様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年６月１４日現在

機関番号：２０１０３
研究種目：基盤研究(B)
研究期間：2009～2011
課題番号：２１３０００２５
研究課題名（和文）無線ネットワークにおけるディジタルフォレンジック基盤技術の構築

研究課題名（英文）Building a digital forensic infrastructure in wireless network

研究代表者
高橋　修　　（TAKAHASHI OSAMU）
公立はこだて未来大学・システム情報科学部・教授
研究者番号：60381282

研究成果の概要（和文）：　無線ネットワークにおいて，悪意のある改ざんや破壊が行われた場合に､法的手段や訴訟を行うためにデータ調査／分析を行うことを可能とする攻撃の検出手法，証拠データの収集･保全･分析方式を提案すると共に，プロトタイプによる実証評価を行った．

研究成果の概要（英文）：We studied the collection/integrity/analysis method of evidence, after a malicious falsification and destruction were done, in order to perform a legal means and a lawsuit, in the wireless networks.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	3,300,000	990,000	4,290,000
２０１０年度	3,100,000	930,000	4,030,000
２０１１年度	3,100,000	930,000	4,030,000
年度			
年度			
総　計	9,500,000	2,850,000	12,350,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：ディジタルフォレンジック，無線ネットワーク，セキュリティ

１．研究開始当初の背景

モバイルアドホックネットワーク（MANET）は無線電波を使用した移動端末（ノード）で構成されているため，1)機器の電力，CPU 能力，及び通信能力に制約があること，2)管理者のいない不特定多数のノードでネットワークが構成されること，3)ノードは常に動いていることが特徴である．特に中継・転送の役割を担うノードが自己の消費電力の節約などを理由にパケットの中継拒否や遮断を行う攻撃が起こりうることが従来のネットワークとは大きく異なる．このため，ネットワーク層のセキュリティを如何に実現するかが重要な課題となっている．

インターネットを始めとする有線ネットワークでは，企業システムを対象に外部からの不正進入や社内データの不正持出しに対処するためディジタルフォレンジック（以下フォレンジックと呼ぶ）の導入が進み，RFC3227 では証拠収集とアーカイブのためのガイドラインが規定されており技術要件も明らかになっている．これに基づき収集された証拠は，労務管理訴訟（過労死訴訟）における勤務実態の把握などに実際に利用されている．

上記の状況を踏まえ，MANET において RFC3227 に準拠した証拠を収集・保全・解析する方式（MANET フォレンジック）を研

究することによって， MANET に関連して発生する法的紛争・訴訟に対応できる安全で安心な MANET ネットワーク基盤が確立できるとの着想に至った．

２．研究の目的

無線ネットワークの中でも特に次世代の通信基盤と期待されるモバイルアドホックネットワーク（MANET）のネットワーク構築・維持・管理において，安全で安心なサービス基盤技術（MANET フォレンジック技術）を確立することを目標に，以下の研究・開発を行うことを目的とする．

(1)証拠の定義，収集契機を含む証拠情報の効率的な作成・収集方式

(2)プライバシを配慮した証拠の解析方法を含む保全・解析方式

(3)安全な MANET プラットフォーム開発と実証評価

３．研究の方法

研究は，以下のステップで進める．

Step1：基本モデルの構築　MANET に関してモバイル性，アドホック性に着目し，主としてネットワーク層に着目してフォレンジックの適用モデルについて検討する．

Step2：脅威の検知　MANET を形成するノードは移動することを前提としているため，小型であり CPU 性能やメモリ量に制約があるため，証拠情報の収集は常時行うのではなく，脅威が発生したことを検知した後に行うのが現実的である．脅威の検出方式は，一般的に不正侵入監視（Intrusion Detection System）と呼ばれ，ルールに基づく検出と，統計的な異常検知方式に分類出来るが，両者について検討する．

Step3　証拠の生成・収集方式　無線ネットワークの特徴は，電波の到達範囲に存在するノードは通信パケットを簡単に受信（傍受）することが出来ることである．この特性を利用して，通信パケットを傍受したノードが受信した通信パケットを基に証拠情報を作成する．

Step4　証拠の保全・解析　収集した証拠は，端末の性能の制約から端末から分離して保存するのが現実的である．証拠を長期保存するためには，定期的に電子署名を行なう必要がある．そのための鍵管理，時刻同期方法を含めた証拠維持管理方式について検討する．

