

経路アグリゲーションを行う移動端末間の中継促進機構

伊藤陽介[†] 峰野博史^{††} 石原進^{†††}

[†] 静岡大学大学院理工学研究科 ^{††} 静岡大学情報学部 ^{†††} 静岡大学工学部

A scheme encouraging mobile nodes to forward packets between the internet and a mobile ad hoc network

Yosuke Ito[†], Hiroshi Mineno^{††} and Susumu Ishihara^{†††}

[†] Graduate School of Science and Technology, Shizuoka University

^{††} Faculty of Information, Shizuoka University

^{†††} Faculty of Engineering, Shizuoka University

1 はじめに

モバイルコンピューティングの発達とともに、携帯情報端末を持つ人口は急増し、移動先であっても時や場所を選ばず、快適にインターネットに接続したいというユーザの要望が強まっている。現在の無線通信環境において限定された地域であれば無線 LAN 等を用いることで高速な通信を行うことが可能であるが、一方で広域サービスが可能な 3G 携帯、PHS を用いた通信では通信速度が制限される。

筆者らは、複数端末が持つネットワークインタフェースを複数同時に利用し、各端末が持つリンクをアグリゲーションすることで、無線通信環境においても高速・高信頼な通信を可能にする通信回線共有方式 SHAKE (SHARing multiple paths procedure for a cluster network Environment) を提案している。SHAKE は、ある地点に集まったユーザ同士が無線 LAN 等の短距離高速リンクを用いて一時的なネットワーク (クラスター) を構築し、クラスター内のメンバが持つ外部ネットワークに接続可能なリンクを複数同時に利用して外部と通信することで、トラフィックを分散させ、通信の高速化を実現する。

SHAKE では、近隣の端末間で協調し合い、ある特定の端末のために自身の外部リンクを用いてトラフィックを中継する端末が必要となる。他ノードのためにトラフィックを中継することは CPU、メモリ、バッテリーに多大な影響を被ることとなるため、これを理由に他ノードに中継を拒否された場合、SHAKE を利用した通信が不可能となる。筆者らは文献 [1] において、その問題を解決するため、中継端末にインセンティブとしてクレジットを与えることで、他ノードに中継を促進する手法を提案・検討した。しかし、文献 [1] で提案した手法では、リンクアグリゲーションを行う端末間でパケットロスが起きた場合、それが単なるリンクロスであるのか、中継端末による意図的なパケットドロップであるのかを判断できず、その際の適切な処理に関して十分な考慮がなされていなかった。

本稿では、文献 [1] の手法を再検討し、中継端末に対して適切に報酬を与える仕組みの再提案・検討を行う。以下、第 2 章では通信回線共有方式 SHAKE の概要について説明し、データ中継に関する問題点と従来の提案手法の問題点を明らかにする。第 3 章では SHAKE においてトラフィックの中継を促進する手法を提案し、そのアーキテクチャを示す。第 4 章では提案手法を適用した際の動作に関して有効性を検討し、第 5 章でまとめとする。

2 通信回線共有方式 SHAKE

本章では、本論文で前提としている通信回線共有方式の概要を説明する。

通信回線共有方式 SHAKE では、複数の移動端末が短距離で高速なリンクを用いて接続し、一時的にネットワーク (クラスター) を構成する。クラスターの中で、ある特定の通信に携わる端末群を Alliance と呼ぶ。Alliance のうちデータを中継する端末を Alliance Member (AM)、データの中継を依頼し受信する端末を Alliance Leader (AL) と呼ぶ。

AL が Alliance 外部の端末と通信を行う際に、AL および AM の持つ外部ネットワークへのリンクへトラフィックを分散させることで高速な通信が可能となる。また Alliance 内の端末は自分の外部リンクが利用不可能な場合でも、他の Alliance 内端末の外部リンクを利用することで、外部のホストと通信を行うことが可能である。

