様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　　３　日現在

機関番号：　３２６３８
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2017
課題番号：　２５３３０１５８

研究課題名（和文）モバイルアドホックネットワークにおけるワームホール攻撃検出

研究課題名（英文）Detection of Wormhole Attacks on Mobile Adhoc Networks

研究代表者

蓑原　隆（Minohara, Takashi）

拓殖大学・工学部・教授

研究者番号：８０２３９３３４

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：近年，モバイルアドホックネットワークの重要性が増大しているが，無線通信の開放性からセキュリティについての脆弱性が懸念されている．中でもワームホール攻撃は攻撃ノードが正常な経路制御を利用していることから検出が困難な攻撃となっている．本研究では，多重経路探索，伝搬遅延時間の矛盾検出，確認応答の認証などの，モバイルアドホックネットワークに対するワームホール攻撃の対策を提案した．提案した対策の有効性はネットワークシミュレーションおよび計算能力が限られた無線ノードへの実装によって確認されている．

研究成果の概要（英文）：In recent years, mobile ad hoc networks(MANET) are becoming more and more important when it is hard to use normal network infrastructures. However, the open nature of the wireless communication makes them vulnerable to various security attacks. Wormhole attack is one of the most serious attacks on MANET. By employing out of band link called as ‘wormhole,' attacker provides routing path and takes illegal actions such as data corruption and eavesdropping over communications.
In this study, I have proposed a set of countermeasures, which include multiple routing path generation, incoherency detection in propagation delay, and authentication of the acknowledgment, to the wormhole attack on MANET. The proposed method is confirmed by network simulation and implementation to wireless nodes which have limited computational power.

研究分野：　ディペンダブルコンピューティング

キーワード：　アドホックネットワーク　ワームホール攻撃　多重経路探索　Ack認証

１．研究開始当初の背景

無線通信装置を搭載した移動端末同士の相互通信中継によってネットワークを構成するモバイルアドホックネットワークは，拡張しやすく，地形や災害に影響されにくいなどの利点を持つことから，有線通信網を利用することが様々な理由で困難な状況を中心にその利用が広がっている．しかし，無線通信は通信の当事者以外にも開かれていることから，パケットの改竄や盗聴などのセキュリティ上の問題に対する脆弱性が懸念されてる．

モバイルアドホックネットワークに対する攻撃として，既存の経路より有利なリンクをアナウンスすることで通信の誘導を行うワームホール攻撃は，ルーティングプロトコルの正しい動作を利用していることから，パケットの暗号化などの通常の防御方法では対応できない困難な問題になっている．

２．研究の目的

本研究では，ノード間のパケット伝送距離を位置情報から算出し，無線通信距離の上限と矛盾する異常なパケット伝播を判定してワームホール攻撃を検出するものとし，攻撃検出率に対する位置計測コストを最適化する検出方法を明らかにすることを目的とする．また，考案した検出手法が実際の携帯機器レベルの処理能力で利用できることを確認するために，携帯機器で実行できるソフトウェアを開発し，動作の検証を行うことを目的とする

３．研究の方法

本研究ではアドホックネットワークの経路制御に AODV と同様のオンデマンド型のプロトコルを利用することを想定している．これは，経路を必要とするノードが経路要求メッセージ(RREQ)をフラッディングによりネットワーク全体に配布し，目的ノードが経路応答メッセージ(BREP)を，BREQ が伝搬してきた経路を逆にたどるように送り返すことで，ノード間の経路を確立する．攻撃検出のための具体的なパケット伝播として BREQ および BREP に位置情報などの攻撃検出のための情報を付加することを考える．特に，攻撃ノードにおける位置情報の改竄に対処し，改竄があったとしても攻撃を検出できる検出方法について検討を行う．

一般に情報の改竄に対する対抗手段として，電子署名などの暗号をベースとした技術が使用されるが，移動端末のように計算資源に限りがある場合には，暗号計算が負担になる可能性がある．そこで，改竄への対抗手段としては独立した複数の経路による情報伝播と伝搬された情報の比較による方法を考える．

さらに，考案した検出手法を実際の携帯機器レベルの処理能力で利用できることを確認するために，携帯機器で実行できるソフトウェアを開発し，動作の検証を行う．

４．研究成果

(1) 経路要求メッセージが複数の経路で伝搬するときの経過時間の矛盾によるワームホール攻撃の検出

ノードが位置情報を取得するタイミングの関係で十分な位置精度が得られない場合のワームホール検出方法として，BREQ の伝搬時に各ノードで経過した時間を加算し BREQ に負荷する．BREQ はフラッディングによって複数の経路で伝搬するが，このとき図 1 に示すように異なる経路での伝搬時間 T(c)と T(e)は一定の誤差の範囲で一致するはずである．

しかし，図 2 に示すように一方の経路にワームホール攻撃が介在している場合，ワームホールで消費される時間が伝搬時間に含まれないため，経路間の伝搬時間に想定される誤差を越える差が生じる．

そこで，BREQ に対して BREP を逆方向に伝搬する際に，通常は中継回数が少ないなどの有利な経路を選択するが，複数経路の伝搬時間の差が想定を越える場合に，有利に見える経

路をあえて選択しないことで攻撃を回避する方法を提案した.

