆者らは，無線通信における移動端末の低速な通信を解決する手法として通信回線共有方式SHAKE (SHAring multipath procedure for a cluster networK Environment) を提案している．これは，近隣にある複数の移動端末を短距離高速リンクで一時的に接続し，各端末がもつ外部へのリンクを同時利用することで通信速度向上を実現する方式である．SHAKEでは任意の近隣移動端末とローカルで一時的にネットワーク（Alliance）を構築するため，悪意のある端末による通信傍受や，ローカルリンクにおける第三者による悪質行為といった危険が存在する．そのためSHAKEでは，近隣移動端末とAllianceを構築する際に接続相手の認証やローカルリンクの安全性を確認することが求められる．本論文では，Mobile IPを用いてSHAKEを実現するMobile IP SHAKEにおいて，セキュアなAlliance構築手法の検討を行う．

Study of secure constructing of Alliance for Mobile IP SHAKE

Masahiro Shijo † and Susumu Ishihara††

We have proposed a system that aggregates links between multiple mobile hosts and the internet, and improves transmission speed (SHAKE: SHAring multipath procedure for a cluster networK Environment). Because a node which communicates using SHAKE depends on neighboring mobile hosts, there are security risks e.g. trafic monitoring by malicious hosts and intentional packet drop. Therefore SHAKE has to include functions of authentication of neighboring mobile hosts and confirming the safety of local link while forming an alliance between mobile hosts. In this paper, we propose secure and fast mechanisms forming an alliance for Mobile IP SHAKE.

1. はじめに

現在の無線通信環境では，短距離の通信であれば無線LANにより高速な通信が可能であるが，外出先でインターネットに接続しようとすると携帯電話やPHS等の比較的低速な広域無線サービスを使用せざるを得ない状況が考えられる．いつでも，どこでも，だれにでも高速で快適なインターネット接続を維持するには遍在するネットワーク資源の効率的な利用が必要である．そこで筆者らは，無線通信における低速で信頼性の低い通信を解決する手法として通信回線共有方式SHAKE（SHAring multipath procedure for a cluster networK Environment）を提案している．SHAKEは，移動端末が近隣の端末と協調して，短距離高速リンクを用い一時的なネットワーク（Alliance）を構築し，ネットワーク外部のホストと通信を行う際，そのネットワーク内の移動端末がもつ外部リンクを同時に複数利用して，各リンクにトラフィックを分散させることにより通信速度，信頼性の向上を実現させる方式である．

SHAKEでは，任意の近隣移動端末とローカルで一時的にAllianceを構築することで，通信相手とのトラフィックをAlliance内の端末がもつ通信経路へ分散させる．しかし，Allianceを構築した移動端末の中に悪意のある端末が存在した場合，その端末による通信傍受やトラフィックの横取りといった危険が存在する．またAllianceに属していなくとも，近隣の悪意のある端末によりAlliance内の端末のローカルアドレスを横取りされてしまえば，SHAKE本来の通信機能は破綻してしまう．そこで本稿では，Mobile IPを用いIP層でSHAKEを実現したMobile IP SHAKE[1)2)]の，Alliance構築時における移動端末の正当性の検証手法，ローカルリンク分断時におけるAllianceのセキュアかつ高速な再構築手法，およびローカルアドレスの割り当て方法の提案を行う．以下，第2章でMobile IP SHAKEについて説明し，第3章でMobile IP SHAKEの課題を整理する．その後，第4章でAlliance構築時における近隣移動端末の正当性検証方法，第5章でローカルリンク分断時におけるセキュアかつ高速なAlliance再構築手法について提案し，第6章でローカルアドレスの割り当て方法を述べる．第7章では関連研究について紹介し，最後に第8章でまとめる．

2. Mobile IP SHAKE

本章ではまず通信回線共有方式SHAKEについて概要を述べた後，本論文における提案手法の前提となるMobile IPv6 SHAKEの説明を行う．

2.1 通信回線共有方式 SHAKE

通信回線共有方式SHAKEでは，**図1**のように，ある移動端末に近隣する複数の移動端末が無線LAN等の短距離高速リンクを用いて一時的にネットワーク（クラスタ）

† 静岡大学大学院理工学研究科
Graduate School of Science and Engineering, Shizuoka University
†† 静岡大学工学部
Faculty of Engineering, Shizuoka University

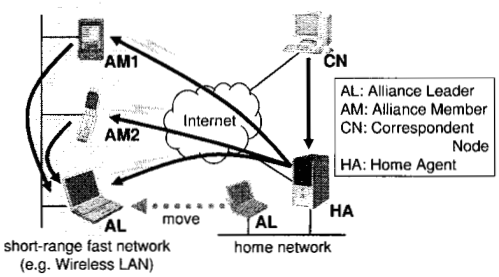

図 1 Mobile IPv6 SHAKE

を構築する．クラスタ内に存在するある端末がクラスタ外部と通信を行う際，他のクラスタ内端末の外部リンクを複数同時に用いて，各経路にトラフィックを分散させる．これにより，単一ホストのみを用いた場合よりも高速な通信が可能になる．また，クラスタ内の端末の外部リンクが使用不可能な場合でも他の端末の外部リンクを用いることにより，クラスタ外部のホストと通信を行うことが可能となる．以下，クラスタを構成する端末のうち，ある特定の通信に関わる端末群を Alliance とし，そのうち SHAKE を利用して通信を行う端末を Alliance Leader (AL)，AL のトラフィックを中継する端末を Alliance Member (AM) と呼ぶ．

