# 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管理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　〒 112–0012 東京都文京区大塚 2–1–1
E-mail: †mio@ogl.is.ocha.ac.jp, ††oguchi@computer.org

**あらまし**　近年広く研究が進んでいるマルチホップ無線ネットワークは，ノードが通信を中継し自律分散的なネットワークを構築できることで注目を集めている．無線通信は有線と比べ通信が傍受されやすく，暗号化によりデータを守ることが必須である．しかし現在無線 LAN で標準的に用いられる WEP 等の暗号化通信方式は，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，その中でマルチホップ通信を行う場合，特定ノード間の通信のみを守ることが望ましい．またノードの参加や離脱等ネットワーク構成が常に変化するマルチホップ環境では，WPA や IEEE802.11i 等の既存の高度なセキュリティ手法の適用が難しい．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，マルチホップ無線ネットワーク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実装を目指し，その一提案としてあるノードが全ノードのコネクションを管理する集中管理型方式の実装を行った．

**キーワード**　セキュリティ，アドホックネットワーク，マルチホップ，モバイルコンピューティング，IPsec

# Proposal and Implementation of a Control Model of a Secure Connection for Multi-hop Wireless Networks

Mio KAMADA† and Masato OGUCHI†

† Ochanomizu University　Otsuka 2–1–1, Bunkyo-ku, Tokyo, 112–0012 Japan
E-mail: †mio@ogl.is.ocha.ac.jp, ††oguchi@computer.org

**Abstract**　A multi-hop network is an autonomous distributed network in which a node relayed other node's packets on MANET. In the case of wireless networks, it is required to secure the data by encryption because communication on wireless networks are easy to be intercepted in contrast with wired networks. We commonly use encryption methods such as WEP in wireless LAN. However, these methods offer same security level for all nodes by sharing encryption key beforehand. It is desirable to secure only particular connection between nodes in the case of multi-hop communication. Moreover, it is difficult to apply advanced security methods like WPA and IEEE802.11i to multi-hop wireless networks, because the structure of multi-hop wireless networks where each node often join in or leave is constantly changed. Thus in this paper, we discuss the handling of the encryption key and the change of network's structure, and propose a control model of a secure connection for muti-hop wireless networks. In addition, we implement centralized management system in which a certain node manages all nodes and its secure connection.

**Key words**　Security，Ad-Hoc Network，Multi-hop，Mobile Computing，IPsec

## 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るようになった．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即座に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 では端末同士が通信を行うことで，自律分散的なネットワークを構成している．しかし無線通信は電波範囲が限られているため，ノードがある程度広い範囲に分散している場合や，ノード間に遮断物が存在する場合，あるノードから目的のノードへ直接無線通信できるとは限らない．そこで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 [図 1].

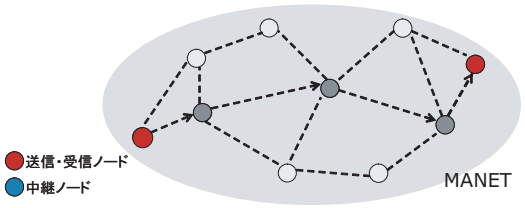


図 1　マルチホップ無線ネットワーク

マルチホップ無線ネットワークは，次世代の無線通信ネットワークの構築技術として期待されるが，そのネットワーク構築には技術的課題も多く残されている．例えば，MANET を構成するノードは一般にバッテリで稼動しているものと考えられ，バッテリ容量が有限であるため効率的な電力使用が必要となる．一般に MANET でマルチホップ通信を行う場合のルーティングプロトコルは，送信ノードから受信ノードまでのホップ数が最小になるような経路を選択するが，論文 [2] や [3] では，それに加えてノードの稼働時間を長引かせられるよう，バッテリ電力を効率的に使用するような経路選択手法を提案している．具体的には，マルチホップ通信経路上の各ノードで消費される電力に関する情報をあらかじめ交換しておき，この情報に基づいて各ノードの消費電力の合計が最小となる経路を選択する [2]．これにより，バッテリの無駄な消耗を減らし各ノードの稼働時間が長くなり，ネットワーク全体における効率的な通信を可能にしている．その他には，ノードでクラスタリング技術を用いることで処理負荷を分散させるような手法として [4] や [5] がある．ノードが自由に移動することによるネットワーク構成や経路の頻繁な変化や，無線通信のノイズ・干渉による通信障害の起こりやすさなど，マルチホップ無線ネットワークに関連した研究の多くは MANET 特有の性質について論じられている．

