DEWS2007 C2-7

マルチホップルーティングプロトコルを用いたセキュアコネクション構築管理手法

鎌田　美緒†　　小口　正人†

† お茶の水女子大学
〒 112-8610 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　近年大きく注目されている MANET は，端末が集まるだけで構築可能な自律分散的なネットワークである．MANET では，マルチホップルーティングプロトコルによりノードが通信を中継する通信経路が構築され，無線の電波範囲にとらわれない広範囲の通信を可能にしている．一方無線通信は有線と比べ通信の傍受や改竄がされやすく，特に MANET は不特定多数のノードが存在するため特にセキュリティ上の危険性が高い環境であると言え，暗号化や認証によりセキュリティを考慮することは不可欠である．そこで本研究では MANET における安全な通信を実現するため，暗号化経路であるセキュアコネクションを構築し管理する手法を提案した．マルチホップルーティングプロトコルとして OLSR を用いることで通信経路を確立し，暗号化手法 IPsec を適用したセキュアコネクションを自動的に制御する手法を示している．そして提案手法により，IP アドレスの取得やセキュアネクションの構築および再構築の実装を，セキュリティ上の問題点を考慮したうえでを行った．

キーワード　ユビキタスコンピューティング，セキュリティ，モバイルアドホックネットワーク

A Control Method of Constructing Secure Connections on a Multi Hop Network

Mio KAMADA† and Masato OGUCHI†

† Ochanomizu University
2–1–1 Ohtsuka, Bunkyo-ku, Tokyo 112-8610, Japan
E-mail: †mio@ogl.is.ocha.ac.jp, ††oguchi@computer.org

Abstract　A Mobile Ad-hoc Network(MANET) is an autonomous distributed network which is constructed only with gathered nodes. In MANET, wide area communication on wireless networks is realized because a node can relay other node's packets by adopting a multi-hop routing protocol. In the case of wireless networks, especially in MANET, it is required to secure the data by encryption because communication on wireless networks are easy to be eavesdropped and manipulated in contrast with that of wired networks. Thus we make a proposal to construct and control secure connections and aim for secure communication on MANET. In this paper, we have established communication routes by adopting OLSR as a multi-hop routing protocol and introduced methods to control secure connections by applying IPsec as a encryption scheme. In addition, besed on the proposed method, we have implemented the acquisition of an IP address and construction / rebuilding of secure connections in consideration of problems in security.

Key words　Ubiquitous Computing, Security, Mobile Ad-hoc Network (MANET)

1. はじめに

近年，無線通信技術の進歩に伴い，様々な形態の無線ネットワークが考えられるようになった．特に，既設のインターネットなどインフラネットワークとの接点を持たず，無線 LAN 機能を持つ端末のみでネットワークを構築することで，より自由な形でネットワークを構築できる MANET (Mobile Ad-hoc Network) [1] が，大いに注目されている．MANET では，ノードがある程度広い範囲に分散している場合など目的のノードへ直接通信できない時に，途中ノードが通信を中継していくこ

とでより広範囲の通信を可能にしている．このように構築されるネットワークを，一般にマルチホップネットワークと呼び，これを図 1 に示す．マルチホップネットワークでは，各端末が

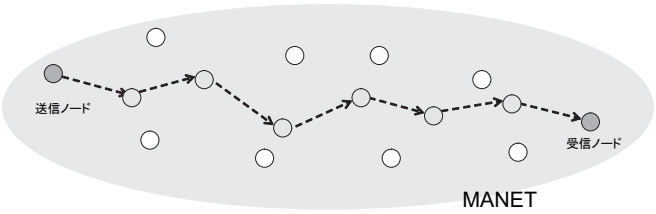

図 1　マルチホップネットワーク

通信経路の制御等を行うルーティングプロトコルに従ってルーティングを行い，ネットワークを構築している．このためノードの参加や離脱によるネットワーク構成の変化を気にすることなく，無線の電波範囲にとらわれない通信が行えるため，ITS (Intelligent Transport Systems) における車車間通信やユビキタスネットワークの実現技術として大いに期待されている．

