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

2008－CSEC－43 (1)
2008／12／5

# アドホックネットワークにおける クラスタリングを用いた階層型トレースバック技術

谷田貝 健　笹瀬 巌

慶應義塾大学理工学部情報工学科 〒223-8522 横浜市港北区 3-14-1

E-mail: yatagai@sasase.ics.keio.ac.jp, sasase@ics.keio.ac.jp

あらまし　近年，送信されたパケットの送信元を特定する技術であるトレースバック技術を，無線アドホックネットワークへ適応する研究が行われている．無線アドホックネットワークでは，インターネットにおけるルータのような固定基盤を期待できないため，トレースバック情報の保持やトレースパスの形成といった処理を，各ノードが単独に行わなければならない．そのため，各ノードの移動やトポロジの変化によるトレースパス形成の成功率の低下や，ネットワーク全体へのトレースバック情報の問い合わせによる通信量の増大といった問題点が存在している．そこで，本論文では，クラスタリング技術を用いることで，複数のノード単位でトレースバック情報の保持，トレースパスの形成を行う方式を提案する．提案方式では，各クラスタヘッド間での情報のやり取りのみでトレースバック処理を行えるため，トレースバック情報の問い合わせ回数や処理時間を低減することが可能となる．計算機シミュレーションにより，トレースバックに要する問い合わせ回数，トレースバックの成功率の評価を行い，提案方式が従来方式に比べ，少ない問い合わせ回数で成功率の高いトレースバックを行えることを示す．

**キーワード**　アドホックネットワーク，クラスタリング，トレースバック技術

# Hierarchical Traceback Method Using Clustering for Mobile Ad Hoc Networks

Takeshi Yatagai　and　Iwao SASASE

Dept. of Information and Computer Science, Keio University

3-14-1 Hiyoshi, Kohoku, Yokohama-shi, Kanagawa, 223-8522 Japan

E-mail: yatagai@sasase.ics.keio.ac.jp, sasase@ics.keio.ac.jp

**Abstract**　Recently, there are many researches about a traceback method which specifies the source of transmitted packets in mobile ad-hoc network. In mobile ad-hoc network, since there is no fixed infrastructure like a router on the internet, each node has to record the trace backing information and reconstruct the trace-path by itself. Therefore, the variation of network topology by mobility of nodes causes a degradation of success rate of the trace-path reconstruction and increase of traffic by inquiring trace back information to the all nodes on the network. In this paper, we propose the traceback method that some nodes act as a unit by using clustering technique. In our scheme, because traceback is handled by only clusterheads we can reduce the traffic and time for taraceback. By a computer simulation, we evaluate the number of queries and success rate of traceback and show that the proposed scheme can reduce the both number of queries and report a high success rate of traceback.

**Keyword**　Ad Hoc Network, Clustering, Traceback Method

## 1. 序論

現在，ネットワークの普及により，インターネットは企業や家庭内のものから，携帯端末など，野外のあらゆる場所まで広がっており，近年では，各端末が協調してパケットのやり取りを行うことで，固定基盤を必要とせずにネットワークを構築する無線アドホックネットワークが注目されている．その一方で，ネットワークに対する様々な脅威も存在している．その一つとして，DoS(Denial of Service：サービス拒否)攻撃，DDoS(Distributed DoS：分散型サービス拒否)攻撃といった脅威が挙げられる．DoS 攻撃とは，悪意のある端末や，ウイルスに感染した端末から，標的となるサーバやクライアント端末に対し大量のパケットを送信することで，通信回線やサーバのリソースを過度に消費させ，サービスの提供を妨げる攻撃である．また，単一の端末から攻撃が発生する DoS 攻撃に加え，複数の端末から攻撃を仕掛ける DDoS 攻撃も大きな問題となっている．これらの脅威に対し，攻撃パケットの発信元を特定する技術として，IP トレースバックという技術が研究されている．代表的な IP トレースバック技術としては，ある確率でパケット中継時にマークをつけ

