MANET における信頼性を考慮した証拠収集手法の提案

三浦愛美† 中村嘉隆†† 白石陽†† 高橋修††

近年，携帯端末同士を無線で接続することによりネットワークを構築する MANET(Mobile Ad-hoc Network)と呼ばれる技術の研究が活発化している．しかし，不特定多数のノードから構成される MANET にはセキュリティ上の問題が多数存在している．一般的に，このような問題の解決手法では誤検知等による個々の端末への影響は考慮されていない場合が多い．そのため，正常なノードであっても通信を制限されるなどといった不当な扱いを受ける可能性がある．そこで本研究では，客観的に評価可能な証拠を各ノードが作成・収集することにより，自身の行動の証明を行うシステムを提案する．

A proposal for an evidence-collection method considering reliability in MANET.

MANAMI MIURA† YOSHITAKA NAKAMURA††
YOH SHIRAISHI†† OSAMU TAKAHASHI††

In recent years, MANET (Mobile Ad-hoc Network) becomes an active area of research. MANET is technology of creating a wireless network by connecting mobile devices to each other. However, there are a lot of security concerns because MANET is composed of the general public. In general, solutions for these problems give little thought about the effect of false detection on individual devices. As a result, a normal node will be jamming of communication by error detection in communications. Therefore、I propose a system that individual devices gather evidence in relation to self-performed action. The evidence can make a dispassionate assessment of self-performed action.

†公立はこだて未来大学大学院
Graduate School of Future University Hakodate
††公立はこだて未来大学
Future University Hakodate

1. はじめに

近年，既存のインフラ環境に依存することなくネットワークの構築が可能なアドホックネットワークに関する研究が活発化している．特に，移動可能な携帯端末同士を無線通信でリンクさせることにより構築される MANET(Mobile Ad-hoc Network) [1]は，インフラ構築が困難な災害現場や海上，上空等での利用も期待されている．

現在のところ MANET にはセキュリティ面での課題がいくつか残されている[2][3]．例えば，通常のインターネットとは異なりデータを中継するノードが信頼できるとは限らないため，攻撃を仕掛けられる可能性を考慮しなければならない．また，利己的に振る舞うセルフィッシュノード等が出現すると，ネットワーク自体が利用不能となってしまう可能性がある．このような情報システムにおけるセキュリティ上の事件や問題のことをセキュリティインシデントと呼ぶ．

MANET におけるセキュリティインシデントへの対策法は，ネットワーク全体としてのセキュリティを高めるようなものが多い．そのため，個々の端末への影響は考慮されていない場合が多いのが現状である．これにより，正常なノードであっても通信に制限を受ける等の制裁が行われる可能性が考えられる．そこで，正常なノードが攻撃ノードと誤認されてしまった場合にえん罪であったことを証明する必要がある．

以上を踏まえ，本研究ではログ等の電子的記録を収集・分析し，その法的な証拠性を明らかにするディジタルフォレンジック[4][5][6]の技術に着目した．現在の MANET におけるセキュリティインシデント検出システムは，その特性上，局所的なパケット増加による接続性の低下や電波干渉等が発生すると誤検出が増加する傾向にある．そのため MANET におけるディジタルフォレンジックは，不正者・犯罪者の同定というよりも，えん罪であったことの証明を行うという意味合いが強い．この事後対処の技術を用いて，各ノードが自身の行動に関する証拠を収集するシステムの構築を行う．

しかし，無闇に証拠収集を行っても，ネットワーク上に大量の証拠が溢れてしまうこととなり，通信の障害になることも考えられる．そこで，周囲の全ノードから証拠を収集するのではなく，信頼できる証拠を効率よく収集するような仕組みが必要である．そのために，証拠の収集範囲や証拠の作成者による信頼性に関しても考慮する必要がある．

また，えん罪の証明に必要な記録の収集は通信開始時と同時に始めるのではなく，セキュリティインシデントの疑いがあった時点で開始するべきである．したがって，証拠収集の開始時期をインシデントの疑いの検出時と定めた．

本研究では作成者毎の証拠の信頼性や収集開始時期を考慮し，よりネットワーク負荷の少ない証拠収集手法を提案する．

2. 関連研究

本研究の前提となる技術として，ディジタルフォレンジックや MANET におけるルーティングプロトコルについて示す．また，関連研究として証拠収集やインシデント検出に関する研究について示す．

2.1 ディジタルフォレンジック

情報通信技術が発達するにつれ，様々な不正や犯罪行為，事故から情報資産を守るために情報セキュリティの技術に関する研究が活発化してきた．しかし，これらの技術を利用しても事件・事故の発生を完全に防ぐことは不可能である．そこで重要視されるようになったのは，原因の究明や被害拡大の抑止，被害からの回復，そして再発防止などの事後対応の技術である．ディジタルフォレンジックとは，このような事後対応に焦点をおいた技術である．

