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

2008－MBL－44　(31)
2008－UBI－17　(31)
2008／3／6

MANETにおけるフォレンジクス技術適用に関する提案

大高　全　高橋　修

公立はこだて未来大学 システム情報科学部　〒041-8655 北海道函館市亀田中野町 116-1
E-mail: {m1204155, osamu}@fun.ac.jp

概要 近年，アドホックネットワークが注目されている．アドホックネットワークとはゲートウェイ等を必要とせず，端末のみで構成可能な無線ネットワークのことである．このアドホックネットワークに対する攻撃法は様々なものが知られており，その対策法も提案されているが，現在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ものが中心になっており，個々のノードへの影響は考慮されていないのが現状である．そのため，攻撃者であると疑われた場合には，否応なく経路から外されることも少なくなかった．本稿では，この”閉鎖的”なセキュリティに対して，客観的に調査可能な証拠を作成及び収集できる手段を提案する．

キーワード モバイルアドホックネットワーク，ネットワークフォレンジクス

Network Forensics on Adhoc Networks

Otaka Akira and Takahashi Osamu

Systems Information Science, Future University-Hakodate
116-2 Kamedanakano-cho, Hakodate Hokkaido, Japan
E-mail: {m1204155, osamu}@fun.ac.jp

Abstract Recently, researchers are paying attention to the adhoc networks. The adhoc networks are the wireless networks composed by end-point computers. The method of attack to the adhoc networks exists variously, and the method of measures is proposed. However, an individual profit has been disregarded because the latest method of measures has aimed to make the entire profit give priority. It was not unusual that the communication was cut when doubted the attack either. In this paper, it proposes the means that 'to make and collect evidences of possible to investigate objectively can be done.

Keyword MANET, Network Forensics

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が構築可能なアドホックネットワークの研究が盛んに行われている．また，アドホックネットワークは，アクセスポイント等を必要としないため，導入時のコストを低く抑えることができ，メンテナンスの手間も省くことができる点が大きなメリットとして挙げられる．このアドホックネットワークには様々な攻撃方法が考えられ，それに対する防御・回避方法が提案されている．しかしながら，それら提案法はネットワーク全体としてはセキュリティが向上しているものの，個々のノードには一定の犠牲が伴っている場合が多い．例えば，送受信記録をレポートとして提出させる防御・回避方法の多くは，レポートを回収することで攻撃ノードを含む周囲のノードの信頼値を評価し，一定の閾値を下回った場合には経路の切断もしくは切り替えを行っている．これは，ネットワーク全体からみれば，セキュリティが向上し，パケット到達率も向上している．しかしながら，正常であるにも関らず，攻撃ノードとして誤認されるケースも多々あり，正常なノードにとっては迷惑そのものである．

そこで本稿では，攻撃者でない場合には身の潔白を証明することができるフレームワークの提供を目的とする．そのための方策として，送信した内容を証拠として収集する．その結果，個々のノードの信頼性を客観的に評価することができるようになるため，攻撃ノードか否かの証明も容易になり得る．但し，これら証拠が必要かどうかはユーザの裁量に委ねられることが望ましいため，ルーティングプロトコルに依存せず，汎用的なモジュールとして組み込まれることを想定している．

本論文では，２章で関連した技術を，３章ではアドホックネットワークへのフォレンジクス技術適用の方式及び詳細なアルゴリズムについて述べる．

2　関連研究

2.1　防御及び回避方法

アドホックネットワークにおけるルーティングプロトコルは様々なものが提案されており，Reactive 型では AODV[1]や DSR[2]が一般的である．これらルーティングアルゴリズムには様々な攻撃方法が存在し，森ら[3][4]は既存の攻撃法及びその防御法について分類している．

HADOF[5]は，セルフィッシュノード及びブラックホール攻撃を対象とした場合の防御法であり，ルーティングプロトコルには DSR を用いている．森ら[6]は HADOF の問題点を改善するプロトコルアーキテクチャを提案している．更に，森ら[7]は，同様の攻撃を対象とした汎用的な防御法の提案を行っている．watchdog[9]は，これらと同様の攻撃を対象とした監視法である．