本稿では、Mobile IP を応用した IP 層における実現手法 Mobile IP SHAKE[2] の動作を対象を絞って議論を進めることとする。

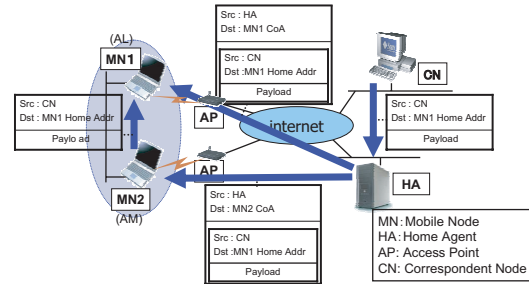


図 1: Mobile IP SHAKE によるデータグラム配送

2.1 Mobile IP SHAKE

SHAKE を IP 層で実現するためには、Alliance 外部にいる通信相手 (Correspondent Node: CN) から Alliance への経路途中にトラフィックを分配するための中継ホストが必要である。この分配ホストが Alliance 内端末への外部リンクの共通の経路上に存在する場合以外には、CN はその分配ホストの存在を知っている必要がある。Mobile IP SHAKE は、Mobile IPv4 において CN から MN へのパケットは経路最適化を考慮しない場合に必ず Home Agent (HA) を経由するという特徴を利用して、HA にトラフィックを分配する機構を設置している。それにより、CN には特別な機構をもたせる必要なく、複数経路を用いた通信を実現できる。

図 1 に Mobile IP SHAKE の動作概要を示す。あらかじめ移動端末 MN1 (AL: Alliance Leader) のホームエージェントである HA に、AL とともに Alliance を構成している移動端末 MN2 (AM: Alliance Member) の CoA (Care-of Address) を登録しておく。HA が CN から届けられた AL 宛てのパケットを転送する際には、AL および AM にパケットをカプセル化して分配・転送する。AM は届けられたパケットのカプセル化を解除し、Alliance 内のリンクを通して AL にパケットを転送する。

クラスター内部から外部リンクへデータを送信する際には、AL にてパケットを各 AM へカプセル化して分配する。クラスター内部から外部への通信を行う場合、HA を経由しない方法と逆方向トンネリング (Reverse Tunneling) を用いて HA を経由する方法のいずれも可能である。

以下、外部からクラスターへのデータ配信を「下り通信」、クラスター内部から外部へのデータ配信を「上り通信」と表す。

2.2 問題提起

SHAKE による通信を行うためには、端末は移動する先方で Alliance 内の端末と協調動作をする必要がある。Alliance 内の端末はその内の通信の信頼性・安全性を確保し、かつメンバの参加、離脱等の管理を行わなければならない。このような問題に関しては、各メンバの IP アドレスや通信状況をモニタする機構を導入することで解決される。

SHAKE では、他の端末のためにトラフィックを中継する端末 (つまり AM) が必要となる。AM は他のノードのために CPU 資源、バッテリー、リンクの帯域等を提供することとなる。中継を行うことが AM 自身にとって全くの無益であり、かつ負担となるならば、友人同士である等あらかじめ信頼のおけるグループ関係を築いていない限り、中継の依頼をされたとしてもその依頼に対して拒否をされると考えられる。そこで本稿では、AM に報酬を与えることで、他ノードのために中継を行うためのモチベーションを持たせる仕組みを導入する。

2.3 関連研究

無線アドホックネットワークにおいて、パス上の中間ノードに中継を促す手法がいくつか提案、評価されている。

文献 [3] では、nuglets と呼ばれる仮想的な貨幣を使用し、中継を行うノードに報酬として nuglets を与える手法を提案している。この手法では、パケットの送信元がパケットに nuglets を搭載して送信し、中間ノードは転送する際にいくらかの nuglets を獲得する。各ノードでの正確な nuglets の量の操作を保証するため、この手法では、耐タンパ性をもつハードウェアを用いてユーザによる不正を防いでいる。Zhong らは集中管理機関を設置することで、中継ノードに報酬を与える手法を提案している [4]。この手法では、送信元から受信元までのパス上の中間端末は、メッセージ中継後、集中管理機関に中継したことを報告する。集中管理機関は、その中継の報告をもとにして、メッセージの送信元への請求と中継ノードへの報酬の支払いを行う。