Step5　プロトタイプシステムへの実装と評価　提案方式の実用性を評価するためにネットワークシミュレータ(OPNET)に提案方式を実装し，検出精度，証拠数，証拠収集の時間を含む各種性能，オーバヘッドなどについて定量的に評価する．

４．研究成果

(1) 基本モデルの構築

MANET に関してモバイル性，アドホック性に着目し，主としてネットワーク層に着目してフォレンジックの適用モデルについて継続して検討した． MANET の脅威体系化を行うと共に，信頼性の高い証拠収集プロトコルアーキテクチャを構築した．

(2) 脅威の検知

脅威を検知するための基本評価として，ペアリング暗号の安全性解析を行った．ペアリング写像を利用することで，ID ベース暗号や効率的なブロードキャスト暗号などの利便性の高い暗号プロトコルが提案されている．GF(3^n) 上の超特異楕円曲線における η_T ペアリングを利用したペアリング暗号に関して，以下の観点からの実装評価実験を進め，拡大次数 n=71 の有限体 GF($3^{6\cdot 71}$)の解読の世界記録を得るなどの成果を上げた．

証拠の収集タイミングを適切に行うためには，攻撃の検知方法が重要である．今年度はこれまで検討してきたルールベースの検知方式を拡張し，攻撃パターンを大規模非線形問題と検討した．具体的には，通信ログをモニタリングし，離散フーリエ展開，サポートベクターマシン，自己組織化マップ，SURF 等の様々な特徴抽出方式により得られた情報を，報酬を考慮した主成分分析（RWPCA）により圧縮する．圧縮された情報を強化学習を用いて学習することにより，(1)観測された情報から特定のパターンを抜き出すためのパターン認識方式，及び(2)複数の非線形時系列から抽出された情報に基づく非線形時系列予測方式を開発した．

(3)証拠の生成・収集・保全・解析

無線電波を傍受できる近隣ノードを目撃者とし，目撃者がパケットを受信する（目撃する）毎に，それらを基に証拠を作成し送信元に返送するモデルに基づき，プロトコルを設計した．さらに，ネットワークシミュレータ上にこれらのプロトコルを実装することで，収集した証拠の信頼性評価，証拠の分析方法の定量的評価を進めた．

さらに，証拠情報をより効率よく収集するためのプロトコルとしてクラスタ-クラスタベースの高信頼な通信経路構築方式， GIS（3 次元位置情報）をベースとしたよりオーバヘッドの少ない次世代高信頼ルーティング方式,などについて検討した.また,DoS 攻撃にロバストであり，大規模システムの制御に有効である多変量解析に基づく状態空間の圧縮方式等を導入した強化学習によるルーティング方式について，ルーティングアルゴリズムの効率を上げるために，非線形目的関数の大域的最適化問題を導出する方法を

検討した．これを基に，高効率なルーティングアルゴリズムを開発した．

無線ネットワーク機器が自律分散的に使用する周波数やチャネルを決定するための方式について検討を進め，2.4Ghz 帯の Wi-Fi を前提に，効率的なチャネル決定アルゴリズムを提案するとともに，その定量的な評価を行いその有効性を明確にした．更に，無線アドホック NW を構築するためには，ノード密度や帯域幅が，通信の性能（遅延時間やスループット等）にどのように影響するかを理論的に解明する必要があり，ルーティングアルゴリズムと通信性能との関係を数学的なモデルで定量的に解析した．

ネットワークシミュレータと数学モデルにいよる評価結果は，最適な方式パラメータの設定指針や，方式設計に反映することによって，無線ネットワークにおけるディジタルフォレンジックに関する基盤技術として集大成させた．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１１件）

① Jiajia Liu, Xiaohong Jiang, Hiroki Nishiyama, and Nei Kato, Reliability Assessment for Wireless Mesh Networks Under Probabilistic Region Failure Model, IEEE Transactions on Vehicular Technology, 査読有, Vol.60, No.5, pp.2253-2264, 2011
DOI:10.1109/TVT.2011.2114684

②Kaikai Chi, Xiaohong Jiang, Baoliu Ye, Yanjun Li, Flow-oriented network coding architecture for multihop wireless networks, Computer Networks, 査読有, Vol.55, No.10, pp.2425-2442, 2011

③ Jiajia Liu, Xiaohong Jiang, Hiroki Nishiyama and Nei Kato, Delay and Capacity in Ad Hoc Mobile Networks with f-cast Relay Algorithms, IEEE Transactions on Wireless Communications, 査読有, Vol.10, No.8, 2738-2751, 2011
DOI: 10.1109/icc.2011.5962997