無線通信を行う場合，そのセキュリティを考慮することは不可欠であるが，現在マルチホップ無線ネットワークにおける研究の大部分は，そのネットワーク構築に関わるテーマを扱っている．そこで，これらの既存研究を踏まえた上でまだあまり議論されていないセキュリティに着目し，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．

本提案では，マルチホップ無線ネットワークで生成される各コネクション間で通信の暗号化を行うことで，セキュリティを提供する．以降ではこのように暗号化されたコネクションをセキュアコネクションと呼ぶことにする．既存の暗号化・認証技術などで MANET 内に属するノードに同レベルのセキュリティを提供することは可能だが，その中でマルチホップ通信を行う場合，特定ノード間のみを暗号化しなければならず，また，既存手法をそのまま適用することは難しい．また，MANET では端末の移動によりノードの参加や離脱が頻繁に起こり，加えてマルチホップ無線ネットワークにおいては中継ノードの離脱により新たな経路の生成も考慮する必要がある．そこで本稿では，マルチホップ無線ネットワークにおいてネットワーク構成の変化を考慮し，自動的にセキュアコネクションの生成・管理を行うモデルを提案した．またその実現に向け，提案モデルの実装手法と，部分的に実装を行ったミドルウェアの動作を示す．

本稿は以下のように構成される．第 2 章では研究背景として無線ネットワークにおけるセキュリティ技術ついて触れ，本稿で暗号化通信方式として用いた IPsec を紹介する．第 3 章ではセキュアコネクションの生成・管理手法の提案モデルを示し，第 4 章でその実現に向けた実装手法として，集中管理型実装方式を検討している．そして第 5 章で具体的なミドルウェアの一部実装として，セキュアコネクション生成までの手順や必要となる処理，またノード離脱による新たな経路生成の手法など詳細な動作例を示す．最後に第 6 章でまとめる．

## 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設定することが可能である [6].

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．以下でこれらの暗号化通信方式について概説する．

### 2.2 無線 LAN における暗号化通信方式

#### 2.2.1 WEP(Wired Equivalent Privacy)

現在無線 LAN では，データリンク層で暗号化を行う WEP の使用が規定されている．WEP では，端末とアクセスポイント間で事前に共有する共通秘密鍵と，初期ベクタ (IV) を用い，実際に暗号化に用いるキーストリームを作り出す．秘密鍵は 40 または 104 ビット，IV は 24 ビットであり，合計で 64 または 128 ビットの鍵長となる．また，WEP で用いられている暗号化アルゴリズムは RC4 で，1 ビット単位で簡単な暗号化を行うブロック暗号アルゴリズムである．しかし WEP では RC4 適用手法の安全性に対する不安や，その鍵長の短さによりブルートフォース（総当たり）攻撃で解読される可能性があるなど，いくつかの脆弱性が指摘されている．

#### 2.2.2 WPA (Wi-Fi Protected Access)

WPA は，WEP で用いられていた RC4 の暗号化ハードウェアを利用し，ファームウェアの変更のみで安全性を高める手法として制定された．暗号化プロトコル TKIP(Temporal Key Integrity Protocol) と安全性の高いユーザ認証を行う規格 IEEE802.1X を併用している．TKIP は鍵の周期的な自動更新などを行い，WEP の弱点を補強している．また，この WPA は次に紹介する IEEE802.11i のサブセットの位置づけとなっている．

#### 2.2.3 IEEE802.11i

IEEE802.11i は，TKIP や IEEE802.1X に加え，RC4 に変わる強度な暗号化アルゴリズムとして AES(Advanced Encryption Standard) を採用している．しかし新しい暗号化アルゴリズムの実現にはハードウェアの変更が必要となるため，新たなハードウェアの普及が進むまでは，WPA で互換性を持たせている．また IEEE802.11i では，IEEE802.1X で認証を行った後暗号通信