ディジタルフォレンジックの典型的な例として，不正アクセス等によって攻撃を受けたサーバや端末が，再発防止のために原因究明を行う作業などが挙げられる．このようなディジタルフォレンジックの技術は個人での利用だけではなく組織での利用も想定されており [7][8]，組織環境の変化にも柔軟に対応できるようになっている[9]．

2.2 MANET におけるルーティングプロトコル

MANET におけるルーティングプロトコルは主に Reactive 型と Proactive 型に分類される．また，ZRP(Zone Routing Protocol)のような Reactive 型と Proactive 型を組み合わせたハイブリッド方式のプロトコルなども存在する．

2.2.1 Reactive 型

Reactive 型ルーティングプロトコルでは，通信の要求が起きてから経路表が作られる．そのため，実際に通信が始まるまでに少し時間差が生じるのが特徴である．通信を行なわない時は電波の発信も行なわれないため，各ノードの省電力化・駆動時間の長時間化が実現可能となっている．Reactive 型ルーティングでは，各ノードが経路表を保持し，それに基づいてパケットの転送を行う．また，各ノードは隣接するノードへのルーティングのみを行う．

Reactive 型ルーティングプロトコルでは，フラッディングによって経路探索を行わないので，ネットワークへの負荷が小さいという利点がある．そのため，移動によるノードの参加・離脱が高頻度で行われるようなネットワークにも適用可能である．

Reactive 型ルーティングプロトコルとして代表的なものに，AODV(Ad Hoc On Demand Distance Vector Algorithm)[10]や DSR(Dynamic Source Routing Protocol)[11]などがある．

2.2.2 Proactive 型

Proactive 型ルーティングプロトコルでは，あらかじめ経路表を作成しておくため，通信の要求が起こるとすぐに通信を開始できるのが特徴である．常にパケットを送出することで周辺に存在するノードの確認を行い，経路表作成のための制御情報のやり取りが必要になるため，無駄な電波発信が頻繁に起こる場合もある． Proactive 型ルーティングでは，送信者がルーティングを行うため，パケットを転送する各ノードが経路表を保持する必要はない．

以上のような性質から，頻繁に経路の再構築を行うようなネットワークには不適切である．そのため，センサネットワーク等のノードが固定されたネットワークで利用される．

Proactive 型ルーティングプロトコルとして代表的なものに，OSLR (Optimized Link State Routing Protocol)[12] や TBRPF (Topology Broadcast based on Reverse-Path Forwarding Routing Protocol)などがある．

2.3 証拠収集方式

大高ら[13]は，動作主体のノードが正しい動作を行ったことを証明する証拠収集方式を提案している．ここでいう証拠とは，動作主体のノードがどのようなデータを送信，もしくは中継したのかが日時情報と共に記されたものである．証拠には電子署名が付与されており，改ざん検知の機能が備わっている．また，前提条件として証拠収集時は通信方式をプロミスキャスモードとし，証拠収集を行っているノードは無線到達範囲内にある全てのパケットを無差別に受信するものとする．

2.3.1 想定環境

この証拠収集方式は，図 1 のような環境に適用されることを想定している．

- 目撃ノード: 送信ノード, 受信ノードに隣接する, 通信可能圏内のノードである．
- 中継ノード : データ通信における中継を行うノードである．中継とはネットワーク層におけるデータの転送を示し，データの到達性についての確認は行わない．
- 送信ノード : データ通信におけるデータの送信元ノードである．
- 受信ノード : データ通信におけるデータの送信先ノードである．