2.2　Double Hash 認証を用いたセキュアルーティング法

織田ら[8]は，Double Hash 認証を用いたセキュアルーティング法を提案している．これはルーティングする際に，全てのパケットに対してハッシュを用いた認証を行うことで改ざん等を防止している．

2.3　ネットワークフォレンジクス

ネットワークフォレンジクスとは，ルータやスイッチ等のネットワーク機器に保存されたログやそれら機器から複製されたパケットを収集・保存し，解析を行う技術の総称である．一般に，ネットワークフォレンジクスは，対象ネットワークに流れる全てのイーサネットフレームを保存する．そして，仁佐瀬ら[10]によれば，これら保存された内容を解析することで次のような証拠を得る．

- 攻撃者の情報(IP アドレス等)
- 攻撃内容
- 攻撃時刻
- 攻撃経路
- 攻撃方法

このようにして収集した証拠を適切に運用することで，攻撃によって被った被害を証明することができ，場合によっては裁判における証拠資料として使用することも可能となる．

3　アドホックネットワークにおけるネットワークフォレンジクスの必要性

3.1　従来方式の問題点

2.1 節で示した防御及び回避機構は，通信中に異常を検知し，経路の切断及び切り替えを目的としてきた．そのため，改ざんの検知や攻撃ノードを検出する方法として大きな効果がある．しかしながら，パケット数の増加等によって接続性が悪くなると“攻撃者”として誤認されることも多い．また，これら方式では信頼できるかどうかを数値で表現し，一定の閾値を超えた場合に経路の切断を行うという方法を採るのが一般的である．

織田らの提案するセキュアルーティングプロトコルは，ルーティングプロトコルに依存し，異常の検知は個々のノードに委ねられる．

図 1 は，インターネットモデルにおけるネットワークとアドホックネットワークによるフォレンジクス適用範囲の違いを示している．

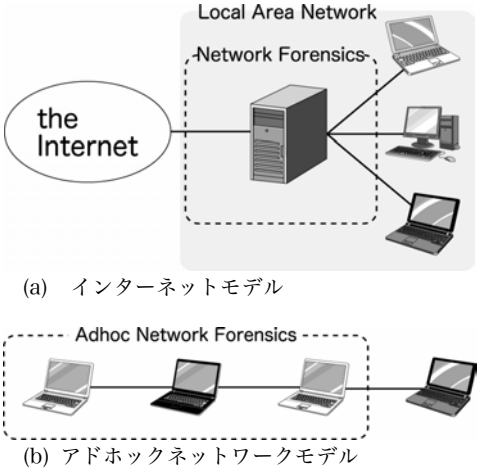

図 1 ネットワークの種類の違いによるフォレンジクスの対象範囲

インターネットモデルでは，サーバが WAN 側から受けた攻撃に対する被害の証明及び LAN 側からの不正（情報への不正アクセス，リーク等）を監視することを目的としており，対象となる LAN 内に流れるデータ（イーサネットフレーム）を全て保存することで実現している．これら証拠は，改ざんされることが無いように暗号化を施すことで第三者への証明をも可能にするが，その方法はネットワークフォレンジクス製品を提供するベンダに委ねられている．そのため，現在のネットワークフォレンジクスにおいては，製品を提供するベンダは信頼でき，攻撃することは無いものと想定している．

一方，アドホックネットワークは端末のみで構成されているため，WAN 及び LAN は区別されず，被害を受けるのは特定ノードに限らない．また，全てのノードがネットワーク内に流れるデータを保存する場合，その証拠は自らが暗号化等の処理を施すために信頼性は低く，第三者が攻撃の有無についての判断が極めて困難である．更には，パケットを破棄するだけの攻撃であれば，その証拠は残らず，経路やその方法を検知することもできない．このため，これらに相当する証拠の種類を再定義する必要がある．そして，攻撃者の存在への疑惑は全ノードに及ぶため，攻撃者でないことの証明は，送信内容の証明を行うことで実現できる．従って，あて先ノードは，本稿の対象範囲外とする．

現状のネットワークフォレンジクスは，企業で使用することを目的に実用化が進められており，個人のプライバシよりも企業の利益を優先させるため，パケット自体の内容も解析の対象となる．しかし，アドホックネットワークは，無関係な個人によってのみ形成されるため，通信の内容などのプライバシは保護されなければならない．