2.2 Mobile IPv6 SHAKE

当研究グループでは，IP 層で SHAKE を実現させる手法として，先の研究で Mobile IPv6 を用いた Mobile IPv6 SHAKE（図 1）を提案し，実装評価している[2]．Mobile IPv6 では，Mobile Node (MN) が通信相手である Correspondent Node (CN) と通信する際，パケットは通常 Home Agent (HA) を経由する．Mobile IPv6 SHAKE では，この特徴を利用し複数のリンクへのパケット分配機構を HA に設置する．AL が SHAKE 通信を利用する際，自身の Home Address (HoA) に対して，自身の Care-of Address (CoA) だけでなく AM の CoA も同時に登録することで，HA は AL と AM がもつ外部リンクへトラフィックを分散させる．

2.3 Mobile IPv6 SHAKE の動作概要

Mobile IPv6 SHAKE では，Mobile IPv6 の経路最適化機構を利用可能であるが，ここではこの機能を用いない場合について述べる．以下の説明では，移動端末は自身の HA に対し，Mobile IPv6 の通常処理である CoA の登録により，自身の位置登録を済ませているものとする．

■ Alliance の構築

MN が SHAKE を利用するとき，短距離高速リンクを用いて近隣の端末とクラスタを構築する．SHAKE を利用する MN は AL となり，Alliance を構築する必要がある．本論文では Alliance の構築手順を再定義するため，以下の Alliance 構築手順の説明は概要にとどめる．

まず AL は近隣の MN に対して Alliance Request をブロードキャストすることで，Alliance への参加要求を行う．Alliance Request を受信した MN は，Alliance へ参加することを承諾する場合のみ，AL に対して Alliance Reply により応答する．この応答には，MN の現在保持するインターネットから到達可能なアドレス（以下，外部アドレス）および，MN が AL とのローカル通信で使用するアドレス（以下，ローカルアドレス），および各リンクの帯域，バッテリー残量，CPU 利用率，位置，速度等の情報を含める．AL は，これらの情報に基づいて，Alliance 参加を要求する MN を選択し，その端末に対して Ack をユニキャストで送信する．この際，AL は自身の Home Address (HoA) を Ack メッセージに付加する．以上により Alliance の構築を完了し，SHAKE を利用する AL は AL 自身と Alliance へ参加した端末（AM）の登録を次の手順により行う．

■ AL，AM の登録

Alliance の構築後，AL は自身の CoA および，Alliance 構築手順において得られた AM の外部アドレスを AL の HoA に対応付けて HA に登録する．しかし，Mobile IPv6 の仕様では，一つの HoA に対して一つの CoA しか登録することができない．そこで，登録する複数のエントリを識別するために，AL の CoA および AM の外部アドレスに対して Binding Unique Identification number (BID)[3] を割り当てる．また，登録先である AL の HA では，AL および AM のエントリを Binding Cach に保持する．

■ 通　信

Alliance 内端末の登録が完了すると，SHAKE を利用した通信が可能になる．HA が CN からのパケットを AL へ転送する際，Binding Cache を参照し，複数の CoA もしくは外部アドレスに対応する経路にパケットを振り分けて送信する．AM は HA から AL 宛のパケットを受信すると，ローカルリンクを用いて AL に転送する．AL が CN へパケットを送信する際は，CN と AM にパケットを分配し，HA を経由してパケットを通信する．なお，各経路へのパケットの分配方法やそのための経路監視の方法については，本論文では扱わない．

3. Mobile IP SHAKE の課題

本章では，以下の環境を前提とした上で Mobile IP SHAKE の課題を述べる．

- **HA は信頼できる存在である**
  HA は通常 Mobile IP 環境における MN のホーム・ネットワーク上のルータであり，通信事業者等により適切に管理され，信頼できる存在であると想定する．
- **AL は不正行為を行わない**
  AL は SHAKE 通信を主導する存在であるため，AL が自身の通信の不利益となる不正行為を行うことはないものとする．

3.1 Alliance 構築時における AM の外部アドレス正当性の検証

Mobile IP SHAKE では，AL が任意の近隣移動端末と Alliance を構築し，通信に AM となった端末の外部リン

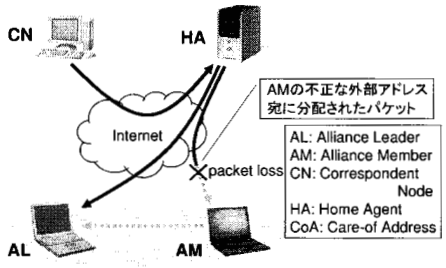

図 2　AM の不正 CoA による問題

クを同時利用することで通信の高速化かつ信頼性の向上を実現する．しかし，Alliance を構成する AM 中に悪意のある端末が存在した場合，AL–CN 間のトラフィックを不正にルーティングさせる可能性が存在する．たとえば，Alliance 構築処理において AM から得られた外部アドレスが誤った情報であると，HA から AM に転送されるべきパケットが失われてしまう（**図 2**）．このような問題を防ぐために，Alliance 構築時に AM から通知された外部アドレスの正当性の検証を行う必要がある．

