情報処理学会論文誌　Vol. 52　No. 3　1021–1032 (Mar. 2011)

移動ネットワーク環境における SNMP を用いた情報収集手法

中村直毅[†1]　丸山貴史[†2]　菅沼拓夫[†3]
グレン マンスフィールド キニ[†4]　白鳥則郎[†2]

ネットワークモビリティ（NEMO）プロトコルが用いられる環境では，モバイルノーやモバイルルータがネットワーク間を移動するため，ネットワーク構成の変化が頻繁に発生する．このような移動ネットワーク環境を遠隔監視する場合，収集する管理情報が経路途中で頻繁に損失するという問題や監視トラフィックが通信帯域を占有して他の通信を阻害するという問題が生じる．そこで本稿では，これらの問題を解決するため，モバイルルータにおいて監視トラフィックの配送を分散する管理情報のバッファリング手法，および，監視トラフィックを圧縮する SNMP メッセージ集約手法を提案する．評価実験を通して，本提案手法の有効性を示す．

SNMP Monitoring Schemes for Network Mobility Environment

Naoki Nakamura,[†1] Takafumi Maruyama,[†2]
Takuo Suganuma,[†3] Glenn Mansfield Keeni[†4]
and Norio Shiratori[†2]

Mobile Nodes and Mobile Routers (MRs) move between networks in an environment where NEMO protocol is used. Hence, network environment changes frequently. In case of remote network management in mobile network, frequent losses of management information can happen due to unstable network environment. In addition, monitoring traffic consumes the bandwidth of MRs and Home Agent's network and affect other traffics. To solve these problems, we proposed a buffering method at the MR to disperse the monitoring traffic. Besides, an aggregation method of SNMP messages is proposed to reduce the monitoring traffic effectively. Through evaluation, we verify that the proposed methods work properly and show their effectiveness.

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を実現するために研究開発がさかんに行われている．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 が重要な役割を果たすと考えられる．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．これにより，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できるようになる．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，従来よりも高度かつ正確に運用管理し，ネットワークの信頼性を担保することが必要となる．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・監視できることは非常に重要である．

ネットワーク管理では，一般に標準技術である SNMP（Simple Network Management Protocol）[2] が用いられる．管理者（Manager）は，管理情報を定期的に収集するため，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，SNMP プロトコルでは，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

†1 東北大学医学系研究科
School of Medicine, Tohoku University
†2 東北大学電気通信研究所
Research Institute of Electrical Communication, Tohoku University
†3 東北大学サイバーサイエンスセンター
Cyberscience Center, Tohoku University
†4 株式会社サイバーソリューションズ
Cyber Solutions Inc.

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いっせいに送信され，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という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手法（**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手法（**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てその流量を制御し，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，移動ルータに接続されたノードの持つ管理情報を取得するための 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．

本稿の構成は以下のとおりである．2 章では，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 章では，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 章では，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，数値計算および実機により性能を評価する．5 章では，提案する 2 つ手法の適用範囲について考察する．最後に 6 章で結論を述べる．

2. 移動ネットワークにおけるネットワーク管理

2.1 ネットワークモビリティプロトコルの概要および管理システム

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 の現在位置にかかわらず通信相手がつね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 の持つつねに不変のアドレス 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し，アドレスの提供を受けた MNN はモビリティの機能を有していなくても，MR とともに移動することで透過的に移動することができる．移動ネットワークでは，MN は，IPv6 プロトコルを搭載するだけでモビリティ機能を有し，電車やバスなどに MR が搭載されていれば，パソコンやカーナビが常時ネットワークに接続することが可能である．また，電車やバスなどに備え付けられている加速度/温度/オイルセンサなどの小型の計測機器を MR に接続して利用することが期待されている．

著者らは，SNMP 技術を基盤とし，移動ネットワークを管理・監視するための仕組みを実現するため，MobileIPv6 MIB[4]，NEMO MIB[5] の標準化を行ってきた．本稿では，Manager が，標準技術 SNMP（Simple Network ManagementProtocol）[2] を用いて，移動ネットワークに接続したネットワーク機器から時系列的に管理情報を損失なく収集する仕組みの実現を目指している．管理情報を収集する仕組みとして，Manager から MR に管理情報を要求する構成と Manager から直接 MN に対して情報を要求する構成の 2 種類の構成が考えられる．移動ネットワークでは，MN は IPv6 プロトコルが搭載されていれば MR に接続することが可能であり，機能/性能的に非力なデバイスなどでも容易に接続することができる．そこで，本稿では，Manager が MR から管理情報を収集する構成を採用するとともに，MN ではなく Manager もしくは MR に管理情報を収集する機能を追加する．なお，Manager および管理対象としている機器（MR，HA，MN）は，同一組織もしくは，Manager の管理下にあるとする．Manager は，必要な情報を管理対象機器から SNMP プロトコルにより必要な管理情報を取得するためのアクセス権を有しているものとし，また，SNMPv3[6] を用いて通信することでセキュリティおよびプライバシを確保する．

2.2 時系列的に管理情報を収集する際の課題

移動ネットワークにおいて，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る場合，大量の監視トラフィックがネットワークに流れ込み，**図 1** に示すように，他の通信に影響を与える問題が生じることが予想される．

MR がネットワーク間を移動する場合，MR が上流のネットワークと切断されている間，MR に接続している MN は，管理情報を収集する Manager との通信が切断され，管理情報を送信することができない．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につれて，その蓄積量が増大する．その後，MR が上流のネットワークに再接続して回線が復旧すると，複数の MN で通信の切断・回復が同時に発生し，各 MN で蓄積していた管理情報がいっせいに送信される．その結果，バースト的なトラフィックが MR のアップリンクを占有する問題が発生する．また，移動ネットワークでは，Manager・MN 間の通信は HA を経由するため，Manager へ送信されるトラフィックが HA のアップリンクを占

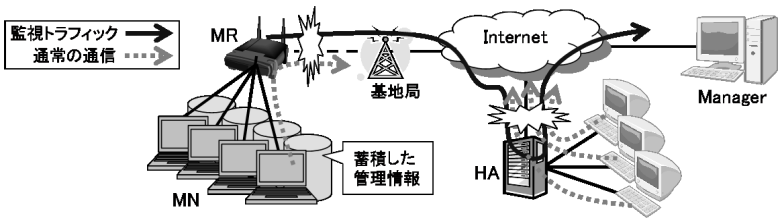

図 1　監視トラフィックが他の通信に影響を与える状況
Fig. 1　Interference of monitoring traffic to other communication.