3.2　アドホックネットワークフォレンジクスの定義

本稿において，アドホックネットワークにおけるフォレンジクスとは，攻撃者（作為的でない場合も含む）の特定及びえん罪の防止であると定義する．そのためには，対象ノードは自身が中継した内容を証明できることが必要となる．本稿

では，これを送信証明もしくは証拠と定義する．そして，この証拠，つまり送信もしくは中継した内容を証明できるフレームワークの構築を目的とする．

3.3 アドホックネットワークフォレンジクスの要求条件

送信証明（証拠）に対して，次の要求条件を満たすことが必要である．

- 改ざん不能性
- 保証性
- 提出の即時性

フォレンジクスとは法的措置も考慮したセキュリティである．そのため，裁判（判定）の際には，証拠の有効性が認められるものでなければならない．従って，証拠は改ざん不能であり，尚且つ第三者によって証明可能な必要がある．また，判定を迅速に行えるようにするためにも，証拠は即時に提出可能でなければならない．

3.4 ネットワークフォレンジクスとの違い

表 1 はイーサネットワークにおけるフォレンジクスとアドホックネットワークにおけるフォレンジクスの違いを示したものである．イーサネットワークでのフォレンジクスでは，対象となるのは受信者であり，攻撃者の特定もしくは攻撃されたことを証明することを目的としている．一方，アドホックネットワークでは，中継者を対象とし，それ故に攻撃者でないものが正常であること，つまり疑われた場合には無実の証明が行えることを目的としている点で大きく異なる．

表 1 ネットワーク毎のフォレンジクスの違い

	イーサネット	アドホック
対象者	受信者	中継者
目的	被害の証明	無実の証明
証拠	攻撃者情報	保証人
	攻撃内容	証明内容
	攻撃経路	
	攻撃方法	
	攻撃時刻	保存時刻

4 提案方式

本提案方式では，ネットワーク全体としてのセキュリティよりも，個々のノードに着目している．そのため，織田らが提案しているセキュアルーティングプロトコルとは異なり，既存のルーティングプロトコルに組み込むことができるモジュールとして実現することを前提としている．

また，提案方式によって保存された証拠は，通信終了後も保存される．これら収集された証拠は，通信終了後に解析を行うことで，通信の事後調査が可能である．但し，本稿では収集を目的とするため，この点については対象外とする．

4.1 対象範囲

図 2 に，本提案方式における対象範囲を示す．一般的に，ネットワークフォレンジクスは，対象とするネットワークにセキュリティポリシを定め，逸脱した行動（インシデント）を監視している．そして，インシデントを検出した場合には，証拠の収集を開始し，終了後に証拠の解析を行う．本提案方式では，インシデント発生後の，証拠の収集に焦点を絞り，それ以外は対象範囲外とする．

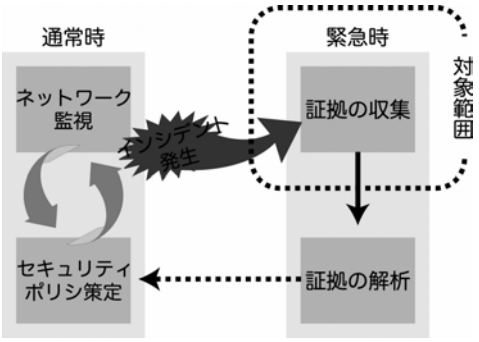

図 2 フォレンジクスのサイクルと本提案方式の対象範囲

4.2 基本動作モデル

図 3 は，提案方式における基本モデルである．本提案方式においては，アドホックネットワークを形成するノードの役割を 3 つに分け，それぞれ中継者，目撃者，保証人と定義する．