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，セキュリティを考慮することは必要不可欠である．特に MANET のような環境は不特定多数のノードが存在し，知らない相手が通信経路に加わるため，よりセキュリティ上の危険性が高くなる可能性がある．既存の無線 LAN 暗号化や認証技術を用いることにより 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であるが，マルチホップ通信を行う場合，データ送受信を行うノード間の通信のみを暗号化することが望ましいため，既存技術の適用は難しい．また MANET の特徴であるネットワーク構成の動的変化も考慮しなければならず，固定インフラの存在しないネットワークにおいても有効となり，かつネットワーク構成の変化にも柔軟に対応するセキュリティ手法を検討する必要がある．

そこで本研究ではこれらの問題点を考慮し，マルチホップネットワークにおける安全な通信の実現を目指すため，セキュアコネクションを構築して管理するモデルを提案した．本提案では，既存の MANET ルーティングプロトコルである OLSR を用いマルチホップ環境を構築し，その上でデータのやり取りを行うノード間の通信を IPsec により暗号化することで，セキュアな通信経路を確保している．また暗号化処理に用いる公開鍵の情報等をリストとして管理することで，セキュア通信路生成時の信頼性を保証している．以降ではこのように確立された，暗号化されているセキュアな通信経路をセキュアコネクションと呼ぶ．

MANET におけるセキュリティ技術は現在研究が急速に広まりつつあり，暗号化や認証手法によりセキュアなルーティングを行う関連研究も多く提案されている [2] [3]．その提案の多くは，暗号化パラメータ等を組み込んだ新たなルーティングプロトコルの開発を目指し，シミュレーション評価により有効性を主張しているものである．一方本研究では，既存技術である OLSR と IPsec を MANET において有効に活用するモデルの提案及び実装を重点としており，これらの関連研究とは方向性が異なるものである．

本稿は以下のように構成される．まず第 2 章では研究背景として無線 LAN におけるセキュリティ技術について触れ，本稿で暗号化手法として用いた IPsec を紹介する．第 3 章ではマルチホップネットワークを実現するルーティングプロトコルを紹介し，本稿で用いた OLSR の詳細を述べ，第 4 章では提案モデルの詳細を説明する．そして第 5 章で具体的な実装として，OLSR によるマルチホップネットワークにおいて目的ノードの IP アドレスをリスト情報と対応付け，セキュアコネクション生成を行う実装例を示し，ネットワーク構成変化時の状況を確認する．最後に第 6 章でまとめる．

2. 背　　景

2.1　無線 LAN におけるセキュリティ技術

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，要求される目的に応じ異なったセキュリティ技術を設定することが可能である [4]．現在無線 LAN では，データリンク層で暗号化を行う WEP (Wired Equivalent Privacy) の使用が標準として規定されている．WEP は，端末とアクセスポイント間で事前に秘密鍵を共有するが，その鍵長の短さや暗号化アルゴリズム RC4 適用手法の安全性に対する不安等，脆弱性が指摘されている．その後，WEP の弱点を補強する暗号化プロトコル TKIP (Temporal Key Integrity Protocol) と，安全性の高いユーザ認証を行う規格 IEEE802.1X を併用した WPA (Wi-Fi Protected Access) が制定された．この WPA は，IEEE802.11i が普及するまでのサブセットの位置づけとなっている．IEEE802.11i は，TKIP や IEEE802.1X に加え，新たな暗号化アルゴリズムとして強固な AES (Advanced Encryption Standard) を採用しており，認証後，暗号通信に用いる秘密鍵の作成と交換を行っている．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た固定インフラ上に置かれることが一般的である．

2.2　マルチホップ環境におけるセキュリティ技術の問題点

これらの既存セキュリティ技術を，新たな無線ネットワークの形態であるマルチホップネットワークに適用する場合，以下に挙げるような問題点が考えられる．まず，現在無線 LAN で標準的に用いられている WEP は，基本的に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．しかしながら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には，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．一方，新たにセキュリティを強化した技術として WPA や IEEE802.11i が挙げられるが，これらの規格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．しかし 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における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．本稿では実装への適応のし易さを踏まえ，ネットワーク層で暗号化と復号を行うIPsec [5] 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 では，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される．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，その交換が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．プロセスは大きく二つの段階に分けられ，Phase 1 で 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 Phase 2 で暗号化経路 IPsec SA の確立を行う．Phase 1 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 Phase 2 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 Phase 2 のやりとりは，Phase 1 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 は各 SA 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．

