Vol.2010-MBL-52 No.13
2010/1/29

移動ネットワークにおける効率的な管理情報の収集制御方式

丸 山 貴 史[†1]　中 村 直 毅[†2]　Mansfield Keeni Glenn[†3]
菅 沼 拓 夫[†1]　白 鳥 則 郎[†1]

NEMO Basic Support プロトコルを用いる移動ネットワークでは，Mobile Router が移動することにより Mobile Router の配下のネットワーク全体が移動する．移動ネットワークにおいて遠隔から管理・監視を行う場合，通信環境が不安定であるため，収集する管理情報が経路途中で損失する問題が生じる．また，監視トラフィックが Mobile Router や Home Agent の通信帯域を占有し，他の通信に悪影響を与えてしまう問題も有している．そこで本稿では，これらの問題を解決するため，移動ルータにおいて一時的に管理情報をバッファリングし，監視トラフィックの配送を分散させる手法と SNMP メッセージの集約により監視トラフィックを圧縮する手法を提案する．評価実験を通して，提案手法が効果的に機能することを確認し，本提案の有効性を示す．

An Efficient Control Method of Information Collection for Management in Mobile Network

Takafumi Maruyama,[†1] Naoki Nakamura,[†2]
Mansfield Keeni Glenn,[†3] Takuo Suganuma[†1]
and Norio Shiratori[†1]

In mobile network where NEMO protocol is used, the movements of Mobile Router(MR)'s sub-network are caused by the movements of MR. But there are some existing problems regarding remote network management in mobile network. Due to unstable network environment, management information can be lost. In addition, monitoring traffic occupies the bandwidth of MR's and HA's network and affect the other traffic. In this paper, we propose two methods to solve these problems. In one method, buffering of the monitoring traffic is used at the MR to disperse it. In the other method, we aggregate the SNMP message to reduce the monitoring traffic.

1. はじめに

近年，従来からの固定的なインターネット接続環境に加え，いつでもどこでもインターネットに接続することが可能な，ユビキタス情報環境の実現のために研究開発が盛んに行われている．ユビキタス情報環境を実現するためには，シームレスなインターネット接続を可能とする MobileIP が重要な役割を果すと考えられる．この MobileIP を拡張した，NEMO(NEtwork MObility) Basic Support プロトコル [1] は，IPv6 に対応するとともに，個々の端末だけでなくサブネットワーク自体の移動が可能となるモビリティ機能を有しており，その実用化が期待されている．この NEMO を用いた移動ネットワークでは，ルータ自身が移動するため，モビリティ機能を持たない機器も移動ルータに接続することでモビリティを有することが可能となる．そこで，様々なモバイル機器がいつでもどこでもインターネットに接続されるようになる．したがって，これらの技術が社会インフラの基盤として利用される場合，従来より高度かつ正確な運用管理が必要であり，ネットワークの信頼性が担保されていることも必要となる．特に，移動ネットワークでは端末自体が移動するため，端末に関する情報を逐次損失なく収集・分析し，端末を追跡・監視できることが非常に重要となる．

一般にネットワーク管理では，標準技術である SNMP(Simple Network Management Protocol) [2] が用いられる．管理者 (マネージャ) は，管理情報を収集するため，管理対象 (エージェント) に SNMP プロトコルを用いてポーリングを行う．しかし，トランスポート層に UDP を使用しており，パケットの衝突などによって生じる管理情報の損失は考慮されていない．ゆえに，通信回線が不安定な無線通信を扱う移動ネットワークでは，移動端末から収集される管理情報の損失が顕著となる．この問題を解決するため文献 [3] では，エージェントが管理情報と取得時刻を合わせて蓄積し，収集する管理情報が損失した場合には，管理情報の再送を可能とする store-and-forward 型の収集手法を提案している．しかし，移動ネットワークでは，サブネットワークが移動すると，複数の端末で回線の切断・回復が同時に発生するため，回線の回復後に蓄積された管理情報が一斉に送信され，バースト的に送出されるトラフィックが増大する．この結果，特に帯域が狭い回線では，大規模な通信障害

†1 東北大学 情報科学研究科/電気通信研究所
GSIS, Tohoku University/Research Institute of Electrical Communication
†2 東北大学 医学系研究科
Tohoku University School of Medicine
†3 (株) サイバー・ソリューションズ
Cyber Solutions Inc.

が発生する．

そこで，本手法では，管理情報の損失を防止するとともに，監視トラフィックにより通信帯域が圧迫される問題を解決するため，監視トラフィックの送信タイミングを分散する (**提案 1: バッファリングによる監視トラフィックの流量制御手法**) と監視トラフィックを削減する (**提案 2:SNMP メッセージ集約による監視トラフィックの削減手法**) を提案する．**提案 1** の手法では，送出される監視トラフィック量を予測し，状況に応じて管理情報を移動ルータで一時的にバッファリングし，その流量を制御することで，監視トラフィックの送出を分散させる．また，**提案 2** の手法では，移動ルータに接続するノードからの管理情報を運ぶ SNMP メッセージを集約することで，監視トラフィック自体を削減する．

本論文の構成は以下の通りである．**2.** では，既存のネットワーク管理手法を移動ネットワークに適用した際の問題点と，関連研究について述べる．**3.** では，バッファリングを用いた監視トラフィックの流量制御手法を提案し，シミュレーションにより性能を評価する．**4.** では，SNMP メッセージ集約による監視トラフィックの削減手法を提案し，数値計算による性能評価を行う．**5.** では，提案する 2 つ手法の適用範囲について考察するとともに，2 つの手法の融合について考察する．最後に **6.** で結論を述べる．

