

MANETにおけるインシデント検出をトリガとした 証拠収集手法の提案

三浦 愛美[†] 白石 陽[†] 高橋 修[†]

公立はこだて未来大学システム情報科学部[†]

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)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。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も考慮しなければならない。また、利己的に振る舞うセルフ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。

これまでのMANETに対する攻撃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ものが中心であり、個々の端末への影響は考慮されていない場合が多い。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ある。そのため、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。

そこで本研究では、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ジタルフォレンジック[1]の技術に着目した。また、えん罪の証明に必要な記録の収集は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、インシデント検出時に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を提案する。

2. 関連研究

一般的に、MANETにおけるデジタルフォレンジックでは、自身の行動の証明によるえん罪の防止を行う。

関連研究として証拠収集とインシデント検出に関する研究について示す。

2.2. 証拠収集方式

大高ら[2]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。

この方式では、(1)証拠収集が行われておらず、自分宛でもない場合はパケットを破棄する。また、(2)証拠収集時は、証拠収集の依頼なのか、証拠として送り返されたものなのかを確認する。証拠は自分宛であれば保存する。

しかし、この方式では通信開始時から継続して証拠収集を行うため、ネットワーク上にパケットがあふれ、パケット到達率が極めて低いという問題点がある。

2.3. 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[3]やwatchdog方式[4]がある。

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。しかし、この方式はあらかじめ全経路が決められているようなルーティングプロトコルに依存している。

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。

ルーティングプロトコルに依存するHADOFを用いると適用可能な状況が限られてしまうため、汎用性が低くなってしまう。そのため、本提案方式ではwatchdog方式を採用する。

3. 提案方式

3.1. 前提条件

証拠収集には関連研究で示した方式を用いる。

A proposal for an evidence-collection method by detecting incident in MANET.

[†]Manami Miura, [†]Yoh Shiraishi, [†]Osamu Takahashi • School of Systems Information Science, Future University Hakodate

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[5]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。

3.2. 対象範囲

ネットワーク監視中にインシデントを検出した場合、証拠収集を開始し、その後収集した証拠の解析や保全を行うのが本来のデジタルフォレンジックのサイクルである。

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。

3.3. 証拠収集フロー

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1に示す。

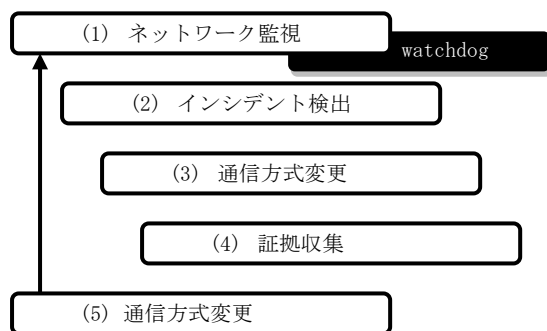


図1 証拠収集フロー

(1) ネットワーク監視

関連研究で述べた証拠収集方式ではこのフローがなく、通信開始時から継続的に証拠収集を行っている。一般的に、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 watchdog を用いてネットワーク監視を開始する。

(2) インシデント検出

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) 通信方式変更

証拠収集を開始するため通信方式をプロミスキャスモードへ移行する。具体的には、通知パケットを無線到達範囲内のノードへブロードキャストしていくことで、通信方式の変更を行う。

(4) 証拠収集

受信したデータのヘッダ情報を確認し、証拠収集を依頼しているのか否かを確認する。証拠収集を依頼している場合(REQ)は、そのパケットを暗号化し、自分の電子署名を付与して証拠として送信元へ返信する。依頼ではなく証拠として送り返されたものだった場合(ACK)、自分宛であれば証拠として保存し、そうではない場合は破棄する。

証拠収集が終了した場合、通信方式を元に戻すための通知パケットを周辺ノードへブロードキャストする。

4. おわりに

本研究では、インシデント検出をトリガとした証拠収集手法を提案した。証拠収集の開始時期をインシデント検出時としたのは、証拠収集によるネットワークへの負荷を軽減するためである。

1000 平方メートルあたり 100 ノードのノード密度で提案方式を実装し実験を行ったところ、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、保全されたものの数は平均で 21 個であった。証拠収集を行っている間はそれだけ余分なパケットがネットワーク上にあふれているということになる。各ノードの記憶容量によって保全できる証拠の数も限られてくるため、闇雲に証拠収集を行うのは無駄だと考えられる。

また、証拠収集のみを行った場合のパケット到達率は 40%程度だったのに対し、証拠収集の割合を 50%にしたところ、それは 70%程度まで回復した。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。

以上のような点から、インシデント検出をトリガとして証拠収集を行うことは、ネットワークへの負荷軽減や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。

参考文献

- [1]. 上原哲太郎, デ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.
- [2]. 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.
- [3]. W. Yu, Yan Sun, and K.J. Ray Liu, "HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks," IEEE INFOCOM, March, 2005.
- [4]. S.Marti, T.Giuli, K.Lai and M.Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of Mobicom 2000, 2000.
- [5]. D.Brezinski and T.killalea, "Guidelines for Evidence Collection and Archiving," IETF-Request-for-Comments, rfc3227.txt, February 2002.