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

2004－MBL－28　(20)
2004／3／5

通信回線共有方式における公平性に関する検討

伊藤陽介[†1]　石原進[†2]　峰野博史[†3]
高橋修[†4]　水野忠則[†3]

筆者らは無線環境等において高速，高品質な通信を行う手法として通信回線共有方式 SHAKE(SHAring multiple paths procedure for a cluster networK Environment) を提案している．SHAKE では，複数の端末が一時的な短距離高速ネットワークを構築し，各端末がもつ外部リンクへの通信路を複数同時に利用することにより，高速な通信を可能にする．SHAKE の実現上，協調した端末にデータを中継してもらう必要がある．しかしデータを中継するには，バッテリ，CPU 等の無駄な消費が生じるため，協調端末へ中継を促すようなインセンティブが必要であった．本稿では，中継のインセンティブとしてクレジットを導入する．中継端末と依頼端末間の二者間でのクレジット交換方法と，信頼できる第三者機関を介したクレジット交換手法を提案し，有効性を検討する．

Study on Fairness in Multiple Wireless Links Sharing Systems

Yosuke Ito,[†1] Susumu Ishihara,[†2] Hiroshi Mineno,[†3] Osamu Takahashi[†4]
and Tadanori Mizuno[†3]

We have proposed a system that uses multiple links in alliance with neighbour nodes and increases communication speed. Using multiple links simultaneously as being established a temporary network by neighbour nodes by short-range wireless link, the system disperses data traffics and enables high-speed and high quality communication even in wireless environment. In this system, data packets have to be relayed by alliance nodes. However alliance nodes might not relay data packets without profits. We introduce credit to give an incentive to alliance nodes to relay packets. We propose two methods to exchange credit between relay nodes and a client node. One is two-sided credit exchanging, and another is credit exchanging that is helped by trusted third party. We discuss efficiency of these methods.

1. はじめに

近年，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は多い．現在の無線通信環境では，短距離間通信であれば無線 LAN や Bluetooth により比較的高速な通信が可能である．しかし，長距離の通信を行う際，2G/3G の携帯電話や PHS では無線 LAN 等に比べて低速な通信となってしまう．時や場所を選ばず高速なインターネット接続を維持するためには，遍在するネットワーク資源を積極的に，効率的に利用する必要がある．

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することで，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)[1] を提案している．SHAKE では，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）を構築し，クラスタ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 による通信を行うためには，別のメンバのためにパケットを転送するノードが必要になる．転送にはバッテリ，メモリ，CPU 等の消費が必要となるので，ノードには他のノードのためにトラフィックの転送を行うモチベーションが必要である．また，自身のために他ノードに大量のトラフィック転送を望む一方で，他人のトラフィックの転送を拒むといった利己的なノードの出現を考慮する必要がある．

本稿では，SHAKE においてそのような問題を解決するため，中継ノードにインセンティブを持たせる手法を提案し，その有効性について議論する．

以下本稿の構成を述べる．第 2 章では通信回線共有方式 SHAKE の概要について説明し，公平性の観点から課題を明らかにする．第 3 章では公平性を保つための手法の提案をし，そのアーキテクチャを示す．第 4 章では提案手法を適応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．

†1 静岡大学大学院理工学研究科
Graduate School of Science and Technology, Shizuoka University
†2 静岡大学工学部
Faculty of Engineering, Shizuoka University
†3 静岡大学情報学部
Faculty of Information, Shizuoka University
†4 NTT ドコモ　マルチメディア研究所
Multimedia Laboratories, NTT DoCoMo, Inc.

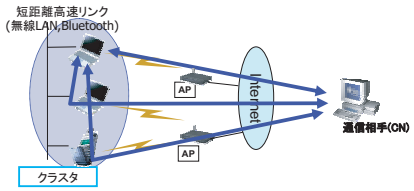

図 1　SHAKE を利用した通信

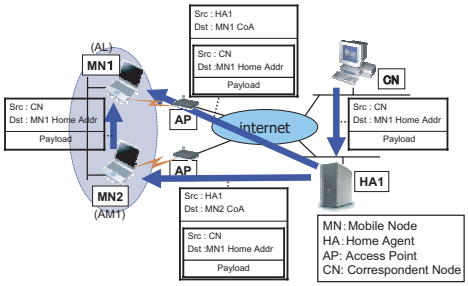

図 2　Mobile IP SHAKE によるデータグラム配送

2.　通信回線共有方式 SHAKE

本稿では，通信回線共有方式において，ノードの中継にインセンティブを持たせる方法を検討する．本章では，通信回線共有方式の概要を示す．

通信回線共有方式 SHAKE では，**図 1** のように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）を構成する．クラスタの内でも，特定の通信に携わる端末群を alliance（アライアンス）と呼び，そのアライアンスでデータを受信する端末を Alliance Leader (AL), データを中継する端末を Alliance Member (AM) と呼ぶ．