2. 移動ネットワークにおけるネットワーク管理の問題

2.1 ネットワークモビリティプロトコルの概要

ネットワークモビリティプロトコルは，移動ノードである Mobile Node(MN) がネットワーク間を移動し IP アドレスが変更されても，トンネリングにより上位レイヤからその変更を隠蔽しセッションを維持する移動透過性と，MN の現在位置に関わらず通信相手が常に一定のアドレスで MN にアクセス可能となる常時発呼可能性を保証する．これらは Home Agent(HA) と Mobile Router(MR) によって実現される．HA はルータであり，MN の持つ常に不変のアドレス Home Address(HoA) と移動先ネットワークでのアドレス Care of Address(CoA) を管理し，通信相手である Correspondent Node(CN) より MN の HoA 宛へ送信されたパケットを CoA 宛に転送する．また，移動ルータである Mobile Router(MR) も HA に管理されており，自身に接続するノード Mobile Network Node(MNN) に一定のアドレスを提供するため，MNN はモビリティの機能を有していなくても，MR と共にサブネットワーク全体の移動と合わせて移動することができる．

2.2 既存の管理情報収集方式を用いた際の問題

移動ネットワークにおいてネットワーク管理を行う際，管理情報を時系列的に損失なく収集する store-and-forward 型の収集手法を用いた場合，監視トラフィックが大量に流れることにより，他の通常の通信に影響を与えることが予想される．

MR のネットワーク間の移動により，MR が上流のネットワークと接続されていない場合，MR に接続された MN は，管理情報を収集するマネージャとの間の回線が切断されているため，管理情報を送信することができない．その後，MR が上流のネットワークに再接続し回線が復旧すると，各 MN に蓄積した管理情報が一斉に送信される．管理情報は定期的に出力されるため，回線の切断時間が長くなると管理情報の蓄積量が増大する．さらに，MR が移動すると，複数の MN で回線の切断・回復が同時に発生するため，蓄積した管理情報が複数の MN から一斉に送信される．その結果，図 1 に示すように，バースト的に増大した監視トラフィックが MR のアップリンクの帯域を圧迫し，他の通常の通信に影響を与える．また，マネージャ・MN 間の通信は Home Agent(HA) を経由するため，増大した監視トラフィックが HA を通過し，図 1 に示すように HA に接続するノードの通信にも影響を与えるという問題が生じる．以上より，移動ネットワークで管理情報を収集する際は，監視トラフィックの増大への対策を講じる必要がある．

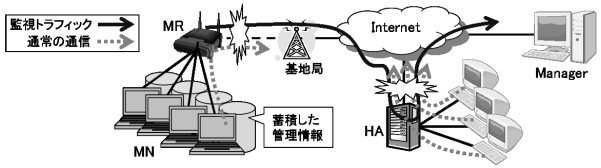

図 1 監視トラフィックが他の通信に影響を与える場合

2.3 関 連 研 究

監視トラフィック量が増大する問題を解決する手法として，監視トラフィックの送信を分散させる手法や監視トラフィック量を削減する手法が考えられる．

監視トラフィックを分散させる手法として，無線センサネットワークにおいては，輻輳制御手法が提案されている．文献 [4] では，ルーティングにより輻輳制御が行われているが，マルチホップ・マルチパス環境が必要であり，MR のサブネットワークへの適用は困難である．文献 [5] においては，パケットの種類やノードの差異により，優先すべきものと優先すべきでないものを分別することでトラフィックを制御しているが，管理情報の種類や移動ネットワークにおける各 MN に応じてでは差異を付け辛く適用が難しい．一方，文献 [6] で提案されている，ノードやネットワークの状態から輻輳を予測・制御する手法では，移動ネットワークでの応用が可能であると考えられる．

監視トラフィック量自体を削減する手法として，文献 [7] では，エージェントが自律的に一定間隔ごとにマネージャへ管理情報を送信する．この手法ではマネージャから送信されるリクエストの分だけ送受信されるトラフィックが減少するが，レスポンスによるトラフィックの増大には効果がない．また，文献 [8] では，エージェントは，管理情報に変更がある場合にのみ，マネージャに管理情報を送信することで監視トラフィック量を削減している．しかしながら，移動ネットワークのように接続状態が頻繁に変化する環境では，さほど改善効果が得られないと考えられる．

以上を踏まえ本稿では，MR での輻輳の予測・制御により監視トラフィックを分散させる手法を **3.** で提案し，また，環境や状況に左右されることなく監視トラフィックを削減する手法を **4.** で提案する．

3. 提案 1:バッファリングによる監視トラフィックの流量制御手法

3.1 提案手法 1 の概要

提案手法 1 では，他の通信への影響を軽減するため，MR で一時的に各ノードの管理情報をバッファリングさせ送信量を調整することで，監視トラフィックを一定の上限値以下に抑制する．そのため本手法では，MR で定期的に MN から管理情報を収集・蓄積し，マネージャからのリクエストには MN に代わって，MR がレスポンスを返す．その上で，MR とマネージャの間で (1)MR における管理情報の送信制御，(2)Home Agent 非経由ポーリングの処理を行う．(1) では今後の各時間に送信される監視トラフィック量を予測し，予測に応じて上限値を超えないよう管理情報を遅延・分割して送信する．また，(2) によりマネージャは MR へ直接ポーリングを行う．なお，流量制御は全て MR とマネージャの間で行われ，MN では特別な制御を行わない．よって，MN へは機能を追加する必要がなく，MN として様々なノードが使用できる．次に，(1)，(2) の処理の詳細について説明する．