有する．これにより，MR や MN が HA に物理/論理的に接続している場合，MR や MN は，バースト的に流れる監視トラフィックから影響を受け，その通信品質が低下するという問題が生じる．なお，物理的に HA に接続しているとは，HA をホームネットワークとするノードが HA に接続している状況であり，論理的に HA に接続しているとは，HA とは異なったネットワークに接続している MR が，NEMO プロトコルを用いて，HA に接続している状況である．

以上のように，移動ネットワークにおいて時系列的に管理情報を収集する場合，Manager へ送信される監視トラフィックが，MR のアップリンクを経由する通信と論理/物理的に HA と接続しているノードの通信に悪影響を与えるという問題を軽減するための仕組みの確立が必要である．

2.3 関 連 研 究

管理情報を時系列的に損失なく収集する際に，監視トラフィック量が増大するという問題を解決する手法として，監視トラフィックを破棄する手法，監視トラフィックの送信を分散する手法，監視トラフィック量自体を削減する手法が考えられる．

バースト的なトラフィックを抑制するため，CBQ（Class Based Queueing）[7] を用いたトラッフィク制御手法があげられる．CBQ では，パケットをトラフィック単位（IP アドレスやポート番号）でクラスに分類し，トラッフィックが閾値を超えると，そのクラスのパケットを破棄するといった制御を行う．CBQ に基づく処理は，トラフィック単位で制御する必要がある．しかし，SNMP のデータ単位である OID ごとに処理することは困難であるため，管理情報の重要度に関係なくデータを破棄してしまうことが懸念される．文献 8) では，無線センサネットワークにおいて，監視トラフィックを分散させる輻輳制御手法を提案している．この手法は，パケットの種類やノードの差異により，優先するもの/優先しないものを分別し，トラフィックを制御する．移動ネットワークでは，各 MN や管理情報の種類に対して優先度の差異を付けることは困難であるため，本方式を適用することは困難である．一方，文献 9) で提案されているノードやネットワークの状態によって輻輳を予測・制御する手法は，移動ネットワークへの適用が可能であると考えられる．

文献 10) では，監視トラフィックを削減するため，SNMP エージェントが，自律的に，一定間隔で Manager へ管理情報を送信する手法を提案している．本手法では，Manager 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を削減することができるが，時系列的に管理情報を収集する際のトラフィックの削減効果は期待できない．文献 11) では，Manager からのリクエストに対し，管理情報の差分のみを SNMP を用いて送信し，監視トラフィック量を削減している．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，管理情報が頻繁に変化するため，この手法による改善効果を望むことはできない．

以上をふまえて，本稿では，MR において輻輳の発生を予測し，監視トラフィックの送信を分散する手法を 3 章で提案し，監視トラフィック自体を削減する手法を 4 章で提案する．

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 において各ノードの管理情報を一時的にバッファリングすることでデータの送信量を調整する．これにより，監視トラフィック量を指定した上限値以下に抑制する．本手法では，MR が定期的に MN から管理情報を収集・蓄積し，Manager からのリクエストに対するレスポンスを MR が返す．また，MR と Manager 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，予測に応じて指定した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，Manager は (2) により MR へ直接ポーリングをする．なお，流量制御は，MR と Manager の間でのみ行われ，MN において特別な制御は必要としないため，様々な MN に対して適用することが可能である．

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

指定した上限値以下に監視トラフィックを抑制するため，今後流れることが予想されるトラフィックの流量を予測する．MR では，**表 1** にあげたパラメータから，単位時間を 1 [s] として各 MN が次に Manager 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

表 1　R'_x・S'_x の算出のためのパラメータ
Table 1　Parameters for calculation of R'_x and S'_x.

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

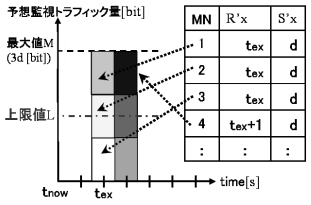

図 2　予想監視トラフィック量
Fig. 2　Amount of estimated monitoring traffic.

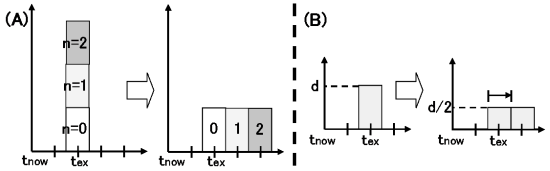

図 3　(A)・(B) の処理を適用した場合の変化
Fig. 3　Overview of result of applying method: (A) and (B).

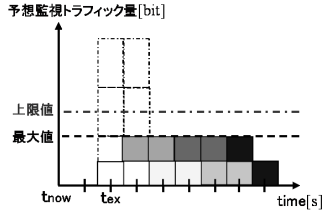

図 4　流量制御後の予想監視トラフィック量
Fig. 4　Amount of estimated monitoring traffic after flow control.