④Masataka Kikawa, Yoh Shiraishi, Osamu Takahashi, A Presence-detection Method using RSSI of a Bluetooth Device, International Journal of Informatic Society (IJIS), 査読有, Vol.2, pp.23-31,2010

⑤ Hideki Sato , Global Nonlinear Optimization Based on Wave Function and Wave Coefficient Equation, IEICE Trans. Fundamentals, 査読有, Vol.E93-A, No.1, pp.291-301, 2010

⑥林卓也，白勢政明，高木剛，GF(3^n) 上の関数体篩法の実装実験，情報処理学会論文誌，査読有，Vol.50, No.9, pp.1956-1967, 2009

〔学会発表〕（計４３件）

①Jiajia Liu, Xiaohong Jiang, Hiroki Nishiyama and Nei Kato, Exact Throughput Capacity under Power Control in Mobile Ad Hoc Networks, IEEE INFOCOM 2012, 2012年3月（米国）

②完山和希，中村嘉隆，白石陽，高橋修，片方向リンクを含む無線ネットワークへネットワークコーディングの適用，電子情報通信学会技術研究報告 111 巻 408 号（NS2011145-178），2012 年 1 月（沖縄県）

③高橋由多加，中村嘉隆，白石陽，高橋修，“2.4GHz 帯における Duty Cycle を用いた最適チャネル選択方式”，電子情報通信学会 SR 研究会 2011 年 10 月 26-28 日 東京

④ Yoh Shiraishi, Masataka Kikawa, and Osamu Takahashi, Estimation of Presence Information of a User by using RSSI of Bluetooth and Acceleration Sensor Data, IWIN (International Workshop on Informatics) 2011, 2011 年 9 月,（イタリア）

⑤ Jiajia Liu, Xiaohong Jiang, Hiroki Nishiyama and Nei Kato , erformance Modeling for Two-hop Relay with Node Selfishness in Delay Tolerant Networks, IEEE Online Conference on Green Communications (IEEE GreenCom’11) , 2011 年 8 月（中国）

⑥ Xiaoliang Wang, Xiaohong Jiang and Achille Pattavina, Network Vulnerability Under Probabilistic Region Failure Model, IEEE HPSR 2011, 2011 年 7 月（スペイン）

⑦三浦愛美，中村嘉隆，白石陽，高橋修，MANET における信頼性を考慮した証拠収集手法の提案，情報処理学会 DICOMO シンポジウム 2011, 2011 年 7 月（京都府）

⑧ Jiajia Liu, Xiaohong Jiang, Hiroki Nishiyama and Nei Kato, Delay and Capacity in Ad Hoc Mobile Networks with f-cast Relay Algorithms, IEEE ICC 2011, 2011 年 6 月（京都市）

⑨三科貴，白石陽，高橋修，“携帯端末での署名履歴交差を用いた証拠保全手法の提案と評価”，情報処理学会研究報告. MBL,［モバイルコンピューティングとユビキタス通信研究会研究報告］2011-MBL-57(14), 2011 年 3 月 東邦大学（千葉県）

⑩大竹健司，白石陽，高橋修，“ネットワークコーディングを用いた ALM における経路構築及び修復法の提案と評価”，電子情報通信学会技術研究報告. NS, ネットワークシステ

ム 110(448), 2011 年 2 月
⑪Yoh Shiraishi, Ryo Miki, Osamu Takahashi, A Geocast-based Multicast Method for Continuous Information Delivery in MANET, IEEE International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Nov. 2010 九州工業大学（福岡県）

６．研究組織
(1)研究代表者
高橋　修（TAKAHASHI OSAMU）
公立はこだて未来大学・システム情報科学部・教授
研究者番号：60381282

(2)研究分担者
佐藤 仁樹　（SATO HIDEKI）
公立はこだて未来大学・システム情報科学部・教授
研究者番号：30360001

Jiang　Xiaohong　（Jiang Xiaohong）
公立はこだて未来大学・システム情報科学部・教授
研究者番号：00345654
（2010 年度～2011 年度）

高木　剛（TAKAGI TSUYOSHI）
九州大学・大学院数理学研究院・教授
研究者番号：60404802
（2009 年度）

(3)連携研究者
高木　剛（TAKAGI TSUYOSHI）
九州大学・大学院数理学研究院・教授
研究者番号：60404802
（2010 年度～2011 年度）