アドホックネットワークにおける信頼性評価による経路選択法の評価と検討

米谷　和也†　井手口　哲夫†　田　学軍†　奥田　隆史†

愛知県立大学情報科学部†

1. はじめに

近年、情報技術は目覚ましく発展し、ユビキタス社会の到来を間近に控え、世界中で様々な研究が行われている。その一つにアドホックネットワークがある。アドホックネットワークの歴史は長く、1970 年代に ARPA プロジェクトの一環として研究されたのが始まりだが、未だに普及には至っていない。その原因の一つにセキュリティの問題がある。アドホックネットワークは参加・離脱の自由なネットワークであるためノードの管理が困難であり、攻撃者の侵入が容易である。通信を中継するものが悪意ある者だった場合、通信が上手く中継されないことやデータを盗聴されてしまう可能性もある。

この問題を解決するために、ネットワークに参加するノードを管理し、中継ノードが信頼できるか判断することで攻撃ノードや不正なノードを回避する方法が考えられる。

そこで本稿では、アドホックネットワーク上の全てのノードが隣接ノードの信頼情報を保持し、その情報に基づいて中継ノードを決定し通信を行う「信頼性評価による経路選択法」を提案する。さらに、この方式をネットワークシミュレータ NS2[1]上で構築し、シミュレーションにより評価を進める。

まず、第 2 章でアドホックネットワークの説明と想定される攻撃を示し、第 3 章で提案方式の詳細を示す。最後に第 4 章でまとめと今後の課題とする。

2. アドホックネットワーク

2.1 アドホックネットワークとは

アドホックネットワークは、各ノードが中継機能とルーティング機能を持ち、マルチホップで通信を行うネットワークである[1]。

2.2 アドホックネットワークのセキュリティ

2.2.1 想定される攻撃

想定される攻撃法の分類を図 1 に示す[2]。

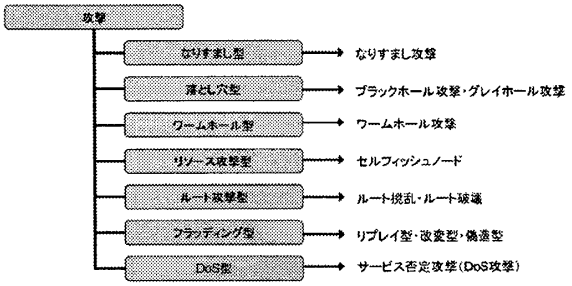

図 1：アドホックネットワークにおける攻撃法の分類

2.2.2 関連研究

偽装した応答メッセージを使って送信元と双方向経路を確立し、送信されたデータを取得、破棄などを行うことで通信を妨害するブラックホール攻撃に対する防御法を提案した研究がある[3]。この防御法では各ノードがブラックホールノードの条件を満たすノードが存在するか監視し、存在した場合はブラックリストに登録、周知を行うことでブラックホールノードの偽装応答メッセージを破棄し、偽装経路作成を未然に防ぐという方式である(図 2)。

結果として、攻撃者の早期発見、攻撃を回避可能であり、誤経路作成を防止可能である。

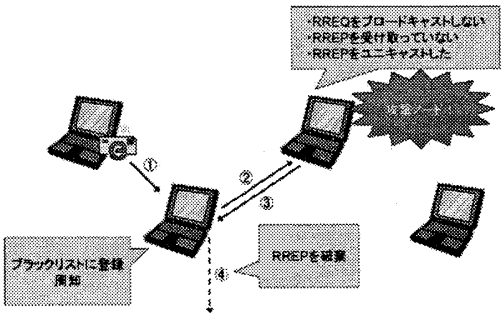

図 2：ブラックホール攻撃に対する防御法

3. 信頼性に基づく経路選択法の提案

3.1 基本方式

本提案方式は各ノードが信頼できる隣接ノードと通信を行うことでセキュリティを保つものである。各ノードは隣接ノードの信頼値を保持し、信頼値の高いノードをデータの中継依頼先として選択し通信する(図 3)。

「The route selection method by the trust for adhocnetwork」

†「Kazuya Yonetani Tetsuo Ideguchi Xuejun Tian Takashi Okuda ,Faculty of Information Science and Technology, Aichi Prefectural University」

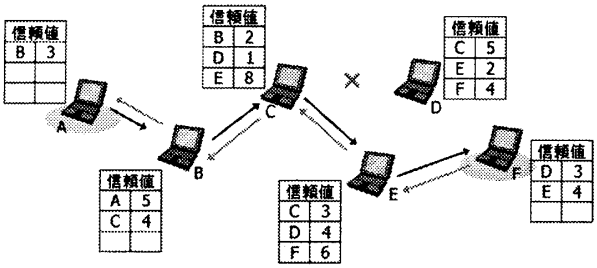

図 3：提案方式

3.2 前提条件

- 本提案方式はネットワーク内に存在する攻撃ノードの検出、攻撃の防御を目的としない
- やり取りされる情報は暗号化されているものとする
- 中継ノードの攻撃に焦点を絞る
- ノードの移動頻度が高いと予測されるネットワークに適合するためルーティングプロトコルは AODV を使用する
-