3.2　SHAKE 通信中の AL–AM 間リンク分断時におけるセキュアかつ高速な Alliance 再構築

Mobile IP SHAKE のように通信トラフィックがローカルの近隣ノードを経由する場合，近隣に存在する悪質端末による通信傍受やトラフィックの改竄，横取りといった問題が考えられる．通常これらセキュリティ問題への対策として，IPsec[4] 等のセキュリティプロトコルの利用が考えられる．しかし，たとえ IPsec 等のセキュリティプロトコルを利用していても，ローカルで悪意のある端末により Alliance 内端末のローカルアドレスが横取りされてしまった場合（**図 3**），もしくはその他の原因でローカルアドレスの変更を余儀なくされてしまった場合，Mobile IP SHAKE における AL–AM 間のクラスタリンクは分断してしまう．これにより SHAKE 通信トラフィックの一部もしくは全てが正常に配送されなくなる可能性がある．また，このような状況時に通信を回復させる場合には，Alliance の再構築，AM の外部アドレスの再検証，トラフィック分配情報の交換等，SHAKE プロトコルが本来の通信を行う上でオーバーヘッドとなってしまう．そのため，Alliance 内のクラスタリンク分断後の，セキュアかつ高速な Alliance 再構築の機構が必要である．

3.3　ローカルアドレスの割り当て

Mobile IP SHAKE では，Alliance を構成する AM が，AL–CN 間トラフィックをローカル通信を用いて中継する．これを実現するためには Alliance を構築する端末群がそれぞれユニークなローカルアドレスを保持していることが前提となる．しかし，Mobile IP SHAKE 環境ではローカルアドレスの割り当てを行うための DHCP サーバ等の存在は想定していない．そのため，クラスタリンクにおける通信に無線 LAN 等の IP 通信を用いる場合，移動端末に対するローカル IP アドレスの割り当てが必要となる．

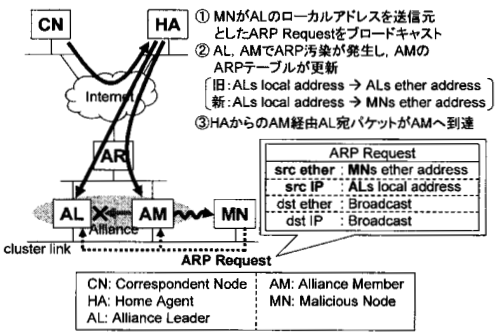

図 3　近隣悪質端末による Alliance 内端末のローカルアドレス横取り

4.　Alliance 構築時における AM の外部アドレス正当性の検証

本章では，Alliance 構築時における Return Routability と同様の機構を利用した AM の外部アドレス正当性の検証方法について述べる．

4.1　AM の外部アドレス正当性の判断基準

Alliance を構成する AM は，少なくとも以下の動作要件をみたす必要がある．

- AM が AL に通知する外部アドレスにより，インターネットを介して AL と相互にパケットが到達可能である．
- AL のローカルアドレス，AM のローカルアドレス間でローカルリンクを介して相互に到達可能である．
- AM が外部アドレス，ローカルアドレス両者からパケットを送信，受信可能である．

4.2　Return Routability の概要

本来 Return Routability とは，Mobile IPv6 における経路最適化において，MN–CN 間のセキュリティを確保するための処理として導入されたものである[5]．Return Routability では，CN が MN から Binding Update が行われた際に鍵付きハッシュアルゴリズムを用いて Binding Update の完全性と MN 認証を行うために，MN–CN 間で共有秘密鍵の代わりとなる共有情報（Binding key）を生成する．ただし Return Routability では，MN–HA 間は IPsec を利用することで通信が保護されていることを前提とする．**図 4** に処理手順を示す．MN はまず，HA を介した MN–CN 間経路と HA を介さない MN–CN 間の両経路において，それぞれ異なる cookie を付加した Test Init メッセージ（Home Test Init，Care-of Test Init）を CN に対して送信する．各 Test Init メッセージに対して，HA は両経路において，Test メッセージを返信する．この際，HA は MN から両経路で Test Init メッセージより取得した各 cookie と，それぞれ異なる署名用トークン，および，各署名用トークンを生成する際に用いられた臨時鍵を区別するための通し番号（臨時鍵番号 i，j）を，各 Test メッセージ（Home Test，Care-of Test）に付加しておく．これにより，MN は両経路

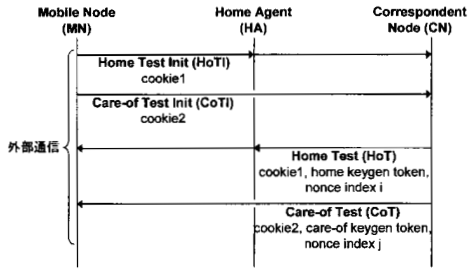

図 4　Return Routability の処理

で得られた署名用トークンのハッシュから Binding Update に用いる Binding key を生成する．また，両経路で HA から返された各 cookie は，それぞれの経路中でパケットの情報が改竄されていないかを検証するために用いられる．

4.3 Alliance 構築時における AM の外部アドレス正当性の検証方法

■ AM の外部アドレス正当性を検証可能な Alliance 構築手順

AM から通知された外部アドレスの検証を行うため，AL を Mobile IPv6 における CN に見立て AM から Return Routability と同様の処理を行う機構を導入する．**図 5** に再定義する Alliance 構築手順を，**図 6** に AM の外部アドレス正当性の検証処理を示す．

