マルチホップ無線ネットワークにおける セキュアコネクションの生成・管理方式の一提案

鎌田 美緒 † 小口 正人 †
† お茶の水女子大学

1. はじめに

近年，無線通信技術の急速な発展により，無線ネットワークの様々な形態が考えられている．その中でも，ルータやアクセスポイントなどの固定インフラを必要とせず端末のみが集まるだけでネットワークを構築できる，MANET(Mobile Ad-Hoc Network)[1] に大きな注目が集まっている．MANET では端末同士が直接通信できない場合，途中ノードにルータ機能を持たせ通信を中継することで，より広い範囲での通信を実現している．このようなネットワークを，一般にマルチホップ無線ネットワークという．本研究では，マルチホップ無線ネットワークにおいてセキュアな通信を行う手法を提案する．

2. 研究背景

2.1 無線ネットワークにおけるセキュリティ

一般に無線通信は有線と比べ通信の傍受や改竄がされやすい環境であり，データの暗号化や認証が必須である．ネットワークにおける通信プロトコルは階層構造を持つことが一般的であるが，暗号化通信方式も各階層に様々な方式が存在し，目的に応じて異なるセキュリティ技術を適用することが可能である [2]．現在無線 LAN の暗号化方式としては，データリンク層で暗号化を行う WEP や WPA，さらに将来的には IEEE802.11i の使用が考えられている．しかし，WEP は事前に暗号鍵を共有することで全ノードに同レベルのセキュリティを提供するため，その中で特定コネクション間のみを暗号化することは難しい．また WPA や IEEE802.11i は認証機能を含むため，アクセスポイント等の固定インフラを含むネットワークにおいて有効となり，MANET での適用は困難である．従ってマルチホップ通信経路で暗号化通信を行うため，本稿では IPsec[3] の使用を検討した．

2.2 IPsec(IP Security)

IPsec はネットワーク層で暗号化・認証を行うことで安全な通信を提供する．共通鍵暗号方式で，暗号化アルゴリズムは DES(Data Encryption Standard) や 3DES が使用される．本稿ではセキュリティプロトコルとして暗号化を行う ESP(Encapsulating Security Payload) を選択し，暗号化アルゴリズムは 3DES を使用している．IPsec では SA(Security Association) の管理・生成や鍵の交換などを行うプロトコルとして，IKE(Internet Key Exchange) がサポートされている．暗号化に使う共通暗号鍵を IKE が作成する際には，公開鍵暗号技術を用いた Diffie-Hellman アルゴリズムが使用されており，安全に共通暗号鍵を作成・共有することができる．IPsec はマルチホップ通信経路を構成する各ホップごとに共通暗号鍵を作成でき，それぞれ独立したセキュアコネクションを生成できる．そのためマルチホップ無線ネットワークの通信を暗号化するのに適していると考え，本研究で用いることとした．

3. セキュアコネクションの生成・管理手法

3.1 マルチホップ無線ネットワークにおけるセキュアコネクション

マルチホップ無線ネットワークは，MANET に集まったノードに通信を中継する機能を持たせ，直接通信できないノード間のコネクションを実現するものである．しかし MANET には様々なノードが存在し，必ずしも安全な環境であるとは限らない．そのためマルチホップ通信経路間で通信を暗号化することが望まれるが，そのためには経路上の各ホップ毎に暗号鍵を作成し，独立したセキュアコネクションを生成する仕組みが必要となる．

一方 MANET はノードの参加や離脱などネットワーク構成が常に変化し，またマルチホップ通信経路においては中継ノードの離脱による新たな経路の生成も考慮しなければならない．そこで本研究では，暗号鍵の取り扱いやネットワーク構成の変化を考慮し，マルチホップ環境においてセキュアコネクションの生成・管理を行うミドルウェアの構築を行う．この実装に向け，まずは１ノードが経路を構成する全ノードの管理情報を持ち，リクエストによりセキュアコネクションの生成や管理を一括して行うような，集中管理型の実装方式を検討した．本稿ではこのような機能を持つノードを管理ノードと呼ぶことにする．

3.2 セキュアコネクションの生成

まず，中継ノードを含む特定ノード間にセキュアなコネクションを生成する手法を検討する．ただし，ルーティングプロトコルにより中継ノードを経由した送信ノードから受信ノードまでの経路は，事前に決まっていると仮定する．またこの場合に用いられる中継ノードは信頼性が保証されており，これを中継してセキュアコネクションを生成しても問題がないものとする．そのような環境において，送信ノードがセキュアコネクション生成のリクエストを出すと，まず管理ノードは経路を構成する各ホップにおいて，IKE 処理に必要な公開鍵の交換と，IPsec SA の確立を行う．このとき隣接するノードには直接制御コマンドを投げ，その他のノードには隣接ノードを介して制御を行うことで，送受信ノード間のマルチホップ経路が全てセキュアなコネクションとなる．

Proposal of Generation and Control systems of a Secure Connection for Multi-hop Wireless Networks

† Mio Kamada, Masato Oguchi
Ochanomizu University (†)

3.3 セキュアコネクションの管理

次にノードの離脱により，マルチホップ経路に変更が生じた場合の手法を検討する．まず，送受信ノードのどちらかが離脱する場合，セキュアコネクションはもはや不要となるため，離脱ノードは IPsec SA の解除をリクエストし，管理ノードはマルチホップに沿って全セキュアコネクションを切断する．