るマーキング方式[1]，ルータがダイジェストと呼ばれる各パケットに対しユニークな値を記憶するHash-Based方式[2]などが提案されている．しかし，これら既存技術はインターネット上での利用を想定しており，固定基盤が存在せず，各端末が移動を繰り返すアドホックネットワークでの利用を想定していない．そこで，各端末が自身の通信に加え，固定基盤の役割を兼ねることで既存のトレースバック方式を無線ネットワークに適応する方式が研究されている．無線ネットワークに対し，パケットマーキング方式を適応している方式としては[3][4]が提案されている．[3]では各端末が移動をしないというセンサーネットワークに特化した方式であり，頻繁にノードの移動が行われるアドホックネットワークへの適応は困難であると考える．また，[4]ではパケットマーキング方式をアドホックネットワークへ適応した場合の評価を行っているが，ネットワークサイズが大きくなった場合や，攻撃経路が複数にわたった場合などには，トレースバックの成功率は約6割にまで低下している．パケットマーキング方式では，パケット長の増加を防ぐため，トレースバック情報は複数のパケットに分散させて記録されるが，全ての同じ経路を通じた攻撃を前提としている．そのため，トポロジが常に変化する無線アドホックネットワークにおいて転送経路を特定することは困難であると考えられる．一方，Hash-Based方式では，各ルータの保存したダイジェストをたどってゆくことでトレースパスを形成するため，パケットの送信元を特定することが可能となり，トレースバックに必要なパケットは一つで済むため，全ての攻撃パケットが同じ経路で転送されていない場合でも経路を辿ることが可能となる．Hash-Based方式を無線アドホックネットワークへ適応した方式としては[5][6]が提案されている．これらの方式では，各ノードが転送したパケットのハッシュ値の他にTTL(Time To Live)，および隣接ノードストを記録することで，ネットワークトポロジが変化した場合においてもパケットを転送したノードの順序を推定することが可能となる．しかし，これらの方式ではトレースバック情報の保持やトレースバック処理を各ノードが単独で行っているため，ネットワークに存在するすべてのノードに対しトレース情報の問い合わせを行う必要があり，ネットワーク規模の拡大に伴う通信量の増大や，ノードの移動により，電波範囲外に外れた場合にトレースバック情報の収集が困難になるなど，トレースパスが欠落する確率が高くなるといった問題がある．

そこで本論文では，クラスタリング技術を用いることで，ネットワーク上に存在するノードをクラスタ単位に分割し，クラスタ単位でトレースバック情報の保持，トレースパスの形成を行う方式を提案する．本方式では，各クラスタおけるクラスタヘッドをトレースバック情報の管理ノードとし，クラスタに属する他ノードのトレースバック情報を集中管理することで，クラスタヘッド間での情報のやり取りのみでトレースバック処理を行うことが可能となり，トレースバック情報の問い合わせ回数や処理時間を低減することができる．計算機シミュレーションにより，トレースバックに要する問い合わせ回数，トレースバックの成功率の評価を行い，提案方式が従来方式に比べ，少ない問い合わせ回数で成功率の高いトレースバックを行えることを示す．以下，2章で従来研究，3章で提案方式についてそれぞれ説明をし，4章で特性評価を行う．最後に5章でまとめる．

## 2. 従来研究

### 2.1 Hotspot-Based トレースバック方式[5]

従来方式である Hotspot-Based トレースバックは，無線アドホックネットワークでの利用を考慮し，各ノードが情報を保存することで，固定的なモニタポイントを想定せずに，パケットを中継したノードの順序を推定することが可能な Hash-Based 方式のトレースバック方式である．パケットを転送したノードはそのパケットの TTL，および自ノードの隣接ノードリストを記録する．TTL はノードを経由するごとに 1 減少するため，記録された TTL が大きい順にパケットが転送されたと推定できる．また，隣接ノードリストとはノードの電波範囲内に存在する隣接ノードのリストのことであり，周囲のノードと定期的に HELLO メッセージをやりとりすることで更新される．トレースバックを開始した時点で既にネットワークから離脱していたなどの理由でパケットを中継したノードからトレースバック情報が得られなかった場合は，その周囲のノードの隣接ノードリストから共通するノードを見つけ出し，中継したノードを推定することが可能である．