図 5 において，AL は，Alliance Request に対し Alliance Reply を返した AM に対して RR Trigger をユニキャストで送信する．これを受けた AM は，AL に対して Return Routability と同様の処理を行う．AM は，AL に対して AL の HA を経由した Home Test Init (HoTI) とローカル通信による Local Test Init (LoTI) を送信する（図 6）．この際，各 Test Init メッセージにそれぞれ異なる cookie を付加しておく．

各 Test Init メッセージを受信した AL は，HoTI に対する応答として自身の HA 経由で Home Test (HoT) メッセージ，LoTI に対する応答として Local Test (LoT) メッセージを返信する．各 Test メッセージには，AM から Test Init メッセージ（HoTI，LoTI）により得られた cookie と署名用トークン，および，各臨時鍵番号 i，j を付加する．ここで，AL から HoT により AM に送られた臨時鍵番号 i を，以降の処理では公開セッション ID（ID_P）として使用する．

AM は各 Test メッセージを受信すると，AL に対して Binding Update Request を送信する．この際 AM は，AL から HoT により取得した公開セッション ID（ID_P），各 Test メッセージにより取得した cookie および，AL との間で図 6 の AM の外部アドレス検証処理により生成した共有情報（Return Routability における Binding key）を用いた鍵付きハッシュ（*MAC_BUReq*）を付加しておく．なお，以降では AM の外部アドレス正当性の検証処理において AL–AM 間で作成した共有情報を，AL–AM 間における共有秘密鍵と同様に使用できるものとし，共有秘密鍵（K_S）とする．*MAC_BUReq* の生成方法を次式に示す．

$$MAC\_BUReq = HMAC\,(K_S, (ID_P \mid cookie1 \mid cookie2))$$

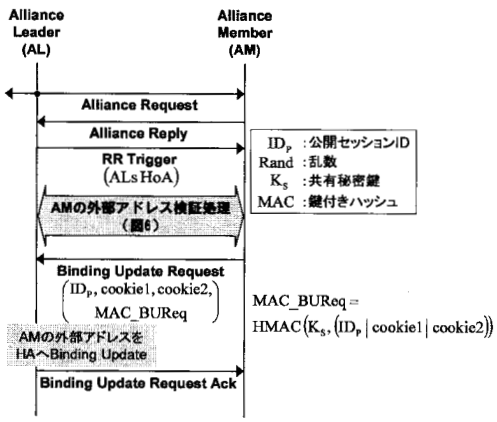

図 5　再定義した Alliance 再構築手順

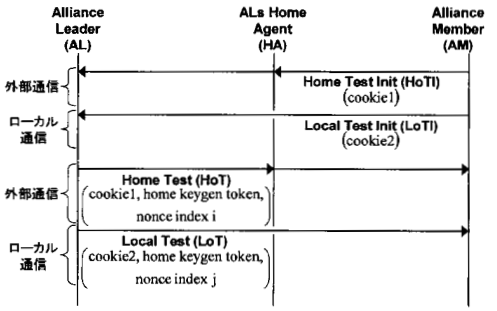

図 6　AM の外部アドレス正当性の検証処理

Binding Update Request を受信した AL は，自身が HoT により AM へ通知した臨時鍵番号 i と一致するセッション ID（ID_P）が含まれていた場合，その *IDP* とメッセージに含まれた cookie（cookie1，cookie2）を用いて共有秘密鍵（K_S）により鍵付きハッシュを計算する．この計算値が Binding Update Request により受信した *MAC_BUReq* と一致した場合，AM の外部リンクを用いた AM–HA 間および，ローカルリンクを用いた AL–AM 間の接続性，両経路においてパケットの改竄といった問題がないことが確認できる．以上により AM の外部アドレス正当性の検証が完了すると，AL は AM の外部アドレスを自身の HA に対して Binding Update を行う．その後 AL は AM に対して Binding Update が完了したことを示す Binding Update Request Ack を送信する．以上により，Alliance の構築は完了する．

5. SHAKE 通信中の AL–AM 間リンク分断時におけるセキュアかつ高速な Alliance 再構築

SHAKE 通信中に，ローカルで悪意のある端末により

Alliance 内端末のローカルアドレスを横取りされた場合，もしくはその他の原因でローカルアドレスの変更を余儀なくされてしまった場合，AL–AM 間のリンク分断により SHAKE 通信が破綻してしまう．そのため，Alliance 内のリンク分断が起きた場合には，Alliance の再構築を行うことで SHAKE 通信を途中から再開させることが有効である．しかし，Alliance の再構築処理において本稿 4.3 節で示した AM の検証処理を行う場合，HA を介した RTT の比較的大きいことが予想される HoTI，HoT パケットが発生してしまううえ，さらにトラフィック分配情報の交換等，Alliance 構築の通常処理がオーバーヘッドとなってしまう．そのため，一度 Alliance を構築し端末の検証処理を行った AM とのリンク分断が発生した場合，その AM との Alliance 関係を，簡単な認証によりセキュアかつ高速に再構築することで，障害が起きた SHAKE 通信を復旧させることが望ましい．