関連研究では，この送信ノードと中継ノードの中継に関わる全てのノードが証拠収集の対象である．

また，ルーティングプロトコルには，Reactive 型である AODV を利用している．

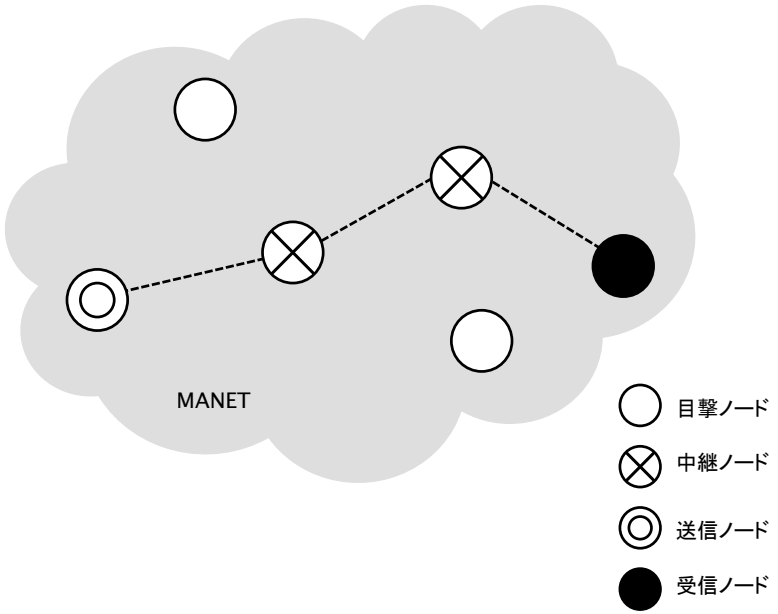

図 1　想定環境

2.3.2 証拠収集方式のモデル

証拠収集方式のモデルを図 2 に示す．この証拠収集方式で用いるパケットは大きく分けて二種類ある．

(1) データパケット

送信者と受信者がやりとりするデータのパケットを表す．周囲のノードに証拠収集依頼を行う場合は，後述する証拠収集プロトコルヘッダ（Forensics Header）を付与する．その中のフィールドに詳細な内容を記述する．

(2) 証拠パケット

証拠収集依頼を受けたノードが作成した証拠を転送するためのパケットである．証拠の信頼性を高めるため, 暗号化やディジタル署名の付与などの処理が行われている．証拠パケットにも証拠収集プロトコルヘッダが付与されており，証拠の作成者の詳細情報がわかるようになっている．

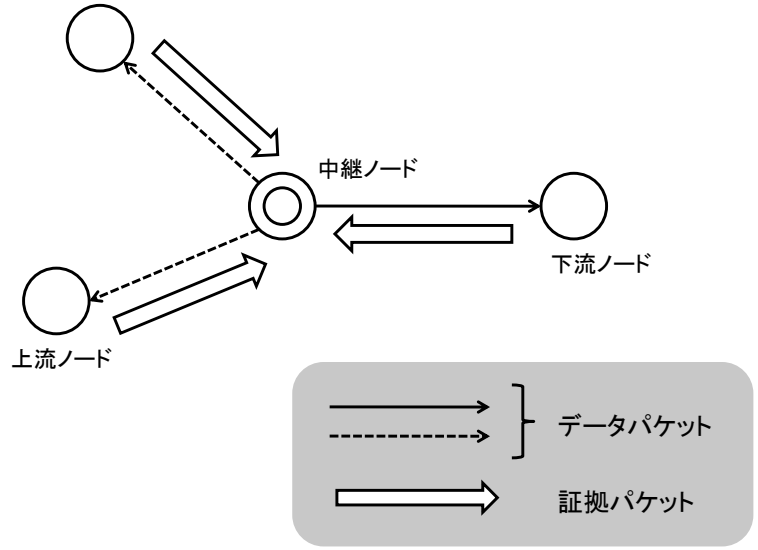

図 2　証拠収集方式のモデル

2.4 インシデント検出

MANET におけるインシデント検出に関する従来の研究として，転送レポート方式である HADOF[14]や watchdog 方式[15]がある．

2.4.1 HADOF

HADOF とは各ノードが定期的に受信パケット数と転送パケット数を送信元ノードに報告し，送信元が転送数の差異により不正を検出するというものである．この方式は DSR のようにパケットの通過経路を送信者が指定するルーティングプロトコルに依存している．

2.4.2 watchdog

watchdog 方式では, watchdog と pathrater という 2 つの機構を用いて不正ノードの検出などを行う．watchdog とは通信経路に沿って直前のノードが自分の送信先のノードの動作を監視するというものである．pathrater は各ノードで動作し，watchdog で検出した不正ノード等の情報を一括管理する．この方式はルーティングプロトコルに依存せず適用可能だが，誤検出が多い．

3. 提案方式

インシデント検出をトリガとした証拠収集手法の前提条件，提案アルゴリズム等について示す．収集された証拠は各ノードが通信終了時まで保持していることとし，収集した証拠の保全や解析等については本研究では考慮しないこととする．

3.1 提案方式の特徴

関連研究で述べたようなインシデント検出機構と証拠収集方式は，お互い独立した技術である．しかし，それらの技術にはそれぞれインシデント検出機構には誤検出，証拠収集方式にはネットワークへの過負荷等といった問題がある．そこで，この二つの技術を連結し,誤検出であったことを収集した証拠を用いて後から証明できるように，また，証拠収集の期間を定めることでネットワークへの負荷を軽減するようにしたのが本提案方式の特徴である．

さらに，証拠を収集する範囲やノードを限定することで

3.2 前提条件

証拠収集には関連研究で示した方式を用いる．また，セキュリティインシデントに関する証拠の収集とそのアーカイビングについてのガイドライン[16]を参考に，証拠の内容を以下のように定めた．