#### 2.1.1 情報の記録

Hotspot-Based トレースバックでは，各ノードはパケットを転送する際，そのパケットのハッシュ値の他に，TTL，およびノードの隣接ノードリストを記録する．

図 1 に，Hotspot-Based トレースバックにおけるパケットの転送の様子を示す．図 1 おいてパケット p がノード A から，ノード B，C，E を経由してノード F へと送信された場合を示している．まず，ノード A はパケット $p$ のハッシュ値 $H(p)$ を，TTL として 6 を，隣接ノードリストとして B を記録した後，TTL を 1 減らしてパケットを転送する．ノード B，C，E も同様にしてパケットの転送を行う．

#### 2.1.2 ハッシュ値の問い合わせ

ノード F は，攻撃を検知すると，攻撃パケットのハッシュ値を計算し，隣接ノードに対しそのハッシュ値

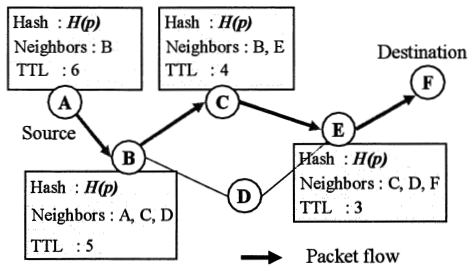


図 1.従来方式におけるパケット転送の概要

を記録しているかを問い合わせる．問い合わせを受けたノードが該当するハッシュ値を記録していた場合，(ノード ID，TTL，隣接ノードリスト)の形式で表されるトレースバック情報を問合せノードへ返信する．ここでは，ノードFがトレースバックを行う状況を説明する．ノードFは，パケット $p$ に対するトレースバック情報を問い合わせるメッセージをネットワーク全体へブロードキャストし，問合せを受けた各ノードは自身の持つ，パケット $p$ に対するトレースバック情報を返信する．例えば，ノード C が問合せを受けた場合，ノード C は(ID:C，TTL:4，隣接ノード:B, E)という形式のトレースバック情報を通知する．他のノードも同様にトレースバック情報を通知するが，同じクエリに対して通知を行うのは一度だけである．

### 2.1.3 攻撃経路の推定

ノードFは，各ノードから送信されてきたトレースバック情報に基づき,パケットの転送経路を推定する．ノードFが受信したトレースバック情報は以下の通りである．

(ID:A, TTL:6，隣接ノード:B)
(ID:B, TTL:5，隣接ノード:A, C, D)
(ID:C, TTL:4，隣接ノード:B, E)
(ID:D, TTL:3，隣接ノード:C, D, F)

トレースバック情報中のTTLはノードAのものから順にノードDまで1ずつ減少している．したがって，攻撃パケットはこの順にノードを経由したと考えられ，攻撃経路はA→B→C→E→Fと推定される．

トレースバックを開始した際に，攻撃パケットを転送したノードが既にネットワークから離脱していたり，他の全てのノードの電波範囲外に移動していて，トレースバック情報が得られなかった場合，そのノードの周囲のノードから送信されてきた隣接ノードリストを参照し，両者に共通するノードを推定する攻撃経路に含める．ただし，共通するノードが複数ある場合は，攻撃経路を一つに特定することはできず，ネットワーク管理者に報告するに留める．例として，図2において，TTLが4であるトレースバック情報を持つノードCがトレースバック情報を送信しなかった場合を説明する．この場合，TTLがそれぞれ5, 3であるノードB，およびEが，ノードCの前後にいたものとし，ノードB, Dから送信されてきたトレースバック情報中の隣接ノードリストを調べる．その結果，ノードB，E両者の隣接ノードに含まれているノードCがその間に存在していたと推定する．Hotspot-Basedトレースバックにおいて，問合せメッセージはネットワーク全体にブロードキャストされるため，存在するノード数に比例してトラヒックは増加する．この問題はネットワークの規模が大きくなるほど深刻になる．また，問合せを行ったノードは，すべてのノードからの返信を待つことが望ましいが，ネットワーク上に存在するノード数を知らない場合，どれほどの時間だけ変身を待てば良いかわからず，トレースバックにかかる時間が増大してしまうといった問題点も存在する．