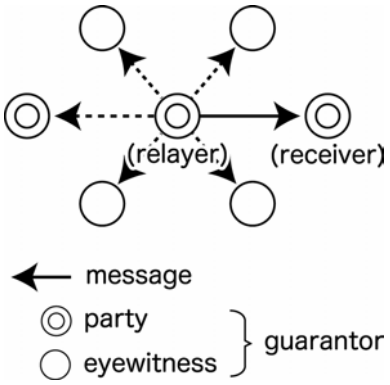

図 3 提案方式における基本モデル

(1) **中継者（relayer）**

中継者は，ある通信において送信を行う全ノードを指す．唯一，受信者は送信を行わないために含まれない．

(2) **目撃者（relayer を除く party, eyewitness)**

目撃者は，ある通信において送信を行うノードに隣接するノードを指す．ここで，隣接するとは通信を行うノードから直接，無線が到達できる範囲であるとする．本稿では，経路上の全てのノードが攻撃し得ると想定している．そのため，当事者以外に証明を依頼することで，証拠の信頼性を向上させることとした．

(3) **保証人（relayer を除く party, eyewitness）**

保証人は，目撃者の中で送信の証明，つまり証拠を提供する中継者又は目撃者である．

4.3 証拠の収集方法

図 4 にモデルを用いた証拠収集の流れを示す．各ノードの通信可能範囲は隣接ノードのみとし，A から C への通信を行うものとする．但し，既存のルーティングプロトコルによって，経路は確立済みであるものとする．また，全ての経路ノードは全ての隣接ノードから証明を求めるものとし，何の処理もなく破棄されるパケットについては，図から省略してある．

STEP 1： A から C へデータを送信する．A の隣接ノードであるノード B,D はデータをプロミスキャスモードを使用可能とすることで受信を行い，証明を求めている事を知る．

STEP 2： ノード B,D はデータのハッシュ値を取得し，各々の秘密鍵で署名を行ったのち，ノード A に送り返す．但し，ノード B が送信した証拠はノード A のみならず，ノード C,D も受信するが，自分宛の証拠ではないため，破棄する．ノード D が送信した証拠も同様である．

STEP 3： B から C へデータを送信する．隣接ノードである A,C,D はデータを受信し，STEP1 と同様に証明を求めている事を知る．

STEP 4： STEP2 と同様に各ノードは証明を行う

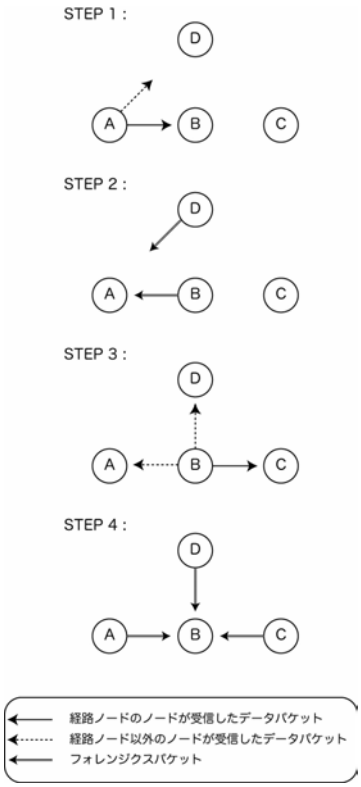

図 4 証明の流れ

ここで，ノード C には証拠は残らない．本提案法は送信したデータの証明を行う事が目的であり，データが送信元から受信先へ正確に届いた事を保証するものではないことによる．

4.4 提案アルゴリズム

4.4.1 パケット処理アルゴリズム

図 5 に各ノードにおけるパケット処理のアルゴリズムを示す．ネットワーク層で受信したデータパケットは，提案するフォレンジクス用ヘッダが存在するかを調べられる．ヘッダが存在しない場合にはそのまま通常のルーティングアルゴリズムに引き渡される．一方，ヘッダが存在した場合には，提案方式に基づいて処理が行われた後，ルーティングアルゴリズムに引き渡される．つまり，本提案法は，既存のルーティングアルゴリズム等に大きな影響を与えることなく導入できるのが利点である．