を行うための秘密鍵の作成と交換を行っており，この認証に必要となる認証サーバ等は，アクセスポイントを介して接続された固定インフラ上に置かれることが一般的である．

現在無線 LAN で標準的に用いられる WEP は，その場にいる全ノードが事前に同じ共通秘密鍵を共有する必要があり，全てのノードに同レベルのセキュリティを提供することは可能である．しかしその中でマルチホップ通信経路のような特定コネクション間の通信のみを暗号化で守りたい場合，WEP の適用は難しい．また WEP 自体の脆弱性も指摘されている．新たに無線 LAN のセキュリティを強化するものとして，WPA や IEEE802.11i などの規格も考えられているが，これらは認証の機能も含んでおり，アクセスポイントなどの固定インフラを含むネットワークにおいて有効となる手法である．従って MANET 内でマルチホップ通信を行うような一時的なネットワークでは適用が難しい．以上の理由により，MANET のように固定インフラを含まず自律的で一時的なネットワークで通信の暗号化を行う場合，異なった方式を考える必要がある．そこで本稿ではネットワーク層で暗号化・復号を行う IPsec [7] の使用を検討した．

### 2.3 IPsec(IP Security)

#### 2.3.1 IPsec 概要

IPsec はネットワーク層で暗号化・認証を行うことでセキュリティを保証する規格で，IP パケットを暗号化するため，上位のアプリケーションは透過的な通信を行うことができる．IP パケットそのものを暗号化することで通信の傍受を防ぎ，また IP パケットに改竄を検知する数値を組み込むことで，パケットが通信経路上で改竄されなかったことを保証する．暗号化には共通鍵暗号方式を用いており，暗号化アルゴリズムとしては DES(Data Encryption Standard) や 3DES が使用される．またセキュリティプロトコルとして，暗号化と認証機能を提供する ESP(Encapsulating Security Payload)，暗号化機能はないがより強力な認証機能を提供する AH(Authentication Header) のどちらかを選択することができる．本稿では暗号化を行う ESP を選択し，暗号化アルゴリズムは 3DES を使用している．

#### 2.3.2 IKE(Internet Key Exchange)

IPsec で生成されるコネクション SA(Security Association) の管理・生成や，ESP や AH で用いる鍵の交換などを行うプロトコルとして，IKE がサポートされている．IKE は IPsec 化すべきパケットが発生すると，セキュリティポリシに従って SA を自動的に生成する．この際，暗号化や認証に使用する鍵なども自動的に生成され，さらに確立した SA では一定期間ごとに使用された鍵を作り直す動作をする．IPsec で使用される鍵は共通暗号鍵であり，送信側と受信側で同じ鍵を持つ必要があるが，この共通暗号鍵を 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，アルゴリズムにしたがって発生した乱数を交換することで，その交換を盗聴されていたとしても盗聴者には知ることのできない共通鍵暗号鍵を作成・共有することができる．

ここで，IKE が IPsec SA 確立までに行うプロセスを説明する [図 2]．IKE は，生成する SA のパラメータをネゴシエートして決定する Proposal 交換，生成する SA の秘密対称鍵を公開鍵暗号技術により安全に作成する Diffie-Hellman 交換，IKE 通信している相手が本物であることを確認する認証（本人性確認），以上 3 つの基本的な機能を通して SA の自動生成を行う．また IKE には Phase1 と Phase2 という 2 つの段階があり，Phase1 では IKE の制御用チャネルである ISAKMP(Internet Security Association and Key Management Protocol) SA の確立を行い，その後 Phase2 で暗号化経路 IPsec SA の確立を行う．