アライアンス内の端末がアライアンス外部の端末と通信を行う際に，各端末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．またアライアンス内の端末は自分の外部リンクが利用不可能な場合でも，他のアライアンス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．

SHAKE ではこれまで，アプリケーション層，TCP 層や IP 層において実現が検討されてきた．本稿で提案する手法については，Mobile IP を応用した IP 層における実現手法 Mobile IP SHAKE[2] での動作を前提として話を進めるが，他の SHAKE の実現手法においても適応可能である．

2.1　Mobile IP SHAKE

SHAKE を IP 層で実現するためには，アライアンス外部にいる通信相手 (Correspondent Node: CN) からアライアンス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．この分配ホストがアライアンス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 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 2 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 とともにアライアンスを構成している移動端末 MN2(AM: Alliance Member) の CoA 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（下り通信）には，AL および AM にパケットをカプセル化して分配する．AM は届けられたパケットのカプセル化を解除し，アライアンス内のリンクを通して，AL にパケットを転送する．

クラスタ内部から外部リンクへパケットを分配させるため，AL でもトラフィックを分散させる機構が必要となる．なお，AL にてパケットを AM へカプセル化して分配する．クラスタ内部から外部への通信を行う場合（上り通信），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，外部からクラスタへのデータ配信を「下り通信」，クラスタ内部から外部へのデータ配信を「上り通信」と表す．

2.2　通信回線共有方式における課題

SHAKE による通信を行うためには，移動する先々で協調動作を行う必要がある．協調関係にあるメンバ同士は信頼性・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[3]．

SHAKE では，他の端末のトラフィックを中継しなければ成り立たない．中継ノードは他人のために負荷を受けることとなるため，中継を行うためのインセンティブが必要である．そこで SHAKE において以下のように公平性を定義する．公平性が保たれているとは，「SHAKE において他のノードのためにパケットを中継したノードは，その転送量に応じた対価を得ることができ，パケットの転送を依頼したノードはその対価を転送ノードに支払わなければならない」状態を指す．

この公平性は以下のような利己的なノードの存在により，破られる可能性がある．

- 中継を行ってもらったにもかかわらず，その対価を支払わないノード
- 中継を行っていないにもかかわらず，偽って中継の対価を求めるノード

本稿では，これらの問題を解決しつつ中継端末へパケット転送のためのインセンティブを与える方法について議論する．

2.3 関連研究

モバイル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研究がいくつか提案，評価されている．

文献 4), 5), 6) では，アドホックネットワークにおいて，他ノードのためにデータを中継する端末に報酬を与えている．これらの文献では，nuglets と呼ばれる仮想的な貨幣を使用し，パケットの転送を行うことにより仮想的な貨幣という報酬を与えている．中継を依頼したノードは nuglets をいくらか失い，中継ノードは nuglets を獲得できる．4), 5) では nuglets を交換するモデルとして 2 つの方法（Packet Purse Model, Packet Trade Model）を提案している．Packet Purse Model では，パケットの送信元はパケットに nuglets を搭載して送信する．中間ノードは転送する際にいくらかの nuglet を獲得する．一方，Packet Trade Model では，各中間ノード間で nuglets の売買をする．各中間ノードは前のノードからパケットを購入し，次ホップのノードに高く売る．それを繰り返し，受信先ノードが総コストを支払う設計となっている．文献 6) では，単一ノード内のクレジットカウンタによる新しいスキームを提案している．このスキームではバッテリ残量とクレジット残量の履歴を保存しており，4 つのルールにより他人のパケットを転送を行うか，自身のパケットを送信するかを決定し，その動作により自身のクレジットカウンタを操作する．これらはすべて各ノードの nuglets で正確な量の操作を保証するため，耐タンパのハードウェアを導入している．また，隣接ノードの通信を確認する方法として，5) では，次ホップノードからの確認応答が確認されなければ，nuglets の量を増加できないこととしている．

Zhong らは集中管理機関を設置することで，アドホックネットワークにおいて同様に charging/rewarding に関するプロトコルを提案している[7]．アドホックネットワークにおいて，送信元から受信元までのパス上の中間端末は，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，パケットの送信元への請求と中継ノードへの報酬を与えている．偽りの報告を防ぐために，送信元ノード，中継ノード，管理機関でそれぞれデジタル署名による認証を行っている．

2.4 SHAKE における中継ノードへのインセンティブ付与に関する問題

SHAKE において中継ノードへインセンティブを与える場合の問題点を以下に述べる．

- AM 間の通信資源の差異

  AM の外部リンクはすべてのノードで均一とは限らない．Mobile IP SHAKE では，HA でデータを分配する際に，各 AM 間とプローブパケットによりリンク遅延を計測し，それに基づいて最適経路へパケットを振り分けている．よって，AM の外部リンクの状態により，AM が受信，転送するパケット量は異なる．転送量の違い，つまり AL への貢献度により報酬に違いを出す必要がある．
- 利己的なノードの存在