・日付と時刻

・関係者に関する情報

関係者に関する情報とは，対象を一意に識別できる識別子や位置情報等である．また，証拠の信頼性を高めるため，各ノードで作成した証拠に暗号化処理を行い，自身の電子署名を付与することで改ざん検知機能を与えることとする．

3.3 対象範囲

図 3 にフォレンジックのサイクルにおける提案方式の対象範囲を示す．

提案方式では，ネットワーク監視からインシデント発生後の証拠収集までを対象範囲とし，それ以外は対象範囲外とした．

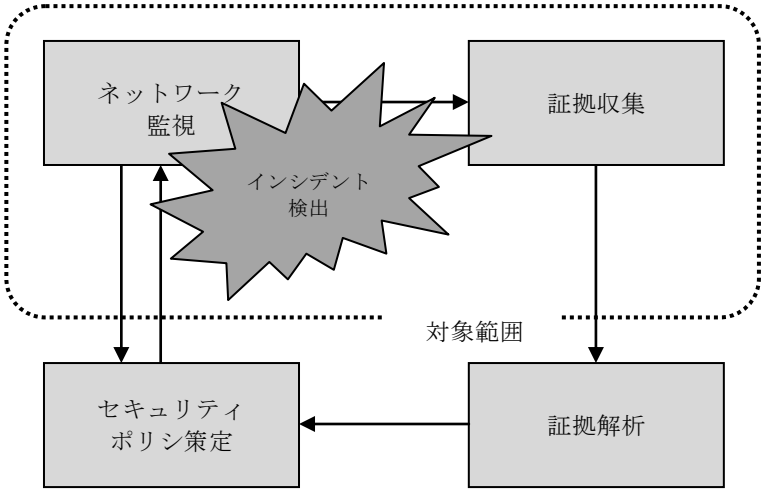

図 3　提案方式の対象範囲

3.4 提案方式の概要

ネットワークの監視からインシデント検出,そして証拠収集までの流れを図 4 に示す．

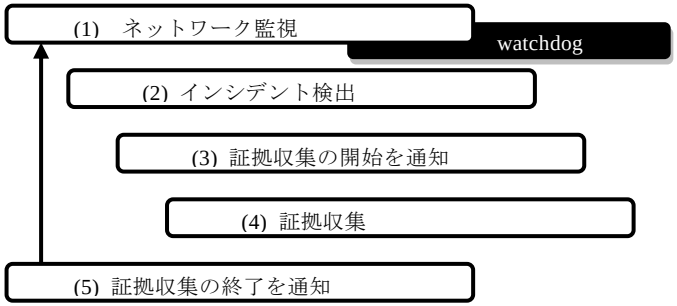

図 4　提案方式の概要

ネットワーク監視やインシデント検出については 3.5 節で説明する．また，3.6 節で証拠収集の開始・終了時の通知方法や証拠収集について述べる．

3.5 インシデント検出

関連研究で述べた証拠収集方式ではネットワーク監視やインシデント検出のフロ

ーがなく，通信開始時から継続的に証拠収集を行っている．証拠収集は送受信パケット単位で行われるため，長時間ネットワーク全体に大きな負荷がかかることになる．提案方式ではその負荷を軽減するため，通信開始と同時にネットワーク監視を開始する．

また，提案方式では汎用性を高めるため，ソースルーティングを行うプロトコルに依存した HADOF ではなく，どのようなネットワークにも適用可能な watchdog 方式を採用する．

watchdog の監視によって収集された情報をまとめ，インシデントの検出を行う．提案方式では，インシデントの「疑い」を検出した段階で証拠収集が開始されるように，pathrater 内部の閾値を変更した．

3.6 証拠収集

インシデントの疑いが検出された場合，証拠収集の開始を周辺ノードに通知することとなる．ただし，ネットワーク内の全ノードに証拠収集を依頼すると，ネットワーク全体に多大な負荷がかかってしまうため，インシデントと疑われたノードから 3 ホップ以内のノードにのみ証拠収集を依頼することとする．

その後，基本的には関連研究で述べた証拠収集手法を用いて証拠収集を行う．目撃ノードの制限方法については 3.6.1 節で述べる．

3.6.1 証拠収集プロトコルヘッダ

証拠収集に用いる証拠収集プロトコルヘッダの構成を図 5 に示す．証拠収集プロトコルヘッダのサイズは，可変長であるオプションフィールドを m[bytes]，証拠収集依頼数を n[bytes]とすると，28＋4*n＋m[bytes]となる．ヘッダの各構成要素の詳細は次のとおりである．

(1) Type (4[bit])