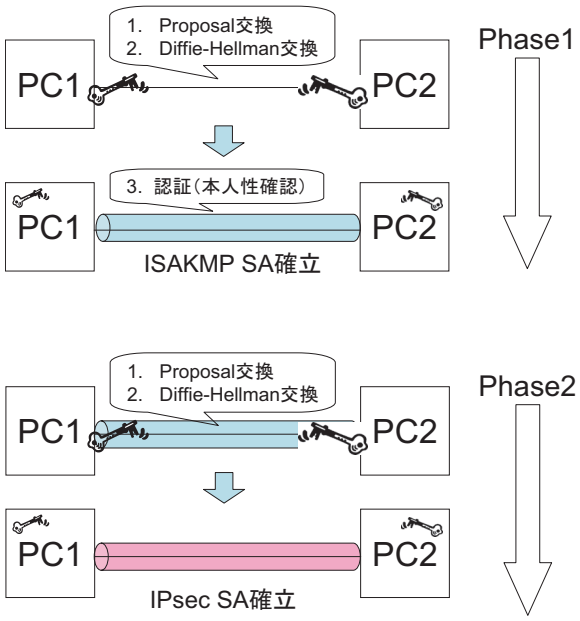


図 2　IPsec SA 確立までの IKE のプロセス

Phase1 ではまず Proposal 交換を行い，続いて ISAKMP SA 用の共通暗号鍵を Diffie-Hellman 交換により作成する．そして，その鍵を用いた暗号化経路上で，IKE 相手の認証（本人性確認）が行われ，制御用チャネル ISAKMP SA が確立される．次に Phase2 では，IPsec SA を生成するための Proposal 交換を行い，実際に暗号化に用いる IPsec SA 用の共通暗号鍵を Diffie-Hellman 交換により作成し，IPsec SA が確立される．この Phase2 のやりとりは，Phase1 で既に作られた ISAKMP SA を通して送られるので，暗号化された安全な経路上で通信を行うことができる．

このように，IPsec はノードとノードをつなぐ各ホップごとに共通暗号鍵を作成することができ，それぞれ独立したセキュアコネクションを生成することができる．そのためマルチホップ無線ネットワークで特定コネクション間の通信のみ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 MANET におけるマルチホップ通信

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．そのためには MANET 内でマルチホップ通信の経路を決めるルーティングプロトコルが必要である．MANET はノードの移動や参加・離脱などネッ

トワーク構成が動的に変化する環境であり，また低速で不安定な無線通信を用いるため，その性質を考慮したルーティングプロトコルが多く提案されている．MANET におけるルーティングプロトコルは，パケットをルーティングする経路の取得方法により，プロアクティブ型とリアクティブ型の大きく 2 つに分けることができる．

プロアクティブ型は，ネットワーク内のノード同士が定期的に経路情報を交換し，他ノードへの経路を常に把握する方法である．各ノードはパケットをルーティングする次ノードを，目的地のノード各々についてルーティングテーブルで保持するため，通信のリクエストが発生した場合即座に経路生成ができる．しかしネットワーク構成の変化に応じて頻繁に経路情報の交換をする必要があり，通信要求の発生パターンによっては無駄な処理が多く起こり得る．プロアクティブ型のルーティングプロトコルには DSDV(Destination Sequence Distance Vector) [8] や，OLSR(Optimized Link State Routing) などがある．DSDV では，各ノードのルーティングテーブルに，受信ノードの宛先，次ホップノードの情報などの他にシーケンス番号を保持する．経路情報交換の際にこのシーケンス番号を比較し，テーブル内のシーケンス番号と同じかそれ以上であれば，短いホップ数の情報をルーティングテーブルに加え，これに基づきマルチホップ通信経路を構築する．

一方リアクティブ型は，通信のリクエストが発生するごとに，送信ノードから受信ノードまでの経路を探索する方法である．経路探索によって経路が構築されてからパケットがルーティングされるため，通信のリクエストが発生してからの処理に遅延が生じるという問題点があるが，AODV(Ad-hoc On-demand Distance Vector) [9] などリアクティブ型のルーティングプロトコルは多く提案されている．リアクティブ型の経路探索の方法は，まず送信ノードが要求パケット RREQ(Route Request) を隣接ノードを介し，ネットワーク内の全ノードに配送する．この RREQ を受信ノードが受け取ると，受信ノードは応答パケット RREP(Route Reply) を返信する．AODV では，ネットワーク内の全てのリンクが双方向接続であることを前提としており，この経路探索によって各ノードのルーティングテーブルに短期間だけ有効な経路を設定することで，マルチホップ通信経路の構築を実現している．

### 3.2 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

MANET 内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で複数ノードを中継する通信を行う場合，送信ノードと受信ノード間の通信を暗号化した，セキュアコネクションの生成が望まれる．しかし，前述のように WEP 等の暗号通信方式はアクセスポイント等の固定インフラが必要となり，また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方式のため，MANET 内において特定ノード間の通信のみを守ることはできない．従って，経路を構成する各ホップごとに共通暗号鍵を作成し，それぞれ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そのネットワーク構成が常に変化し，またマルチホップ通信環境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，マルチホップ無線ネットワーク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を提案する．