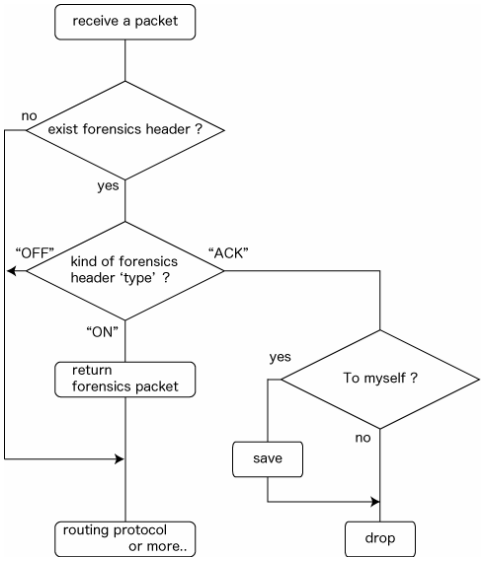

図 5 提案アルゴリズムのフローチャート

4.4.2 フォレンジクスパケットの内容

自身が正常であることを証明するためには，送信内容が適切であったかを証明できることが必要である．アドホックネットワークおいて，この目的を達するため,保存すべき証拠の種類を次のように定義するものとする．

- 保存時刻
- 証明内容
- 保証人情報
- オプション
  - GPS 情報

保存時刻とは，証拠を収集した時刻を表す．これは解析時に，パケットに矛盾がないかをチェックする指標の一つとして用いられる．

証明内容とは，送信した内容を明らかにできるものである．図 6 は提案方式を有効にした場合の IP パケットを示している．既存のネットワークフォレンジクスは，外部からの攻撃が想定されており，発信元の追跡に利用するため，イーサネットヘッダを含む，完全なイーサネットフレームを保存する．しかしながら，アドホックネットワークにおいては中継者の特定が非常に困難なため，完全な形でのイーサネットフレームの保存することの意義が小さい．そのため，データとしての重要性が高いトランスポートレイヤ以上の部分，つまり IP ペイロードを保存するものとする．この部分のハッシュを取得することにより，データの大きさが一定になるとともに，解析する際にはデータが不正に読み取られる可能性を低くすることができる．また，このハッシュ値に対して署名を行うことで，証拠の信頼性を向上させる．本稿では，ハッシュ関数に sha-512，署名には楕円曲線暗号を用いたモバイル向け公開鍵暗号方式である wNAF[11]を使用することを想定している．但し，これら技術には拠らないため，安全性に問

題が生じた場合には変更することも可能である．

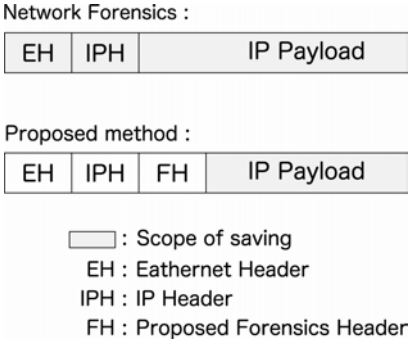

図 6 ネットワーク毎の保存部分の違い

保証人とは．送信した内容を証明するノードのことである．本稿では，証拠は保証人，つまり隣接ノードによる署名によって作成されるため，解析時には署名者の公開鍵を取り寄せる必要がある．このため，公開鍵を要求するためには，保証人に関する情報を保存していなければならない．

オプションの GPS 情報は，GPS が取得可能な機器を搭載している場合，証明書保存場所も記録することができる．

4.4.3 証拠収集のタイミング

一般に，証拠収集は，送受信パケット単位に行われるため，ネットワーク全体に大きな負荷をかけるとともに，収集情報を記録する資源も必要となる．そのため，通信の開始直後から証拠を収集するよりは，開始のきっかけを与えられてから開始することで効率が良くなる．また，本提案方式では，このきっかけをトリガと定義し，watchdog のような中継ノードによる通信異常（攻撃ノード）検出時とする．通信を監視する研究は，他にも HADOF 等があるが，いずれもレポート報告という形式をとっている場合が多く，パケット数が大幅に増加している．本提案方式においても，証拠収集のためのパケットの増加が考えられるため,通信の監視中に負荷が増加しない watchdog を採用する．