アドホックネットワーク環境と、SHAKE で想定する環境には以下のような違いがある。文献 [3], [4] で想定しているアドホックネットワーク環境では、パケットロスが発生しない限り、中継路上のどの中継端末も同量のトラフィックを中継することとなる。一方、SHAKE においては複数の性質の異なる AM によって Alliance が構築されることがあり得るので、AM 間で中継データ量に違いが生じる。また、文献 [3][4] では、データの送信元が報酬の支払いをすることとしているが、SHAKE では AL 自身がデータの送信元、受信先いずれであっても、AM の協力を受けていることとなり、中継を行ってもらった AM に対して適切な量の報酬を与える仕組みが必要となる。

2.3.1 SHAKE における従来のトラフィック中継促進機構

筆者らは、文献 [1] で、SHAKE に特有のデータ中継量の違いに関する問題および報酬の支払い者に関する問題を考慮しつつ、中継端末に適切に報酬（クレジット）を与える仕組みを提案した。具体的な実現手法として、文献 [3], [4] と同様、耐タンパハードウェアを用いる手法、信頼できる第三者機関が管理を行う手法を提案している。

耐タンパハードウェアを用いた手法では、ハードウェアに依存することで正確なクレジット処理を行うことが可能である。第三者機関を導入したモデルは、第三者機関が中継に携わった端末からの報告に基づき、クレジットの請求・報酬処理を行う。

第三者機関を導入した手法では、上り通信時 (AL AM HA CN) は、AM, HA が中継の報告を第三者機関へ行くと、第三者機関が AL への請求および AM への報酬の支払いを行う。下り通信時 (CN HA AM AL) では、HA および AM から第三者機関への中継実施報告に加え、AL から受信確認報告を行う。これは AM が確かに中継を行ったことを確認するために行われる。しかし、AL にとってこの報告処理によって何らかの利益がないと、AL が受信の報告を行わない可能性が生じる。[1] では、この問題に対して、HA から AM を中継した AL への配送に関して、事前に AL へ通常の数倍の請求額を設定するモデルを提案した。AL が受信報告を行えば、請求額は通常額に戻る仕組みとすることで報告の動機付けを生み出すことが可能となった。この手法を用いれば、確実に中継を行った AM に対して適当な報酬が保障される。ただし、この方法の枠組み内では AM の中継時の意図的なパケットドロップと、リンク上での意図しないパケットロスとを判別することが不可能であり、意図しないパケットロスが起きた場合、適切な AL への請求 / AM への報酬を与える仕組みが考慮されていなかった。

本稿では、第三者機関がクレジットの管理を行う手法において、AL の受信確認の報告に関する問題、意図的なパケットドロップと意図しないリンクロスにおける適切な処理に関する解決を図るため、文献 [1] に改良を加えた手法を提案する。

3 SHAKE におけるトラフィック中継促進機構

本章では、文献 [1] の問題であった下り通信時の AL の報告動機付け、意図しないパケットロスと意図的なパケットドロップとの判別を考慮した新たな手法を提案する。

文献 [1] で提案した第三者機関と同様の機能を有するクレジット管理機関 (Credit Server: CS) を導入する。CS は中継端末である AM への中継量に応じた報酬（クレジット）の支払いと、依頼端末 AL への請求を行う。支払われるクレジットの量は、中継したパケットサイズに比例させる。このクレジットは、換金可能あるいはプロバイダサービス上の優遇を得られるものとする。CS は、AM および HA からの転送報告 (Forward Report: FR) に基づき、請求・報酬の支払いを行う。CS, HA は完全に信頼における機関という前提に基づき設計されているものとする。