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されるかを見積もり，予測送信データサイズに反映させる．

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．たとえば，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] があらかじめ指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，これらを分割するとともに送信タイミングを遅らせて送信することにより，$M \leq L$ を実現する．具体的には，以下の (A)・(B) の手順により各管理情報の遅延時間・分割度を算出する．

(A) 遅延時間を算出し，同じ時刻に送信予定のデータの送信タイミングを遅延させ，トラフィックを分散させる．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徐々に分散させ，監視トラフィック量の最大値が上限値以下に収まる遅延時間を探す．たとえば，$\lceil M/L \rceil + \alpha = 3$ 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した結果，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分割する．たとえば，$\beta = 2$ 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 の値を探索する．

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．送信スケジュールは Manager からのリクエストに従い，管理情報を Manager へ送信する．なお，送信する管理情報のデータ量が十分に大きく，データの送信を終了できない場合には，処理を中止し管理情報を破棄する．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上限値以下に抑制する．

なお，遅延を時間は，管理情報の種類や情報の質によって異なることが想定されるため，管理情報ごとに遅延時間を選択する仕組みや管理情報ごとに制御する仕組みの検討は，今後の課題とする．

3.3 (2) Home Agent 非経由ポーリング

MR や MR に接続している MN の通信は，移動ネットワークのプロトコル上，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ると，HA に接続しているノードの通信にも悪影響を与える．そこで，提案手法では，HA を経由しない通信路を使って，Manager が MR からデータを収集する方式を提案する．

Manager は，管理対象の MN が接続する MR の HoA（つねに不変のアドレス）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．要求を受けた HA は，Manager が MR の CoA 情報を格納している MobileIPv6 MIB/NEMO MIB にアクセスする権限を有している場合に限り，Manager に MR の CoA を通知する．また，Manager は，MR の CoA に宛にポーリングすることで，直接 MR から管理情報を収集する．ただし，CoA は MR の移動にともなって変化するため，Manager は新しい CoA を取得するまでの間，MR から管理情報の収集することができない．本手法では，管理情報を MR で蓄積しているため，Manager が新しい CoA を取得した後，改めて管理情報を要求することで，管理情報を損失することなく収集できる．

以上のように，本提案手法では，HA を経由せずに管理情報を収集することで，HA のネットワークに接続しているノードの通信への影響を軽減することができる．

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

本提案手法によって，監視トラフィックが MR/HA において帯域を占有するという問題を軽減し，監視トラフィックが他のノードの通信に及ぼす影響を削減できることを確認するため，**図 5** に示すトポロジで ns2 を用いたシミュレーションを行った．

本実験では，複数の HA/MR を Manager が管理する状況を想定し，HA と異なったネットワークに Manager を配置する．配置された Manager は，SNMP を用いて監視対象にしている 50 台の MN から管理情報を遠隔から収集する．物理/論理的に複数の MR や MN が HA に接続している状況を模擬するため，複数のノード（C.1〜C.5）を HA の配下に配置する．また，Home Agent 非経由ポーリング手法の効果を確認するため，Manager・MR 間の通信経路と重ならない位置に C.1〜C.5 および Host B を配置して，C.1〜C.5・Host B 間にトラフィックを流す．なお，Manager・MR 間と重なる位置に Host B を配置する場合には，Manager・MR の監視トラフィックの上限値を調整することで，C.1〜C.5・Host B 間の通信の影響を軽減することができると考えられる．トラフィックの上限値の動的な調整方法は，今後の課題とする．

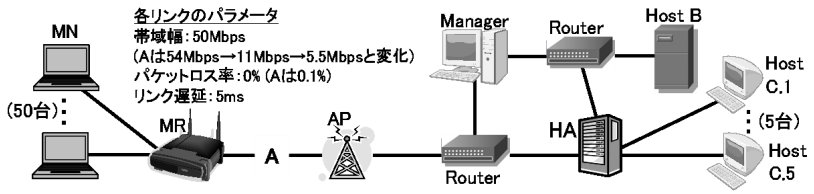

図 5　シミュレーションに用いたトポロジ
Fig. 5　Topology of the simulation environment.

具体的な評価実験シナリオは以下のとおりである．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，Manager は 30 秒ごとに MR にポーリングをする．また，Manager は MR に接続する 50 台の MN へ同時にポーリングをするため，通常時は Manager から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 1 度に送信される．MR のアップリンクであるリンク A は，無線リンクを想定してパケットロス率を 0.1%とした．また，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] および 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いっせいに流れ，監視トラフィック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] で送信する．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する．

以上のシナリオで，提案手法において監視トラフィック量の上限値を，MR のアップリンクの通信帯域の 10%に抑制する場合と，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．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計測し，提案手法の効果により監視トラフィック量を指定した上限値以下に抑制することが可能であるかを確認する．また，1 台の MN もしくは Host C.1〜C.5 から Host B へ流した CBR トラフィックのスループットおよびジッタを計測し，提案手法を用いた際の，監視トラフィック

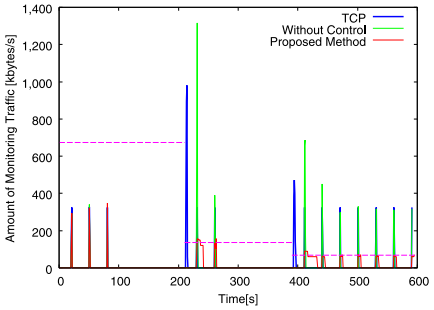

図 6　監視トラフィック量
Fig. 6　Amount of monitoring traffic.

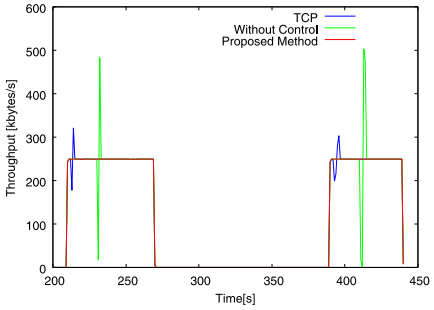

図 7　CBR トラフィックのスループット（MN → Host B）
Fig. 7　Throughput of CBR traffic (transmission is between MN to Host B).