  以下のような利己的なノードの存在も考慮しなければならない．
  - AL として動作していたが，自分の通信終了後，他ノードのための中継を行わずに即座にアライアンスから離脱してしまうノード
  - AM として参加しているが，意図的なパケットドロップを行う悪意のあるノード

本稿では，上記のそれぞれの問題を解決しつつ中継ノードにインセンティブを与える手法を提案する．

3. SHAKE における公平性管理

3.1 クレジットの導入

SHAKE において各ノードに中継を促すために，中継ノードへインセンティブを与える．インセンティブとしてクレジットを導入したモデルを提案する．各ノードは，中継の対価としてクレジットを受け取り，他のノードに中継を依頼するためにはクレジットが必要となる．基本的なルールを以下に示す．

- AL は，AM にパケットを中継してもらうためにパケットサイズに比例したクレジット量を必要とする．
- AM（中継ノード）は，中継したパケットサイズに比例したクレジット量を AL から獲得する．

クレジットの量は，パケットサイズ L_P に対し，パケットサイズに比例した量 aL_P とする．

AL は，クレジットを保持していなければ，AM に中継を依頼することができなくなり．クレジットを獲得するためには他のノードのためにパケットを中継しなければならない．これにより，AM には中継することに対する動機付けが行われ，AL は自身のパケットを依頼するばかりでなく，他人からのパケットの転送することとなる．

クレジットを交換する手法として以下の 2 つのモデルを提案，検討する．

- 耐タンパのハードウェアを用いた二者間でのクレジット交換モデル
- 信頼できる第三者機関（クレジット管理機関）を導入したクレジット交換モデル

3.2 二者間でのクレジット交換モデル

3.2.1 基本概念

AL と AM 間でクレジットの交換を行う．AL は AM にパケット毎にパケットサイズに比例したクレジット量 aL_P を支払う．

クレジットを交換する方法としては，クレジットをパケットに搭載して送信する手法[4] を SHAKE 用に拡張する．

3.2.2 従来方式との変更点

文献 4) は無線アドホックネットワークを前提とした環境での提案手法である．4) での想定環境と SHAKE の環境では大きな違いが生じる．まず，2.4 節に示されている

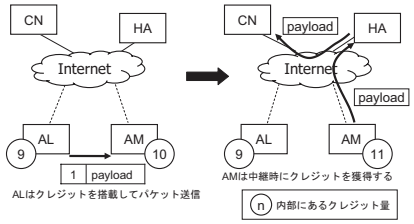

図 3　上り通信時のクレジット交換

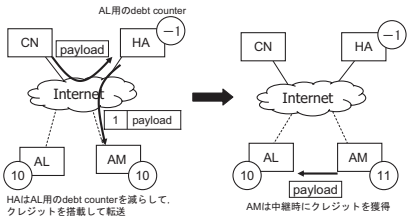

図 4　下り通信時のクレジット交換

ように，SHAKE では AL,AM の持つ通信資源は均質ではなく，中継データ量に違いが生じうる．加えて，AM の中継の確かさを確認する方法，および SHAKE における HA を介した下り通信，上り通信にてどちらにおいても適応可能なモデルを考慮する必要がある．以下に各々に関して説明する．

AM 間での通信資源の不均質性　従来手法では，パケット・メッセージ単位で課金している．しかし SHAKE では，AM 間で通信資源に違いがある場合，AM により中継データ量が異なる．そこで，AM の中継データ量に応じた報酬を与えるように拡張する．AM 間で通信資源に違いがある場合，AM により中継データ量が異なる．パケット・メッセージ単位で課金するのなら従来手法にて適応可能であるが，AM の中継データ量に応じた報酬を与えるように拡張する．

AM における中継の信頼性　無線アドホックネットワークでは，中間パケットが確かに中継するかどうかを送信元ノードが中継ノードの送信パケットをモニタすることによって可能である．しかし，SHAKE では，アライアンスを無線 LAN 等で構成しつつ，外部とは PHS, PDC, 3G セルラ等で通信することを想定している．このような条件では，AM が確かに転送しているかどうかを AL が直接モニタすることは困難である．そこで，SHAKE での上り通信時に HA を経由する手法を用いることとする．AM が確かに転送したかどうかは，HA が確認を行う．下り通信時には，AL が AM からの転送を確認する．また，AL, HA にて AM が中継を行う信頼性を管理し，中継を行わないノードを排除する．