3.2 (1) MR における管理情報の送信制御

3.2.1 監視トラフィックの予測

監視トラフィックを設定した上限値以下に抑制するため，今後流れるトラフィックの流量の予測が必要となる．MR では，表 1 に挙げたパラメータから，単位時間を 1[s] として各 MN が次にマネージャからのリクエストを受信する時刻 R'_x，その際送信する管理情報のデータサイズ S'_x を得る (x はノード番号)．R'_x は式 $R'_x = R_x + \gamma \times P_x$ により導出される．γ は現在時 $t_{now} < R'_x$ となる整数の最小値であり，最後にリクエストを受信した時刻から，γ 回分のリクエストの受信間隔だけ経過した時間が次にリクエストを受信する時刻 R'_x となる．また，S'_x は式 $S'_x = S_x \times \lfloor T/P_x + 1 \rfloor$ により導出され，T と P_x から切断時間中に何回分の管理情報が蓄積するか見積り，予測送信データサイズに反映する．

次に各 MN の R'_x と S'_x から，現在時 (t_{now}) 以降の各秒における予想送信データサイズを算出し，図 2 のように今後の各時間に MR から送信される監視トラフィック量を見積もる．例えば，図 2 中の表のように MN1・2・3 のリクエストの受信時刻 R'_x が $t_{ex}[s]$，その際送信する管理情報のデータサイズ S'_x が $d[bit]$ と算出されていたとすると，$t_{ex}[s]$ には $d \times 3 = 3d[bit]$ の監視トラフィックが MR から送信されると見積もれる．

3.2.2 管理情報の送信の調整による流量制御

予想監視トラフィック量の最大値 $M[bit]$ があらかじめ設定しておいた上限値 $L[bit]$ よりも大きい場合，M を L 以下に抑制するため流量制御を行う．図 2 に示す 6 つの箱の高さは，それぞれ各 MN が送信する管理情報のデータサイズに対応しており，これらを分割して，また送信タイミングを遅らせて，送信することにより $M \leq L$ の条件を実現する．そこで次の (A)・(B) の手順により $M \leq L$ とするための各管理情報の遅延時間・分割度を算出する．

(A) まずは遅延時間を算出し，同じ時刻に送信予定であるデータの送信タイミングを遅らせ分散させる．遅延時間の算出は次のように行う．図 3 に示すように同じ時刻に送信予定のデータにシーケンス番号 (n とする) を付けて，n に応じて異なる遅延時間 $D(n)[s]$ を与

表 1 R'_x・S'_x の算出のためのパラメータ

$R_x[s]$	最後に MN_x へのリクエストを受信した時刻
$P_x[s]$	直前 2 回の MN_x へのリクエストの受信間隔
$S_x[bit]$	最後に送信した管理情報のデータサイズ (送信した全種類の管理情報の合計)
$T[s]$	MR の上流のネットワークとの切断時間

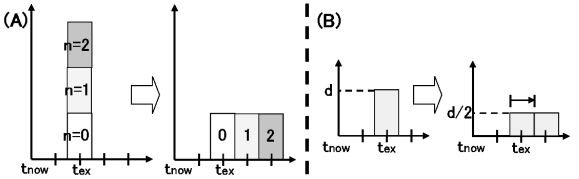

図 3 (A)・(B) の処理を適用した場合の変化

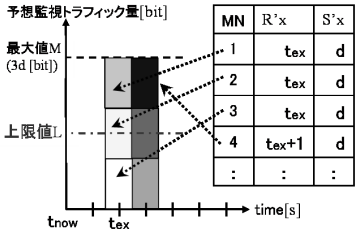

図 2 予想監視トラフィック量

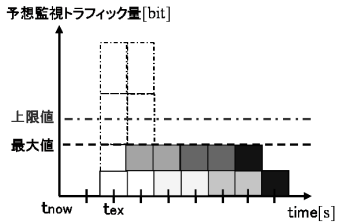

図 4 流量制御後の予想監視トラフィック量

える．$D(n)$ は式 $D(n) = mod(n, \lceil M/L \rceil + \alpha)$ により算出する．$\lceil M/L \rceil + \alpha - 1$ は遅延時間の最大値を表しており，α の初期値を 0 として単位時間 $1[s]$ ずつ増やすことで送信タイミングをより分散させ，監視トラフィック量の最大値が上限値以下に収まるような遅延時間を探す．例えば，$\lceil M/L \rceil + \alpha = 3$ の場合，$D(n) = mod(n, 3)$ なので $t_{ex}[s]$ に送信予定の 3 つのデータは，図 3 に示すように $t_{ex}[s]$，$t_{ex} + 1[s]$，$t_{ex} + 2[s]$ にそれぞれ送信することになる．ただし，同時刻に送信予定のデータの個数を数え，その中の最大値 (図 2 では 3 となる) が $\lceil M/L \rceil + \alpha$ より大きくなる場合，送信タイミングを分散させる処理のみでは最大値を上限値以下に抑制できないため，(B) の処理を適用する．