本提案手法では、上り通信においては従来手法と基本的に同じ動作を行う。下り通信時に関して機能の追加を行っている。AL にパケットが届いた場合、AL は HA と AM の両方へ受信報告 (Receive Report: RR) を新たに行うこととした。

この RR に基づき、HA に AL からの RR が送信されないと、HA は

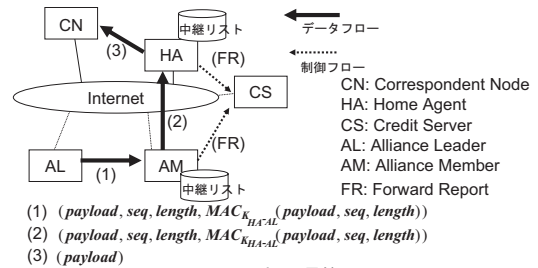


図 2: 上り通信

RR で報告されていない経路に対するトラフィック分配を停止する。このため、AL はパケットを受信しているにもかかわらず RR を送信しなければ、SHAKE を利用した通信の継続が不可能となるので、AL の報告送信に対する動機付けができる。また、AM, HA は RR をもとにして FR を送信するため、リンク上でロスもしくはドロップされたパケットに関しては、請求・報酬処理が行われないことを保障することができる。これにより、文献 [1] における下り通信時の AL の報告動機付け、意図しないパケットロスと意図的なパケットドロップとの判別に関する問題が解決される。

以下、SHAKE における上り通信時、下り通信時のクレジット処理動作について、詳しく説明する。

3.1 上り通信時の処理

概要

図 2 は、上り通信時のデータパケットの流れおよびクレジット処理に関するメッセージの流れを示している。2.1 節で、Mobile IP SHAKE では上り通信時、HA を経由しない方法と逆方向トンネリング (Reverse Tunneling) を用いて HA を経由する方法のいずれも可能であると述べたが、本稿では、HA を経由した方法のみを用いることを前提とする。これは HA を経由させることで、HA は AM の中継が確実に行われたことを確認することが可能となるためである。

AL から CN へ送られるデータパケットは、AL が自身の外部リンクを使ってこれを送らない場合、AL から AM, HA を経由して CN 届けられる。AM, HA はパケットを受信・転送後、転送報告書 (FR) を作成し、CS へ送信する。CS は、AM, HA からの FR を比較参照し、正しく照合されたパケットが転送に成功したパケットであると判断し、そのパケットに関して AM への請求、AL への報酬の支払いを行う。

AM, HA からの FR により、CS は AM が確かにパケットが中継しているのかを確認する。AM, HA どちらからかの FR がなかった場合、CS は転送が失敗していると判断し、クレジットの請求・報酬処理を行わない。

上り通信時のプロトコルの詳細

上り通信時のプロトコルの詳細を示す。上り通信時、AL から CN へのパケットは、AL HA CN の自身の外部リンクを利用した通信路と AL AM HA CN の AM を経由した通信路へ分配される。AL から直接 HA へ届けられるパケットに関しては、請求・報酬の処理は行われなため、新たな動作処理は行われない。以下、AM を経由した通信路でのクレジット処理を含んだプロトコルに絞って説明する。

鍵交換プロトコルにより HA と AM, HA と AL は、それぞれあらかじめ共通鍵 K_{HA-AM} , K_{HA-AL} を保持することを前提とする。以下、 $MAC_{K_{HA-AM}}$, $MAC_{K_{HA-AL}}$ は、それぞれ HA と AM, HA と AL のセッション鍵を用いた鍵付きハッシュ値によるメッセージ認証コード (MAC) を示す。また、AM, HA は AL のために中継を行ったパケットを記録する中継リストを持つこととする。