### 3.3 提案モデル

#### 3.3.1 セキュアコネクションの生成

まずマルチホップ無線ネットワークにおいて，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．MANET に新しくノードが参加し，あるノードとの通信をリクエストした場合，まずルーティングプロトコルにより送信ノードから受信ノードまでの中継ノードを含む経路が構築される．本研究の提案モデルにおいて，この経路はセキュアコネクションを生成する時点で決まっていると仮定する．経路決定には，前節で説明した MANET におけるルーティングプロトコルを用いることができる．またこの場合に用いられる中継ノードは信頼できることが保証されており，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，セキュアな通信を希望する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，まず送信ノードと中継ノードの間に，IPsec の通信フェーズに基づき共通暗号鍵が作成され，セキュアコネクションが生成される．隣接ノードを介してホップごとに同様の処理が受信ノードまで行われ，送信ノードと受信ノードとの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．この場合，IPsec による共通暗号鍵はホップごとに作成されており，各ホップはそれぞれ独立したセキュアコネクションから成っている．[図 3]

#### 3.3.2 セキュアコネクションの管理

MANET は各ノードがネットワークへの参加や離脱を頻繁に繰り返すものであり，またネットワーク内でも各ノードが移動する可能性があるため，構築されたマルチホップ経路に変更の必要が生じる場合がある．まず，セキュアな通信の送受信を行っている両端どちらかのノードが離脱する場合，セキュアなマルチホップ通信経路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，マルチホップに沿って全てのセキュアコネクションは切断される [図 4].

一方，中継ノードが離脱する場合，以下の 3 つの可能性が考えられる．1 つは，セキュアコネクションの維持はもはや不可能になり，これを切断するケースである．この場合は，前述の端ノード離脱のケースと同様に IPsec SA の解除がリクエストされ，マルチホップに沿って全てのセキュアコネクションは切断される [図 5].

2 番目は，中継ノードが中継を行っていた 2 つのノードが直接通信を行えるケースである．MANET ではノードの位置関係が頻繁に変更されるため，このようなケースは十分にあり得る．この場合，中継ノードが中継を行っていた 2 つのノード間の IPsec SA が解除され，同時に 2 つのノード間で新たなセキュアコネクションが生成される．送信ノードと受信ノードは，中継ノードの離脱を意識することなく，引き続き安全な通信を行う

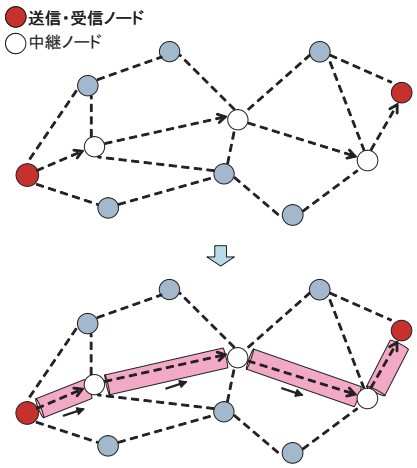


図 3　提案モデル：ノードの参加とセキュアコネクション生成

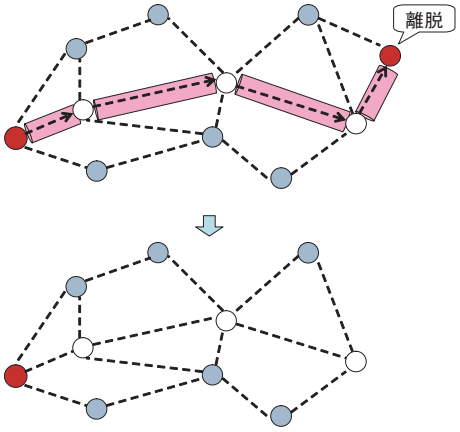


図 4　提案モデル：端ノードの離脱

ことができる [図 6].

3 番目は，離脱する中継ノードの近くに，通信の中継を代替できるノードが存在するケースである．ここで，代替ノードは既に信頼できることが保証されているものとする．この場合，離脱する中継ノードが中継を行っていた 2 つのノード間の IPsec SA が解除され，同時に 2 つのノード間で代替ノードを中継ノードとした新たなセキュアコネクションが生成される．直接通信できるケースと同様に，このケースでも送信ノードと受信ノードは引き続き安全な通信を行うことができる [図 7].