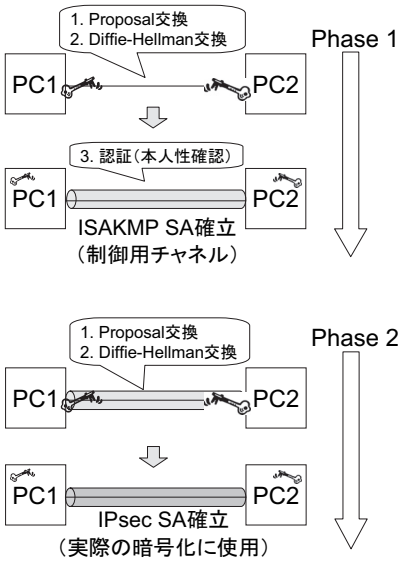

図 2　IPsec SA 確立までの IKE のプロセス

3. MANET におけるマルチホップ通信

3.1 マルチホップルーティングプロトコル

マルチホップネットワークは，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探して選択す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，また低ビットレート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フォワーデ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，OLSR (Optimized Link State Routing) [6] や TBRPF (Topology Broadcast based on Reverse-Path Forwarding) [7] などがある．

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．リアクティブ型のルーティングプロトコルには，AODV (Ad-hoc On-demand Distance Vector) [8] や DSR (Dynamic Source Routing) [9] などがある．

本研究では，セキュアコネクションの生成の際，事前に目的ノードへの経路が確定していることが望ましいと考え，経路制御プロトコルとしてプロアクティブ型である OLSR を使用した．

3.2 OLSR 概要

OLSR はプロアクティブ型のルーティングプロトコルであり，定期的にルーティングテーブルを更新しているため，即座に通信を開始することができる．特に OLSR は他のルーティングプロトコルと比較し，より効率の良いフラッディングを行っていることが特徴として挙げられる．プロアクティブ型のルーティング手法は頻繁に経路情報を交換するため，通常のフラッディングの場合多くのノードが重複したパケットを受け取ることになり，ネットワークへの負荷が増大する可能性がある．これに対し OLSR では，パケットを再送信するノードを最小限に抑えるために MPR 集合 (Multi - Point Relay) を決定することで，無駄な再送信が行われないようノードを制限することができる．

OLSR のパケットには制御メッセージが含まれており，経路表生成に関わるメッセージとしては HELLO メッセージと TC (Topology Control) メッセージがある．HELLO メッセージにより各ノードが持つ周辺情報を隣接ノードへ送信することで，各ノードは自身の周辺 2 ホップ以内の情報を得ることができる．TC メッセージはネットワーク全体にフラッディングされるメッセージであり，全ノードに各ノードの持つトポロジ情報を通知し，これにより各ノードにおいて経路表が作成される．このため，上記 2 つのメッセージは，経路制御において最も重要なメッセージであるといえる．他に，実用性を考慮した補助的なメッセージとしては，ノードが複数のインタフェースを備えている場合に使用される MID (Multiple Interface Declaration) メッセージと，ノードがゲートウェイとして機能する場合に使用される HNA (Host and Network Association) メッセージがある．

4. セキュアコネクション構築の制御手法

4.1 セキュアコネクションの概念

MANET 内には不特定多数のノードが存在し，様々なノードが通信経路に加わる可能性があるため，必ずしも安全な環境であるとは限らない．そのため複数のノードを中継する通信を行う場合，図 3 に示すような送信ノードから受信ノードまで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．このようなセキュアコネクションは，事前に互いが信頼できると判っているノード間でマルチホップ通信を行う際に必要となると考えられる．

本研究では，IPsec により通信を暗号化することでセキュア

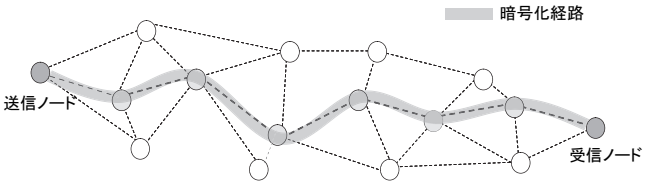

図 3　セキュアコネクション

コネクションを確立する手法をとっている．そのため，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ことができるよう，IPsec SA の確立方法を最適化する必要がある．また，一般に MANET 内の各ノードは固定アドレスを持たないため，有線向け仕様である 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．