5.1 Alliance 内のクラスタリンク分断が起きた際の，セキュアかつ高速な Alliance 再構築手順

■概　要

Alliance 内において，AL–AM 間のクラスタリンク分断が発生した場合の AM の検証処理やトラフィック分配情報の交換等の Alliance 再構築にかかるプロトコルオーバーヘッドを抑制するため，分断を起こした AM の簡易認証により，AL–AM 間の Alliance 関係を再構築する．ある AM とのクラスタリンクが分断し，必要に応じて AL もしくは AM のローカルアドレスの変更を行った後，AL はリンク分断を起こした AM と共有している公開セッション ID，および，その ID に対する鍵付きハッシュを含んだ Ext-Alliance Request をブロードキャストする．この鍵付きハッシュは，先の AM 検証処理において AL–AM 間で作成された共有情報を共有秘密鍵として生成したものである．この Ext-Alliance Request を受信した近隣移動端末（AM）では送信元 AL を認証後，Ext-Alliance Reply により公開セッション ID と鍵付きハッシュを返信する．これを受信した AL において送信元端末の認証が済めば，AL–AM 間の Alliance 関係の再構築が完了する．

■AM のローカルアドレス変更に伴うリンク分断発生時

以下に，AM のローカルアドレスが変更され，AL–AM 間のクラスタリンク分断が起きた場合における Alliance 再構築手順を示す（**図 7**）．

(1)　**AM がアドレス変更後，AL へアドレス変更報告を行う**

クラスタリンク内で悪質端末により AM のローカルアドレスを横取りされた際，もしくは他の近隣端末とアドレスが衝突した場合など，AM はローカルアドレスの再設定を行うことで自身のローカルアドレスの衝突を解決し，分断の起きた AL–AM 間クラスタリンクの修復を行う．AM は自身のローカルアドレス変更後，AL に対してアドレス変更報告を行う．このアドレス変更報告メッセージには

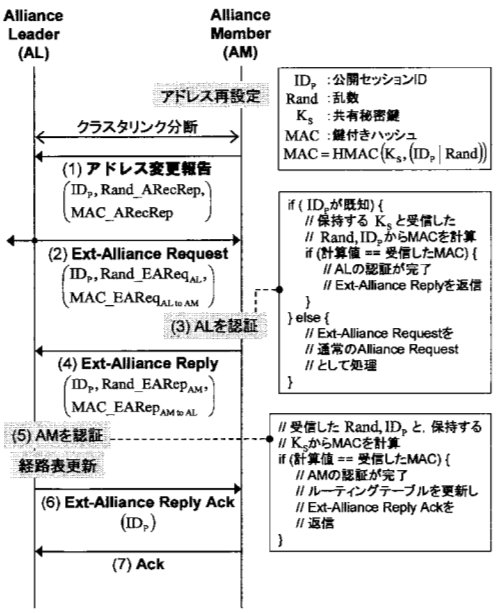

図 7　AM のローカルアドレス変更に伴うリンク分断発生時の Alliance 再構築処理

AL–AM 間で共有した公開セッション ID（ID_P）と，AM が生成した乱数（*Rand_ARecRep*），および AL との間で 4.3 節 AM 検証処理により共有した秘密鍵（K_S）を用いた鍵付きハッシュ（*MAC_ARecRep*）を付加しておく．*MAC_ARecRep* の生成方法は次式で与えられる．

$$MAC\_ARecRep = HMAC(K_S, (ID_P \mid Rand\_ARecRep))$$

(2)　**アドレス変更報告を受けた AL は Ext-Alliance Request をブロードキャストする**

AL がアドレス変更報告を受け，メッセージに自身が Alliance 内の AM と共有した公開セッション ID（ID_P）が含まれていた場合，アドレス変更報告メッセージが Alliance 関係を構築していたはずの AM からのものであるか確認を行う．AL は，アドレス変更報告メッセージに含まれるセッション ID（ID_P）と乱数（*Rand_ARecRep*）から，セッション ID（ID_P）を共有した AM との間で作成した秘密鍵（K_S）を用いて鍵付きハッシュを計算する．計算値がアドレス変更報告メッセージに含まれた *MAC_ARecRep* と一致した場合，AL は Ext-Alliance Request をブロードキャストする．AL はこの際，受信したアドレス変更報告に含まれていたセッション ID（ID_P）と AL が生成した乱数（$Rand\_EAReq_{AL}$），およびアドレス変更報告の送信元端末（AM）との間で共有した秘密鍵（K_S）を用いた鍵付きハッシュ（MAC_EAReq_{ALtoAM}）を Ext-Alliance Request に付

加しておく．MAC_EAReq_{ALtoAM} の生成方法は次式で与えられる．

MAC_EAReq_{ALtoAM} =

$HMAC\,(K_S, (ID_P \mid Rand\_EAReq_{ALtoAM}))$

(3) **Ext-Alliance Request を受信した AM は Ext-Alliance Request の送信元端末（AL）を認証する**

AM は自身が保持するセッション ID（ID_P）が含まれた Ext-Alliance Request を受信すると，送信元 AL の認証を行う．メッセージに含まれた ID_P と $Rand\_EAReq_{AL}$ から，AL と共有した鍵（K_S）を用いて鍵付きハッシュを計算し，これがメッセージに含まれた MAC_EAReq_{ALtoAM} と一致すれば，以前 Alliance 関係を構築していた AL からの Ext-Alliance Request であると認められる．

(4) **AL の認証が完了した AM は AL に対して Ext-Alliance Reply を返信する**

AM において AL の認証が完了したら，AM は AL へ Ext-Alliance Reply を返信する．この際，Ext-Alliance Request と同様に，セッション ID（ID_P），AM が生成した乱数（$Rand\_EARep_{AM}$）および鍵付きハッシュ（MAC_EARep_{AMtoAL}）をメッセージに付加しておく．