## 4.　提案モデルの実装手法

### 4.1　集中管理型実装方式

第 3 章で提案したモデルに基づくセキュアコネクションの生成・管理ミドルウェアの実装に向けて，まずは 1 ノードが経路を構成する全ノードのコネクションに関する情報を管理する形の実装方式を検討した．これは，マルチホップ通信経路を構成するノードのうち，ある 1 ノードが全ノードに関する管理情報を持ち，各ノードからの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，集中管理型の仕組みである．このとき，通信経路上において全ノードの管理情報を持ち，セキュアコネクション生成などの指令を発行するノードを，管理ノードと呼ぶことにする．ノードの参加や離脱など，ネットワーク構成の変化による各処理について次に詳しく述べる．

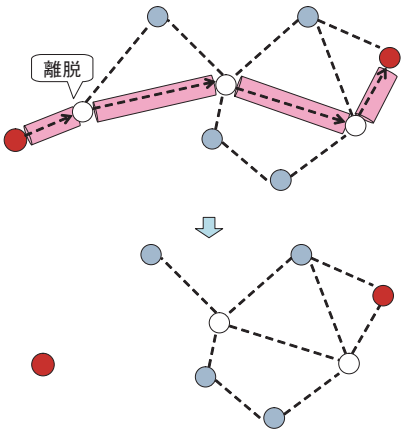


図 5　提案モデル：中継ノード離脱（セキュアコネクションの維持が不可能な場合）

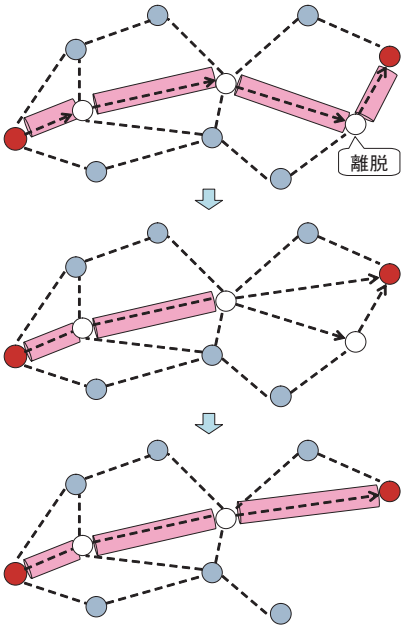


図 6　提案モデル：中継ノード離脱（隣接ノード間が直接通信できる場合）

### 4.2　ノードの参加によるセキュアコネクションの生成

まずは提案モデルの説明で述べたように，ルーティングプロトコルによって送信ノードから受信ノードへマルチホップ通信経路が構築される．次に送信ノードは経路上にいる管理ノードに，受信ノードとのセキュアなコネクションをリクエストする．管理ノードはリクエストを受けると，経路を構成する各ホップにおいて，IPsec SA 確立にあたって必要な処理と SA の確立を行い，セキュアコネクションを生成する．このとき管理ノードは，隣接するノードには直接制御コマンドを投げることで制御を行い，その他のノードには隣接ノードを介して制御を行う [図 8].

### 4.3　ノードの離脱

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

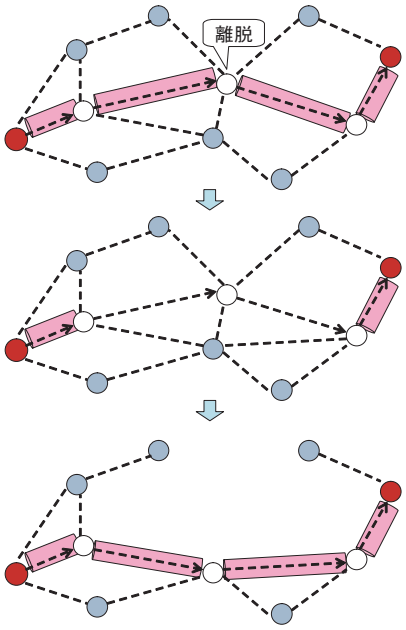


図 7　提案モデル：中継ノード離脱（付近に代替ノードが存在する場合）

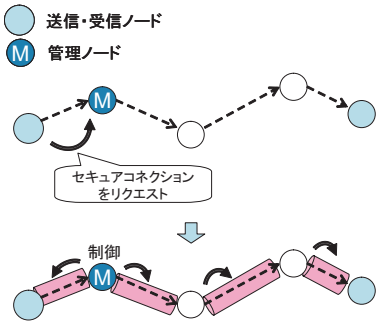


図 8　セキュアコネクションの生成

ノードへ IPsec SA 解除のリクエストをし，管理ノードはセキュアコネクションを構成する各ノードに制御コマンドを投げ，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が中継を行っていた場合には，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，送信ノード・受信ノード間のセキュアコネクションを継続させる [図 9].