そこで本研究では，暗号鍵の取り扱いを考慮し，OLSR によって制御されたマルチホップネットワークにおいて，セキュアコネクションを構築，制御するモデルを提案した．提案手法では，まず信頼できるノードの情報を事前に把握するため，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する．次節以降で，提案手法の詳細を述べる．

4.2 ノードのリスト管理

4.2.1 ID・公開鍵リスト

マルチホップネットワークにおいて通信を行う場合，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．そのため本提案では，信頼性の保証された通信相手ノード群を事前にリストとして各ノードで保持し，同時にセキュアコネクション生成で必要となる情報もリストに格納し，管理を行うことにした．一般に MANET では各ノードは固定アドレスを持たず，個々のノードは ID で識別される．またセキュアコネクションの生成においては，各ノードが個別に保持する公開鍵が用いられる．そこで，各ノードはリストに，信頼できるノードの ID と公開鍵の組を事前に格納し，MANET 参加後これに IP アドレス情報を追加していく．なお，この公開鍵は IKE の処理過程で使用され，実際に IPsec の暗号化に用いられる鍵ではない．リスト内のメンバーとセキュアな通信を行う場合，この情報をもとに各処理を行い，万一通信経路上になりすましや中間者攻撃等を行う悪意を持ったノードが存在した場合も，安全に通信を行えるようにする．信頼性が確かめられているノードのみの情報をリストとして管理することにより，相手と直接通信できないマルチホップ環境においても正しい相手と判断することができる．

4.2.2 リストの作成と更新

セキュアコネクションを生成できるのは，互いのノードの信頼性が保証されている場合に限られる．そこでリストの作成に

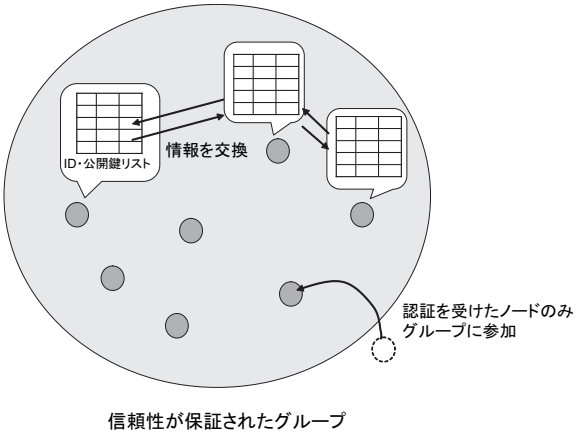

図 4　リストの作成

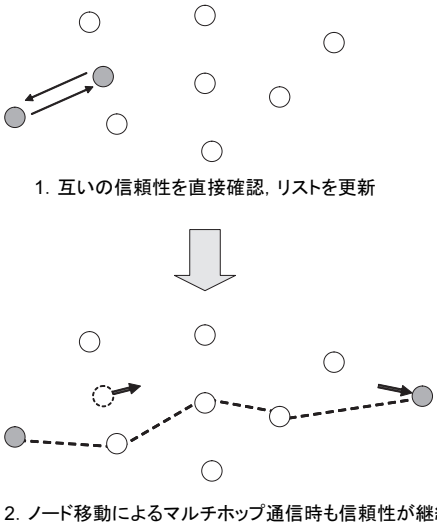

図 5　リストの更新

あたり，信頼性の保証された安全なグループをあらかじめ構成し，グループに属するノード間で各情報をやりとりできることとする．このグループには，認証を受けたノードのみが参加でき，図 4 に示すようにグループ内の各ノードは ID と公開鍵を互いに交換し，リストに追加していく．グループに属するノード同士が，MANET 上においてセキュアな通信が必要となった場合，リストに記載されているノードは全て安全であることが判っているため，リストの情報を利用するだけで，直接通信できないノードとセキュアコネクションを生成することができる．