パケットタイプを格納するフィールドである．次の二つのうち，どちらかがここに格納される．

Forensics Request: 証拠収集を依頼したデータパケットを示す．

Forensics Echo: 依頼されて作成した証拠パケットを示す．

(2) NOE(Number Of Evidence) (8[bits])

証拠を収集したい目撃ノードの数を格納するフィールドである．ただし，上下流ノード（2 ノード）は含まない．また，ここで入力した数値分だけ Request Host フィールドに IP アドレスを入れる必要がある．

例外として，最大値 255 が入った場合のみ，周辺のすべてのノードに依頼を行うこととし，Request Host フィールドには何も格納しない．

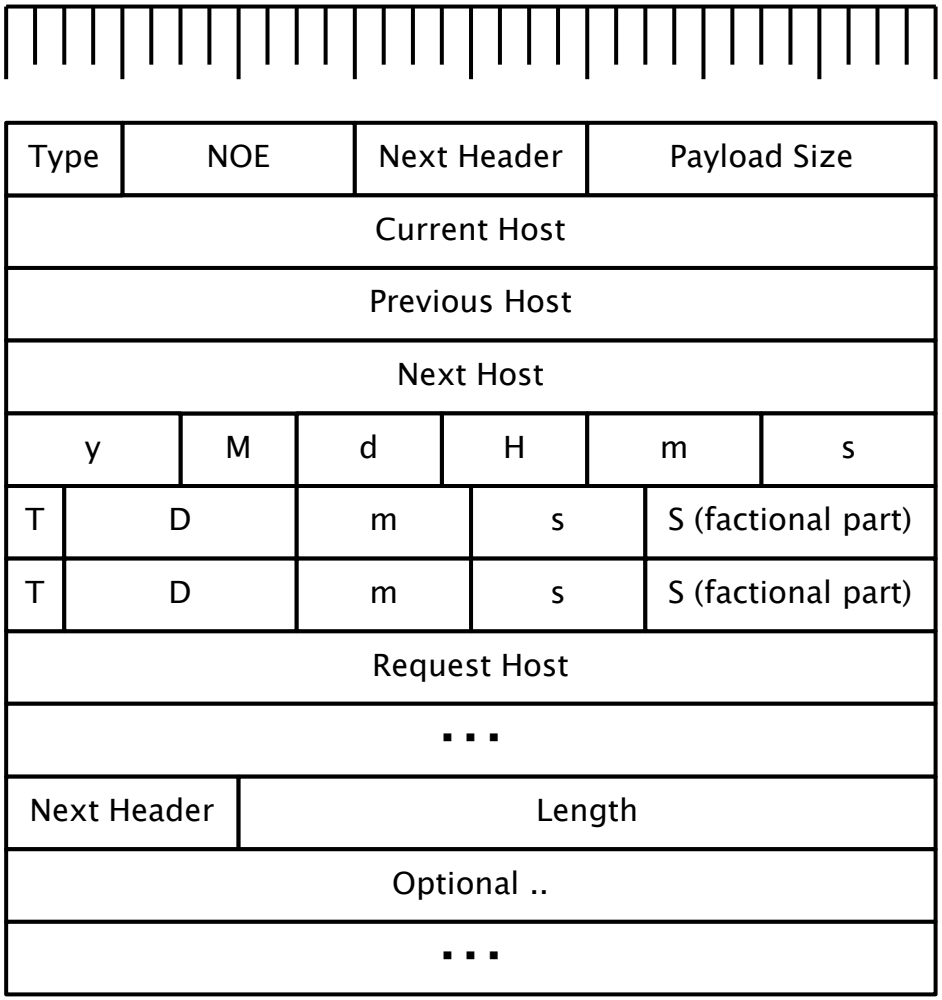

図 5　証拠収集用パケットヘッダ

(3) Next Header (8[bits])
(11) のオプション領域を示すフィールドである．オプションによりフィールドのサイズが変化する．
(4) Payload Header (12[bits])
ペイロード部分のサイズを示すフィールドである．証拠パケットの場合，ここに格納する値は 192[bytes]となる．
(5) Current Host (32[bits])
着目ノードの IP アドレスを格納するフィールドである．
(6) Previous Host (32[bits])
上流ノードの IP アドレスを格納するフィールドである．
(7) Next Host (32[bits])
下流ノードの IP アドレスを格納するフィールドである．
(8) y (6[bits]), M (4[bits]), d (5[bits]), H (5[bits]), m (6[bits]), s (6[bits])
日時を格納するフィールドである．それぞれ年月日時分秒の順で格納する．その際，年は西暦下二桁，時は 24 時間表記とする．
(9) T (2[bits]), D (8[bits]), m(6[bits]), s1 (6[bits]), s2 (10[bits])
緯度及び経度を格納するフィールドである．T は南／北緯，東／西経のいずれかが格納される．以下，度分秒の順に格納される．
(10) Request Host (32[bits])
NOE にて示された数の IP アドレスを格納するフィールドである．ただし，前述の通り上下流ノードは含まない．
(11) Option
(3) の Next Header が指し示すオプションのフィールドである．このフィールドは拡張用に作成したものである．オプションフィールドでの Next Header では，更に次のオプションか，なければルーティングプロトコルなどのプロトコルヘッダを指すこととなる．

