ISS-A-051

MANETにおけるRTS/CTSを用いたブラックホール攻撃検出法の研究

橋口 亮志　吉田 政望　野口 拓
Katsuyuki Hashiguchi　Masami Yoshida　Taku Noguchi

立命館大学大学院情報理工学研究科
Graduate School of Information Science and Engineering, Ritsumeikan University

1　まえがき

近年, 既存のインフラを用いずモバイル端末だけでネットワークを構築する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ではノードが自律分散的にルーチングを行う. このルーチングを悪用し攻撃を行うルーチング攻撃は深刻な問題の一つであり, 攻撃の検出, 防御方法の研究は盛んにおこなわれている [1]. ルーチング攻撃には様々な攻撃が存在し, パケットドロップ攻撃はその一種である. このような攻撃に対する対策の一つに, パケットの損失率から攻撃確率を推察する方法がある [2]. しかし, アドホックネットワークにおけるパケットドロップにはパケット衝突やチャネルエラーに起因する自然なパケットドロップが存在し, 攻撃によるパケットドロップと誤検知する問題がある.

本研究では, パケットドロップ攻撃の一種であるブラックホール攻撃（BH 攻撃）に対して, RTS/CTS を用いて攻撃を検出する手法を提案する.

2　パケット損失率を用いた攻撃検出メカニズム

攻撃検知にパケット損失率を用いる既存研究 [2] では, パケットドロップを行う悪意のあるノードの検出のために, パケットドロップの原因推定を用いた検証を行った. この方式では, オーバーヒアリングを用いた観測によって得られる自然なパケット損失率から, 悪意のあるパケットドロップによるパケット損失率を計算する. しかし, この研究では固定トポロジかつ観測対象が既知の場合を前提としており, ランダムなトポロジにおいてはオーバーヒアリングの観測対象をネットワーク全体にすることが必要となる.

3　RTS/CTS 数を用いた BH 攻撃検出法

本研究では, BH 攻撃下での RTS/CTS に着目し, RTS/CTS の受信状況から攻撃ノードを推定する. BH 攻撃による影響が大きい場合, MAC 層での RTS/CTS の観測では, 攻撃ノードはチャネルビジーのノードと似た振る舞いをする. BH 攻撃では, 攻撃ノードに隣接するノードのパケット送信数が増加するため, RTS/CTS の観測結果はビジーノードと判別がつかない. このため, MAC 層の観測だけで BH 攻撃を判別する事は困難である. また, ネットワーク層でパケット損失率によって攻撃を判別する場合, オーバーヒアリングの観測対象を全てのノードにする必要がある. 提案手法では, 各ノードが送信した RTS と返送された CTS の数を観測し, 衝突回数が閾値 T を超えた時のみ, オーバーヒアリングを用いた観測を行う. 閾値 T は, チャネル制御によって回避された衝突のリスクを考慮し, 送信対象へ RTS を送信するノードの数（Nrts）が閾値 Tn より大きい場合は無効にする.

4　性能評価

本研究では, 前述の検出手法を用いて, [2] で検証されなかったランダムかつ静的なトポロジでの検証を行った. BH 攻撃を実装し, 検出率について調べた.

表 1　パラメータ

ルーチング	DSR
データレート	11 Mbps
キューサイズ	無限
送信範囲	250 m
MAC 層プロトコル	802.11
シミュレーション時間	500 秒
トラフィックの種類	CBR
パケットのサイズ	512 B
パケット間隔	1 秒
Tn の設定値	1〜5
T の初期値	30

4.1　パラメータ設定

ns-3 を用いて, ノードが最初の 100 秒間ランダムに分散し, その後に 500 秒間通信を行うシミュレーションを行う.

シードによって, ノード数 50 の 10 種類のトポロジを用い, 5 つの送信ノードそれぞれが, 1 つにつき 5 つの宛先に対して送信を行う. 悪意のあるノード数は 1 で, 到達したすべてのパケットをドロップする.

4.2　実行結果

悪意のあるノードと相互通信する周辺ノードの数に対する, 悪意のあるノードを検出した周辺ノードの数の割合を検出率 D とし, Tn 毎にシミュレーション回数で平均した D のグラフを (図 1) に示す. Tn が 3〜4 で減少率が最も大きくなったため, 本研究における Tn の最適値は 3 である.

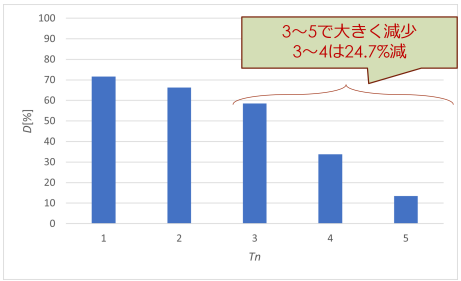

図 1　Tn に対する検出率

5　まとめ

本研究では, ランダムかつ静的なトポロジにおける RTS/CTS を用いた攻撃検出を行った. ネットワーク層の観測に MAC 層の RTS/CTS を用いることで, オーバーヒアリングの観測対象を絞れることを示した. 検出率は Tn とトレードオフの関係であり, 今後は, T と Tn を動的に変化させた検証が必要である.

参考文献

[1] A. Nadeem, M P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", pp.2027–2045, 2013.

[2] T. Hayajneh, P. Krishnamurthy, D. Tipper, T. Kim, "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks", IEEE.Communications, pp. 1062-1067, 2009.

Copyright © 2022 IEICE