一方，MANET 参加後，信頼性が保証されたグループに属さず，またリストにも載っていないノードとセキュア通信が必要になった場合を考える．この場合，通信を行うノードが信頼できる相手であるかどうかが最も考慮すべき点であり，図 5 に示す手順によりリストを更新することとする．まず，両ノードが MANET 内で一時的に直接通信が可能な状態で，互いが信頼できるノードであるかどうかを判断する．そして信頼性が確認できた場合のみ，ID と公開鍵の組を交換しリストを更新する．判断の方法については，本稿では議論の対象外とする．一度直接通信を行いノード同士の安全性を確認することにより，ノードの移動により中継ノードを経由したマルチホップ通信が必要となった場合も，信頼性を保つことができる．

4.3　IP アドレスの取得

MANET にノードが参加すると，OLSR の定期的な経路情報交換によりノードが発見され，そのノードを含んだ経路表が各ノードで作成されることで，IP アドレスを元に経路制御を行うマルチホップネットワークが構築される．MANET では各ノードは 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，通信の開始にあたり参加ネットワークにおける目的ノードの IP アドレスと，リストに保持されているノードの ID とを対応付ける必要がある．IP アドレスの取得方法として，本研究では図 6 に示すような手法を検討した．

まず通信を開始したいノードは，自分の ID やアドレス，通信を行いたい目的ノードの ID を含んだメッセージを，現在属しているマルチホップネットワークでブロードキャストする．自分へ向けたメッセージであることが判った目的ノードは，自分の ID と IP アドレスを含んだメッセージを，送信元ノードへ返信する．このような手順で，取得した IP アドレスは，このネットワークにおける一時的に有効な目的ノードの IP アドレスとして，リストに保持する．別のネットワークにおいて同一ノードとの通信を希望する場合は，再度 IP アドレスを取得し，リストを更新する必要がある．

また，この段階で交わされるメッセージは，セキュリティのない通信経路を経由するため，中継ノードにおけるメッセージの改竄やなりすましなどにより，IP アドレスの詐称が行われる可能性が考えられる．そこで本提案では，次節で説明するセキュアコネクション生成の段階で，リストの情報と IKE の処理機能を用いることにより，IP アドレスが正しく目的ノードから送られてきたものであるかどうかを確認する．

4.4　セキュアコネクション生成と再構築

4.4.1　セキュアコネクションの生成

OLSR により構築されたマルチホップネットワークにおいて，上記の手順を経て取得した IP アドレスにより，目的ノードとの通信をリクエストすると，即座に途中ノードを経由した経路によって通信が開始される．この段階ではまだ通信は暗号化されていない．通信経路の確立後，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暗号化通信経路である IPsec SA を生成することで，セキュアコネクションを構築する．このセキュア通信路上では，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中身を知ることはできない．

IPsec SA を生成する過程では，リストの公開鍵が参照され IKE 処理による本人性確認が行われる．そのため万が一 IP アドレス取得の際に，IP アドレスの詐称が行われていた場合，リストで事前に保持している公開鍵情報に基づく本人性確認が認証されず，悪意のあるノードによるなりすましを防ぐことができる．

4.4.2　再構築によるネットワーク構成変化への適応

提案モデルにおいては，送受信ノード間で安全に暗号化通信が行われ，かつ通信経路を構成している中継ノードの離脱等によりネットワーク構成が変化した場合にも，セキュアコネクショ