関連研究では，ノードによる証拠の信頼性を考慮せず，通信範囲内の全ノードに証拠収集を依頼している．そこで，提案方式では，証拠の信頼性が最も低いと考えられる目撃ノードへの証拠収集依頼を制限することとした．そのために，証拠収集用パケットヘッダを拡張し，目撃ノード数の制限を行うこととした．証拠の信頼性に関する考察は 4.4 節で述べる．

4. 評価

提案手法の有用性を示すため，全ノードに証拠収集を依頼した場合のシステムの評価を行う．以下，実装したシステムや実験内容，実験結果と考察を述べる．また，証拠収集の依頼先の制限に用いる証拠パケットの作成者による信頼性に関する考察を行った．

4.1 実験環境

前述のシステムを NS-2(Ver.2.34)というネットワークシミュレータ上に実装し，表 1 のような条件で実験を行った．NS-2 は離散イベント型のネットワークシミュレータであり，MANET などの無線通信ネットワークのシミュレーションも実行可能であるため採用した．OS として用いたのは，Linux ディストリビューションのひとつである Ubuntu10.04 である．

表 1 実験環境

ノード配置範囲	1000 × 1000 [m]
無線到達距離	250 [m]
ノードの移動速度	最大 1.4 [m/s]
シミュレーション時間	100 [s]
ノード数	10 – 100 [nodes]
通信プロトコル	UDP, IP
パケットサイズ	最大 1000 [Byte]

4.2 ノード数毎の平均保全証拠数に関する評価と考察

平均保全証拠数とは，送信者・中継者が送信したひとつのデータパケットに対して送り返された証拠のうち，保全された平均の証拠数のことを指す．図 6 に示したように，ひとつのデータパケットに対して少なくとも 10 以上，多いときは 20 近くの証拠が送り返されていることがわかる．ノード数が 10 や 20 のときは，そのノード密度から無線到達範囲内に他のノードが存在しにくいため，極端に低い値となってしまったと考えられる．

これにより，証拠収集の期間を定めなければ，ひとつのデータパケットにつき 10 以上もの無駄なパケットがネットワーク上にあふれてしまうことがわかる．証拠収集

の必要な期間は，必要な証拠の量や各ノードの記憶容量によっても変化する．特にMANET のような携帯端末を利用する通信では，記憶容量が限られるような状況も少なくない．そのため，既存研究のように通信中に証拠収集し続けるのは現実的ではないといえる．

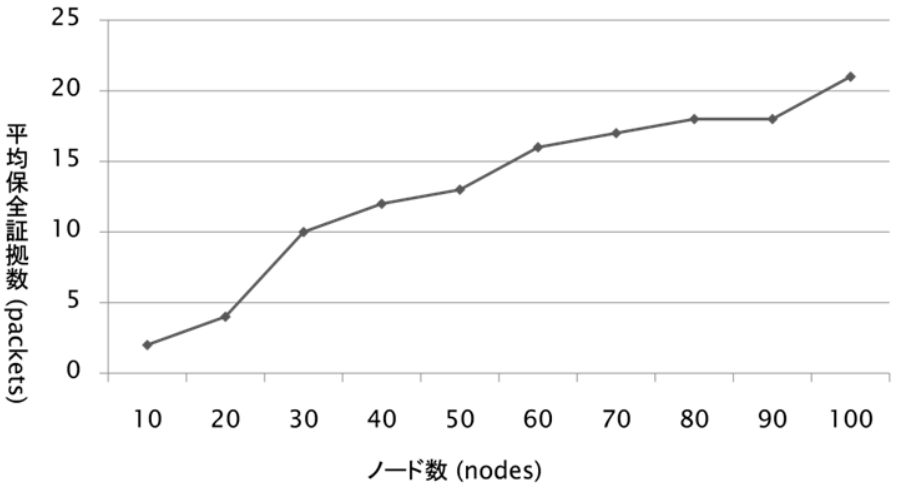

図 6　ノード数毎の平均保全証拠数

4.3　到達率と各ノードの平均保全証拠数に関する評価と考察

通信全体における証拠収集時間の割合毎のパケット到達率と，そのときの各ノードの平均保全証拠数を図 7 に示す．なお，通信とは最初に経路確立用のルートリクエストパケットが送出されてから，最後のデータパケットの送信が完了するまでである．実験中，利用するシナリオファイルによってインシデント検出までの時間が異なり，証拠収集の期間によってパケット到達率に大きな差が出てしまった．そこで，インシデント検出までの時間が異なるシナリオを多数用意し，そこから得られた実験結果を証拠収集時間の割合（10%毎）で分類し，その集合内での平均を算出した．