2 番目は，セキュアコネクション上で管理を行っていたノードが離脱するケースである．この場合，離脱のリクエストにより上記と同様の処理が行われるが，その後全ノードに関する管理情報やセキュアコネクション生成・管理の権限を，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 [図 10].

## 5.　提案手法のミドルウェア実装

### 5.1　実 験 環 境

本稿では上で提案したミドルウェアのうち，管理ノードとそれに隣接する 2 つのノードの，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 11 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

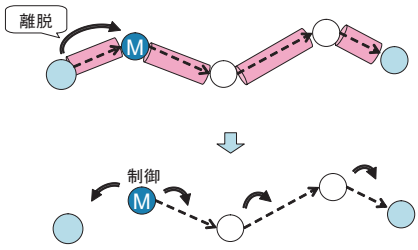


図 9　管理ノード以外のノードの離脱

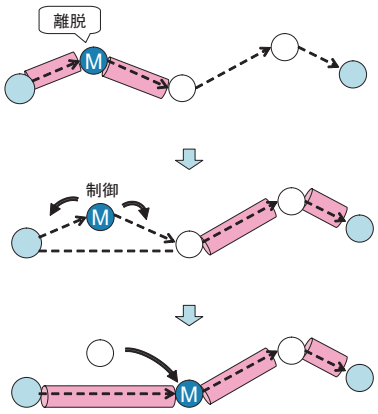


図 10　管理ノードの離脱

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 コマンドにより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 [10] を用いた．IPsec の設定では，暗号化アルゴリズムは 3DES，セキュリティプロトコルは暗号化を行う ESP，パケットのカプセル化モードはネットワーク間の通信を行うトンネルモードを選択している．

- 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

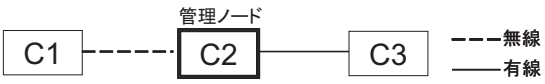


図 11　実 験 環 境

上記の実験環境において，マシン C2 をマルチホップ通信経路上の管理ノードとし，C1 を送信ノード，C3 を受信ノードとする．C2 は C1-C3 の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．次節で実装したミドルウェアの動作例を示す．

### 5.2　ノードの参加によるセキュアコネクション生成

まずノードの参加によるセキュアコネクション生成の動作例を示す [図 12]．C2 を中継した C1 から C3 への経路は事前に構築されている．まず管理ノード C2 は C1 からセキュアコネクション生成のリクエストを受け，C1-C2 間と C2-C3 間において IKE 処理で用いる公開鍵の交換を行う．その後各ノードにおいて IPsec 設定ファイルを書き換え，IPsec SA を確立することに

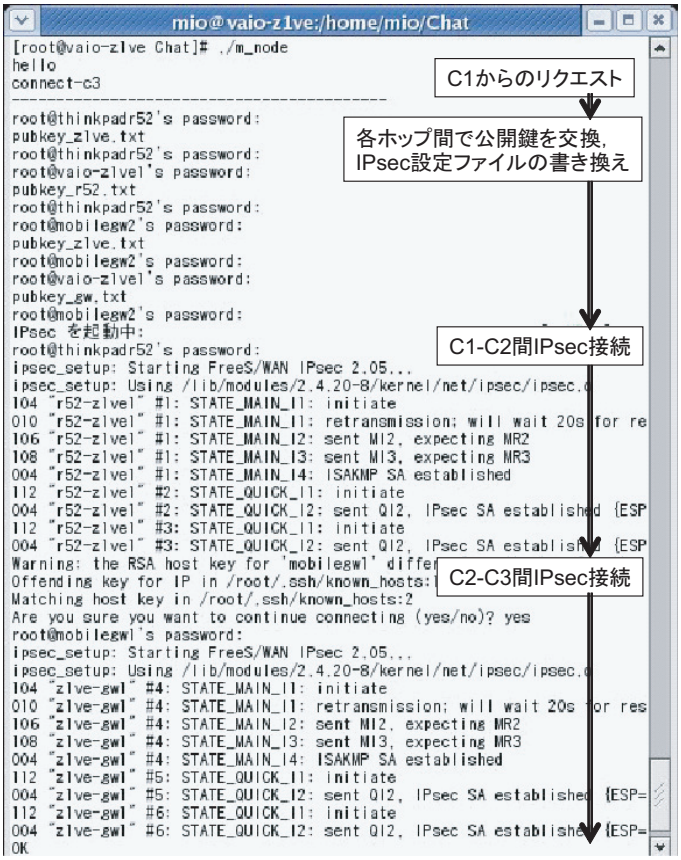


図 12　ノード参加時の管理ノードにおける実行例

より，C1-C3 間のセキュアコネクションが生成された．

### 5.3　ノードの離脱における動作例

次に，ノードの離脱によるコネクション切断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 13]．C2 を中継して C1 と C3 が既にセキュアコネクションでつながっている状況で，中継ノードである 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．まず管理ノードは離脱のリクエストを受け，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．前述の生成動作例と同様に，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．