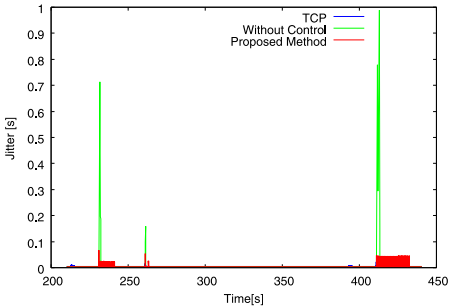

図 8　CBR トラフィックのジッタ（MN → Host B）
Fig. 8　Jitter of CBR traffic (transmission is between MN to Host B).

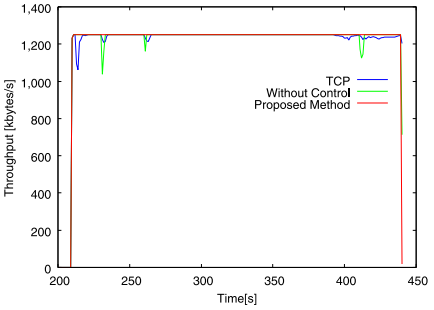

図 9　CBR トラフィックのスループット（Host C.1 → Host B）
Fig. 9　Throughput of CBR traffic (transmission is between Host C.1 to Host B).

の他の通信へ与える影響の軽減効果を確認する．さらに，提案手法で用いる上限値に応じた改善効果を確認するため，上限値を MR のアップリンクの通信帯域の 10%，50%，90%とした場合の MR のアップリンク（リンク A）を流れる監視トラフィック量と 1 台の MN から Host B へ送信する CBR トラフィックのスループットを計測する．

3.4.2　実 験 結 果

MR のアップリンクを流れる監視トラフィック量の変化を**図 6** に示す．なお，図中の横軸と平行に引かれた点線は，各時間帯の MR のアップリンクの通信帯域幅の上限値（10%）を示している．制御なしの場合では，いっせいに監視トラフィックが流れ，特に回線の回復直後は，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] 付近で監視トラフィックが増大しているのは，切断中に送信された Manager からのリクエストが TCP の機能により再送され，回線の回復直後に MR まで届き管理情報が送信されるためである．一方，提案手法の場合では平常時や回線の回復後も，管理情報を分散して送信するため，監視トラフィック量を指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 へ送信レート 2 [Mbps] で流した CBR トラフィックのスループットを**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したり，ジッタが増加したりする箇所が見られる．TCP 手法の場合は，ジッタは増加しないが，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，監視トラフィック量が指定した上限値以下に抑制されるため，スループットの低下やジッタの増加を回避することができている．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 Host B の間の通信を**図 9** に示す．制御なしや TCP 手法の場合，増加した監視トラフィックが HA を通過するため，その影響を受けて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] 付近に比べて，制御なし・TCP 手法のどちらも，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] であるのに対し，210〜230 [s] 付近では 11 [Mbps] であり，後者のときの方が同時に MR のアップリンクを流れる監視トラフィックが多くなり，HA へ 1 度に流れてくる監視トラフィック量が増加するためである．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，HA のネットワークの端末の通信は監視トラフィックの影響を受けず，スループットが低下することなくつね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．

提案手法で用いる上限値を，MR のアップリンクの通信帯域幅の 10%，50%，90%とした場合に，MR のアップリンクを流れる監視トラフィック量の変化を**図 10** に示す．提案手

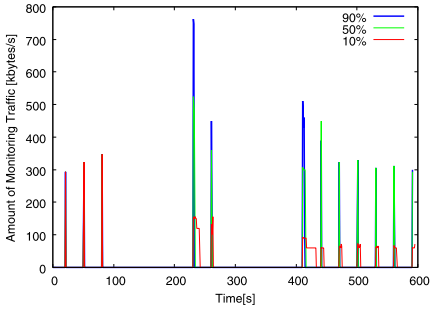

図 10　アップリンクの上限値を変化させた際の MR のアップリンクを流れる監視トラフィック
Fig. 10　Amount of monitoring traffic varying upper limit of the up-link.

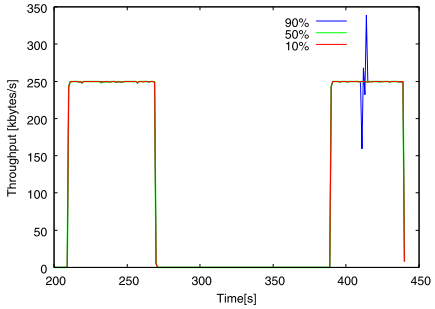

図 11　アップリンクの上限値を変化させた際の CBR トラフィックのスループット（MN → Host B）
Fig. 11　Throughput of CBR traffic varying upper limit of the up-link.