(B) 次に (A) で送信タイミングを分散させた結果，トラフィックを上限値以下に抑制できない場合，分割度 (β とする) に従って各データを分割して送信する．各データは管理情報の種類ごとに区切りを付けることで分割できる．例えば，$\beta = 2$ の場合，図 3 に示すように $t_{ex}[s]$ に送信予定の $d[bit]$ のデータを区切り，半分ずつ $t_{ex}[s]$ に $d/2[bit]$，$t_{ex} + 1[s]$ に $d/2[bit]$ 送信する．ゆえに，図 2 において $\lceil M/L \rceil + \alpha = 3[s]$，$\beta = 2$ とした場合，$t_{ex}[s]$ に送信予定のそれぞれ $d[bit]$ の 3 つのデータは，$t_{ex}[s]$〜$t_{ex} + 5[s]$ の各秒に半分の $d/2[bit]$ ずつ送信，つまり $(\lceil M/L \rceil + \alpha) \times \beta = 6[s]$ に分けて送信する．以上の処理を，β の初期値を 2 として 1 ずつ増やし，監視トラフィック量の最大値が上限値以下となる β の値を探す．

最後に (A)・(B) より決定した α，β の値に応じて，各データの送信スケジュールを決定する．マネージャからのリクエストには送信スケジュールに従い，管理情報を送信する．以上の調整によって，図 4 に示すように MR のアップリンクを流れる監視トラフィック量を設定した上限値以下に抑制する．

3.3 (2) Home Agent 非経由ポーリング

MR や MR に接続するノードの通信は必ず HA を通過するため，MR から大量の監視トラフィックが流れた場合，HA に接続するネットワークのノードの通信にも影響を与える．そこで，マネージャが HA を経由せず MR に直接ポーリングを行うための制御を行う．

前提条件として，マネージャは管理対象の MN が接続する MR の HoA(常に不変のアドレス) を既知であるとし，定期的に MR を管理する HA に対して，MR の CoA(移動先ネットワークでのアドレス) の通知を要求する．マネージャはこの CoA に対してポーリングを行うことで，直接 MR から管理情報を収集できる．ただし，CoA は MR の移動に伴い変化するため，マネージャは新しい CoA を取得するまで MR と通信できず，管理情報を収集できなくなる．しかし，本手法では MR に管理情報を蓄積するため，マネージャが新しい CoA を取得後，改めて収集しても問題ない．ゆえに，HA を経由せずに管理情報を収集することで，HA に接続するネットワークのノードの通信への影響を軽減できる．

3.4 シミュレーションによる提案手法の評価

3.4.1 実 験 方 法

提案手法の有効性を評価するため，ネットワークシミュレータ ns-2 を用いて実験を行い，提案手法による他の通信への影響の軽減の効果を確認した．

本実験では，図 5 に示すトポロジにおいてシミュレーションを行った．シミュレーション時間は 600[s] とし，その中で SNMP の通信は，MR が MN から 5 秒ごとに 10 種類の管理情報 (100[byte/個]) を収集・蓄積し，マネージャは 30 秒ごとに MR にポーリングを行う．また，マネージャは MR に接続する 50 台の MN へ同時にポーリングを行うため，通常時はマネージャのポーリングにより，合計 $30/5 \times 50 \times 10 \times 100[byte] = 300[kbyte]$ の管理情報が一度に送信される．MR のアップリンクであるリンク A は，無線であるとしてパケットロス率を 0.1%に設定した．リンク A の帯域幅に関しては，0〜90[s] は 54[Mbps]，210〜270[s] は 11[Mbps]，390〜600[s] は 5.5[Mbps] と変化させ，MR の移動により発生する接続先 AP や通信環境の変化を模擬する．90〜210[s]・270〜390[s] は MR の移動時間としてリンク A を切断し，リンクの再接続後に蓄積した管理情報が一斉に流れ，監視トラフィック量が増加する状況を発生させる．210〜440[s] には 1 台の MN から Host B へ送信レート 2[Mbps] で，また Host C.1〜C.5 から Host B へ送信レート 10[Mbps] で UDP により CBR トラフィックを送信し性能を計測する．

以上のシナリオにおいて，上限値を 10%として提案手法を用いた場合と，流量制御を行わずに store-and-forward 型の収集を行った場合 (以降，制御なしとする)，トランスポート層に TCP を使用し管理情報の収集を行った場合 (以降，TCP 手法とする) を比較する．TCP 手法は，TCP の再送機能と輻輳制御機能により，管理情報の損失の防止と監視トラフィック量の流量制御を行うことを想定している．比較項目は，まず MR のアップリンクのリンク A を流れる監視トラフィック量を調べ，提案手法の効果により監視トラフィック量を設定した上限値以下に抑制可能かを確認する．また，1 台の MN から，もしくは Host C.1〜C.5

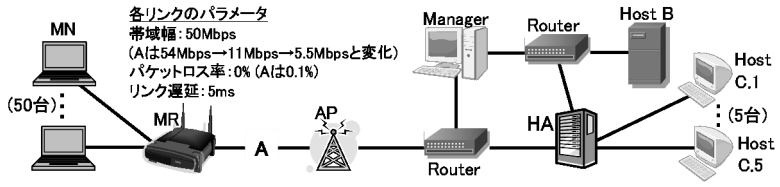

図 5 シミュレーションに用いたトポロジ

から Host B への各 CBR トラフィックのスループット・ジッタを調べ，提案手法により他の通信への影響を軽減できるかを確認する．

3.4.2 実験結果

提案手法の上限値を帯域幅の 10%に設定した場合の，MR のアップリンクを流れる監視トラフィック量の変化の結果を図 6 に示す．なお，図中の横軸と平行に引かれた点線は上限値を示している．制御なしの場合では，一斉に監視トラフィックが流れ，特に回線の回復後には，切断中に蓄積した分だけ増加した監視トラフィックが流れる．また，TCP 手法を用いた場合も，トラフィックの流量を任意の値以下に調整できるわけではないため，制御なしの場合と同様の結果となっている．ここで TCP 手法において，回線の回復直後の 210，390[s] 付近に監視トラフィックが増大して流れているのは，切断中に送信されたマネージャからのリクエストが TCP の機能により何度も再送され，回復直後に MR まで届き管理情報が送信