## 6.　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実装を目指し，そのモデルを提案した．またその実現に向け，マルチホップ通信経路上のある 1 ノードに全ノードの管理情報を持たせ，集中的な管理を行う形式の実装手法を検討した．そして管理ノード周辺 3 ノードにおける，部分的実装の動作例を示した．

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，また今回実装し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を行うノードの処理に

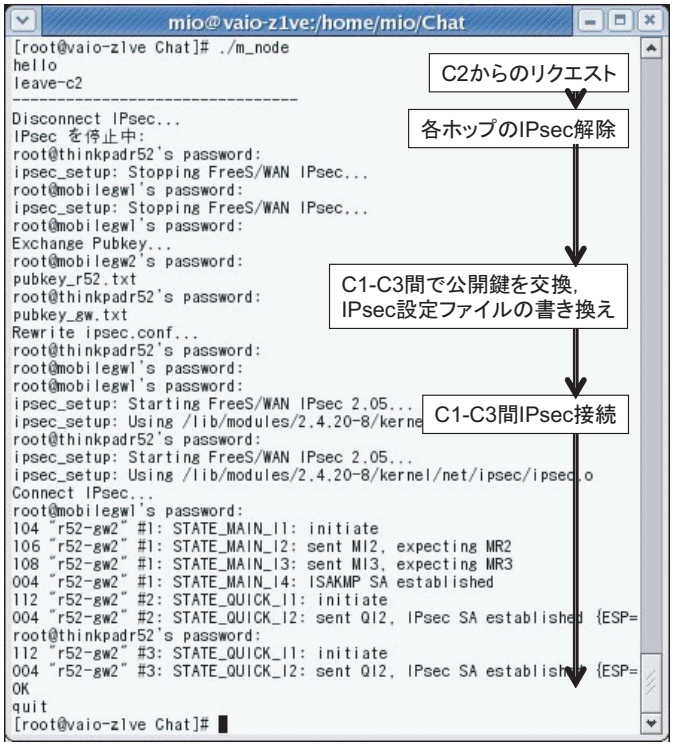


図 13　ノード離脱時の管理ノードにおける実行例

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．

## 文　　献


[1] MANET：http://www.ietf.org/html.charters/manet-charter.html

[2] S.Singh, M.Woo and C.Raghavendra：“ Power-Aware Routing in Mobile Ad-hoc Networks, ”in Proc. of MobiCom, Oct.1998

[3] J.H.Chang and L.Tassiulas：“ Energy conserving routing in wireless ad-hoc networks, ”in Proc. of HICSS 2000, 2000

[4] B.Chen, K.Jamieson, H.Balakrishnan and R.Morris：“ SPAN：An energy-efficient coordination algorithm for topology maintenance in ad-hoc wireless networks, ”in Proc. of INFOCOM 2000, Mar.2000

[5] W.Rabiner Heinzalman, A.Chandrakasan and H.Balakrishnan：“ Energy-efficient communication protocol for wireless microsensor networks, ”in Proc. of MobiCom 2001, 2001

[6] 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

[7] 小早川知昭：IPsec 徹底入門，翔泳社

[8] C.E.Perkins and P.Bhagwat：“ Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, ”in Proc. of SIGCOMM’94, 1994

[9] C.E.Perkins, E.M.Belding-Royer adn S.R. Das：“ Ad-hoc On-Demand Distance Vector Routing, ”Internet-Draft, draft-ietf-manet-dsr-08.txt, Feb.2003

[10] Linux FreeS/WAN：http://www.freeswan.org/

[11] 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

[12] 岡林希，小口正人：“ 無線アドホックネットワークにおける安全な通信方式の検討 ”，電子情報通信学会総合大会，B-15-24，pp.817，2004 年 3 月