### 2.2 クラスタリング技術（ID 法）

クラスタリング技術とは，ネットワークを複数のクラスタと呼ばれる端末の集合に分割し，クラスタをクラスタヘッドと呼ばれる代表ノードに管理させる手法である．現在，様々なクラスタリング技術が研究されているが，最も単純であり，処理コストの少ない方式として，ID法が知られている[7]．ID法は各ノードがIDとなる乱数を発生し，周囲のノードの中で最大のIDを持つノードをクラスタヘッドとするクラスタリング技術ある．ノードがクラスタヘッド選ばれた場合，自身がクラスタヘッドであることをネットワーク全体へフラッディングし，クラスタヘッドリストを生成しることで，ネットワーク上に存在するクラスタヘッドを知ることができる．ID法を用いた場合，他のクラスタリング手法に比べ，クラスタヘッドの数が多くなることが知られている[8]．

## 3. 提案方式

本研究では，クラスタリング技術を用いることで，ネットワーク上のノードをクラスタに分割し，クラスタヘッドがトレースバック情報を集中管理することで，クラスタ単位でのトレースバックを行う階層型トレースバック方式を提案する．提案方式では，排他的論理輪を用いることでトレースバック情報の集中管理によるクラスタヘッドのメモリ消費を抑え，同時に，クラスタ内でのトレースパスの形成を行う方式を提案する．また，各クラスタヘッドが保持する情報からクラスタ間でのトレースパスを形成する方式を提案する．

### 3.1 クラスタリングの再構築

提案方式では，2.2節で説明したID方式を用いて初期クラスタリング処理が行う．しかし，アドホックネットワークではノードの位置は常に変化するため，最適なクラスタを再構築する必要がある．ノードの移動により，自身の属するクラスタヘッドが電波範囲内

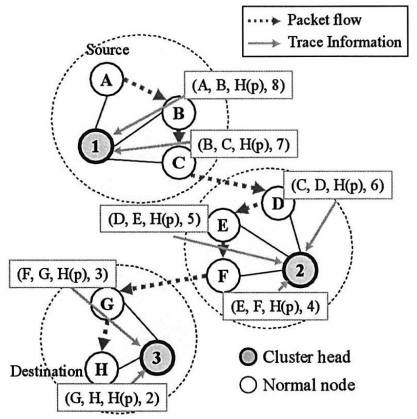


図 2.提案方式におけるトレースバック情報の収集

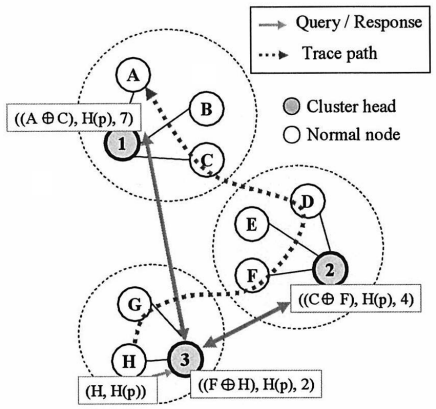


図 3.提案方式における外部トレースバック

から外れてしまった場合，子ノードは別のクラスタヘッドに属するか，もしくは，自身がクラスタヘッドに立候補する．クラスタから孤立した子ノードは，新たに所属するクラスタを探すために，電波範囲内のノードに対し孤立したこと通知するメッセージをブロードキャストする．電波範囲内に他のクラスタヘッドが存在した場合，クラスタヘッドは孤立ノードに対し受け入れを許可するメッセージを送信し，クラスタを再構築する．一方，電波範囲にクラスタヘッドが存在していない場合，初期クラスタリング同様，最小 ID 法を用いてクラスタリングを行うことで，クラスタの再構築を行う．