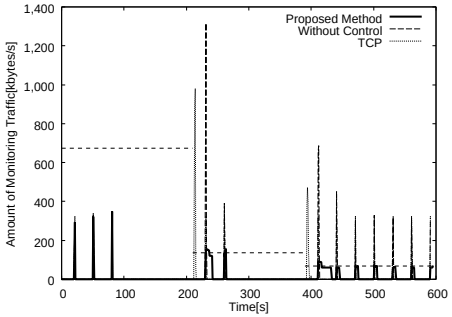

図 6 監視トラフィック量の変化

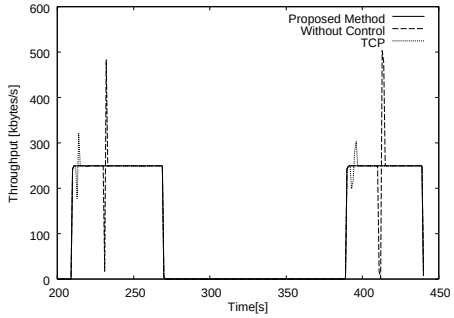

図 7 CBR トラフィックのスループット (MN → Host B)

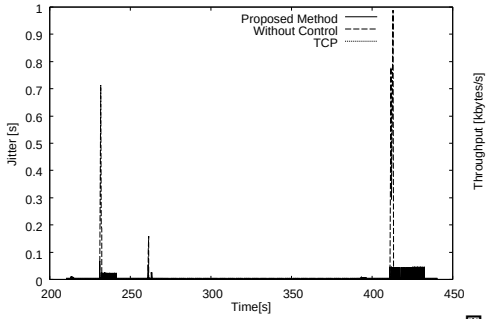

図 8 CBR トラフィックのジッタ (MN → Host B)

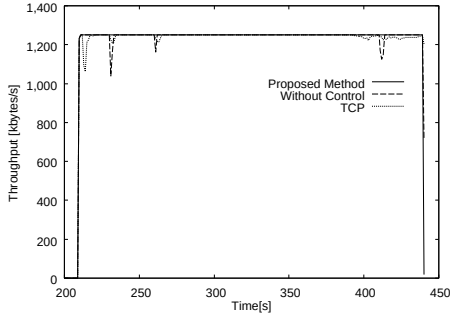

図 9 CBR トラフィックのスループット (Host C.1 → Host B)

されたためである．一方，提案手法の場合では平常時や回線の回復後も，管理情報の送信を分散させることで，その都度監視トラフィック量を設定した上限値以下に抑制できている．

次に，1 台の MN から Host B へ流した送信レート 2[Mbps] の CBR トラフィックのスループットの結果を図 7，ジッタの結果を図 8 に示す．制御なしの場合では，回線の回復後に監視トラフィックが増加し MR のアップリンクの帯域が占有されるため，著しくスループットが低下する箇所やジッタが増加する箇所が見られる．TCP 手法の場合は，ジッタの増加は見られないものの，スループットが低下する箇所がある．一方，提案手法の場合では，監視トラフィック量が設定した上限値以下に抑制されているため，スループットの低下やジッタの増加を回避できている．以上から，提案手法により監視トラフィックを効果的に抑制し，他の通信への影響を低く抑制できることが示された．

Host C.1〜C.5 から Host B へそれぞれ送信レート 10[Mbps] で流した CBR トラフィックのスループットのうち，Host C.1 からのものの結果を図 9 に示す．制御なしや TCP 手法の場合では，増加した監視トラフィックの影響を受け，スループットが低下する箇所が見られる．210〜230[s] 付近では，390〜440[s] 付近に比べよりスループットが低下している．これは，390〜440[s] 付近では MR のアップリンクの帯域幅が 5.5[Mbps] なのに対し，210〜230[s] 付近では 11[Mbps] であり，HA へ流れる監視トラフィック量の増加の影響をより受けやすいためである．一方，提案手法の場合では，監視トラフィックが HA を経由しないため，スループットは低下することなく，常に一定の値を維持している．また，省略した Host C.2〜C.5 からのトラフィックに関しても同様の結果が得られた．以上から，提案手法により HA を経由せずに管理情報を収集することで，HA に接続するネットワークのノードの通信への影響を防止できることが示された．

4. 提案 2:SNMP メッセージ集約による監視トラフィックの削減手法

4.1 提案手法 2 の概要

提案手法 2 では，他の通信への影響を軽減するため，SNMP メッセージが含む管理情報の識別子をまとめ複数のメッセージを 1 つに集約し，全体のメッセージサイズを削減することで，監視トラフィック量自体を削減する．さらに本手法では，移動ネットワークにおいて通信を行うことを考慮し，(1) 複数ノードの SNMP メッセージの集約，(2) タイムスタンプによる集約情報の管理の処理を行う．(1) では MR に接続するノードからのメッセージを MR で集約し，複数のノードの管理情報をまとめてマネージャへ送信する．また，(2) では MR でタイムスタンプと共に管理情報を集約して蓄積し，タイムスタンプを指定して再リ