図 2 は上り通信時の転送プロトコルの動作概要である。以下、図 2 に従って動作を説明する。

- AL は、CN へ送信するパケットのペイロードに加え、シーケンス番号、パケット長、 $MAC_{K_{HA-AL}}$ を付加し、AM に分配・送信する (図 2(1))。
- AM は、AL から送られたパケットを受信し HA へ転送する (図 2(2))。転送後、AM はパケットの中継リストにエントリを追加する。中継リストのエントリには、パケット毎のシーケンス番号、パケット長、 $MAC_{K_{HA-AL}}$ に加え、 $MAC_{K_{HA-AM}}(seq. length, payload)$ の計算結果が含まれる。
- HA は、AM から転送されたデータパケットに付加された $MAC_{K_{HA-AL}}$ の値が正しいかどうかを、HA 自身が持つ K_{HA-AL} により (seq. length, payload) の鍵付きハッシュ値を求め、それと比較

(A) ALのReceive Report

請求先	報酬先	seq	length	$MAC_{K_{HA-AL}}$ (seq, length, payload)
AL	AM	150021	1500	sdfiou3...ew
		150022	1500	eew3w5...er

(B) AM, HAのForward Report

上り (0) or 下り (1)	請求先	報酬先	seq	length	$MAC_{K_{HA-AM}}$ (seq, length, payload)	$MAC_{K_{HA-AL}}$ (seq, length, payload)
1	AL	AM	150021	1500	sd3asfasf...dsf	sdfiou3...ew
			150022	1500	dsafasf23...5d	eew3w5...er

図 3: 報告書の例

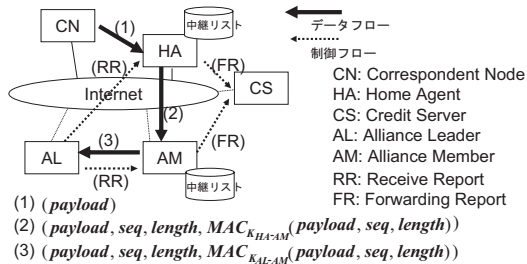


図 4: 下り通信

することで検証する。正しくなかった場合、そのパケットは破棄される。正しいと判断された場合、HA は CN へデータパケットを転送する (図 2(3))。転送後、HA はパケット中継リストに、パケット毎のシーケンス番号、パケット長、 $MAC_{K_{HA-AL}}$ 、 $MAC_{K_{HA-AM}}$ のエントリを追加する。

- AM, HA は定期的あるいは決められた量の中継リストエントリがたまった段階で、それぞれの中継リストを転送報告 (FR) として CS へ送信する (図 2, 図 3(B))。
- CS は AM と HA からの FR の内容を比較する。CS は正しく照合されたパケットを請求・報酬対象とし、パケット転送量に応じて AL へのクレジット請求および AM への報酬の支払いを行う。

3.2 下り通信時の処理

概要

図 4 は、下り通信時のデータの流れおよびクレジットに関するメッセージの流れを示す。データパケットは CN から HA, AM を経由して AL に届けられる。AM を経由して転送されたパケットが AL まで届けられると、AL は HA および AM に対して受信報告 (RR) (図 3(A)) を送信する。RR は、パケット毎のシーケンス番号、パケット長、HA-AL の共通鍵による MAC を含む。AM, HA は自身で管理している中継リストと RR をもとにして、転送報告 (FR) を作成し、CS へ送信する。CS は、AM・HA からの FR を比較し、確かに転送されたパケットを確認し、AL への請求と AM への報酬の支払い処理を行う。