上り通信，下り通信の両方への対応　従来研究のモデルでは，データの送信元がクレジットの支払いをすることとしている．しかし，SHAKE では上り通信時（AL が送信元），下り通信時（AL が受信先）のともに AL が請求されるべきである．AL が送信元，受信先，どちらの場合も AL にクレジットが請求されるモデルを提案する．

3.2.3　クレジット交換の概要

以下に，クレジット交換の概要を述べる．

■上り通信 (AL → AM → HA → CN)

上りの通信をする際のイメージ図を**図 3** を示す．AL はデータパケットのヘッダ部分にクレジットを付加して送信する．AM は中継時に，パケットからクレジットを取り出す．AM は，もし AL からのパケットにクレジットが付加されてなかったら，パケットの中継は行わない．なお，図 3 では，搭載するクレジット量を 1 と仮定しているが，実際の搭載クレジット量はパケットサイズにより異なる．

■下り通信 (CN → HA → AM → AL)

下りの通信の場合 (**図 4**)，CN からのパケットは HA を経由して AM に届けられる．HA でクレジットを付加して，パケットを AM1 へ転送する．AM は，クレジットを獲得し，パケットを AL へ転送する．HA では，AL 用の debt counter を用意しており，後で AL とクレジット量の同期を図る．

3.2.4　ハードウェアモジュールの導入

AM がクレジットを獲得するためには，中継を本当に行ったことが AL によって確かめられることが重要となる．不正な AM がクレジットを獲得してデータの中継を行わないことを防ぐ必要がある．また，各ノードがクレジットカウンタを保持しているとすると，クレジット量が改竄される恐れがある．これらの問題を解決するため，4) と同様に耐タンパのハードウェアモジュールを導入する．耐タンパのハードウェア内でクレジットカウンタを管理することで改竄不可能とする．また，AM のハードウェアモジュールは，確かに中継が行われ成功したということを HA, AL より確認応答を受けてからクレジット量の増加が可能とする．

AL のハードウェアモジュール M_{AL} は，AM のハードウェアモジュール M_{AM} とあらかじめ公開鍵暗号アルゴリズム等により秘密鍵 $K_{AL,AM}$ を保持しておくことを想定する．

なお，本モデルでは HA は，AL および AM から見て完全に信頼できる機関であるということを前提とする．

3.2.5　転送プロトコル

以下，ハードウェアモジュールを導入した詳細な転送プロトコルを示す．

■上り通信

図 5 にパケット転送時の処理の流れを示す．AL は，データパケットにクレジット用のヘッダを付加する．このヘッダには，M_{AL} の識別子 ID_{AL}，M_{AM} の識別子 ID_{AM}，シーケンス番号 seq とクレジット量 C（クレジット量は，パケットサイズ（L_P）に比例した量 $n(L_P)$ である）と，それらにデータをハッシュ関数 h で計算したもの（$h(payload)$）を加えて秘密鍵 $K_{AL,AM}$ により暗号化されたもの (SHAKE

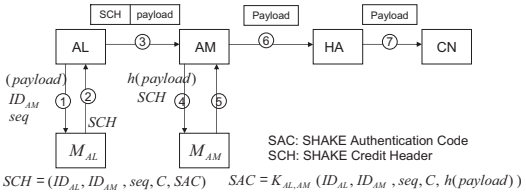

図 5 ハードウェアモジュールを用いた転送プロトコル（上り通信）

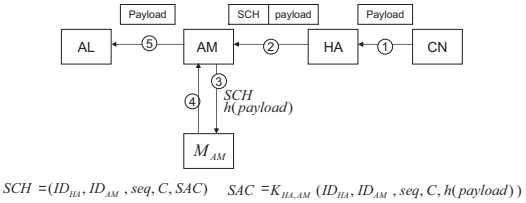

図 6 ハードウェアモジュールを用いた転送プロトコル（下り通信）

Authentication Code(SAC) と呼ぶ）を含む．以下，このヘッダを SHAKE Credit Header(SCH) と呼ぶ．

(1) AL はデータを送信する際に (*payload*)，ID_{AM}，seq 等を耐タンパハードウェア M_{AL} に渡す．

(2) M_{AL} は，受け取ったデータからクレジット量 C をパケットサイズより計算し，クレジットカウンタをその分だけ減らす．*h*(*payload*), ID_{AM}，ID_{AL}，*seq*, *C* から $K_{AL,AM}$ を用いて SCH を作成し，AL へ渡す．M_{AL} は，クレジットカウンタを *C* だけ減らす．