クエストすることにより，収集に失敗した管理情報の取得を可能にする．次に (1)，(2) の処理の詳細について説明する．

4.2 (1) 複数ノードの SNMP メッセージの集約

SNMP では，マネージャは収集したい管理情報である MO(Managed Object) を，リクエストの中で識別子である OID(Object Identifier) により指定する．MO には，例えば受信ユニキャストパケット数や MTU の値などがあり，それらの識別に数値である OID が利用される．マネージャは希望する MO を OID で指定してリクエストし，エージェントはレスポンスに OID と OID で指定された MO の値を含め返信する．以上のようにしてマネージャはエージェントから管理情報を収集する．通常の SNMP メッセージでは，図 10 のように 1 メッセージに含まれる OID は 1 つであり，管理情報 1 項目ごとにそれぞれ 1 つのリクエスト/レスポンスのパケットが必要である．ゆえに，複数の管理情報を一度に収集する場合，監視トラフィックが増大しやすい．そこで，図 11 のように 1 メッセージ中で複数の OID を指定し，一度に複数の管理情報を取得する Bulk 形式の収集方法がある．しかし，Bulk 形式を用いても，一定時間ごとに繰り返し管理情報を収集する場合，収集する管理情報が固定であれば，毎回複数の OID をメッセージ中で指定する事は無駄が多い．

MO Aggregation MIB [9] では，2 種類の方式により複数の OID を集約しメッセージサイズを削減する．1 つは，事前に複数の種類の OID をまとめた Aggregation MO(Ag MO) を定義し，マネージャとエージェントで共有する．これにより，Ag MO1 つをリクエスト

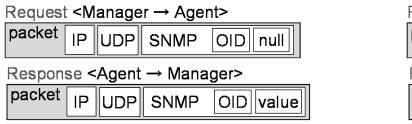

図 10 通常の SNMP メッセージ

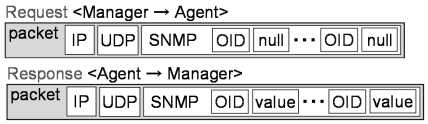

図 11 Bulk 形式の SNMP メッセージ

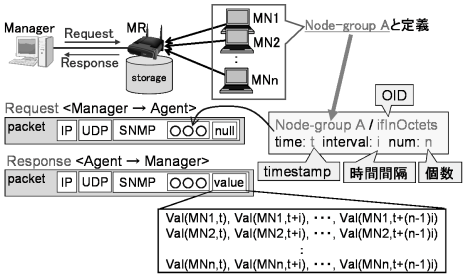

図 12 複数ノードの SNMP メッセージ集約

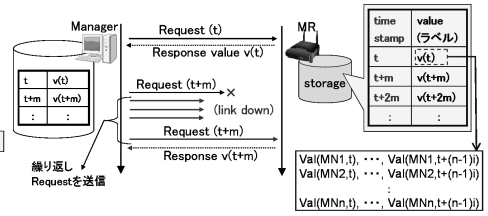

図 13 タイムスタンプによる集約情報の管理

で指定するだけで，複数の管理情報を 1 つのレスポンスで得ることができる．また，リクエストでタイムスタンプ・時間間隔・個数・OID を指定することで，複数時間分の管理情報をまとめて得ることが可能である．ただし，MO Aggregation MIB では特定の時間帯の管理情報を集約するだけで，損失した情報を時間を遡って収集することはできない．以上のように，1 メッセージ中に複数存在する OID 部分を集約することで SNMP のメッセージサイズを削減し，監視トラフィック量自体を削減する．また，集約を行うのは OID の部分のみで，管理情報の値に欠損は発生しない．本稿では，この手法を移動ネットワークに応じたものに拡張する．

提案手法では，さらに MR に接続するノードから管理情報をまとめて収集する．まず，MR が各 MN から管理情報を収集し蓄積する．そして，複数のノードをまとめたノードグループを定義し，マネージャは図 12 のようにノードグループを指定したリクエストを MR に対して送信し，MR が各 MN の管理情報をまとめてレスポンスとして返信する．以上により，さらに全体のメッセージサイズが削減され，MR のアップリンクを流れる監視トラフィック量を削減することができる．

4.3 (2) タイムスタンプによる集約情報の管理

移動ネットワークでは，MR の移動などにより MR がネットワークに接続されていない状況が頻繁に発生し，マネージャが管理情報の収集に失敗する場合が多くなる．そこで，収集に失敗した管理情報の再収集を可能にするため，図 13 のように，MR で集約した管理情報にラベルを付け，ラベルをタイムスタンプと関係付けて管理する．マネージャは管理情報の収集に失敗した場合，タイムスタンプを指定して再度リクエストを送信し，レスポンスが得られるまで繰り返しリクエストを送信する．これにより，時間を遡って管理情報を収集することが可能となり，管理情報の損失を防止できる．また，マネージャ・MR 間のリンクの切断時間が長くなると，リンクが回復した後にマネージャから，切断中に失敗していた複数のリクエストが同時に再送される．その結果，MR から送信される監視トラフィックがバースト的に増大する．一方，提案手法ではメッセージの集約の効果により，監視トラフィックの増大を抑制し，効率的に管理情報の損失を回復できる．

4.4 計算による提案手法の評価

4.4.1 評 価 方 法

提案手法によって，監視トラフィックを削減し，他の通信への影響を軽減できるか確認するとともに，管理情報の損失を効率的に回復することができるかどうかを数値計算により評価し，提案手法の有効性を示す．