法は，帯域幅の大きさに応じて，監視トラフィック量がほぼ上限値以下に抑制されている．ゆえに，提案手法の効果により，任意に指定した上限値以下に監視トラフィック量を抑制できることが示された．また，提案手法において上限値をそれぞれ 10%，50%，90%とした場合に，1 台の MN から Host B へ送信レート 2 [Mbps] で流した CBR トラフィックのスループットを**図 11** に示す．上限値を通信帯域幅の 10%，50%とした場合，スループットは低下せず一定の値を維持している．一方，上限値を通信帯域幅の 90%とした場合には，流れる監視トラフィック量が 1 度に増加するため，410 [s] 付近でスループットが低下する箇所が生じている．特に 390 [s] 以降は MR のアップリンクの帯域幅が 5.5 [Mbps] と狭くなるため，監視トラフィックによる帯域の占有率が高くなり，CBR トラフィックの通信が妨害される．以上より，提案手法を効果的に機能させるため，通信帯域幅など，状況に合わせて適切な上限値を与えることは重要である．

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，監視トラフィックの増大による他の通信への影響を軽減するため，複数の SNMP メッセージを集約し，全体のメッセージサイズを削減する．具体的には，提案手法は，(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，から構成されている．(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，MR のサブネットワークに所属する複数のノードの管理情報をまとめて Manager へ送信する．また，(2) では MR においてタイムスタンプとともに管理情報を集約して蓄積し，Manager が集約した情報のタイムスタンプを指定して再度リクエストすることにより，収集に失敗した管理情報を効率的に取得することを可能にする．

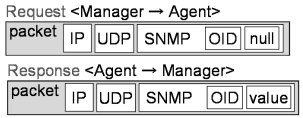

図 12　通常の SNMP メッセージ
Fig. 12　Example of normal SNMP message.

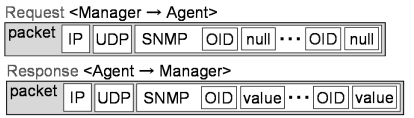

図 13　Bulk 形式の SNMP メッセージ
Fig. 13　Example of bulked SNMP message.

4.2 既存の SNMP メッセージの集約方法

SNMP では，Manager 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 OID（Object Identifier）で指定する．MO には，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．Manager は MO を OID で指定してリクエストを送信し，エージェントはレスポンスとして OID と OID で指定された MO の値を返信する．以上のようにして Manager 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 12** のように 1 メッセージに含まれる OID は 1 つであり，収集する管理情報の個数と同数のリクエスト・レスポンスのパケットが必要となる．複数のリクエスト・レスポンスのパケットが Manager とエージェント間で送受信されるため，監視トラフィックが増大しやすい．そこで，**図 13** のように 1 メッセージ中で複数の OID を指定し，1 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．Bulk 形式の収集手法を用いることにより，Manager・エージェント間で送受信されるメッセージ数を削減し，監視トラフィックの増大を抑制することができる．しかし，この方式は，ノードや時間ごとにそれぞれパケットが必要であるとともに，収集する管理情報の個数と同じだけの数の OID をメッセージ中で指定することが必要であるため，監視トラフィックを削減する余地が残っている．

MO Aggregation MIB [12] を用いた MO Aggregation 方式では，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，Manager とエージェントで共有する．Ag MO 1 つをリクエストで指定し，複数の管理情報を 1 つのレスポンスで取得する．もう 1 つは，リクエストにタイムスタンプ・時間間隔・個数・OID を指定し，複数時間分の管理情報をまとめて取得する．MO Aggregation MIB は単一のノードでの使用が想定されてお

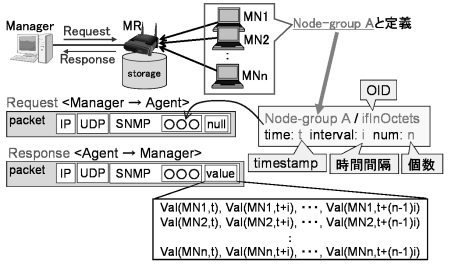

図 14　複数ノードの SNMP メッセージ集約
Fig. 14　Overview of SNMP aggregated message.

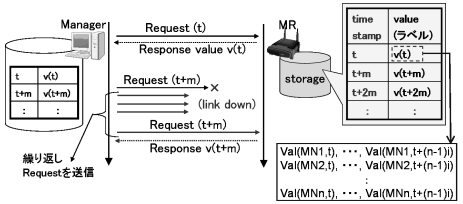

図 15　タイムスタンプによる集約情報の管理
Fig. 15　Overview of management of aggregated information with time stamp.

表 2　パケットサイズに関するパラメータ
Table 2　Parameters of packet size.

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

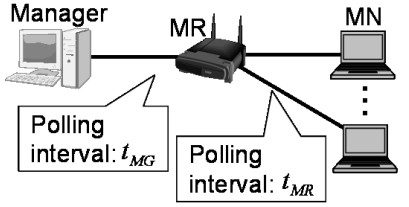

図 16　数値計算に用いたトポロジ
Fig. 16　Topology for experimental network in numerical calculation.

り，複数のノードでの使用に対応していない．また，特定の時間帯の管理情報を集約する方式のため，時間を遡って収集に失敗した管理情報を再度収集することはできない．

4.3　(1) 複数ノードの SNMP メッセージの集約

移動ネットワークでは，MR と MR に接続するノードで構成されるサブネットワークが移動することから，MR のサブネットワークで 1 つの管理対象の単位と見なせる．そこで提案手法では，定期的に MN から管理情報を MR で収集し，Manager との管理情報の送受信は MN の代わりに MR が行い，各 MN からの管理情報をまとめて扱う．また，**図 14** に示すように，複数のノードをまとめたノードグループを定義し，Manager とエージェントである MR において，定義情報を共有する．Manager は MR にノードグループ（図 14 中における Node-group A）のリクエストを送信することで，MR から複数の MN の管理情報を 1 つのレスポンスで取得する．したがって，Manager と各 MN 間で別々に送受信されていたメッセージを 1 つにまとめるだけでなく，1 メッセージ中で複数個指定していた OID を 1 つに集約することが可能となる．また，ノードグループに加え，複数種類の MO をまとめた識別子，タイムスタンプ，時間間隔，個数をリクエストで指定することで，レスポンスとして複数のノードの，複数種類の管理情報を，複数時間分まとめて収集する．これによって，MR のサブネットワークで扱われる SNMP メッセージを集約し，MR のアップリンクを流れる監視トラフィックを削減することができる．