(5) **Ext-Alliance Reply を受信した AL は Ext-Alliance Reply の送信元端末（AM）を認証する**

AL は Ext-Alliance Reply を受信すると，送信元端末（AM）の認証を行う．メッセージに含まれた ID_P と $Rand\_EARep_{AM}$ から AL–AM 間の秘密鍵（K_S）を用いて鍵付きハッシュを計算し，これがメッセージに含まれた MAC_EARep_{AMtoAL} と一致すれば，以前 Alliance 関係を構築していた AM からの Ext-Alliance Reply であると認められる．

(6) **AM の認証が完了した AL は，AM に対して Ext-Alliance Reply Ack を返信する**

AL において AM の認証が完了したら，AL は AM に対して Ext-Alliance Reply Ack を返信する．このメッセージには AL–AM 間で共有していたセッション ID（ID_P）を付加しておく．

(7) **AL から Ext-Alliance Reply Ack を受信した AM は，AL へ Ack を返信する**

AM は AL から Ext-Alliance Reply Ack を受信すると，AL に対して Ack を返信する．以上により AL–AM 間のクラスタリンク分断時における AL–AM 間 Alliance の再構築は完了する．

■ AL のローカルアドレス変更に伴うリンク分断発生時

以下に，AL のローカルアドレスが変更され，AL–AM 間クラスタリンク分断が起きた際の Alliance 再構築手順を示す（**図 8**）．

基本的な方法は AM のローカルアドレス変更に伴うリンク分断発生時の Alliance 再構築手順と同様である．しかし AL のローカルアドレスが変更された場合，Alliance

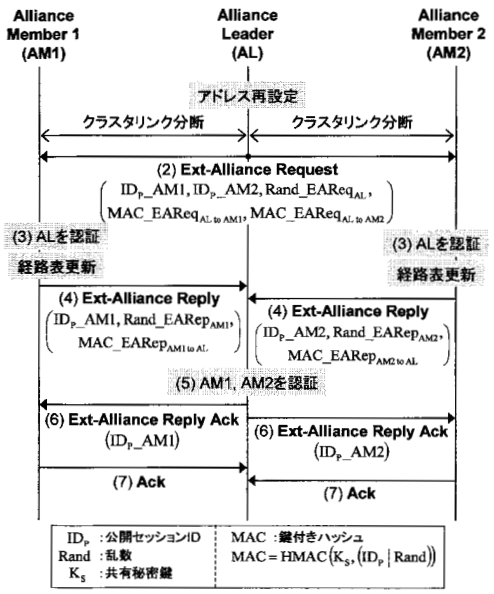

図 8 AL のローカルアドレス変更に伴うリンク分断発生時の Alliance 再構築処理

内の全ての AL–AM 間クラスタリンクは分断してしまう．そのため全ての AL–AM 間における Alliance 関係を再構築しなければならない．そのため，AM のローカルアドレス変更に伴う Alliance 再構築時における Ext-Alliance Request とは若干の変更を施した．以下，AM と AL のローカルアドレス変更に伴う Alliance 再構築処理の相違点を示す．

AL は自身のアドレス変更後，Ext-Alliance Request をブロードキャストするが（図 8: (2)），この Ext-Alliance Request には以前 Alliance 関係を構築していた AM に対応する AL の認証情報，つまり公開セッション ID と各 AL–AM 間で交換した秘密鍵を用いた鍵付きハッシュを付加する．例えば，AL が 2 つの端末（AM1，AM2）と Alliance を構築していた場合，Ext-Alliance Request には AM1 および AM2 とのセッション ID（ID_P_AM1，ID_P_AM2），AL が生成した乱数（$Rand\_EAReq_{AL}$），AM1 および AM2 に対応する鍵付きハッシュ（$MAC\_EAReq_{ALtoAM1}$，$MAC\_EAReq_{ALtoAM2}$）を付加する．これを受信した AM1，AM2 では，それぞれが保持するセッション ID（ID_P_AM1，ID_P_AM2）を検出し，対応する鍵付きハッシュを生成することで AL の認証を行う．この例における AL がブロードキャストすべき Ext-Alliance Request を以下に示す．

Ext – Alliance Requests payload :

(ID_P_AM1，ID_P_AM2，$Rand\_EAReq_{AL}$，

$MAC\_EAReq_{ALtoAM1}$，$MAC\_EAReq_{ALtoAM2}$)

AM1 および AM2 において AL から Ext-Alliance Request を受信し，AL の認証完了後（図 8: (3)），以降の処理は AM のローカルアドレス変更に伴う Alliance 再構築