下り通信時のプロトコルの詳細

図 4 に下り通信時の転送プロトコルを示す。以下、図 4 に従ってプロトコルの動作を説明する。

- CN が AL に向けてデータパケットを送信する (図 4(1))。
- HA は受信したパケットから、そのセッションのシーケンス番号を生成し、パケット長、 $MAC_{K_{HA-AM}}$ を付加して AM へ転送する (図 4(2))。HA はこの転送後、転送したパケットのシーケンス番号、パケット長、 $MAC_{K_{HA-AM}}$ に加え、 $MAC_{K_{HA-AL}}$ (seq, length, payload) の計算結果からなるエントリを中継リストに追加する。
- AM は受信したデータパケットを K_{HA-AM} を用いて認証し、確かに HA からのデータであることを確認する。そして、AL と AM の共通鍵 K_{AL-AM} を用いて MAC を計算し、それを付加して AL へ転送する。AM は転送後、転送したパケットのシーケンス番号、パケット長、 $MAC_{K_{HA-AM}}$ からなるエントリを中継リストに追加する。
- AL は確実に受信したパケットに対して RR を作成し、HA と AM へ返信する。RR は図 3(A) のようにパケット毎のシーケンス番号、パケット長、 $MAC_{K_{HA-AL}}$ のエントリを含んだリストとなる。
- AM, HA は RR と自身で保持する中継リストから、CS への FR を作成し、それを CS へ送信する。FR の内容は、パケットのシー

ケンス番号、パケット長、 $MAC_{K_{HA-AL}}$ 、 $MAC_{K_{HA-AM}}$ のエントリを含んだリスト (図 3(B)) となっている。

- CS は報告を受けた AM と HA の FR を比較し、正しく照合されたパケットが転送に成功したパケットであると判断し、そのパケットのみ請求・報酬対象とし、パケット転送量に応じて AL へのクレジット請求および AM への報酬の支払い処理を行う。

3.3 CS・HA による不正検出機構

CS および HA は、AL, AM による不正を検出するため、以下の処理を行う。

CS の動作

CS は、インターネット上にいくつか存在することとする。相互で定期的に交信を行い、利己的な動作を行うノードの取り締まりを行う。具体的には、クレジットの支払いの拒否を行うノードや、転送を行っていないにもかかわらず報酬を要求するようなノードを記録し、その情報を CS 同士で共有する。また、その情報をすべてのノードが参照可能とし、Alliance 構築時の指標として利用する。

HA の動作

Mobile IP SHAKE において、HA および AL は、AM の通信資源、リンク状態に応じて、各 AM への分配率を動的に調整し通信速度の向上を図っている。下り通信時には、AL は RR を HA へ送信することとしているが、HA は AL からの RR が一定時間届かない場合、HA-AM 間、AM-AL 間のリンク上で何らかの異変が起きていると判断し、その経路への分配の停止を行う。

4 検討

4.1 AL の不正行為

以下、AL の不正行為に対する提案方式の耐性について考察する。

1. AL の支払い不履行

不正内容

AL が、AM に中継を行ってもらったにもかかわらず、CS からの支払い請求を拒否する。

解決方法

CS は、AL が支払いに拒否した場合、その AL を支払いを拒否したノードとして記録し、この情報を他のノードに向けて公開する。支払いを拒否することによって、今後 SHAKE を利用する上で他のノードから信頼を得ることができなくなる。ノードが信頼を失うと中継依頼を拒否されるなど、SHAKE 利用に関して不利となるので、この仕組みによって AL の支払い不履行を抑制することが可能である。

2. AL の不正な MAC 送信

不正内容

上り通信時に、AL が不正な MAC を AM, HA に送信する。

解決方法

上り通信時に、AL は、 $MAC_{K_{HA-AL}}$ をパケットに付加して送信する。その MAC が正しいかどうかは、これが AM に届けられた時点で AM は確認できないが、HA において検証可能である。MAC が不適合であると判断されると、HA はそのパケットを破棄する。もし AL が不正な MAC を作成した場合、通信相手にデータを届けることが不可能となる。ゆえに AM は不正な MAC を送信しないこととなる。

3. AL の RR 送信不履行

不正内容

下り通信時に、AL が AM を経由してパケットを受信していないと偽り、RR を送信しない。AL がクレジットの支払いを逃れようという行為。

解決方法

3.3 節で述べたように HA は RR が返ってこない経路への分配を停止する。AL が不正に RR を送信しない場合、自身の行為により通信性能が悪化することとなるので、RR 送信の不履行は防止可能である。