(3) AL は，受け取った SCH をデータに付加して送信する．

(4) AM はデータを受信すると，*h*(*payload*)，ID_{HA}，SCH を M_{AM} へ渡す．

(5) M_{AM} は，SCH の認証を行う．まず SCH 内のシーケンス番号を確認し，以前に受信していないことを確認する．これは再送攻撃 (Replay Attack) を防ぐための処理である．そして，SCH 内の ID_{AL}，ID_{AM}，*seq*，*C* を取り出し，*h*(*payload*) を加えて $K_{AL,AM}$ により新たに SAC の計算をする．計算した結果と SCH 内の SAC とを比べる．これらの内容が等しかった場合，確かに AL からのデータパケットであるということを認識し，搭載されたクレジット C を獲得し，クレジットカウンタを加算する．

(6) AM は AL から受信したデータから SCH を取り外し，残ったデータパケットを HA へ転送する．

(7) HA はデータを受信し，CN へ転送する．

■下り通信

図 6 は下り通信時の転送プロトコルである．CN からのパケットを HA が転送する際，HA が SCH を付加して転送する．HA にてクレジットを搭載する際には，HA 内の AL 用の debt counter を減少させる．HA と AL は，AM の更新等，頻繁に交信している．その際に HA は AL へ debt counter の量を通知し，AL は debt counter 分だけクレジットカウンタの量を減少させる．

(1) CN がデータを送信する

(2) HA がそのデータを受信する．パケットサイズよりクレジット量 C を計算し，AL 用の debt counter を減少させる．HA は ID_{HA}，ID_{AM}, *seq*，*C*，*h*(*payload*) と $K_{AM,HA}$ により SCH を作成し，データに SCH を付加して AM へ転送．

(3) AM はそのデータを受信すると，SCH, *h*(*payload*), ID_{AL} を M_{AM} へ渡す．

(4) M_{AM} は，*seq* を確かめ以前に受信したパケットでないことを確認する．*h*(*payload*) と SCH 内の ID_{HA}, ID_{AM}, *seq*，*C* と $K_{AM,HA}$ から新たに SAC を計算し，SCH 内の SAC と比較し確かに HA からのパケットであることを確認する．確認後，搭載されたクレジット量 C を獲得し，クレジットカウンタを加算する．

(5) AM は HA から受信したデータから SCH を取り外し，残ったパケットを AL へ転送する．

3.2.6 AM の信頼性の管理

AL, HA は連携して AM による中継を監視し，信頼できない AM を排除する．

上り通信では，AL からのパケットは AM を経由して HA に届けられる．このとき AM が AL からのパケットを受信すると，クレジットを獲得するにもかかわらずパケットを転送しない可能性が生じる．下り通信でも同様に AM がクレジットを獲得しつつパケットを転送しない可能性が生じる．この不正ノードを排除するために，HA は AM の信頼性の管理を行う．

AL, HA では，AM 経由で送信，到着したパケット数を管理し，定期的にそれらを照合する．不適合がおきた場合には，AM の信頼性評価値を下げる．

なおこの仕組みを実現するために，HA は，別の HA と評価値の情報を共有できるものとし，AL は HA に保存された AM の評価値をいつでも参照できることが必要である．また，AM の評価値は，以降のアライアンス構築時の判断基準とすることができるものとする．

3.3 信頼できるクレジット管理機関を導入したクレジット交換モデル

3.3.1 基 本 概 念

二者間でクレジットを交換する際には，ハードウェアモジュールを用いることで正確にクレジットを制御することが可能である．しかし，すべてのノードにそのハードウェアを設置する必要があり，コストがかかる．そこで，インターネット上の任意の位置にクレジットの集中管理機関を設置し，クレジットの管理機関がクレジットの支払い，報酬に関する管理を行うモデルを提案する．アライアンスの各ノードは，インターネットに接続可能であれば，この機関と通信可能である．この手法は文献 7) を基に，SHAKE で適用するために拡張を行った．拡張に関する考慮点は，2.4 節，3.2.2 節で述べられたものと同様である．

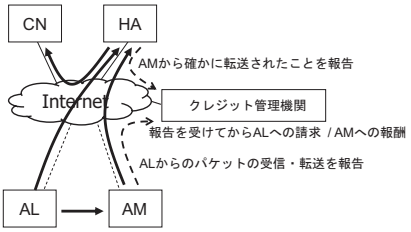

図 7 クレジット管理機関を導入したモデル（上り通信）

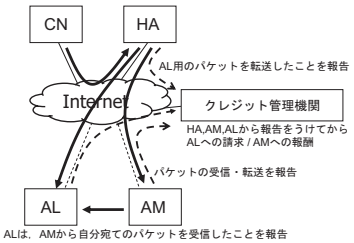

図 8 クレジット管理機関を導入したモデル（下り通信）

転送ノード AM がクレジットを獲得するためには，データの転送を行ったということを管理機関に報告する．その後，管理機関を経由してクレジットが AM に支払われる．この報告はデータ転送直後に行う必要はない．すなわち，AM は報告を行うまで自身のストレージにパケットの受領書を保存しておき，時間やバッテリ残量に余裕がある時等にいつでも行うことが可能とする．管理機関への報告には，AL のためのデータを受信，転送したことを意味する極微量のものを用いる．