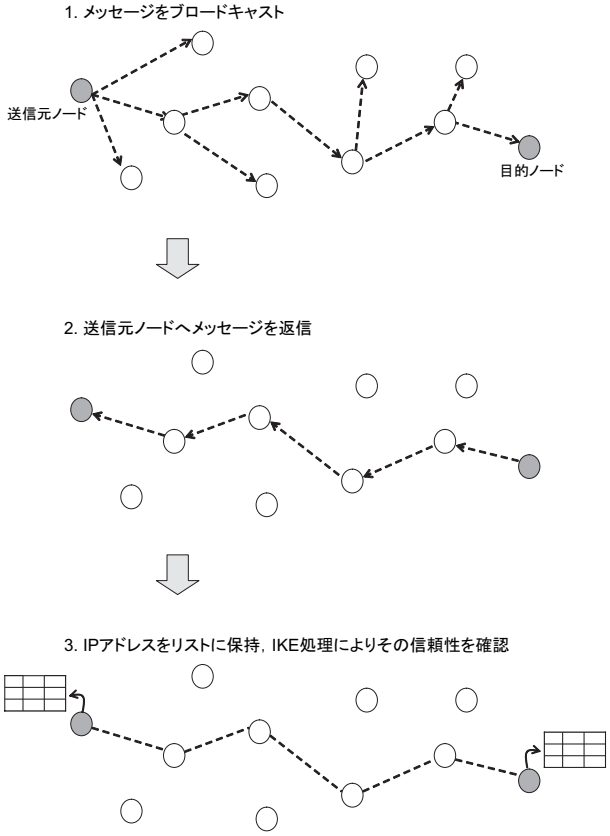

図 6　IP アドレスの取得

ンが柔軟に適応できることが重要である．本提案では図 7 のように，中継ノードの参加・離脱や送受信ノードが移動した場合，OLSR の経路情報交換により定期的にネットワーク状況が把握され，即座に新たな経路表が各ノードで作成される．そのため，エンドツーエンドで確立された送受信ノード間のセキュアコネクションは自動的に再構築され，途中通信経路の構成変化を意識することなく，引き続き安全な通信を継続することができる．

5.　提案手法の実装

5.1　実 験 環 境

本稿では提案したモデルのうち，OLSR によるマルチホップ環境上において，IP アドレスを取得し対応するリストを更新した後，それらの情報をもとにセキュアコネクションを生成し制御する処理の実装を行った．またセキュアコネクション構築時に，マルチホップネットワーク構成を変化させ，セキュアコネクションの再構築が行われる動作を確認した．なお，現実装においては，リストを作成するノードは全て信頼性が保証されているものとする．

実験環境としては，4 台のマシンを用い，図 8 のようなマルチホップネットワーク環境を構築した．マルチホップ環境の構築手法については次節で説明する．ルーティングプロトコルとしては OLSR を使用し，Linux における実装として olsrd [10] を用いた．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 openswan [11] 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エ

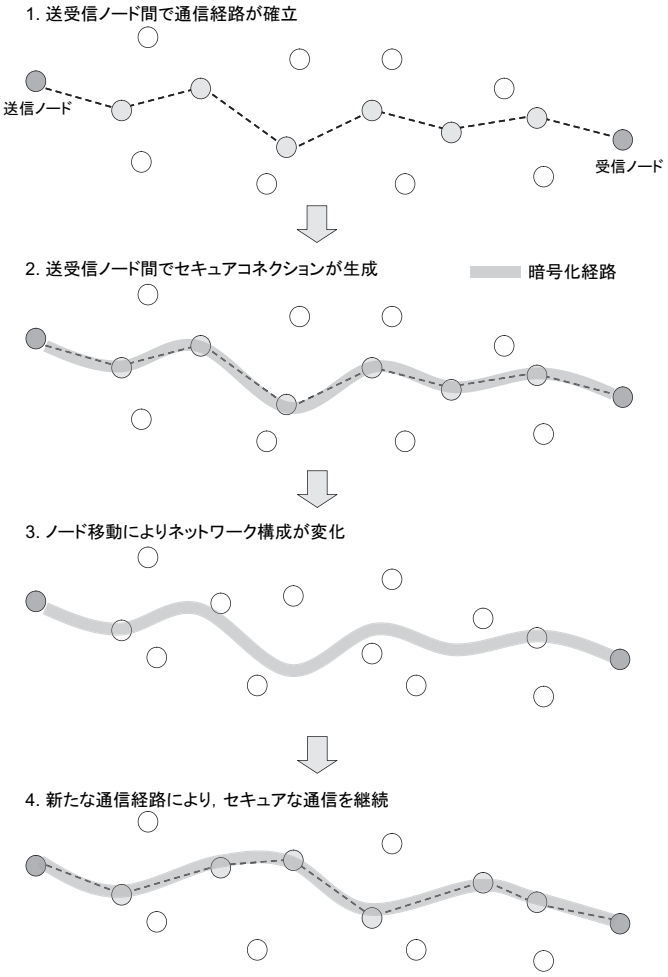

図 7　セキュアコネクションの生成と再構築

ンドツーエンドの通信を行うトランスポートモードを選択している．マシンは全て IEEE802.11b 無線 LAN を使用し，以下のような構成となっている．

- A: Linux2.6.9-1, Intel Pentium4 3.06GHz, 512MB
- B: Linux2.6.9-1, Intel Pentium4 3.06GHz, 512MB
- C: Linux2.6.9-1, Intel Pentium4 3.06GHz, 512MB
- D: Linux2.6.15-1, Intel Pentium4 3.2GHz, 512MB