(1) 開始決定者が送信者の場合

図 7 に証拠収集の開始決定者が送信者である場合を示す．

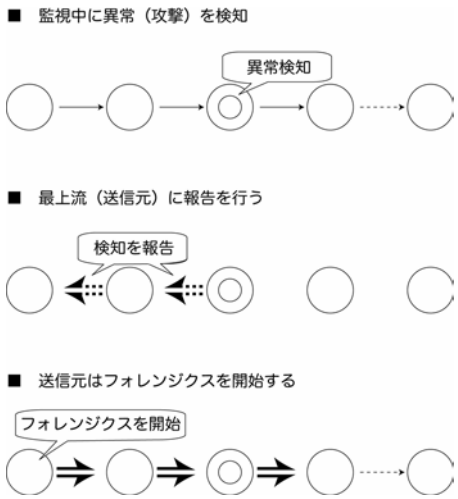

図 7 フォレンジクス開始決定者が送信元の場合

先ず，監視者が通信を監視中に何らかの攻撃を検知する．このとき，監視者は検知したことを最上流のノードである送信元にまで報告を行う．報告を受けた送信元は，フォレンジクスを行うかどうかの決定を行い，フォレンジクスを行う場合には，以後のパケットにフォレンジクス専用のヘッダを付加して送信を行う．特徴としては，通信経路全体で証拠収集を行うために，解析（比較）が容易になる．

(2) 開始決定者が検知者の場合

図 8 にフォレンジクスの開始決定者が検知者である場合を示す．この場合は，
図 7 とは違い，攻撃の監視者が即座にフォレンジクスの開始を行う．特徴として，送信元への報告ないため，フォレンジクスの開始にタイムラグが発生せず，多くの証拠を得ることができることが挙げられる．

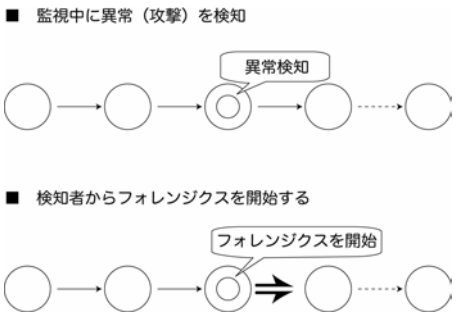

図 8 フォレンジクス開始決定者が監視者である場合

通信の異常が検出された場合，証拠収集の開始を決定するノードによって，収集量が変化する．(1)では，開始までにタイムラグが生じるが，ネットワーク全体で証拠を収集できるのに対して，(2)では，検知と同時に証拠の収集が可能となるが，証拠の収集量は少ない．このため，大きな信頼性が求められる場合には(1)を，証拠の収集を即時に開始したい場合には(2)を採用する等，柔軟な選択ができるものとする．

4.4.4 ユーザポリシ

本提案法は個々のノードに着目し，その信頼性を他ノードに証明してもらうという手法をとっている．特定のネットワークにおいて，フォレンジクスが必要ないノードが混在するケース等に柔軟に対応するため，ポリシをユーザ（各ノード）が決定できる事は重要である．これにより，一律に隣接ノードから証拠を収集するよりも，信頼性の向上及びネットワーク全体としてもパケットの軽減を期待することができ，結果として負荷が低減する．

(1) フォレンジクス必要度による切替

まず，証拠保全の必要性の有無を決定できる事が重要である．前述した通り，公衆アクセスポイントのような場所や，企業内での会議等の限られた人間が使用する場所においては，証拠保全の必要性が小さい．逆に，不特定多数の人間が参加しているネットワークにおいては，証拠保全の必要性が大きくなる．このように，場合に応じて切り替える事ができなければならない．

(2) フォレンジクス有効時の証明依頼先

最初に，証明してくれる相手を選ぶ必要がある．隣接ノードが少なければ，周囲の全てのノードから証拠を収集する

ことは有効であるが，周囲のノードが多い場合には，収集のオーバヘッドにより，通信そのものに影響を及ぼしかねない．その場合には，通信に参加している経路ノードのみから証拠を収集したり，公的な公衆アクセスポイント等の信頼できる隣接ノードのみから証拠を収集できるようにすることが有効である．そこで提案方式では，以下の選択方法を可能とする．