3.3 制御パケット

(1) Complete パケット（COM パケット）
データ受信後、宛先ノードから送信先に向けて送信される通信成否判定パケット

(2) Value パケット（VAL パケット）
COM パケット受信後、送信元が中継ノードに送信する評価用パケット

(3) Dummy パケット（DUM パケット）
ネットワーク参加初期に用いる偽のデータパケット

3.4 隣接ノードの評価基準

ネットワーク参加当初の隣接ノードの信頼値は全て初期値(0)とし、通信が成功すれば中継に参加したノードの信頼値を+1 し、失敗すれば-1 する。

3.4.1 通信の成否判定

データ送信後、応答タイマー(RES タイマー)の設定時間内に COM パケットが宛先ノードから返信されれば通信成功(図 4)とし、返信されなければ通信失敗とする(図 5)。

3.4.2 評価の連鎖

通信の成否判定後、送信元ノードは VAL パケットを送信して中継依頼した隣接ノードを評価する。VAL パケットを受信した隣接ノードは同様にフォワードを行った隣接ノードを評価し VAL パケットを送信する。この処理は宛先ノードまで行う(図 4，図 5)。

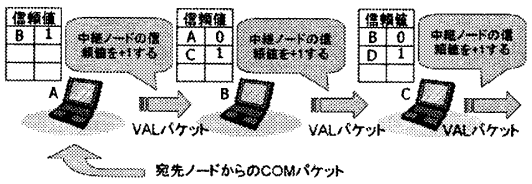

図 4:COM パケットの受信(通信成功)

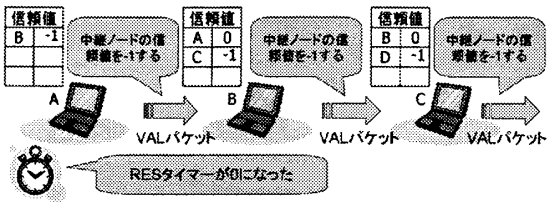

図 5：RES タイムマーのタイムアウト(通信失敗)

3.5 初期動作時の問題解決

隣接ノードの信頼値が不明である初期状態では、データを送る前に DUM パケットを送信して経路を評価する(図 6)。DUM パケットを受信した宛先ノードから COM パケットが返送されれば、通信成功とみなし中継ノードの信頼値を上げる。RES タイマーがタイムアウトすれば通信失敗とし中継ノードの信頼値を下げ、再度別の中継ノードに DUM パケットを送る。

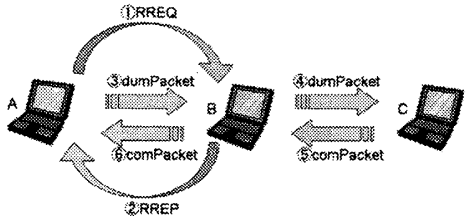

図 6：DUM パケットの送信動作

4. まとめと今後の課題

本論文では、アドホックネットワークのセキュリティの問題点に焦点を当て、経路選択の際に新たな条件「信頼値」を付加することで通信の信頼性を確保する方法を提案した。

今後の課題として本提案方式を NS2 上で構築し、シミュレーションにより評価を行う。シミュレーションの際は攻撃ノードを配置し、攻撃ノードを回避しつつ信頼値の高いノードと通信を行うことを目標とする。

参考文献

[1]University of Southern California, 「The Network Simulator – ns-2」, http://www.isi.edu/nsnam/ns/

[2]斉藤匡人, 「無線アドホックネットワーク」, 2003 年 8 月 24 日

[3]森郁海, 森拓海, 高橋修, 「AODV ベースセキュアルーティングプロトコルの提案とその実装・評価」, マルチメディア, 分散, 協調とモバイル(DICOMO2007)シンポジウム論文集, pp.906-917(2007)

[4]森郁海, 横山信, 高木剛, 山崎憲一, 高橋修, 「アドホックネットワークにおけるブラックホール攻撃に対する防御法の提案と実装・評価」, 情処研報, pp.47-52, 2006

[5]米谷和也, 井手口哲夫, 田学軍, 奥田隆史, 「アドホックネットワークにおける信頼性評価による経路選択法の一考察」, 情報学ワークショップ 2007(WiNF2007)論文集, pp.89-92, 名古屋大学(2007-9)