4.4　(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 の移動などによって，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，Manager による管理情報の収集が頻繁に失敗する場合が多くなる．そこで，本手法では，収集に失敗した管理情報の再収集を可能にするため，**図 15** 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．なお，既存の store-and-forward 型の収集手法は，1 つの管理情報を管理するため，1 つのタイムスタンプが必要であったが，本手法では，複数の管理情報を 1 つのタイムスタンプで管理することができる．Manager は管理情報の収集に失敗すると，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，Manager・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 Manager から，切断中に失敗し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，損失した管理情報を効率的に回復することができる．

4.5　数値計算による提案手法の評価

4.5.1　評 価 方 法

提案手法によって監視トラフィックを削減し，損失した管理情報を効率的に回復できることを確認するため，**図 16** に示すトポロジにおいて数値計算により性能を評価した．パケットサイズに関するパラメータは**表 2** で与えた．Manager が 1 度に収集する管理情報数 N は，$N = \frac{t_{MG}}{t_{MR}} \times \sum_{i=1}^{n} m(i)$ で算出することができる．本計算式をもとに，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），提案手法を用いた際の性能を計測する．

- MR のアップリンクを流れる監視トラフィック量

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評価し（今回はレスポンスによるトラフィックのみを調査），提案手法によりどの程度監視トラフィック量を削減することができるかを確認する．

- 管理情報の収集率

  Manager と MR 間のリンクのパケットロス率を変化させた場合の，Manager における管理情報の収集率を計算し，提案手法により損失した管理情報を効果的に回復することができるか確認する．

また，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）とで比較し，提案手法が損失した管理情報を効率的に回復することが可能であることを確認する．

4.5.2 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 Manager 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などの増分である．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) を図示したものを**図 17** 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 の増加にともな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．また，MO Aggregation 方式のメッセージ集約は，4.2 節で述べたように，単一ノードのみに対応しているため，SNMP メッセージ数は，ノードの数だけ分割する必要がある．そのため，得られた結果をもとに，MO Aggregation 方式と提案方式を比較すると，ノード数が 1 の場合には，MO Aggregation 方式のトラフィック量は，提案方式のトラフィック量と同等程度になり，ノード数が増加する場合には，Bulk 方式のトラフィック量に徐々に近づきながら増加するといえる．以上より，提案手法は，他の方式と比較し，監視トラフィック量を効果的に削減し，他の通信への影響を軽減できることが示された．

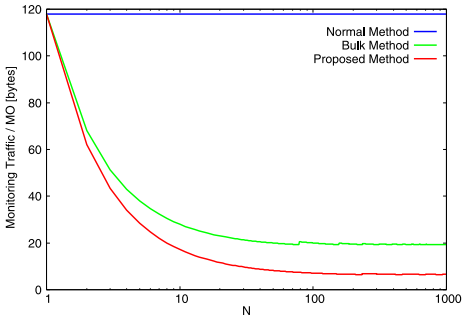

図 17　管理情報 1 項目の取得に必要なトラフィック量
Fig. 17　Amount of monitoring traffic for each Management Object.

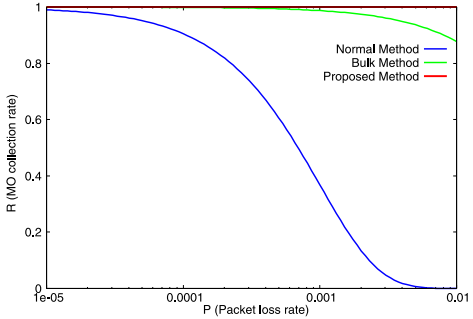

図 18　Manager が管理情報をすべて収集できる確率
Fig. 18　Probability of manager able to collect entire Management Objects.

次に，Manager と MR 間のリンクのパケットロス率 P を変化させた場合に，マネージャが管理情報をすべて収集できる確率 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：$R = 1$ と算出することができる．$t_{MG} = 30$ [s]，$t_{MR} = 6$ [s]，$n = 20$ [nodes]，$m = 10$ [個]，$N = 1000$ とした場合のグラフを**図 18** に示す．Bulk 方式の N_x はメッセージの集約を行う際に MTU を超えないように分割され生じたパケット数であり，最小値は 1 になる．図 18 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，損失した管理情報を回復することができるため，管理情報の損失はない．この結果を用いて提案方式と MO Aggregation 方式を比較することにより，MO Aggregation 方式は，損失した管理情報を回復する機能を有していないため，Bulk 方式と同様に，P の増加により R が減少することが分かる．また，MR の配下のノード数が増加する場合には，SNMP メッセージ数が増加し，Bulk 方式の R に徐々に近づくといえる．以上より，提案方式は，他の

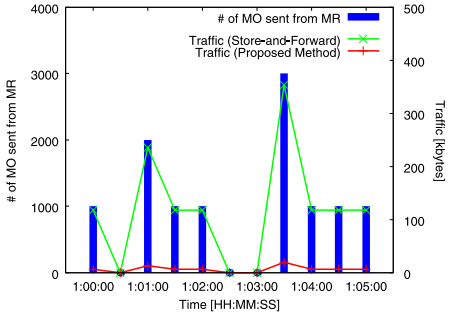

図 19　損失を回復する際に流れる監視トラフィック量
Fig. 19　Amount of monitoring traffic to recover lost data.