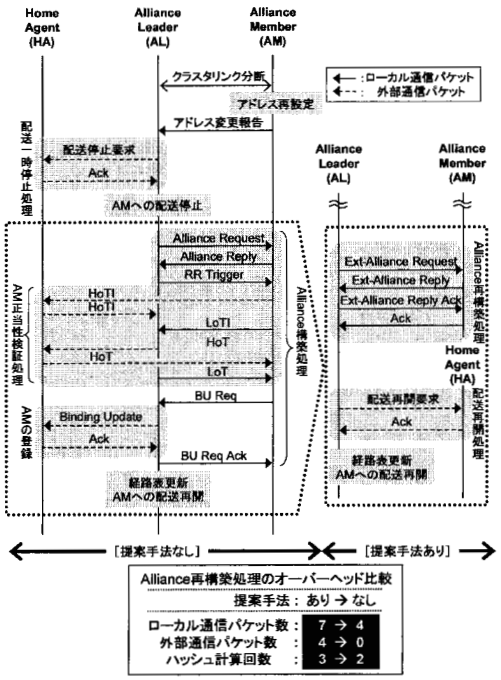

図 9　Alliance 再構築処理のオーバーヘッド比較

手順と同じになる．

5.2　提案手法ありの場合となしの場合のオーバーヘッドの比較検証

本稿で提案した，Alliance 内におけるクラスタリンク分断時の Alliance 再構築処理について，提案手法がなかった場合とのオーバーヘッドの比較検証を行う．以下，AM のローカルアドレスの変更が必要となった場合を想定する．

■ クラスタリンク分断発生時の Alliance 内端末への配送抑制

Alliance 内においてクラスタリンク分断が起きた場合，HA から AM へ分配されたパケットおよび AL から AM へ分配されたパケットはローカルリンクで失われてしまう．そのため，クラスタリンク分断が起きた際のパケットロスを抑制するため，HA に対して AM へのトラフィック分配を停止させる機構が必要になる．そこで先の研究で提案実装されている，Mobile IPv6 SHAKE に Mobile IPv6 の経路最適化通信を適応した環境における，Alliance 内端末がハンドオーバーした際のハンドオーバーした端末へのトラフィック配送抑制機構[6] を応用することで，Alliance 内でクラスタリンク分断時に HA に対して AM へのトラフィック分配を抑制することが可能であると想定する．**図 9** に，AM のローカルアドレス変更に伴う Alliance 再構築時における，提案手法を用いなかった場合の Alliance 再構築処理と用いた場合の Alliance 再構築処理について，オーバーヘッドの比較を示す．

■ 提案手法を用いない Alliance 再構築処理

提案手法を用いない場合，図 9 のように，本稿 4.3 節で再定義した Alliance の構築が行われる．また，AM の正当性検証処理では，HA を介した AL–AM 間の外部通信や，ハッシュ計算が行われる．以下にローカル通信と外部通信による送信パケット数，ある端末によって行われるハッシュ計算の回数を示す．

- ローカル通信パケット数：7
- 外部通信パケット数：4
- ハッシュ計算回数：3

■ 提案手法を用いた Alliance 再構築処理

提案手法を用いた場合，図 9 のように，以前 Alliance 関係を構築していた AM との Alliance 再構築処理は全てローカル通信により行われる．しかし，AL–AM 間認証を行うため，AL，AM それぞれにおいてハッシュ計算が必要になる．以下に，提案手法を用いた場合の Alliance 再構築処理に必要な送信パケット数，ハッシュ計算の回数およびその他必要な処理をまとめる．

- ローカル通信パケット数：4
- 外部通信パケット数：2
- ハッシュ計算回数：2

以上から分かるように，AM のローカルアドレス変更に伴う Alliance 再構築処理では，本稿で提案した手法を用いることで，3 つのローカル通信パケット，2 つの外部通信パケット，1 つのハッシュ計算を省くことが可能となる．

6.　ローカルアドレスの割り当て

本章では Mobile IP SHAKE におけるローカルアドレス割り当て方法を述べる．先に述べたように Mobile IP SHAKE 環境では，AL–AM 間のローカル通信でトラフィックの転送が行われる．そのため，Alliance 内端末に対するローカルアドレスの割り当てが必要となる．Mobile IP SHAKE 環境では，Alliance 内における AL–AM 間は 1 ホップ通信を想定している．

6.1　Mobile IPv4 SHAKE におけるアドレス割り当て

Mobile IPv4 SHAKE におけるローカルアドレスの割り当て方法として IETF の Zeroconf Working Group で標準化された AutoIP[7] を利用する．AutoIP では，リンクローカル通信で利用可能な 169.254/16 アドレス空間からランダムに仮アドレスを生成し，仮アドレスに対し送信元アドレスに未指定アドレスがセットされた ARP Request（ARP Probe）をブロードキャストすることで仮アドレスの衝突検出を行う．もし ARP Probe に対する ARP Reply が返ってくれば，自身のローカル通信用インタフェースに仮アドレスを設定する．

6.2　Mobile IPv6 SHAKE におけるアドレス割り当て

Mobile IPv6 SHAKE では，IPv6 ULA[8] を用いてローカルアドレスを割り当てる．IPv6 ULA では，FC00::/7 プレフィックスアドレスにおいて，擬似乱数による Global ID と Subnet ID，64 ビットのインタフェース ID を利用してローカル IPv6 アドレスを生成する．Subnet ID について

は，SHAKE の Alliance 内通信用アドレスのためにサブネット ID を統一する．このアドレス生成アルゴリズムは，擬似乱数 Global ID とインタフェース ID をアドレス生成に用いることで，アドレスの唯一性を高めている．そのため，ULA によりアドレスを割り当てた場合，実運用上はアドレスの衝突が起きないと考えられ，アドレス設定後通信前のアドレス衝突検出処理はオーバーヘッドとなりかねない．そのため，アドレス衝突検出は，次節に示すアドレス衝突検出処理においてのみ行うこととする．