なお，クレジット管理機関からのクレジット請求を拒絶したノードは，ネットワーク全体に通知され，そのノードは排除させられるものとする．

3.3.2 クレジット管理の概要

以下にクレジット管理の概要を示す．

■上り通信

図 7 はクレジット管理機関を導入した際の上り通信時の概念図である．上り通信時，AL からパケットが AM, HA を経由され CN へ届けられる．AM はパケットを受信した際に，パケットから受領書を作成する．その受領書をクレジット管理機関へ提出する．また，HA で AM が確かに転送したことを確認させるため，HA はパケットの受領書を作成しそれをクレジット管理機関へ提出する．

■下り通信

下り通信時のモデルを**図 8** を示す．CN からのパケットが HA，AM を経由して AL に届けられる．AM は上り通信時と同様にパケットの受領書を作成し，その受領書をクレジット管理機関へ提出する．下りでの通信では，AM の次ホップ端末が AL であるため，AL が AM が確かに転送したかどうかの報告をクレジット管理機関へ行う．しかし，AL はクレジットの支払い者である．AL は報告することで支払いの義務を負わされるため，クレジット管理機関への報告を行わない可能性が高い．この問題を解決するため，以下のような AL の報告を動機付けるモデルを提案する．

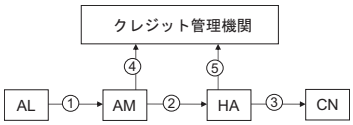

図 9 クレジット管理機関を導入したモデルでの転送プロトコル（上り通信）

CN からのパケットが HA へ到着すると，HA はクレジット管理機関へ AL 用のパケットが到着したことを報告する．すると，クレジット管理機関は，この時点で，AL への請求額として通常の ϵ 倍の額を保管しておく $(1 < \epsilon < 2)$. AM にパケットが到着すると，AM は受領書をクレジット管理機関へ報告する．AL にパケットが到着し，AL がパケットの受領書をクレジット管理機関へ報告したとする．すると，クレジット管理機関から AL への請求額は通常の額に戻る．しかしながら，もし AL が報告を行わなければ通常の ϵ 倍の額を請求されてしまう．この請求されたクレジットをクレジット管理機関が徴収し，AM は何も受け取らないものとする．ゆえに，AL はパケットを確かに受信したならば，クレジット管理機関へ報告を行うと考えられる．なお，AM からのパケット受領の報告がなかった場合は，クレジット管理機関での AL への請求はなくなる．

以下，クレジット量をパケットサイズ L_P に比例した aL_P として，状況による請求額を示す．HA は信頼できる機関であり，パケットを受領した際には必ず報告を行うと想定している．

- HA, AM, AL がパケット受領の報告を行った場合
  AL へのクレジット請求額：aL_P,
  AM へのクレジット報酬額：aL_P
- HA, AM がパケット受領の報告を行った場合
  AL へのクレジット請求額：ϵaL_P,
  AM へのクレジット報酬額：0
- HA, AL がパケット受領の報告を行った場合
  AL へのクレジット請求額：0,
  AM へのクレジット報酬額：0
- HA のみがパケット受領の報告を行った場合
  AL へのクレジット請求額：0,
  AM へのクレジット報酬額：0
- HA からのパケット受領の報告がなく，AM から受領の報告があった場合
  管理機関は AM が偽りの報告を行ったとみなす．
  AL へのクレジット請求額：0,
  AM へのクレジット報酬額：0

3.3.3 プロトコル詳細

AL はデータを送信する際にデジタル署名を行い，AM では AL からのパケットであることを，クレジット管理機関では AL 用のパケットの受領書であることを認証する．以下，ノード i の公開鍵を P_i, 対応する秘密鍵を S_i で表す．MD5，SHA-1 のようなメッセージダイジェスト関数

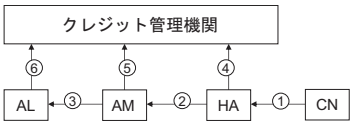

図 10 クレジット管理機関を導入したモデルでの転送プロトコル (下り通信)

を MD() と表す．またデジタル署名を $(sign_{P_i}, verify_{S_i})$ と表す．

■上り通信

図 9 に上り通信時の転送プロトコルを示す．

(1) AL は自身の秘密鍵 S_{AL} を用いて *payload* にメッセージダイジェスト関数をかけた結果，シーケンス番号，ID_{AL} をデジタル署名する．デジタル署名の結果を s とする（$s \leftarrow sign_{S_{AL}}(MD(payload), seq, ID_{AL})$）．
そして $(payload, seq, ID_{AL}, s)$ を AM に向けて送信する．