パケットサイズに関するパラメータを表 2 の値に設定する．また，SNMP の通信は図 14 のようにパラメータを与え，マネージャが一度に収集する管理情報数 N を式 $N = \frac{t_{MG}}{t_{MR}} \times \sum_{i=1}^{n} m(i)$ により算出する．以上の計算式をもとに，通常の管理情報収集方式 (以降，通常方式とする)，Bulk 形式による収集方式 (以降，Bulk 方式とする)，提案手法を比較する．比較項目は，MR のアップリンクを流れる監視トラフィック量として，N を変化させた場合に管理情報 1 項目あたりの取得に必要となるトラフィック量を調べ (今回はレスポンスのみを調査)，提案手法によりどの程度監視トラフィック量を削減可能か確認する．また，マネージャと MR 間のリンクのパケットロス率を変化させた場合の，マネージャが管理情報を全て収集できる確率を調べ，提案手法により管理情報の損失が回復できるか確認する．最後に，損失の回復が行われる際に流れる監視トラフィック量を，提案手法と単純な回復手法である store-and-forward 型の収集方式 [3](以降，S-F 方式とする) で比較し，提案手法が効率的に損失の回復が可能であることを確認する．

4.4.2 評価結果

式 (1)〜(3) により，N を変化させた場合に各手法が管理情報 1 項目あたりの取得に必要となるトラフィック量 T を算出する．ここでは，MR からマネージャに送信されるレスポンスによるトラフィックのみを考慮している．式 (1) は通常方式のトラフィック量を示し，管理情報 1 項目あたりに一定量のトラフィックが必要となる．式 (2) は Bulk 方式，式 (3) は提案手法のトラフィック量を示しており，N の増加に従い集約の効果によって，トラフィック量が減少する．式中の X は集約されたパケットのサイズが MTU を超えないよう，分割される際に追加されるヘッダ等の増分である．また，Bulk 形式では N に従い l_{oid} の数が増加するが，提案手法では l_{oid} の数は一定である．

$$T = l_{const} + l_{oid} + l_{val} \tag{1}$$

$$T = (l_{const} + (l_{oid} + l_{val}) \times N + X)/N \tag{2}$$

$$X = \begin{cases} 0 & (\text{if } l_{const} + (l_{oid} + l_{val}) \times N - l_{eth} \leq M) \\ (\lceil N/\lfloor \frac{M-(l_{const}-l_{eth})}{l_{oid}+l_{val}} \rfloor \rceil - 1) \times l_{const} & (\text{else}) \end{cases}$$

$$T = (l_{const} + l_{oid} + l_{val} \times N + X)/N \tag{3}$$

$$X = \begin{cases} 0 & (\text{if } l_{const} + l_{oid} + l_{val} \times N - l_{eth} \leq M) \\ (\lceil N/\lfloor \frac{M-(l_{const}+l_{oid}-l_{eth})}{l_{val}} \rfloor \rceil - 1) \times (l_{const} + l_{oid}) & (\text{else}) \end{cases}$$

式 (1)〜(3) をグラフにしたものを図 15 に示す．通常方式では，N が増加してもトラフィック量は変化しないが，Bulk 方式・提案手法では，N の増加に伴い必要なトラフィック量が減少する．特に提案手法では集約による効果が大きく，$N > 10$ の場合では通常方式の 10 分の 1 以下となる．以上より，提案手法は監視トラフィック量を通常方式に比べて，大幅に削減することが可能であり，他の通信への影響を軽減できることを示している．

次に各手法の，マネージャと MR 間のリンクのパケットロス率 P を変化させた場合の，マネージャが管理情報を全て収集できる確率 R は，通常方式: $R = (1-P)^N$，Bulk 方式:$R = (1-P)^{N_x}$(ただし，$N_x = \lceil N/\lfloor \frac{M-(l_{const}-l_{eth})}{l_{oid}+l_{val}} \rfloor \rceil$)，提案手法:$R = 1$ で算出することができ，これらをグラフ化したものを図 16 に示す．今回は $t_{MG} = 30[s]$，$t_{MR} = 6[s]$，$n = 20[nodes]$，$m = 10$[個] として $N = 1000$ と N を固定している．Bulk 方式の N_x は集約を行うにあたり MTU を超えないように分割され生じたパケット数である．図 16 に示されているように，通常方式や Bulk 方式では，P の増加により R が減少するが，提案手法では，損失を回復する機能を有しているため，管理情報の損失は無い．

表 2 パケットサイズに関するパラメータ

Ethernet ヘッダ長	$l_{eth} = 14[bytes]$
IPv6 ヘッダ長	$l_{ip} = 40[bytes]$
SNMP フレーム長 (OID,value 部除く)	$l_{const} = 100[bytes]$
OID(1 項目)	$l_{oid} = 12[bytes]$
value(1 項目)	$l_{val} = 6[bytes]$
データリンクの MTU(Ethernet)	$M = 1500[bytes]$

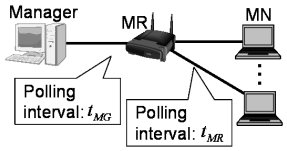

図 14 SNMP の通信に関するパラメータ

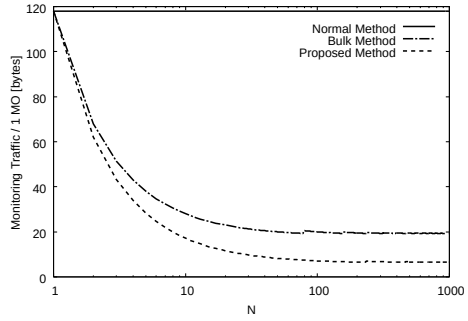

図 15 管理情報 1 項目の取得に必要なトラフィック量)