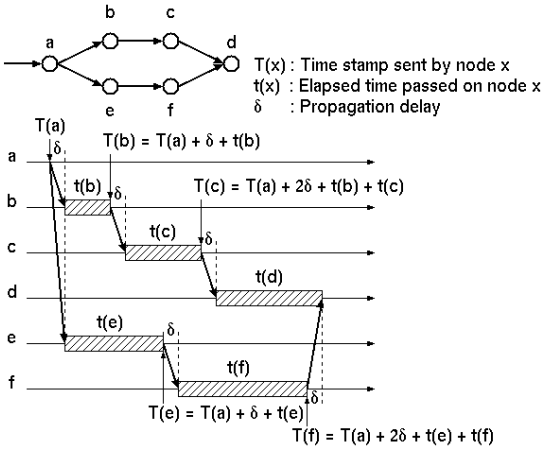

図 1 複数経路による経路探索メッセージの伝搬

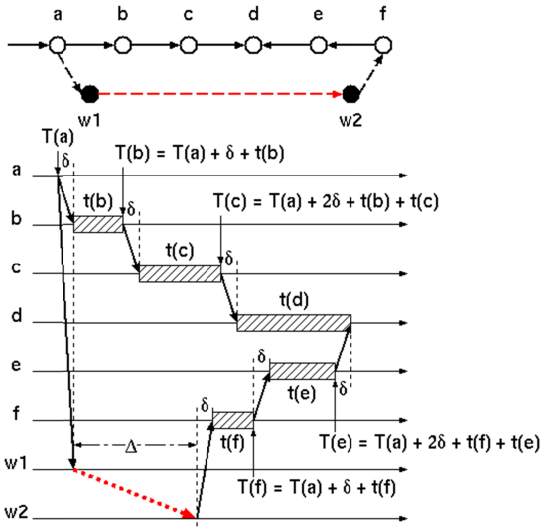

図 2 攻撃下での複数経路による経路情報の伝搬

提案手法が移動端末の制限された計算機資源のもとで実現可能であることを確認するために，実際の無線センサーネットワークに検出機能を実装し，その有効性を確認した.

(2) 複数の独立した経路の探索方法とワームホール攻撃検出への有効性の確認

単一の経路探索ではワームホール攻撃が介在している可能性があることから，複数の独立した経路を探索する方法を AODV の拡張である AOMDV をベースにしたプロトコルを提案し，ネッワークシミュレーションによって攻撃検出に対する有効性を調査した.

提案したプロトコルは，図 3 に示すように，AODV が BREP を逆伝搬するための経路情報を 1 つだけ保存するのに対し AOMDV の経路情報と同様に，経路要求を行ったノードへ到達する最終ホップが異なる情報を保存する.

destination	sequence no.	hop count	next hop	time out

(a) AODV

destination	sequence no.	advertised hop count	route list

next hop 1	last hop 1	hop count 1	time out 1
next hop 2	last hop 2	hop count 2	time out 2
next hop 3	last hop 3	hop count 3	time out 3
⋮			
next hop n	last hop n	hop count n	time out n

(b) AOMDV

図 3 多重経路探索のための経路表

目的ノードからは BREQ を受け取った全隣接ノードに対して BREP を送信する. 中間のノードには複数の BREP が到着するが，ここで，BREP ごとに異なるリンクに伝搬させることで独立した複数の経路を形成する.

提案した方法によって作られた多重経路によってワームホール攻撃を検出できるかネットワークシミュレーションを行って調べたところ，攻撃に使用されるワームホールの距離が大きい場合には経路の矛盾が検出できるが，攻撃の成功率は低いものの短いワームホールは検出が困難であることがわかった.

(3)探索した複数経路の情報に矛盾が無い場合に 2 番目に良い経路を選択することによるワームホール攻撃の回避

多重経路探索によるワームホール攻撃の検出が困難であるような短いワームホールによる攻撃について，ワームホール攻撃が介在する経路が最も有利な経路となるように攻撃を実施することは容易であるが，2 番目に有利な経路になるように制御することが困難なことに着目して，次点の経路を選択することによ

る攻撃回避方法を提案し，ネットワークシミュレーションによって評価を行った．

表 1 シミュレーション結果のまとめ

評価対象	該当数
全シミュレーション	1960
第 1 経路がワームホールを通過するもの	124 (6.3%)
上記のうち第 2 経路の選択で回避できるもの	106
第 2 経路の選択でワームホールを通過するもの	33
選択した経路がワームホールを通過するもの	51 (2.6%)