4. AL の不正な RR 送信

不正内容

下り通信時における AL による不正な RR の送信として、HA と AM への RR が共に不正である場合と、HA と AM への RR が

異なっている場合が考えられる。RR が不正であるということ、HA では検証可能であり、AM では検証不可能である。そのため、問題となりうるのは HA へは正しい RR を送り、AM へは不正な RR を送信する場合である。

解決方法

HA と AM で AL から受け取った RR が異なっているかどうかは、CS において HA と AM からの RR をもとに比較されなければ判断できない。CS において HA と AM で RR が異なっていると判断された場合、CS は不正な RR を送信したノード (AL) の情報を記録し公開する。AL の支払い不履行の時と同様、これは AL の今後の SHAKE 利用に関して不利に働く。この仕組みによって AL の不正な RR 送信を防止可能である。

4.2 AM の不正行為

以下、AM の不正行為に対する提案方式の耐性について考察する。

1. AM の不当な報酬要求

不正内容

AM が、転送していないデータに関して報酬を要求する。

解決方法

AM が報酬を受け取るには、CS へ転送報告 (FR) を行う必要がある。この FR を作成する際には、AM が作成不可能な HA-AL の共通鍵による MAC が必要となる。この MAC は、上り通信時には AL からのパケットに付加され、下り通信時には RR によって AL から AM に送られる。したがって、AM が FR を偽造し、不正な報酬を要求することは不可能である。

2. AM の中継時のパケットドロップ

不正内容

依頼を受けたデータの中継を行わず、パケットを意図的にドロップする。

解決方法

AM は、中継依頼されたパケットを意図的にドロップすることが容易に可能である。ただ、HA または AL にパケットが届かなければ、AM が報酬を受け取るとは前項で述べた通り不可能である。パケットロスが続いた場合、HA または AL は、その経路にはパケットの分配を行わないこととしているため、たとえ AM がパケットドロップしたとしても通信性能への影響も少なく、請求・報酬の処理も行われず。したがって、AM の中継時に意図的にパケットドロップが行われていても、実用上の問題は発生しないと考えられる。

4.3 第三者による不正

本方式は HA が完全に信頼できる機関であるという前提に基づき、設計を行っている。すべてのデータが HA を経由するという特徴により、多くの不正行為を防止可能となる。特に Alliance と関係ない第三者との共謀による不当な策略にも問題なく対応可能となる。

例えば、AM が第三者と共謀し不当に報酬を受け取ろうと考えたとしても、HA はその第三者の存在を認証できなければ、FR を作成しない。すべてのパケットが HA を経由し、HA はその通信に携わったノードの認証を行っているため、不当な報酬獲得は不可能である。

4.4 意図しないパケットロスによる影響

通信中では、中継端末の意図的なパケットドロップだけでなく、意図しないパケットロスが起りうる。それぞれ上り通信、下り通信の場合を考える。パケットロスによる通信性能への影響ではなく、パケットロスにより不当な請求 / 報酬が起りえないかを考察する。

上り通信

● AL AM 間のパケットロス

AM へパケットが届かないのであれば、AM による中継処理は行われず、AM が報酬を受け取ることも、AL が請求を受けることも不可能であるので問題は起らない。

● AM HA 間のパケットロス

AM が確かに転送したとしても、AM-HA 間でパケットロスしてしまえば、HA にパケットが届かないこととなる。HA に届かなければ、AM は確かに転送を行ったにもかかわらず、報酬を受け取れないこととなる。ただ、提案手法は転送が成功して初めて AM が報酬を受け取れる仕組みとしているので、AM-HA 間のパケットロスにより報酬の支払いに関する矛盾はおきかない。