(2) AM は AL の公開鍵 P_{AL} を用いて受信したデータの署名を検証．確かに AL からのデータであることを確認する
（ $verify_{P_{AL}}((MD(payload), seq, ID_{AL}), s)$ ）．
そして $(payload, seq, ID_{AL}, s)$ を HA へ転送する．
また，署名から受領書を作成し，保存する．受領書は $(MD(payload), seq, ID_{AL}, s)$ とする．

(3) HA は P_{AL} を用いて受信したデータの署名を検証する
（$verify_{P_{AL}}((MD(payload), seq, ID_{AL}), s)$ ）．
検証後，$(payload)$ を CN へ転送する

(4) AM は受領書をクレジット管理機関に提出する．クレジット管理機関は AM からの受領書を P_{AL} を用いて検証する．
$verify_{P_{AL}}((MD(payload), seq, ID_{AL}), s)$

(5) HA も同様に受領書をクレジット管理機関に提出する．クレジット管理機関は HA からの受領書を P_{AL} を用いて検証する．検証後，AL へクレジットの請求をし AM へ報酬を与える．

■下り通信

図 10 にて下り通信時の転送プロトコルの概念図を示す．CN からのデータは，HA にてデジタル署名されてから転送され，AM を経由して AL に届けられる．HA, AM, AL で受領書を作成し，クレジット管理機関に提出する．

(1) CN がデータを送信する．

(2) HA は自身の秘密鍵 S_{HA} を用いてデジタル署名する．デジタル署名の結果を s とする（ $s \leftarrow sign_{S_{HA}}(MD(payload), seq, ID_{HA}, ID_{AL})$ ）．
それから HA は $(payload, seq, s, ID_{HA}, ID_{AL})$ を AM に向けて転送する．また，HA は受領書 $(MD(payload), seq, ID_{HA}, ID_{AL}, s)$ を作成し，保存する．

(3) AM は HA の公開鍵を用いて署名 P_{HA} を検証．確かに HA からのデータかを確認する
$verify_{P_{HA}}((MD(payload), seq, ID_{HA}, ID_{AL}), s)$.
$(payload, seq, ID_{HA}, IDAL, s)$ を AL へ転送する．
また署名から受領書を作成し，保存する．受領書は $(MD(payload), seq, ID_{HA}, ID_{AL}, s)$ となる．
AL へパケットが届くと，AL は P_{HA} を用いて同様に署名を検証し，受領書を作成する．

(4) HA は受領書をクレジット管理機関に提出する．クレジット管理機関は HA からの受領書を HA の公開鍵を用いて検証する．また，報告された受領書から，AL 用のパケットの受領書であることを確認する．
$verify_{P_{HA}}((MD(payload), seq, ID_{HA}, ID_{AL}), s)$.

(5) AM は受領書をクレジット管理機関に提出する．クレジット管理機関は HA からの受領書を P_{HA} を用いて検証する．

(6) AL は受領書をクレジット管理機関に提出する．クレジット管理機関は HA からの受領書を P_{HA} を用いて検証する．検証後，AL へクレジットの支払いを命じ，AM へ報酬を与える．

4. 検　　討

前述してきたモデルの有効性について検討する．

4.1 モデルの有効性

SHAKE において中継ノードへ報酬を与える場合，中継ノード間で不平等さが生じる可能性があることを 2.4 節等で述べた．以下，提案モデルを用いて，想定される問題へ対応可能であるかを示す．

- データを中継してもらったにもかかわらず，クレジットを支払わないノードの存在

ハードウェアを用いた二者間の交換モデルにおいて，パケットにクレジットを搭載させ，AM はクレジットが付加されていないパケットはドロップしてしまう．クレジットを支払わずにパケットを中継してもらうことは不可能である．

クレジット管理機構を導入した場合では，クレジット管理機関からの支払いを拒絶すると，そのことはクレジット管理機関から参照可能としネットワーク全体へ伝わることとしている．すると，支払いを拒絶するノードは，SHAKE を用いた通信は不可能となる．ゆえに，支払いを拒絶することはノード自身にとって有益なものではない．

- データ中継を行っていないにもかかわらず，不正に報酬を求めるノードの存在

二者間での交換モデルでは，データの送信元からクレジットが付加されて送られてくる．クレジットはパケットの送信元からのクレジットのみを獲得可能で，不正な報酬を請求することは不可能である．