6.3 アドレスの衝突検出

Mobile IP SHAKE で想定するようなアドホック無線通信環境では，端末の移動によりアドレス設定後においてもアドレスの衝突が起きる．以下，アドレス設定後におけるアドレス衝突検出方法を述べる．

Mobile IP SHAKE では，Alliance は基本的に 1 ホップ通信環境を想定している．そこでアドレスの衝突検出は ARP パケット（Mobile IPv6 SHAKE 環境では NDP パケット．以下同様）に含まれている IP アドレスと MAC アドレスを利用する．隣接端末から受信した ARP パケットの送信元 IP アドレスが自身と同じで送信元 MAC アドレスが自身と異なる場合，自身が隣接端末とアドレス衝突を起こしていると判断できる．その際は，アドレスの再設定を行うことで，アドレス衝突を解決する．

しかし，Mobile IP SHAKE で想定するような 1 ホップ無線通信環境では，隠れ端末とのアドレス衝突も問題になるそこで，各端末においてそれぞれの 1 ホップ内の隣接端末の IP アドレス，MAC アドレスを保持しておき，各端末の 1 ホップ内における 2 者端末間におけるアドレス衝突についても監視を行う．自身以外の 2 者端末間でアドレス衝突を検出した場合には，アドレス衝突を起こした 2 者端末に対してアドレスの変更要請を行うことでアドレス解決を図る．

7. 関 連 研 究

マルチホームな NEMO (Network Mobility) 環境において，複数の Mobile Router (MR) を利用することで移動ネットワークを冗長化，および付加分散等の機能を提供するシステムが研究されている．このシステムの実現方法として，文献[9] では複数の MR を一つの Home Agent (HA) に対して登録することで，HA–MR 間の通信経路の冗長性を持たせる方式を提案している．また[9] では，HA へ近隣 MR の登録を行う前段階処理として，Return Routability と同様の機構を利用した近隣 MR の認証方法を提案している．この近隣 MR の認証処理では，マルチホーム NEMO 環境構築を主導する MR と，その MR の近隣 MR 間において Return Routability 処理を互いに行う．これにより，それぞれの MR は互いの Care-of Address (CoA) の正当性を検証している．一方，Mobile IP SHAKE では，Alliance を構成する AM は必ずしも Mobil IP 対応端末とは限らず，AM に対応する HA が存在しない場合も想定される．そのため Mobile IP SHAKE では，本稿で提案したように SHAKE 通信を行う AL に対し，AM のみが AL の HA を介した Return Routability と同様の処理を行うことが望ましい．

8. ま と め

本稿では，Mobile IP SHAKE における Alliance 構築時の AM の正当性検証方法と，SHAKE 通信中の AL–AM 間リンク分断時におけるセキュアかつ高速な Alliance 再構築方法について提案を行った．Alliance 構築処理において，もし AM から取得した外部アドレスが不正なアドレスであった場合，HA から AM へ分配されたパケットは AM へ届かず失われてしまう．このような AM による不正ルーティングを未然に防ぐため，Alliance 構築処理時に Mobile IPv6 の Return Routability と同様な機構を導入することで，SHAKE 通信前に AM の外部アドレスによる外部リンクの接続性を検証する．また，SHAKE 通信中に AL–AM 間のクラスタリンク分断が発生した場合，以前 Alliance 関係を構築していた AM については，AM の外部アドレス正当性の検証処理において作成した共有情報を用い，鍵付きハッシュ等の簡単な認証により Alliance の再構築を行う．これにより，Alliance 構築処理における AM の外部アドレス検証処理等のプロトコルオーバーヘッドを抑制することが可能となる．今後の課題として，本稿で提案した AM の外部アドレス正当性の検証処理および，AL–AM 間のクラスタリンク分断時における Alliance 再構築処理の実装が挙げられる．

参 考 文 献

1) K. Koyama, Y. Ito, H. Mineno and S. Ishihara: “Performance evaluation of TCP on Mobile IP SHAKE,” *IPSJ Journal*, Vol. 45, No. 10, pp. 2270–2278 (2004).
2) 舛田知広, 大木一将, 峰野博史, 石原進: “Mobile IPv6 を用いた通信回線共有方式の実装,” 情報処理学会論文誌, Vol. 46, No. 9, pp. 2214–2225 (2005).
3) R. Wakikawa, T. Ernst and K. Nagami: “Multiple Care-of Addresses Registration,” *Internet Draft*, draft-wakikawa-mobileip- multiplecoa-05 (2006).
4) S. Kent and K. Seo: “Security Architecture for the Internet Protocol,” *Request for Comments 4301* (2005).
5) D. Johnson, C. Perkins and J. Arkko: “Mobility Support in IPv6,” *Request for Comments 2755* (2004).
6) K. Ogi, T. Masuda, H. Mineno and S. Ishihara: “Design and Implementation of Mobility Mechanisms for Mobile IPv6 based Link Aggregation System,” Proc. of *SAINT 2005 workshop* (2005).
7) S. Cheshire, B. Aboba and E. Guttman: “Dynamic Configuration of IPv4 Link-Lokal Addresses,” *Request for Comments 3927* (2005).
8) R. Hinden and B. Haberman: “Unique Local IPv6 Unicast Addresses,” *Request for Comments 4193* (2005).
9) S. cho et al: “Neighbor MR Authentication and Registration Mechanism in Multihomed,” *Internet Draft*, draft-cho-nemo-mr-registration-00 (2004).