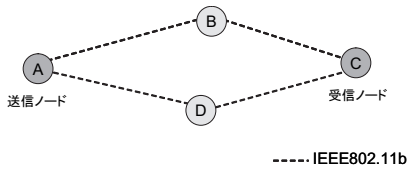

図 8　実 験 環 境

本環境において，ノード A を送信元ノード，ノード C を宛先ノードとし，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．

5.2　マルチホップ環境の構築

OLSR を用いマルチホップネットワーク環境を構築する場合，実験の都合上，全ノードが直接無線通信できる範囲に存在してしまうため，送信ノードと受信ノードが直接通信を行わないよう互いのパケットを遮断させる必要がある．本研究の実験

環境においては，例えばノード A からノード B を中継しノード C に辿り着く経路を構築したい場合，ノード A ではノード C からのパケットを，ノード C ではノード A からのパケットを，iptables コマンドにより遮断することで，マルチホップ通信を行う環境を実現できる．

また olsrd 実行時に IPsec 接続を行うと，IPsec 処理により経路表が書き換えられてしまい，その後 OLSR により正しい経路表に戻らず通信ができなくなってしまう問題が発生した．これは IPsec または olsrd の実装上の問題と考えられ，両端のノードを一時的にネットワークから落とし，すぐ復活させることで OLSR により正しい経路表が作成されるため，今回の提案モデルの実装にあたってはこの方法により問題を回避した．

上記の実験環境において OLSR による通信経路確立後，ノード A がノード C とのセキュアな通信を必要とする場合，これを自動的に構築，制御する仕組みを実装した．使用言語は C 及び Perl を用いている．また実装において，ノード A は事前にノード C のリストを作成しており，ID と公開鍵を保持している状態とする．以下に動作の詳細を示す．

5.3 提案手法の実装

5.3.1 IP アドレスの取得

送信元ノードが目的ノードとのセキュアコネクションを生成するため，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，リストに追加する必要がある．まず，送信元ノードは参加しているネットワーク内において，「送信元ノードの ID，送信元ノードの IP アドレス，セキュアな通信を行いたい目的ノードの ID」を含むリクエストメッセージを全ノードに対し送信する．次にリクエストメッセージを受信した各ノードは，メッセージに自分の ID が含まれているか各々チェックを行い，含まれていなければこのメッセージは無視する．ここで，メッセージに自分の ID が含まれていることを確認した目的ノードは，「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．送信元ノードは目的ノードから返信メッセージを受け取ると，メッセージをもとにリストへ目的ノードの IP アドレスを追加する．

このような手順で動作を行う制御スクリプト実行時の一連動作例を，図 9 に示す．本実験環境においては，まずノード A は OLSR が構築する通信経路に基づき，B と D へは直接，C へは B を経由し，ソケット通信によりリクエストメッセージを送信する．リクエストメッセージには，ノード A の ID と IP アドレス，目的ノード C の ID が載せられており，リクエストメッセージを受信したノードは各々メッセージをログファイルへ格納する．次にメッセージを受信した B，C，D はそれぞれ，ログファイルへ格納されたメッセージを一行ずつ読み込みチェックを行い，メッセージ内に自分の ID を発見したノード C は，C の ID と IP アドレスを載せたメッセージをノード A に返信する．また同時に C の保持するノード A のリストに IP アドレスを上書きする．このとき，返信メッセージを受け取ったノード A も，同様の動作により保持しているノード C のリストに IP アドレスを格納する．