### 3.2 トレースバック情報の収集・内部トレースバック

本提案方式におけるトレースバック情報の収集の様子を図 2 に示す．図 2 ではノード 1，2，3 をクラスタヘッドとするクラスタに対し，A から H までのノードが属していることを想定し，ノード A を送信元とし，ノード H に向けてパケット p の送信が行われた場合を仮定する．

**・手順 1 ：レースバック情報の収集**

各ノードはパケットを受信・中継した際に，以下に示す情報を自信のクラスタヘッドへ送信する．

（受信元 IP アドレス，自身の IP アドレス，
パケットのハッシュ値，パケットの TTL）

クラスタヘッドは受け取ったトレースバック情報の中から，同じハッシュ値が記されている情報を検索し，TTL の値に対し降順に並べ替えを行う．例として，図 2 においてクラスタヘッド 1, 2, 3 はハッシュ値 ***H(p)*** に関し，以下に示す情報をそれぞれ持っている．

・ クラスタヘッド 1

(A, B, H(p), 8)
(B, C, H(p), 7)

・ クラスタヘッド 2

(C, D, H(p), 6)
(D, E, H(p), 5)
(E, F, H(p), 4)

・ クラスタヘッド 3

(F, G, H(p), 3)
(G, H, H(p), 2)

**・手順 2 ：内部トレースパスの形成**

各クラスタヘッドがこれらの情報をそのまま保持してしまうと，クラスタヘッドにおけるメモリ消費量は自身のクラスタに存在する子ノードの数に比例して増大してしまうことが考えられため，提案方式では排他的論理輪を用いることでこれを回避する．

トレースバック情報を受信したクラスタヘッドは，保持する 2 つの情報から自身のクラスタ内でのパケットの流れを復元する．図 2 の例では，クラスタヘッド 1 は A→C，クラスタヘッド 2 は C→F，クラスタヘッド 3 は F→H というパスを復元することとなる．

**・手順 3 ：情報の保持**

次に各クラスタヘッドは手順 2 で求めたトレースパスの始点・終点ノードの IP アドレスの排他的論理輪，ハッシュ値，用いた情報の中で最も小さい TTL の値を保持する．

図 2 であれば，各クラスタヘッドは以下に示す情報をそれぞれ保持している．

・クラスタヘッド 1

((A ⊕ C), ***H(p)***, 7)

・クラスタヘッド 2

((C ⊕ F), ***H(p)***, 4)

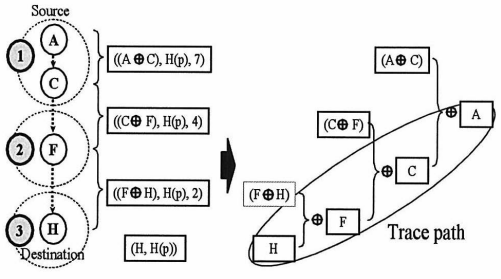


図 4.外部トレースにおける排他的論理和計算

・クラスタヘッド 3

((F⊕H), ***H(p)***, 2)

このように，各クラスタヘッドは，始点・終点ノードの IP アドレスを，排他的論理和を用いて纏めた値のみの保持となるため，自身のクラスタに属する子ノードが増加した場合であっても，クラスタヘッドのメモリ消費量の増大を防ぐことが可能となる．

### 3.3 外部トレースバック

図 3 にクラスタ間の外部トレースバック処理の様子を示す．図 3 において，クラスタヘッド 1，2，3 は 3.2 節で説明した内部トレースバックを終了した状態であるとすし，クラスタヘッド 3 のクラスタに属するノード H からパケット ***p*** に対するトレースバック要求が行われた場合を例に，外部トレースバック処理の手順を以下に説明する．

**・手順１：トレースバック要求**

ノード H は自身が属するクラスタのクラスタヘッドであるクラスタヘッド 3 に対し，自身の IP アドレスとトレースバックを行うパケットのハッシュ値に関する情報(H, ***H(p)***)を送信する．

**・手順２：トレースバック情報の要求**

トレースバック要求を受けたクラスタヘッド3は，自身の保持するクラスタヘッドリストに記載されている順番に，パケット***p***に関するトレースバック情報の要求を行う．図3では，クラスタヘッド1，2に対しトレースバック情報の要求を行う．