● HA CN 間のパケットロス

この場合、AL から CN へのパケットは宛先ノードである CN へパケットが届かないこととなる。しかし、経路上の中継端末 AM が HA へ確実に転送している場合には、AL はその AM へ報酬を与えなければならない。この場合、AM が HA へのパケット転送に成功したことを確認できるので、この報酬の支払いに関する矛盾はおきかない。

下り通信

● CN HA 間のパケットロス

● HA AM 間のパケットロス

上記 2 つの場合ともに、AM にパケットが届かなければ、クレジットの請求・報酬の支払いは起りえない。いずれのパケットロスも問題とならない。

● AM AL 間のパケットロス

AM が AL へ確かに転送を行ったとしても、この場合、AM による意図的なパケットドロップであるのか、意図しないパケットロスであるのかを判別できない。ただし、本提案方式では、AM の転送が成功しているかを確認できれば報酬を与えない仕組みとしている。したがって、AM AL 間でパケットロスが起きた場合、不正に AL に請求がされることがないため、クレジットの支払いに対する矛盾は発生しない。4.2 節に述べた通り、AM の意図的なパケットドロップに対しても実用上の問題はない。

4.5 オーバヘッド

SHAKE は、複数経路を同時に利用し通信性能の向上を目指した仕組みである。クレジット操作のオーバヘッドが、通信性能向上分に対して十分小さいことが求められる。

通信中は、HA と AM、HA と AL は計算コストの少ない共通鍵による認証を行っているため、通信性能への影響は少ない。AM、HA による CS への FR 送信において、パケット毎ではなく、数パケット分をまとめて送ることで通信性能への影響を減らすことができる。

クレジットに関する動作により、HA の処理は増大する。HA の処理としては、データパケットの転送処理に加えて、下り通信時には共通鍵によるハッシュ値の作成、上り通信時には鍵付きハッシュ値の検証、下り・上りともにそれらのハッシュ値を基にした FR の作成が追加されている。クレジットの処理に関しては、CS を導入しそちらに処理を集中させることで、HA の負担を減らしている。しかし、追加された処理によるデータパケットの転送処理への影響を最小限にとどめたい。これらの処理オーバヘッドに関しては今後シミュレーション等によりその影響を評価する予定である。

5 まとめ

本稿では、通信回線共有方式において中継処理を行う移動ノードに中継を行うモチベーションを持たせるため、中継量に応じた対価を与える仕組みを再検討した。提案手法は、クレジット管理機関 (CS) を導入し、確実に転送を行った端末に適切な報酬を与え、転送を依頼した端末にはその支払いを請求する。従来提案されていた手法では、意図的なパケットドロップと意図しないパケットロスが起きた場合、それらを判別し適切な処置が行う点が考慮されていなかった。本提案方式では、受信端末からの受信報告 (RR) を新たに取り入れ、中継端末はその RR を基に作成した転送報告書 (FR) を CS へ送信することで、パケットロス・ドロップの際の不適切な請求・報酬処理の問題を解決した。また本提案手法を用いることで、受信端末、中継端末が不正行為を働いたとしても適切な処理がなされることを示した。

今後は、提案手法を実装し、有効性を定量的に評価する予定である。

参考文献

- [1] 伊藤陽介, 峰野博史, 石原進, “通信回線共有方式における公平性に関する検討,” 2004-MBL-28 (20), Vol.2004, No.21, pp.147-154, 2004.
- [2] 伊藤陽介, 小山健二, 太田賢, 石原進, “Mobile IP を用いた通信回線共有方式の実装,” DICO2003 シンポジウム論文集, Vol. 2003, No. 9, pp. 97-100, 2003.
- [3] L. Buttyan and J.-P. Hubaux, “Enforcing Service availability in mobile ad-hoc WANS,” in: proceedings of the IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), 2002.
- [4] S. Zhong, Y. R. Yang, and J. Chen, “Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad Hoc Networks,” In Proceedings of INFOCOM. IEEE, 2003.