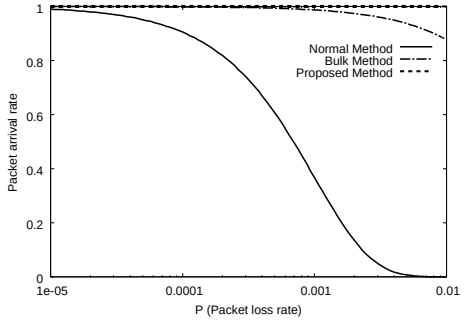

図 16 マネージャが管理情報を全て収集できる確率)

Vol.2010-MBL-52 No.13
2010/1/29

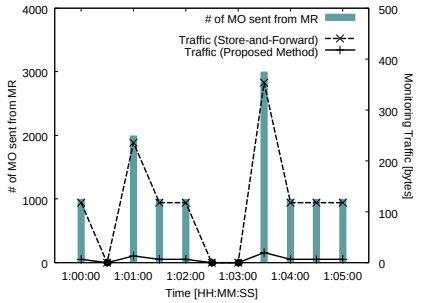

図 17 損失の回復が行われる際に流れる監視トラフィック量)

最後に，図 14 のトポロジにおいて 1:00:00〜1:05:00 の時間中，30[s] 間隔でマネージャから MR にポーリングを行い，1:00:01〜1:00:59，1:02:01〜1:03:29 にマネージャと MR の間のリンクが切断するとしたシナリオを設定し，損失の回復が行われる際に流れる監視トラフィック量を提案手法と S-F 方式で比較したグラフを図 17 に示す．今回も $t_{MG} = 30[s]$，$t_{MR} = 6[s]$，$n = 20[nodes]$，$m = 10$[個] として $N = 1000$ と N を固定している．図 17 中の棒グラフは MR から送信される管理情報の個数を示しており，リンクの切断時間に収集に失敗した管理情報の送信と通常の送信が重なることで，1:01:00 では通常の 2 倍の 2000 個，1:03:30 では 3 倍の 3000 個が送信される．折れ線グラフが実際に流れる監視トラフィックであり，S-F 手法では回復分によりトラフィックが倍増する箇所があるが，提案手法では集約の効果によりトラフィックの増加を防いでいる．以上より，提案手法は S-F 手法のような単純な回復手法に比べ，効率的に管理情報の損失を回復できることを示している．

5. 2 つの提案手法の適用範囲について

本研究では，パケットロスによって発生する管理情報の損失と，監視トラフィックによる帯域の占有・圧迫の 2 点を解決することを目的としている．**提案手法 2** は，管理情報の損失を回復するとともに，監視トラフィック量を削減することでこれらの問題を解決している．しかし，帯域幅に対して送信される監視トラフィック量が多い状況，例えば，帯域幅が狭い通信経路に大量の監視トラフィック量が送信される状況では，**提案手法 2** による監視トラフィックの削減効果だけでは，問題を軽減することはできない．そこで，監視トラフィックの流量を調整する**提案手法 1** による送信タイミングの調整により，問題を効果的に解決することができると期待できる．**提案手法 1** と**提案手法 2** の組み合わせ手法については，今後の課題である．

6. ま と め

本稿では，移動ネットワークにおいて，既存のネットワーク管理手法を適用すると管理情報が損失するとともに，監視トラフィックが通信帯域を占有・圧迫する問題を解決するため，バッファリングによる監視トラフィックの流量制御手法と SNMP メッセージ集約による監視トラフィックの削減手法を提案した．性能評価を通して，本提案方式が効果的に機能することを示し，提案手法の有効性を示した．今後は，提案した 2 つの提案手法を組み合わせた手法について検討し，さらなる性能改善を目指す．

謝辞 本研究の一部は，総務省 SCOPE プロジェクト (071502003)，および科学研究費補助金 (19200005) の援助を受けて実施した．

参 考 文 献

1) V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert: “Network Mobility(NEMO) Basic Support Protocol”, RFC3963 (2005).
2) J.Case, M.Fedor, M.Schoffstall and J.Davin: “Simple Network Management Protocol(SNMP)”, RFC1157 (1990).
3) K.Koide, G.Kitagata, H.Kamiyama, D.Chrakraborty, G.M. Keeni and N.Shiratori: “MobiSNMP - A model for Remote Information Collection from Moving Entities using SNMP over MobileIPv6”, IEICE Transactions on Communications, VOL.E88-B, NO.12, pp. 4481–4489 (2005).
4) J.-Y. Teo, Y. Ha and C.-K. Tham: “Interference-Minimized Multipath Routing with Congestion Control in Wireless Sensor Network for High-Rate Streaming”, IEEE Trans. on Mobile Computing, Vol. 7, Issue 9, pp. 1124–1137 (2008).
5) C.Wang, B.Li, K.Sohraby, M.Daneshmand and Y.Hu: “Upstream congestion control in wireless sensor networks through cross-layer optimization”, IEEE Journal on Selected Areas in Communications, Vol. 25, Issue 4, pp. 786–795 (2007).
6) M. Zawodniok and S. Jagannathan: “Predictive Congestion Control Protocol for Wireless Sensor Networks”, IEEE Trans. on Wireless Communications, Vol. 6, Issue 11, pp. 3955–3963 (2007).
7) K.S. Shin, J.H. Jung, J.Y. Cheon and S.B. Choi: “Real-time network monitoring scheme based on SNMP for dynamic information”, Journal of Network and Computer Applications, Vol. 30, Issue 1, pp. 331–353 (2007).
8) S.hyun Park and M.soon Park: “An efficient transmission for large MIB tables in polling-based SNMP”, ICT 2003 (International Conference on Telecommunications), pp. 246–252 (2003).
9) G.M. Keeni: “The Management Object Aggregation MIB”, RFC4498 (2006).