トレースバック情報の要求を受けたクラスタヘッド 1，2 は自身の保持するトレースバック情報の中からパケット ***p*** に関する情報を探しだし，クラスタヘッド 3 へ送信する．図 3 では，クラスタヘッド 1 は((A⊕C), ***H(p)***, 7)を，クラスタヘッド 2 は((C⊕F), ***H(p)***, 4)をそれぞれ送信する．

**・手順３：トレースバック処理**

トレースバック情報を受信したクラスタヘッド3は，受信したトレースバック情報を元に，クラスタ間での外部トレースバック処理を行う．まず，受信したトレースバック情報をTTLの値に対して昇順に並べ替え，図4に示すように，IPアドレス同士の排他的論理和を計算する．各クラスタヘッドから受信したトレースバック情報には，クラスタ内における各末端ノード（隣接クラスタに属すノードへパケットを転送したノード）のIPアドレスが2回ずつ現れる．そのため，排他的論理和の計算を繰り返すことで，(b⊕a)⊕b=aという排他的論理和の性質から，中間の経由ノードのIPアドレス情報は打ち消しあうこととなり，終点ノードのIPアドレスとの排他的論理和を繰り返してゆくことで，パケットの始点ノードのIPアドレスを取り出すことができる．この計算により，図4ではA→Hといったトレースパスが形成されることとなる．

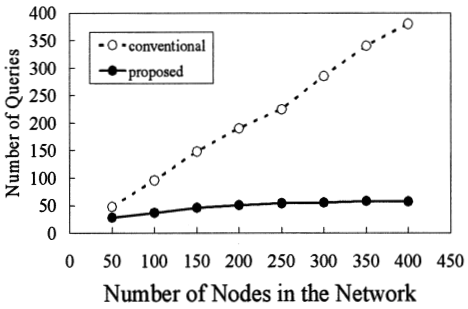


図5.トレースバックに必要な問合せ回数

## 4. 特性評価

提案方式の有効性を検証するために，トレースバックに必要となる問合せ要求の回数，トレースバック成功率の評価を行う．ノードの移動モデルはランダムウェイポイントとし，シミュレーション範囲は 1000m×1000m，ノードの電波範囲は 150m とする．

### 4.1 トレースバックに要する時間

従来方式では，トレースバック要求を受けたノードは，ネットワーク全体のノードに対し，トレースバック情報の問合せを行うため，必要な情報を収集するために多くの時間を要するとともに，すべての情報を受け取れたかどうかの判別が困難であるため，ある一定のタイムアウトを設定する必要がある．これに対して提案方式では，トレースバック情報の問合せは，リストに従いクラスタヘッド間のみで行われるため，必要となる情報のすべての情報を受信できたかどうかを判断することが可能となり，収集にかかる時間が短縮できる，タイムアウトなどの設定を行う必要がない．

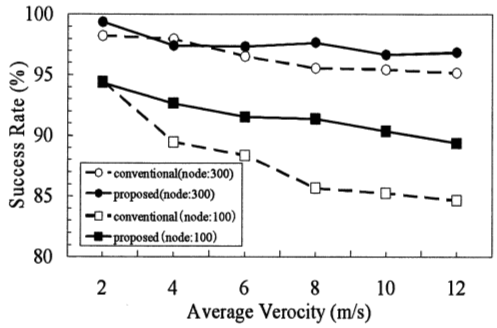


図 6.トレースバックの成功率

### 4.2 トレースバック情報の問合せ回数

図 5 にトレースバックに必要となる問合せ回数を示す．従来方式はネットワーク全体への問合せが必要であったため，ネットワーク上に存在するノード数に比例して問合せ回数が増加していることがわかるが，提案方式ではクラスタヘッドへの問合せのみトレースバックが行えるため，ノード数が増加した場合であっても，従来方式に比べて，必要な問合せ回数を低減できることがわかる．