既存方式のように通信開始時から証拠収集を継続して行う場合，パケット到達率は約 40%と極めて低いことがわかる．しかし，インシデント検出時に証拠収集を開始し，それ以外はネットワーク監視だけにとどめておくと，最高 75%程度までパケット到達率が向上している．これにより，証拠収集時のパケット到達率に変化はないが，通信全体の平均パケット到達率を向上することは可能であることがわかった．そのため，既存方式より提案方式を用いた方がパケット到達の信頼性の部分から見て有効的だと考えられる．

一方，各ノードに保全される証拠数は，証拠収集の期間が短くなるにつれて減少していく．そのため，ただ証拠収集の期間を短くするだけでは，証拠不足により証拠収集の意味がなくなる可能性が出てくる．そこで，証拠の必要量に応じて収集期間を定めるような仕組みが必要であると考えられる．たとえば，災害現場等で利用する際には，主に携帯電話等の記憶容量の少ない機器の使用が想定される上，証拠収集よりも信頼性の高い通信が求められるため，証拠収集時間を抑えるような仕組みが必要となってくると考えられる．

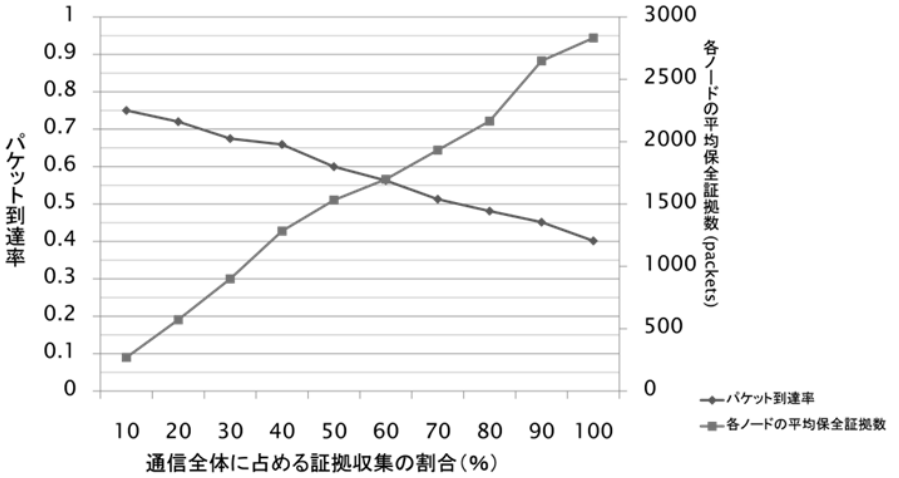

図 7 パケット到達率と平均保全証拠数

4.4　証拠パケットの作成者による信頼性に関する考察

提案方式において，着目ノードは上・下流ノードおよび目撃ノードの全てから証拠パケットを収集することが望ましい．しかし，上・下流ノードおよび目撃ノードになんらかの問題が発生した場合や，無線ネットワークの状況によって全てのノードからの証拠パケットを収集できない場合も考えられる．

さらに，記憶容量の限られた状況下で証拠収集を行った場合，利用価値の低い証拠を大量に収集してしまうと大切なデータパケットを破棄してしまう可能性も出てくる．

そこで，証拠パケットの作成者による信頼性の評価を行う．証拠パケットの作成者

によって信頼性が異なるのは，MANET の特徴であるため，その信頼性の評価には，次の指標を定義し，使用する．

(1) 送信性

データパケットを送信したことを保証することである．着目ノードからみて上・下流ノードおよび目撃者のいずれかから証拠パケットを得ることで満たすことができる．これにより，ブラックホール攻撃やセルフィッシュノード問題などの攻撃を行っていないことを証明することができる．ただし，データパケットが下流ノードに届いたかどうか，データパケットに改ざんなどが加えられていないかどうかなどについては証明することはできない．

(2) 到達性

データパケットが下流ノードに到達したことを保証することである．着目ノードは，下流ノードから証拠パケットを得ることで満たすことができる．これにより，着目ノードは，データパケットを正しく下流ノードに送信したことが証明される．データパケットの内容に改ざんなどが加えられていないことを証明することはできない．

