2E-6

無線LANマルチホップネットワークにおける セキュアコネクション構築モデルの提案と実装

鎌田 美緒† 小口 正人†

†お茶の水女子大学

1 はじめに

近年，固定インフラを必要とせず複数端末が集まるのみで自律分散的なネットワークを構築するMANET (Mobile Ad-Hoc Network) が，大いに注目されている．MANETでは，モバイルノードのルータ機能により通信を中継することで，より広範囲の通信を可能にしており，このように構築されるネットワークをマルチホップネットワークという．

一般に無線通信はセキュリティを考慮することが不可欠であるが，特にMANETのような環境は不特定多数のノードが存在するため，セキュリティ上の危険性がより高いといえる．そのため，データ送受信を行う特定ノード間の通信の暗号化が望ましく，さらにMANETの特徴を考慮し，ノード移動によるネットワーク構成の変化に柔軟に対応できるセキュリティ手法が必要である．そこで本研究では，IPsec (IP Security) を用いて暗号化通信経路であるセキュアコネクション [図1] を構築することにより，セキュリティを提供する手法を検討した．IPsecは暗号化及び認証により安全な通信を提供する規格で，構築された通信経路毎に独立したコネクションが生成可能であり，鍵交換や認証機能を提供するIKE(Internet Key Exchange) の処理過程で通信相手の本人性確認を行う．

本研究では，MANETにおける端末同士の安全かつ信頼できる通信の実現を目指し，無線LANマルチホップネットワーク上においてセキュアコネクションを構築および管理するモデルを提案した [3]．本稿では，既存のMANETルーティングプロトコルであるOLSR (Optimized Link State Routing) を用いマルチホップ環境を構築し，提案モデルに基づき，IPアドレスの取得やセキュアコネクションの確立に関する制御の実装を行った．

2 セキュアコネクション構築モデル

2.1 提案モデル概要

本稿では，通信経路の構築をOLSRに任せネットワーク構成を意識せずセキュアコネクションを生成するモデルを提案している．一般にMANET内の各ノードは固定アドレスを持たないため，固定網向け仕様であるIPsecを適用する場合，通信相手のアドレス決定に関する処理を行わなければならない．提案モデルでは，まず事前にノード情報をリストとして作成し管理を行うことにより通信相手の信頼性を確保し，セキュアコネクションを構築する際のセキュリティを提供する．そしてMANET参加後，参加ネットワークにおける目的ノードのIPアドレスとIDを対応付け，実際のセキュアコネクションを生成することで，送受信データの暗号化を行う安全な通信経路を提供している．次節以降で，提案手法の詳細を述べる．

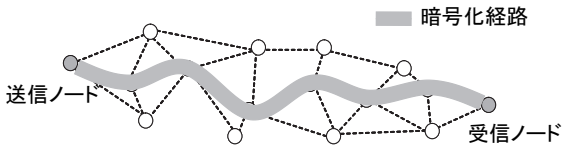

図 1: セキュアコネクション

2.2 ノードにおけるリスト管理

マルチホップ通信を行う際，データの暗号化が必要となるのは，互いのノードが信頼できると判っているときに限られる．そこで本手法では，予め信頼が保証されたノードのIDや公開鍵等の情報を，各ノードが事前にリストとして保持することにした．この公開鍵はIPsecの処理過程で認証等に使用されるものであり，実際の暗号鍵とは異なる．リストの情報と照らし合わせ処理を進めることで，通信相手の信頼性を確認することができる．

2.3 IP アドレスの取得

MANETにノードが参加すると，OLSRによりマルチホップネットワークが構築される．MANETでは一般に各ノードはIDで識別され，参加するネットワークにより異なるIPアドレスが割り当てられるため，セキュアコネクションの生成にあたり目的ノードのIPアドレスを知る必要がある．そこで送信元ノードはネットワーク内で用いられている目的ノードのIPアドレスの問い合わせを行い，取得したアドレスをリストに保持する．

2.4 セキュアコネクションの構築

IPアドレスの取得後，送信元ノードは送受信ノード間をエンドツーエンドで結ぶIPsecによる暗号化通信経路を生成することで，セキュアな通信路を構築する．IPsecのコネクション生成過程でリストの公開鍵が参照され本人性確認が行われるため，万一IPアドレス取得の際詐称が行われた場合もこれを防ぐことができる．このセキュアコネクション上では既に暗号化されたパケットがやり取りされるため，中継ノードはデータの

Proposal and Implementation of a Secure Connection Construction Model on a Multi-Hop Wireless Network
† Mio Kamada, Masato Oguchi
Ochanomizu University (†)

中身を知ることはできない.