### 4.3 トレースバックの成功率

図 6 にノードの平均移動速度に対するトレースバック処理の成功率を示す．図 6 から，提案方式は従来に比べて，高いトレースバック成功率を示していることがわかる．特に，ノードの平均移動速度が高い場合であっても，従来に比べてトレースバック成功率の低下を防いでいる．これは，クラスタリングを用いてトレースバック情報を集中管理することで，ノードの移動によるトレースパスの欠落を防いでいるためと考える．また，本提案方式はノードの密度が高いほど，有効な方式であると言える．

### 4.4 クラスタヘッドのメモリ消費の増加量

図 7 に提案方式を用いることによる，クラスタヘッドにおけるメモリ消費の増加量を示す．図 7 より，ノード数が 300 と多い場合であっても，クラスタヘッドにおけるメモリ消費量は 3Mbytes 低くさえられており，現在一般的な端末を用いた場合であっても，本方式の実装が実現可能な数値であると考える．

## 5. 結論

本研究では，クラスタリング技術を用いることで，ネットワーク上に存在するノードをクラスタ単位に分割し，クラスタ単位でトレースバック情報の保持，トレースパスの形成を行う方式を提案した．本方式では，各クラスタヘッド間での情報のやり取りのみでトレースバック処理を行ことで，トレースバック情報の問い合わせ回数や処理時間を低減した．また，計算機シミュレーションにより，トレースバックに要する問い合わせ回数，トレースバックの成功率の評価を行い，提案方式が従来方式に比べ，少ない問い合わせ回数で成功率の高いトレースバックを行えることを示した．

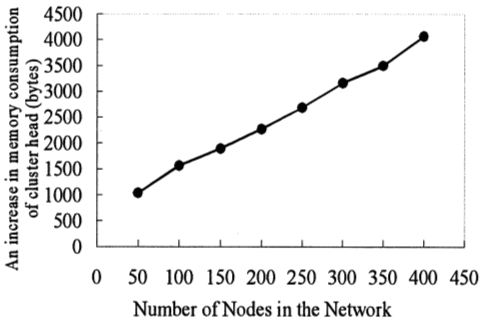


図 7.クラスタヘッドにおけるメモリ消費の増加量

## 謝　辞

本研究の一部はグローバル COE プログラム「アクセス空間支援基盤技術の高度国際連携」により行われた．また，本研究を進めるにあたり，有益な助言を頂いた KDDI 研究所の竹森敬祐氏に，深く感謝する．

## 文　献

[1] Stefan Savage, David Wetherall, Anna Karlin, Tom Anderson, “Practical Network Support for IP Traceback” ACM SIGCOMM, pp.224-236, 2000

[2] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez‡, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer et al, “Hash-Based IP Traceback”, ACM SIGCOMM, pp.3-14 2001

[3] Feng Yang, Xuehai Zhang, Jing Xie, “On the performance of Probabilistic Packet Marking for Traceback in Sensor Networks”, IEEE Consumer Communications and Networking Conference (CCNC), pp.682-686 2008

[4] Vrilynn L. L. Thing, Henry C. J. Lee, “IP Traceback for Wireless Ad-hoc Networks”, IEEE Vehicular Technology Conference, pp.3286-3290, Sept. 2004

[5] Yi-an Huang, Wenke Lee, “Hotspot-Based Traceback for Mobile Ad Hoc Networks”, ACM Proceedings of the 4th ACM workshop on Wireless security, pp.43-54, Sept. 2005

[6] Naofumi Sugaya, Takeshi Yatagai, Iwao Sasase, ”Hotspot-Based traceback scheme iusing overhearing in mobile ad-hoc network”, The 11th International Symposium on Wireless Personal Multimedia Communications (WPMC), Sept. 2008

[7] A. Ephremides, J.E. Anthony, and D.J. Baker, “A designconcept for reliable mobile radio networks with frequency hopping signaling,” Proc. IEEE, vol.75, no.1, pp.56-73, 1987

[8] 谷口博人，井上美智子，増沢利光，藤原秀雄，“アドホックネットワークにおけるクラスタ構成法”，電子情報通信学会論文誌，Vol.J84-D-1, No.2, pp.127-135, 2001 年 2 月