(3) 中継性

データパケットを中継したことを保証することである．着目ノードは，上流ノードから証拠パケットを得ることで満たすことができる．これにより，着目ノードはデータパケットを正常に受信し，正常に送信したこと，つまり正しく中継が行われたことを証明できる．

図 8 に，着目ノードから見た証拠パケットの作成者による信頼性の考察について示す．

上・下流ノードから証拠パケットを得た場合が最も信頼性が高い組合せである．下流ノードからの証拠パケットのみ得られない場合，目撃ノードからの証拠パケットが，正しく中継したことを示すために，信頼性は 2 番目に高いものとする．上流ノードからのみ証拠パケットが得られた場合には，中継性は保証されるものの，先の組合せより若干信頼性が低くなる．また，下流ノードとの組合せでは，正常に送信したことを当事者自身が証明することが重要であるため，下流ノードと目撃ノードの組合せが続き，下流ノードのみと目撃ノードでは下流ノードのみの証拠パケットの方が目撃ノードのみの証拠パケットよりも信頼性は高いものとした．

信頼性 高 ↑ ↓ 低

収集した証拠パケットの作成者	中継性	到達性	送信性
上流＋下流（＋目撃）	○	○	○
上流＋目撃	○	−	○
上流のみ	○	−	○
下流＋目撃	−	○	○
下流のみ	−	○	○
目撃のみ	−	−	○

図 8　証拠パケットの信頼性

5. まとめと今後の課題

本稿では証拠パケットの作成者による信頼性を考慮した MANET 上での証拠収集手法について示した．また，提案方式との差異を明らかにするために，改良を加える前の証拠収集手法を実装・評価した．今後は実際に実装を行い，提案方式の有効性を調査することが課題となる．

参考文献

[1] Mobile ad hoc network (MANET) http://www.ietf.org/html.charters/manet-charter.html

[2] 森拓海，森郁海，高橋修，アドホックネットワークにおける防御法の分類と耐攻撃性アドホック・ルーティング・プロトコルアーキテクチャの提案，情報処理学会研究報告 モバイルコンピューティングとユビキタス通信(MBL)，2007(15), pp.73-78(2007).

[3] 森郁海，森拓海，高橋修，アドホックネットワークにおける攻撃法・防御法の分類と AODV ベースセキュアルーティングプロトコルの提案，情報処理学会研究報告 モバイルコンピューティングとユビキタス通信(MBL)，2007(16), pp.79-84(2007).

[4] 上原哲太郎，ディジタルフォレンジック：電磁的証拠の収集と分析，情報処理，48(8), pp.889-898(2007).

[5] 仁佐瀬剛美, 伊藤光恭, ネットワーク情報を活用するフォレンジクス技術の動向，NTT ジャーナル，pp36-40(2004).

[6] 辻井重男(監修) : デジタル・フォレンジック辞典，デジタル・フォレンジック研究会(2006).
[7] 加藤弘一，川西英明，勅使河原可海，西垣正勝，佐々木良一 : 組織環境に対応したデジタル・フォレンジック対策選定手法の検討，コンピュータセキュリティシンポジウム 2007 論文集，pp. 513‐518 (2007).
[8] 中村逸一，兵藤敏之，曽我正和，水野忠則，西垣正勝 : セキュリティ対策選定の実用的な一手法の提案とその評価，情報処理学会論文誌， Vol. 46, No. 8, pp. 2120‐2128(2004).
[9] 加藤弘一，勅使河原可海 : 利便性とセキュリティを両立させるための最適対策組合せに関する検討，情報処理学会マルチメディア通信と分散処理研究会 (DICOMO) 論文集，pp. 1578‐1585 (2007).
[10] C.Perkins, E.Belding-Royer and S.Das: Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561 (Experimental) (2003).
[11] D.Johnson, Y.Hu, and D.Maltz: The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, RFC 4728 (Experimental) (2007).
[12] T.Clausen and P.Jacquet: Optimized Link State Routing Protocol (OLSR), RFC 3626 (Experimental) (2003).
[13] 大高全，高橋修，MANET におけるフォレンジクス技術適用に関する提案，情報処理学会研究報告 ユビキタスコンピューティングシステム(UBI)，2008(18), pp.217-222 (2008).
[14] W.Yu, Y.Sun and K.Liu: HADOF: Defense against routing disruptions in mobile ad hoc networks, IEEE INFOCOM, Vol. 2, p. 1252 (2005).
[15] S. Marti, T. Giuli, K. Lai, and M. Baker: Mitigating routing misbehavior in mobile ad hoc networks, Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255–265 (2000).
[16] D.Brezinski and T.killalea: Guidelines for Evidence Collection and Archiving, IETF-Request-for-Comments, rfc3227.txt, February (2002).