3 提案手法の実装

3.1 実験環境

本研究では，エンドツーエンドでセキュアコネクションを生成する手法に基づき，セキュアコネクション生成制御の実装を行った．実験環境としては，IEEE802.11b 無線 LAN 機能を持つ 4 台の Linux マシンを用い，マルチホップネットワーク環境を図 2 のように構築した．OLSR と IPsec の Linux における実装として，それぞれ olsrd[1] と openswan[2] を用いている．

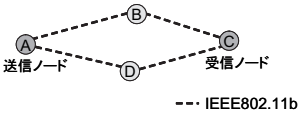

図 2: 実験環境

本環境において，ノード A を送信元ノード，ノード C を目的ノードとし，B と D はマルチホップ環境に自由に参加や離脱するノードと想定している．実験上，全ノードが直接通信できる範囲内に存在するため，iptables コマンドによりパケットの遮断を行うことで，ノード A から C へのマルチホップ通信を実現している．

上記実験環境において OLSR による通信経路確立後，IP アドレスの取得とセキュアコネクションの構築を行う制御を実装した．

3.2 IP アドレスの取得とリストへの追加

OLSR によるマルチホップ通信経路確立後，参加ネットワークにおける互いの IP アドレスを通信相手 ID と対応付けるため，まず送信ノードは「送信元ノード ID・送信元ノード IP アドレス・目的ノード ID」を含むリクエストメッセージを全ノードに送信する．次にリクエストメッセージを受信した各ノードは，メッセージのチェックを行い，自分の ID が含まれていた場合「自身の ID・IP アドレス」を含む返信メッセージを送信元ノードに返信し，同時にリストに送信元ノードの IP アドレスを追加する．また，送信元ノードは返信メッセージを受信するとリストへ目的ノードの IP アドレスを追加する．このような手順で制御を行うスクリプト実行例を図 3 で示す.

3.3 セキュアコネクション生成動作

IP アドレス取得後，セキュアコネクションを自動生成する制御スクリプト実行例を図 4 に示す．まずリストの公開鍵と IP アドレスをもとに，両ノードにおいて IPsec の設定ファイルが書き換えられる．そして送信元ノード A が両ノードで IPsec の起動と接続を行い IPsec 処理が進められ，送受信ノードにおいてエンドツーエンドの IPsec 暗号化経路を確立することで，セキュアコネクションが生成される.

3.4 ネットワーク構成変化時の動作

一度セキュアコネクションが生成された後，中継ノード B が離脱し，ノード D がネットワークに参加して，中継ノードが B から D に入れ代わった場合のセキュア

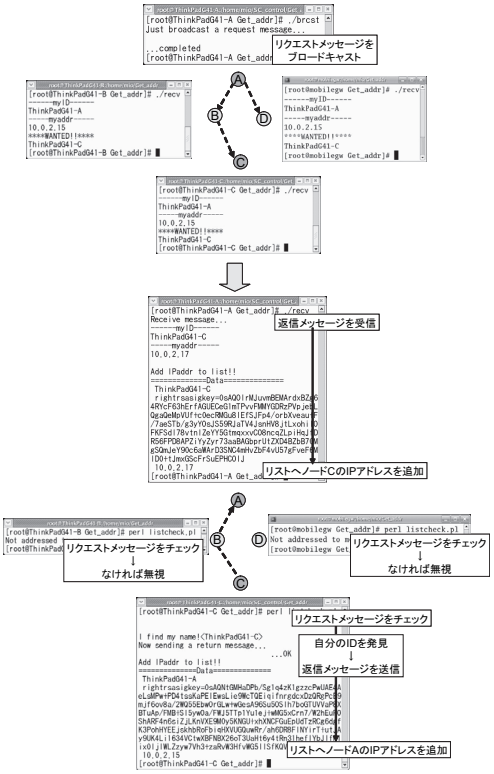

図 3: IP アドレスの取得とリストへの追加

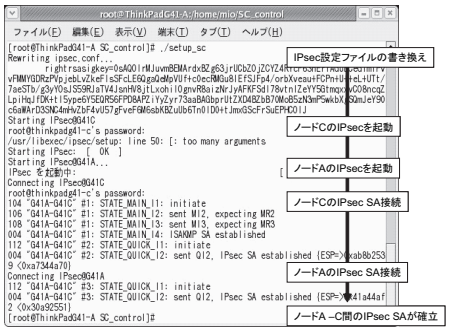

図 4: ノード A のセキュアコネクション生成動作

コネクションへの影響を tcpdump により観察すると，中継ノードが変化した場合も，A-C 間の通信を暗号化したパケットが流れ続けていた．これにより，OLSR によるセキュアコネクションの自動再構築が確認できた.

4 まとめと今後の課題

本研究ではマルチホップネットワークにおける安全な通信の実現のため，OLSR と IPsec を用いセキュアコネクションを構築する手法を提案し，一部実装を行った．今後は詳細な実装を進め，より現実的なモデルへと発展させたい.

参考文献

[1] olsrd：http://www.olsr.org/
[2] Linux openswan：http://www.openswan.com/
[3] 鎌田美緒，小口正人：“ マルチホップネットワークにおけるセキュアな通信路構築に関する制御手法 ”，電子情報通信学会技術研究報告，ITS2006-39，pp.25-30，2006 年 12 月