クレジット管理機構を導入した場合では，上り通信の場合では HA が確かに AM から転送されたことをクレジット管理機関へ報告する．下りの場合であっても，

AL が AM から転送されたことを報告する．それぞれの報告がなければ AM は報酬を受け取れない．ゆえに中継を確かに行わなければ報酬は得られない．

- AM 間の通信資源の違い

  クレジットはパケットサイズに比例した量である．よって，AM はデータ転送量に比例してクレジットも増加されるため，AM 間で通信資源が異なっても問題にならない．

- 二者間での交換モデルにおける AM での意図的なパケットドロップ

  AM が意図的に転送しないでいると，AL はクレジットを失い続けることになり，AM は AL を破産させることができる．HA において AM の信頼性評価モデルを導入することで，この問題に対処させる．上り通信を例に考えると，AL からのパケットは AM を経由して HA に届けられる．AL と HA は定期的に交信することが可能となっているので，HA は届くはずのパケットが AM から届いていないことを確認できる．AL はその情報より AM へはパケットを送信しないこととなる．また，HA にて AM の信頼性評価値を下げ，インターネット上の別の HA に情報を通知させることが可能となる．AM にとってそのようなことは有益ではないため，意図的なパケットドロップは減少されると考えられる．

- クレジット管理機関を導入したモデルでの，下り通信における問題点
  - AL がパケットを受信しているにもかかわらず報告を怠った場合

    AL はクレジットの支払い者であり，AM から確かにパケットが届けられても，管理機関に報告を怠る可能性があった．しかし，AL が報告を怠った場合，通常よりも多めにクレジットを請求されることとなるため，AL は正直に報告を行うこととなる．
  - AM がパケットを受信したが転送を行わずに，管理機関に受信の報告のみ行う場合

    AM は自身の報告だけでは報酬を獲得できない．管理機関にて AL からの報告があってから AM へ報酬は与えられる．AL へ転送せずに，管理機関に報告だけすることは，AM にとって全く有益ではなく，管理機関への報告に要する処理の分だけ無駄になる．そのため，このような問題はなくなると考えられる．

4.2 オーバヘッド

SHAKE に影響を及ぼすと考えられるオーバヘッドについて考察する．SHAKE は複数回線の同時利用により通信速度の向上を実現する仕組みであるので，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．

二者間の交換モデルについて考える．下りの通信時には，新たに HA の debt counter を利用して，クレジットの交換を行った．HA は AL に debt counter の量を知らせる必要があり，HA と AL 間の交信量が増えることとなる．しかし，debt counter の通知は SHAKE の利用時に特に行う必要はなく，SHAKE を用いた通信のスループットには影響を及ぼさない．

次に信頼できるクレジット管理機関を導入した場合を考える．デジタル署名を用いているため，データ量が増えるにつれシステムへの影響も大きくなる可能性が考えられる．クレジット管理機関に受領したことを報告する必要があるが，この報告はデータ通信中に行う必要はなく，時間的またはバッテリ残量に余裕があるとき等いつでも可能であり，SHAKE の通信には影響は及ぼさない．デジタル署名による影響を減らすため，数パケットの認証をまとめて処理すること，もしくは計算処理の速い共通鍵での認証を行うことでデジタル署名の処理に要するオーバヘッドを減少可能と考える．

5. ま と め

本稿では，通信回線共有方式においてノードにデータの中継を行うモチベーションを持たせるため，中継ノードにインセンティブを与えた．インセンティブにはクレジットを用いて，中継ノードと中継の依頼ノード間の二者間での耐タンパハードウェアを用いたクレジット交換モデルと，信頼できるクレジット管理機関を導入した交換モデルでの手法の検討を行った．それぞれの方式で，協調端末間で通信資源が異なる場合であっても，依頼人への貢献度に応じた報酬を受け取れる．また，不正ノードの存在やクレジット改竄といった問題をともに解決可能であることを示した．

今後は，シミュレーションにより提案手法の有効性を定量的に検証する予定である．

参 考 文 献

1) H. Mineno, S. Ishihara, K. Ohta, M. Aono, T. Ideguchi, and T. Mizuno, “Multiple paths protocol for a cluster type network,” Int. J. Commun. Syst., vol. 12, pp. 391–403, 1999.
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,” マルチメディア，分散，協調とモバイル（DICOMO2003）シンポジウム論文集, 情報処理学会シンポジウムシリーズ, Vol. 2003, No. 9, pp. 97–100, 2003.
3) 伊藤陽介, 峰野博史, 石原進, “通信回線共有方式における動的クラスタ管理に関する検討,” 情報学ワークショップ 2003 (WiNF2003), 2003.
4) 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.
5) L. Buttyan and J.-P. Hubaux, “Nuglets: a virtual currency to stimulate cooperation in selforganized ad hoc networks,” Technical Report DSC/2002/002, Swiss Federal Institute of Technology – Lausanne, 2002.
6) L. Buttyan and J.-P. Hubaux. “Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks,” ACM/Kluwer Mobile Networks and Applications (MONET), 8(5), 2003.
7) S. Zhong, Y. R. Yang, and J. Chen, “Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad Hoc Netoworks,” In Proceedings of INFOCOM. IEEE, 2003.