1.5km 四方の平面上にランダムに 100 個のノードを配置し，2 つのノードをランダムに選んで有線リンクで結合してワームホール攻撃を実現し，さらに 2 つのノードをランダムに選んで通信を行わせるというシナリオを 98 通り用意し，通信タイミングを変更して各 20 回シミュレーションを行った結果を表 1 に示す．このように次点の経路を選択することで，通常の経路探索を行う場合に比べて攻撃の成功率を半分以下にすることができることが確認された．

(3)ワームホール攻撃検出のためのリンクレベルでの Ack 認証の実現

無線通信における通信確認のための確認応答(Ack)の伝送を考えると図 4 に示すようにワームホール攻撃が介在する場合には，1 ホップ分の通信で 2 回ワームホールを通過するため遅延が大きくなる．そこで，Ack の遅延によってワームホール攻撃を検出することが考えられるのだが，攻撃ノードがあたかも正規のノードが応答したかのように Ack を偽装すると検出が困難になる．この Ack の偽装を防ぐために Ack に署名を付加して，その正当性を確認する方法を提案した．このとき攻撃ノードが正規の Ack を保存しておいて，それを再送する，いわゆるリプレイ攻撃を防ぐために，毎回署名が変化するようにチャレンジレスポンス型のワンタイム署名を使用する．

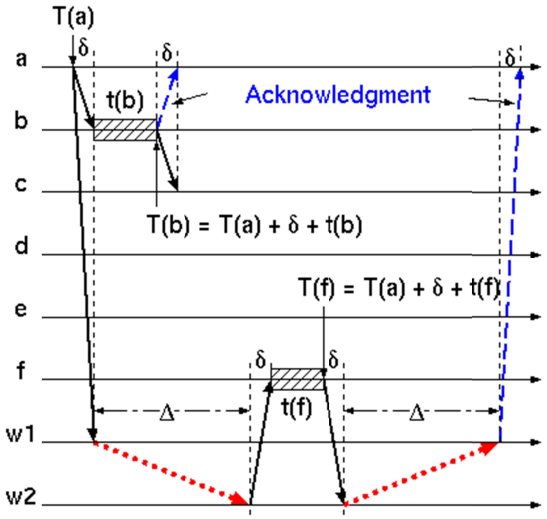

図 4 ワームホールによる確認応答の遅延

このように Ack にワンタイム署名を使用する場合，署名の計算が必要になるが，無線ノードの限られた計算機資源で実現可能かどうか，8 ビットマイコンを使用した無線センサーネットワークにワンタイム署名による Ack 認証を実装し，AES 暗号を使用した署名を実現できることを確認した．

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　7 件）

(1) 蓑原 隆，吉井 碧，XMesh プロトコルを用いたワイヤレスセンサーネットワークに対するワームホール攻撃の検出，電子情報通信学会技術報告，査読無，113 巻，2014，pp.73-78

(2) 蓑原 隆，西山 響翼，低電力モードの無線センサーネットワークに対するワームホール攻撃の検出，電子情報通信学会技術研究報告，査読無，115 巻，2015，pp.23-28

(3) Takashi Minohara，Kyosuke Nishiyama，Detection of Wormhole Attack on Wireless Sensor Networks in

Duty-Cycling Operation, Proceeding of the 2016 International Conference on Embedded Wireless Systems and Networks, 査読有, 2016, pp.281-282

(4) 小野寺 睦, 蓑原 隆, 多重経路探索を利用した MANET のワームホール攻撃対策, 電子情報通信学会技術研究報告, 査読無, 116 巻, 2017, pp.309-314

(5) 王 文揚, 蓑原 隆, デューティサイクル動作を行う無線センサーネットワークにおけるワームホール攻撃とその対策,電子情報通信学会技術研究報告, 117 巻, 2017 年, pp.67-72

(6) Wenyang Wang, Takashi Minohara, Wormhole Attacks on Asynchronous Duty-Cycling Sensor Networks and Their Countermeasures, Proceeding of the 2018 International Conference on Embedded Wireless Systems and Networks, 査読有, 2018, pp.183-184

(7) 蓑原 隆, 王 文揚, 無線センサーネットワークにおける Ack 認証の実装, 電子情報通信学会技術研究報告, 査読無, 117 巻, 2018 年, pp.275-279

〔学会発表〕（計　1 件）

(1) Li Wei, Takashi Minohara, Enhancing Location Privacy in Host Identity Protocol using Multiple Forwarding Session Initiation, The 19th IEEE Pacific Rim Internatinal Symposium on Dependable Computing, 2013 年 12 月 2 日, Vancouver, British Columbia, Canada

〔その他〕

ホームページ等

http://www.cs.takushoku-u.ac.jp/dcl/

６．研究組織

(1)研究代表者

蓑原 隆（MINOHARA, Takashi）

拓殖大学・工学部情報工学科・教授

研究者番号：80239334