1X-6

MANET フォレンジクスにおける証拠解析方式の提案

三科貴† 高橋修†

公立はこだて未来大学システム情報科学部 情報アーキテクチャ学科†

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クライアント端末のみで構築可能なモバイルアドホックネットワーク（MANET）の研究が盛んに行われている．MANET にはさまざまな脆弱性が指摘されており，それらへの対策として攻撃をパターンで検知し，回避する方式が提案されている．検知の代表的な方法の 1 つでは，パケット中継動作の監視を行って受信パケット数と転送パケット数を比較することにより不正なノードを検出する．そしてそれに伴うレポートの交換・提出を義務付けている．回避では，検知によって検出された不正なノードに対し，経路構築の過程で攻撃ノードとして別の経路を作成して避けるといったルーティングを行う．これらの方式では，移動性や局所的なパケット増加による持続性の悪化が生じると，正常なノードであっても「攻撃」と誤認されるケースが多くなる．一旦攻撃ノードと誤認されてしまうと，正常なノードは通信に制限を受けるなどの制裁が行われる可能性があり，緊急性の高い通信を行う際に大きな問題となる可能性が考えられる．このような理由から，正常なノードが攻撃ノードと誤認されてしまった場合のえん罪を防止する必要がある．

そこで，証拠を収集・保全し，それを解析して提出を行い攻撃が存在したこと，及び攻撃を受けたことを証明するフォレンジクス技術[1]に着目し，MANET への適用を行う．本稿では，MANET のノードが CPU やメモリなどの計算資源が限られているといった特徴を考慮し，効率的な解析を行うことを目的として解析方式の提案を行う．

2. 関連研究

MANET フォレンジクスでは攻撃ノードの誤認防止を目的としている．また，MANET ではネットワークはクライアント端末のみで構成されているため，攻撃ノードでないことを証明するためには，自身が中継した内容を自身で収集、解析できる必要がある．

MANET フォレンジクスに関する研究として，証拠の収集と，任意のデータが集合に含まれるかどうかの判定に関する研究について示す．

2.1 証拠収集方式

大高ら[2]は MANET フォレンジクスを適用した際の誤認の対象を中継ノードに限定し，中継したことを送信証明として周囲にいる目撃者から証拠を収集する方式を提案している．

この方式では，ある中継ノードがデータパケットを中継する際，その周囲にいるノードは(1)証拠収集が行われていない場合は受信したパケット全て破棄する．しかし，(2)証拠収集中には，受信した全てのパケットを破棄せず，証拠生成及び証拠パケットの返送を行う(図 1)．

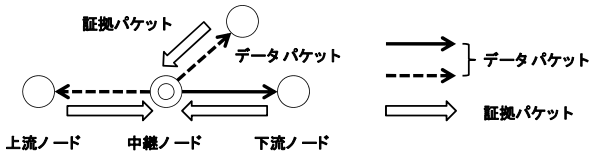

図 1 証拠収集方式のモデル

本研究では，この証拠収集方式を用いることで攻撃ノード誤認防止に関する証拠を周囲のノードから得る．

2.2 Bloom Filter

Bloom Filter[3]は，ある要素が対象とする集合に含まれるかどうかのテストのために適当な数のハッシュ関数を用意し，使用されるビット列のことである．

Bloom Filter では，含んでいない要素が対象とする集合に含んでいると誤判定する False Positive が発生する可能性がある．その確率は，m を Bloom Filter のビット数，n を集合に追加した要素数，k をハッシュ関数の個数とすると，

$$\epsilon = \left[1-\left(1-\frac{1}{m}\right)^{kn}\right]^{k} \approx \left(1-e^{-\frac{kn}{m}}\right)^{k}$$

で与えられる．またハッシュ関数の個数 k を

$$k = \frac{m}{n}\ln 2 \approx \frac{9m}{13n} \approx 0{,}7\frac{m}{n}$$

と設定することでエラー率が最小となる．

本研究では，Bloom Filter を用いて証拠の要素を表現する．Bloom Filter を用いることで，少ないメモリ領域で証拠を管理できるようになり，また複数の証拠をまとめて表現することで検索する対象範囲を狭め，検索を高速化することが可能となる．

3. 提案方式

MANET フォレンジクスにおける証拠解析手法での前提条件，提案アルゴリズムなどについて示す．通常のネットワークフォレンジクスでは，証拠の解析としてデータを属性毎に仕分けて整理し，その中から目的の情報を検索･抽出して結果を提示する[4][5]．提案方式でもこの流れを踏襲することとし，以下にその方式を示す．

A proposal for the evidence analysis method in MANET forensics

† Takashi Mishina ・Future University-Hakodate

† Osamu Takahashi ・Future University-Hakodate

3.1 前提条件

証拠は関連研究で示した方式を用いて収集されることとし，証拠パケットの内容としてイーサネットヘッダ，MANET フォレンジクスで使用されるフォレンジクスヘッダ，IP ヘッダ，IP ペイロードの中に以下の 4 つの情報が必ず含まれていると定義する．