方式と比較し，管理情報を効率的に収集できることが示された．

最後に，図 16 のトポロジにおいて，提案手法と S-F 方式を用いる場合に，$t_{MG} = 30$ [s]，$t_{MR} = 6$ [s]，$n = 20$ [nodes]，$m = 10$ [個] として $N = 1000$ として与え，

- 1:00:00〜1:05:00 の時間中，30 [s] 間隔で Manager から MR にポーリングを行う，
- 1:00:05〜1:00:55，1:02:05〜1:03:25 の時間中，Manager と MR の間のリンクが切断する，

を行う．このとき，損失した管理情報を回復するために流れる監視トラフィック量を比較したグラフを**図 19** に示す．図 19 における棒グラフは，MR から送信される管理情報の個数を示しており，Manager と MR のリンクの切断によって，通常の送信に加えて，収集に失敗した管理情報が送信されるため，1:01:00 では通常の 2 倍の 2,000 個，1:03:30 では 3 倍の 3,000 個が送信されている．また，監視トラフィックを示す折れ線では，S-F 手法では損失した管理情報を回復するためトラフィックが倍増しているが，提案手法では，メッセージの集約の効果によりトラフィックの増加を抑制していることが分かる．以上より，提案手法は，S-F 手法のような回復手法と比較し，損失した管理情報を効果的に回復できることが示された．

4.6　実環境での提案手法の評価

4.6.1　実 験 方 法

バスや電車などに搭載されている電圧/温度センサなどの計測機器を MR に接続することを想定して，提案する SNMP メッセージの集約手法によって，計測機器から出力される時系列的データを遠隔から効果的に収集できることを確認するため，**図 20** の環境において，

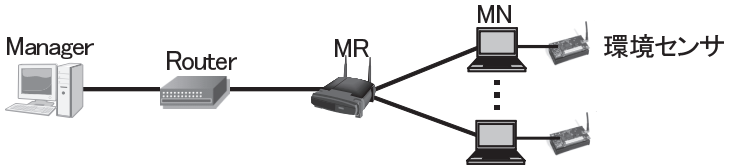

図 20　実環境で実験に用いたトポロジ
Fig. 20　Topology of experimental network in real world.

実機を用いて評価実験を行った．

本実験では，環境センサの管理情報を MR が MN から SNMP 経由で収集・蓄積する SNMP Agent を MN に実装した．また，SNMP メッセージを集約する提案手法を Manager および MR に実装し，提案手法を用いて環境センサから気温や電圧などの管理情報を収集する．Manager は，SNMP メッセージ集約する提案手法を用いて，MR に蓄積された管理情報を収集する．SNMP の通信に関するパラメータとして，Manager・MR 間のポーリング間隔 20 [s]，MR・MN 間のポーリング間隔 10 [s]，MN の台数 n [台]，MN から収集する管理情報の種類 8 [個] で与えた．

以上の環境において，管理情報を収集する際の監視トラフィックの削減効果を確認するため，MN の台数 n を 1〜15 で変化させ，通常方式，Bulk 方式，提案手法のそれぞれを用いた際の，MR のアップリンクを流れる監視トラフィック量（MR から Manager へ送信されるレスポンスのみを考慮）を計測する．また，損失した管理情報を回復する効果を確認するため，MN の台数 $n = 2$ とし，

- 10:00:00〜10:05:00 の間，Manager で継続して管理情報を収集する，
- 10:01:05〜10:01:35，10:03:05〜10:03:55 の時間中，MR と Router の間のリンク（MR のアップリンク）を切断する，

を行った場合に，S-F 手法（store-and-forward 型の収集手法）と提案手法が損失した管理情報を回復するために必要となる監視トラフィック量を計測する．

4.6.2　実 験 結 果

管理情報を収集した際に計測された監視トラフィック量を**図 21** に示す．通常方式は，n の増加にともない必要な監視トラフィック量が倍増しているが，Bulk 方式・提案手法は，n が増加しても監視トラフィック量の増加を抑えている．特に提案手法は，$n \geq 10$ の場合，通常方式と比べ監視トラフィック量を 95%以上削減している．以上のように，提案手法は通常方式と比べて，監視トラフィックを大幅に削減している．

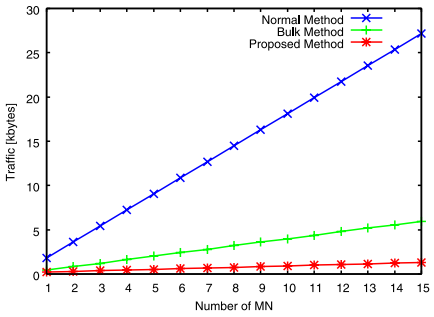

図 21　管理情報収集に必要な監視トラフィック量
Fig. 21　Amount of traffic to collect Management Objects.

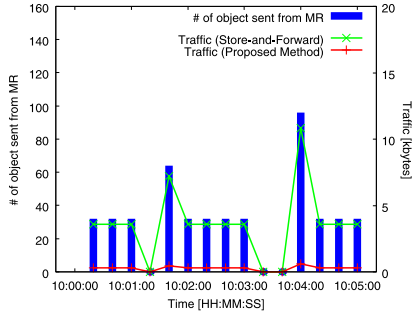

図 22　損失を回復する際に流れる監視トラフィック量
Fig. 22　Amount of monitoring traffic to recover lost data.

次に，損失した管理情報を回復する際の監視トラフィックを計測した結果を**図 22** に示す．棒グラフ（MR から送信される管理情報の個数）を確認すると，MR から Manager に対して通常 20 [s]/10 [s] × 2 [台] × 8 [個] = 32 [個] の管理情報が送信されている．一方，リンクが切断されると，通常の送信に加えて，収集に失敗した管理情報の再送信が重なるため，10:01:40 に，通常の 2 倍の 64 個，10:04:00 では 3 倍の 96 個が送信されている．また，S-F 手法ではリンク切断中の損失した管理情報を回復するため，10:01:40，10:04:00 に流れる監視トラフィックが倍増している．一方，提案手法は SNMP メッセージの集約の効果によって，データ損失を回復する際に監視トラフィックを増加させることなく，損失した管理情報を効率的に回復している．

これらの結果は数値計算の結果と一致しており，実環境においても提案手法が有効に機能するといえる．以上より，提案手法は，実環境において監視トラフィックの増加を効果的に削減し，他の通信への影響を軽減することができることが示された．