中継ノードが離脱する場合，次の 2 つの可能性が考えられる．1 番目は，セキュアコネクション上の管理ノード以外の中継ノードが離脱するケースである．この場合，離脱するノードは管理ノードへ IPsec SA 解除のリクエストを出し，管理ノードは離脱するノードが中継していたノード間のセキュアコネクションを切断する．このとき離脱するノード付近のネットワーク構成の状況により，直接通信を行うか代替ノードで中継させるなどして，切断していたノード間で新たなセキュアコネクションを生成し，送受信ノード間のセキュアコネクションを継続させる．2 番目は，セキュアコネクション上で管理ノードが離脱するケースである．この場合，離脱に際して上記と同様の処理が行われるが，その後管理ノードの機能を同じセキュアコネクション内の他ノードに渡すことにより，新たな管理ノードが引き続きセキュアコネクションの管理を行うことができる．

4. 提案モデルのミドルウェア実装

4.1 実験環境

本稿では提案したモデルに基づき，管理ノード付近の計 3 ノードにおける処理の実装を行った．実験環境としては，図 1 のように 3 台のマシンを IEEE802.11b 無線 LAN と Fast Ethernet で接続し，C2 でルーティングを行い通信を中継することでマルチホップ無線ネットワーク環境を模擬した．これは Linux の iptables コマンドによりマシン C2 カーネルにおいてパケットフォワード機能を動作させ，さらにマシン C1 と C3 において route コマンドでルーティングテーブルを書き換えることにより実現している．また暗号化通信方式として IPsec を使用し、IPsec の Linux における実装として FreeS/WAN[4] を用いた．

- C1: Linux2.4.20-8, Intel PentiumM 1.8GHz, 512MB
- C2: Linux2.6.9-1, Intel PentiumM 1.3GHz, 256MB
- C3: Linux2.4.20-8, Intel PentiumIII 1GHz, 512MB

図 1: 実験環境

上記の実験環境において，C2 をマルチホップ通信経路上の管理ノードとし，C1 と C3 がセキュアな通信を行いたいとする．C2 は各ノードからのリクエストを随時受け付け，リクエストを受けると自動的にセキュアコネクションの生成・管理を行う．

4.2 中継ノード離脱の動作例

実装したミドルウェアのうち，ノードの離脱とそれに伴う新たなセキュアコネクション生成の動作例を示す [図 2]．C2 を中継して C1-C3 間が既にセキュアコネクションである状況で，中継ノード C2 が離脱する場合を考える．また，このとき C1 と C3 は直接通信できる範囲内にいると仮定する．まず C2 は離脱する旨を中継を行っていた各ノードへ伝え，各ホップで張られている IPsec SA を一旦切断する．その後直接通信が可能である C1-C3 間で新たなセキュアコネクションの生成を行う．C1-C3 間で IKE 処理に用いる公開鍵をそれぞれ交換し，その公開鍵をもとに設定ファイルの書き換えなどを行い，IPsec SA が確立される．これにより，C1-C3 間は引き続きセキュアな通信を続けることができる．

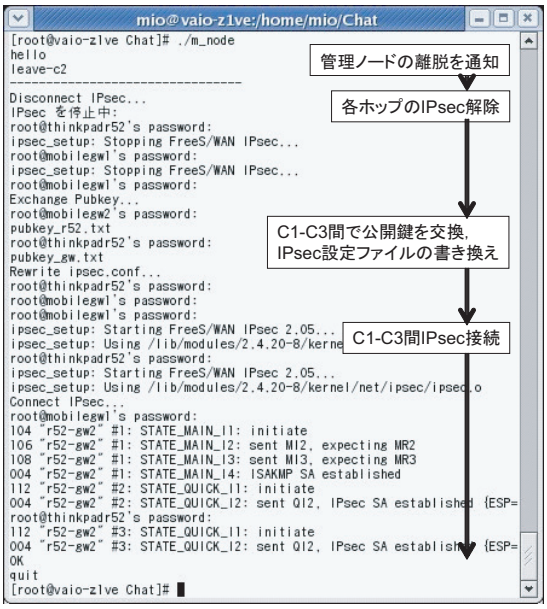

図 2: ノード離脱時の管理ノードにおける実行例

5. まとめと今後の課題

本稿では，マルチホップ無線ネットワークにおいてセキュアコネクションを生成・管理するミドルウェアの構築を目指し，その一提案として集中管理形式の実装手法を検討し，管理ノード周辺における部分的実装を行った．しかし本来マルチホップ無線ネットワークは自律分散型のネットワークであり，また集中管理形式のモデルでは，参加ノード数の増加により管理ノードの処理に限界が考えられる．そこで今後は，個々のノードが分散的にセキュアコネクションの生成・管理を行う，分散型モデルの適用について検討していきたい．

参考文献

[1] MANET:http://www.ietf.org/html.charters/manet-charter.html
[2] 難波誠一，小口正人：インターネット・無線 LAN・放送における暗号化技術，情報処理，vol.45，no.11，pp.1143-1145，2004 年 11 月
[3] 小早川知昭：IPsec 徹底入門，翔泳社
[4] Linux FreeS/WAN：http://www.freeswan.org/
[5] 鎌田美緒，小口正人：“ 有線及び無線リンク経由の通信における IPsec 適用手法の一検討 ”，FIT2005 第 4 回情報科学技術フォーラム，L-030，pp.71-72，2005 年 9 月