・送信内容
・証拠生成時刻
・保証ノード情報
・証拠生成位置情報

3.2 証拠解析フロー

データの分類・整理から検索･抽出，そして結果を提示するまでの流れを示す(図 2)．

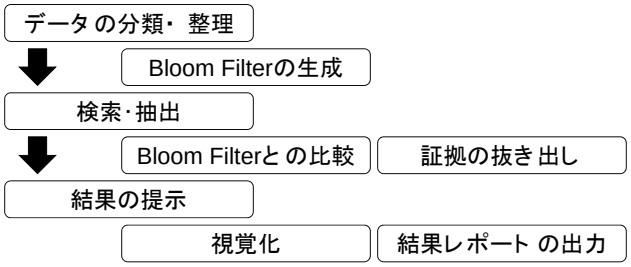

図 2　証拠解析フロー図

(1)　データの分類・整理

通信中に何らかの問題が発生し証拠を収集する際，解析時の処理を容易にするため， Bloom Filter を生成する．

この場合，全てのビットを 0 に設定した m ビットのビット列と，異なるハッシュ関数を k 個用意する．証拠を収集した際に証拠パケットから 4 つの情報をそれぞれ抜き出し，ハッシュ関数を用いてハッシュ値を計算した後にビット列の対応するビットを 1 にする．これを全ての証拠から n 個を抜き出して行い，n 個の証拠が含む要素を表す Bloom Filter とする．全ての収集した証拠に対してこの操作を行った後，終了する．

(2)　検索･抽出

何らかの問題が生じた場合収集した証拠の解析を行う．証拠の中から前提条件で示した 4 つの情報のうち，求めている特定の要素を持つものを見つけ出して抽出するために，事前処理として作成した Bloom Filter を利用して検索を行う．

この場合，要素 d が現在までに収集した証拠の中に含まれるかを検索する．まず要素 d を k 個のハッシュ関数を用いてハッシュ値を計算し，その計算したハッシュ値に対応するビット列のビットを 1 にする．これを検索する要素の Bloom Filter とする．そして検索する要素の Bloom Filter と証拠の Bloom Filter 全てとを比較し，検索する要素の Bloom Filter を包含する Bloom Filter を検索する．包含する Bloom Filter が発見された場合，その Bloom Filter に対応する範囲の証拠を全て検索し，目的の要素を含む証拠を抽出する．データの分類・整理と検索・抽出の処理の例を図 3 に表す．

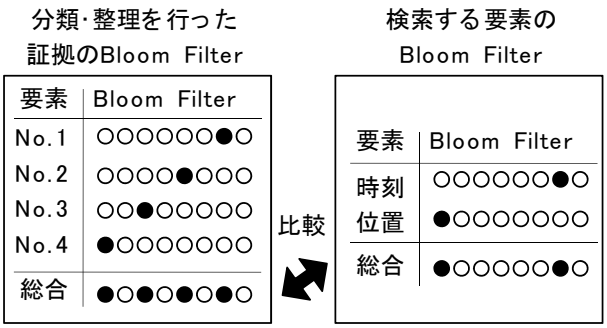

図 3　分類・整理及び検索･抽出処理

結果として，検索を行った特定の要素(ある時刻やある位置など)を含む証拠全てが抽出される．

(3)　結果の提示

特定の要素を持つ証拠が抽出された後，専門知識を要するログ情報を分かりやすくし，結果を解釈するために証拠収集状況の再現などの視覚化や，再現された内容やログ情報といった解析結果をレポート出力し，終了する．

4.　おわりに

本研究では，収集した証拠から特定の要素を含む証拠を検索するための効率の良い解析方式を提案した．MANET におけるそれぞれのノードが端末内にどのような要素を含む証拠を保持しているかを限られた計算資源で効率的に行うために False Positive の確率を考慮し，Bloom Filter を用いることで実現する．

今後，提案方式を実装し，同様の集合的データ構造(2 分探索木，線形リストなど)と使用するメモリ領域の比較，及び特定の要素を含む証拠を発見するまでの時間の計測を実験することで，提案方式が空間的・時間的に効率的であるかを評価する．また視覚化･レポートの出力に関して，検索結果にどのくらいの False Positive が含まれるかを定量的に求め，解析システムと操作者の対話的な動作による False Positive の除去など，MANET フォレンジクスでの最適な方法を検討する必要がある．

参考文献

[1] Robert Jones :インターネットフォレンジック- ネット犯罪を解決する電子証拠の収集と分析, 株式会社オライリージャパン(2006)
[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, Vol. 2008,No18, pp.217-222(2008)
[3] Bloom, B. H. Space/time trade-offs in hash coding with allowable errors, Communications of the ACM, Vol. 13,No,7, pp.422-426 (1970)
[4] 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)
[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 pp-36-40，2004.6