5. 2 つの手法の適用範囲について

本稿では，監視トラフィック量が増大するという問題に対して，監視トラフィックの送信を分散させる手法と，監視トラフィック量を削減する 2 つの手法を提案した．提案手法 1 は，接続する各ノードの管理情報を収集・蓄積し，情報の送信をバッファリングすることで送信量を調整している．これにより，監視トラフィックを一定の上限値以下に抑制し，通信帯域の占有や圧迫を回避している．狭帯域の通信路に大量の監視トラフィックが送信される場合には，管理情報の送信の遅延・分割を大きくすることで問題を軽減することができるため，本方式の適用範囲は，比較的広い．一方，提案手法 2 は，提案手法 1 と比較し，監視トラフィック量を大幅に削減することができる．しかしながら，狭帯域幅の通信経路に大量の監視トラフィック量が送信される場合には，トラフィックの削減効果は限られるため，通信帯域幅が狭く少量の監視トラフィックで帯域の圧迫が発生する状況では，提案手法 2 を適用することは困難である．そこで，各手法の特徴をふまえ，適用範囲が広い提案手法 1 と，改善効果高いが適用範囲が狭い提案手法 2 を組み合わせることにより，各手法を単独で用いるよりも効果的に機能することが期待できる．提案手法 1 と提案手法 2 を組み合わせた手法の検討は，今後の課題とする．

6. ま と め

本稿では，監視トラフィックが通信帯域を占有・圧迫する問題を軽減し，移動ネットワークを円滑に管理監視するため，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．2 つの方式に対して性能評価を行い，その有効性を示した．今後は，2 つの提案手法を組み合わせた手法を検討し，遠隔から移動ネットワークを効果的に監視する仕組みの確立を目指す．

参 考 文 献

1) Devarapalli, V., Wakikawa, R., Petrescu, A. and Thubert, P.: Network Mobility (NEMO) Basic Support Protocol, RFC3963 (2005).
2) Case, J., Fedor, M., Schoffstall, M. and Davin, J.: Simple Network Management Protocol (SNMP), RFC1157 (1990).
3) Koide, K., Kitagata, G., Kamiyama, H., Chrakraborty, D., Keeni, G.M. and Shiratori, N.: MobiSNMP – A model for Remote Information Collection from Moving Entities using SNMP over MobileIPv6, *IEICE Trans. Commun.*, Vol.E88-B, No.12, pp.4481–4489 (2005).
4) Keeni, G.M., Koide, K., Nagami, K. and Gundavelli, S.: Mobile IPv6 Management Information Base, RFC4295 (2006).
5) Gundavelli, S., Keeni, G.M., Koide, K. and Nagami, K.: Network Mobility (NEMO) Management Information Base, RFC5488 (2009).
6) Harrington, D., Presuhn, R. and Wijnen, B.: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, RFC3411 (2002).
7) Floyd, S. and Jacobson, V.: Link-sharing and Resource Management Models for

Packet Networks, *IEEE/ACM Trans. Networking*, Vol.3, No.4 (1995).
8) Wang, C., Li, B., Sohraby, K., Daneshmand, M. and Hu, Y.: 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).
9) Zawodniok, M. and Jagannathan, S.: Predictive Congestion Control Protocol for Wireless Sensor Networks, *IEEE Trans. Wireless Communications*, Vol.6, Issue 11, pp.3955–3963 (2007).
10) Shin, K.S., Jung, J.H., Cheon, J.Y. and Choi, S.B.: 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).
11) hyun Park, S. and soon Park, M.: An efficient transmission for large MIB tables in polling-based SNMP, *ICT 2003* (*International Conference on Telecommunications*), pp.246–252 (2003).
12) Keeni, G.M.: The Management Object Aggregation MIB, RFC4498 (2006).

(平成 22 年 5 月 21 日受付)
(平成 22 年 12 月 1 日採録)

中村　直毅（正会員）

2006 年東北大学大学院情報科学研究科博士課程単位取退学．博士（情報科学）．2006 年同大学院医学系研究科助手．2007 年同研究科助教．無線アドホックネットワークおよびネットワーク管理手法等の研究開発に従事．情報処理学会第 44 回 MBL 研究会優秀発表賞，DICOMO2010 優秀論文賞受賞．

丸山　貴史

2009 年東北大学大学院情報科学研究科修士課程修了．無線ネットワーク管理手法の研究に従事．2009 年株式会社日立製作所入社．

菅沼　拓夫（正会員）

1997 年千葉工業大学大学院博士後期課程修了．博士（工学）．1997 年東北大学電気通信研究所助手，2003 年同研究所助教授，2007 年同研究所准教授を経て，2010 年から東北大学サイバーサイエンスセンター教授．やわらかいネットワーク，エージェント指向コンピューティング，ネットワークミドルウェア，共生コンピューティング等の研究開発に従事．UIC2007 Outstanding Paper Award 等受賞．IEEE，電子情報通信学会各会員．

グレン マンスフィールド キニ

1988 年東北大学大学院工学研究科情報工学博士課程修了．1999 年株式会社サイバー・ソリューションズ代表取締役社長．ネットワーク管理/セキュリティ/モビリティ等の研究および IETF における標準化活動に従事．ACM，IEEE 各会員．

白鳥　則郎（フェロー）

1977 年東北大学大学院博士課程修了．1990 年同大学工学部教授を経て 1993 年同電気通信研究所教授．2010 年同大学客員教授・名誉教授，公立はこだて未来大学理事．人と情報環境の共生等の研究に従事．文部科学大臣表彰「研究部門」，本会功績賞，電子情報通信学会・業績賞等受賞．本会フェロー，IEEE フェロー，電子情報通信学会フェロー．本会会長．