選択肢：

1. 全ノード
2. 指定ノード
   (ア) 経路ノードのみ
   (イ) 隣接ノードのみ（(ア)を含まない）
   (ウ) 個別指定したノードのみ

但し，経路ノードから証拠を収集しない場合には，正しいデータが到着できている事を証明できないため，推奨されないものとする．

4.4.5 フォレンジクス有効時の証明依頼先数

ユーザポリシを適切に利用することで，有効な証拠を効率よく収集することが可能になる．そこで，ユーザポリシで決定した証明依頼先数を N と定義することとする．

$$N = \text{証明依頼先数}\ (0 \leqq N \leqq m)$$

(m：周囲全てのノード)

ここで，0 は証明依頼先が無い，つまりは明示的に証拠収集をしない場合であり，最大値 m は，周囲全てのノードから証拠を収集することを示す．

4.4.6 フォレンジクスヘッダの要求条件

フォレンジクス用ヘッダは，証拠収集の有無及び，収集用証拠パケットのいずれであるかを区別できなくてはならない．また，証拠収集が必要である場合には，ユーザポリシに応じて，証明依頼先数及び証明依頼先が記述できなくてはならない．

4.5 提案方式の特徴と課題

収集した証拠は，周囲のノードがハッシュ値の計算及び署名を行うことにより，改ざんが不可能となるため，証拠の信頼性が保証されたことになる．また，証拠は，個々のノードが保存しているため，即時に提出することが可能となった．これらにより，アドホックネットワークにおけるフォレンジクスの要求条件を満たしたということができる．

本提案方式では，トリガとして watchdog を想定している．但し，本提案法はこれらに依る必要はなく，リアルタイムの監視から，トリガを与えられる事で証拠の保全が開始され，経路が切断･切り替えされるまで継続する．これら watchdog 等の技術が本提案法と連携を取る事が可能であるかどうかの検証が必要である．また，本提案方式では，証拠の収集方法を目的としているため，解析に問題が生じないのかについては，別途議論する必要がある．特に，証拠に含まれる内容として，ペイロード部のハッシュ値及びそれを署名したものだけで良いのかどうかについて，慎重に検討しなければならない．また，証拠を必要とした場合，その解析の手法についても確立されていなければならない．

今後は，本提案方式を実機，もしくはシミュレータ上において実装を行う．これによって，本提案方式における理論上の矛盾点が存在しないかどうか，ネットワーク内に増加するパケットの影響の有無などについて，検証する必要がある．

5 おわりに

本稿では，複数の隣接ノードから正常に送信を完了したことを証明する証拠を収集する方式を提案した．提案方式では，隣接ノードが証拠の収集を望んでいる場合には，データ部のハッシュを取った上で署名を行うことで，送信の証明とその証明の改ざん防止の役割を果たすことができるようになった．証拠の収集プロセス中，ネットワークへの負荷が増加することが想定されるが，ユーザポリシを正しく設定することで，その負荷を低減が可能であることについて示した．

参考文献

[1] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On Demand Distance Vector (AODV) Routing.”, IETF-Request-for-Comments, rfc3561.txt, July 2003

[2] D. Johnson, Y. Hu, and D. Maltz, “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4”, IETF-Request-for-Comments, rfc4728.txt, February 2007

[3] 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」，MBL-41，情報処理学会研究報告 pp73-78

[4] 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」，MBL-41，情報処理学会研究報告 pp79-84

[5] Wei Yu, Yan Sun and K.J. Ray Liu, “HADOF:Defense Against Routing Disruptions in Mobile Ad Hoc Networks”, in INFOCOM 2005, March 2005

[6] 森郁海，森拓海，高橋修「AODV ベースセキュアルーティングプロトコルの提案とその実装・評価」，DICOMO2007, 2007.7

[7] 森拓海，森郁海，高橋修「AAAr: Anti Attack Ad-hoc routing protocol の提案と実装・評価」，DICOMO2007, 2007.7

[8] 織田学，佐藤文明「アドホックネットワークにおけるセキュアルーティング方法」，DICOMO2004, 2004.7

[9] S.Marti, T.Giuli, K.Lai and M.Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, in Proceedings of Mobicom 2000, 2000

[10] 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

[11] Katsuyuki Okeya, Tsuyoshi Takagi, “The Width-w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks”, IEICE Transactions, Vol.E87-A, No.1, pp.75-84, 2004