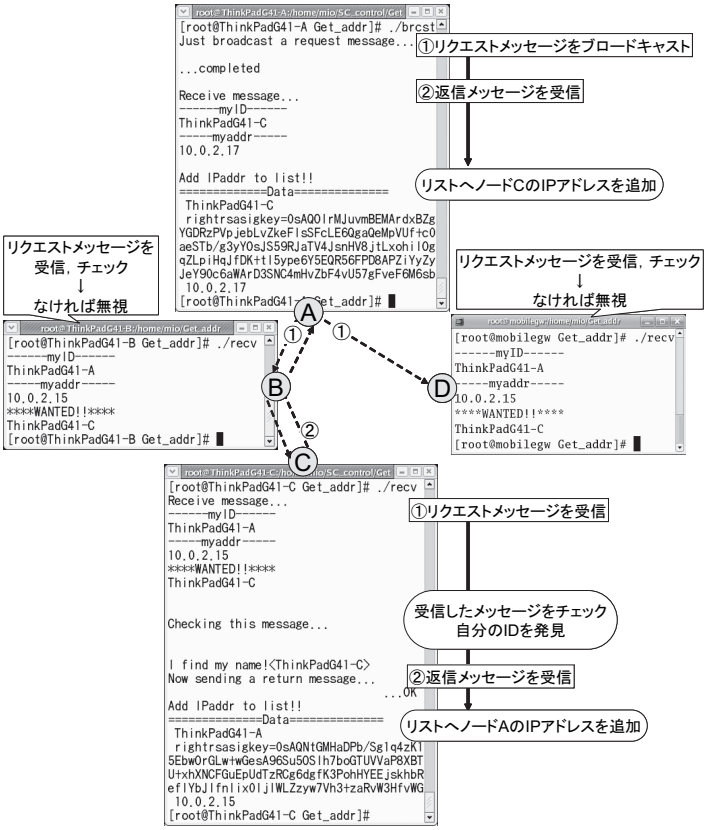

図 9　IP アドレスの取得とリストへの追加

5.3.2 セキュアコネクション生成の動作

前項の手順を終え，データの送受信を行うノード A と C は，それぞれ相手の公開鍵と IP アドレスを把握している．マルチホップ通信経路の確立後，両ノードにおいて相手公開鍵をもとに IPsec の設定ファイルが書き換えられる．その設定ファイルに基づきノード A は自マシンとノード C との間で IPsec の起動および接続を行い，両ノード間でエンドツーエンドの IPsec SA が確立される．このような手順で送受信ノード間におけるセキュアコネクションが自動的に生成される．

図 10 に，セキュアコネクション生成スクリプト実行時の一連動作例を示す．まずリストの公開鍵と IP アドレスをもとに，両ノードにおける IPsec の設定ファイルの指定行（公開鍵及び IP アドレス記入行）が書き換えられる．次にノード A が自身及びノード C で IPsec の制御コマンドを実行することで，設定ファイルに基づき IKE により実際の暗号化に用いる共通暗号鍵が作成され，送受信ノードにおいて IPsec で暗号化されたセキュア通信路が生成される．

5.3.3 ネットワーク構成変化時の動作

次に，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，代わりにノード D がネットワークに参加した場合の動作を確認した．ネットワーク構成の変化によるセキュアコネクションへの影響を見るため，A-C 間で定期的に暗号化通信を行っている状態で，tcpdump コマンドにより経路上を流れるパケットの様子を確認し，図 11 に示す．

ノード B がノード A － C 間の通信を中継しているとき，経路上では OLSR によるメッセージ交換のパケットと，IPsec に

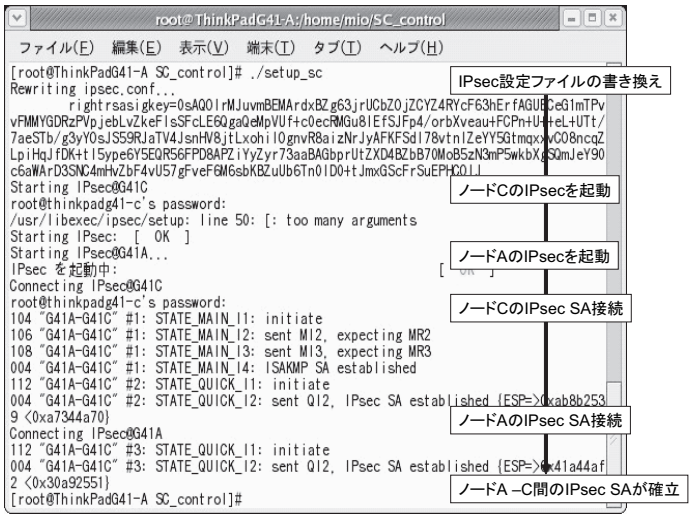

図 10　ノード A によるセキュアコネクション生成の実行例

より暗号化された ESP パケットが流れている．ここでノード B がネットワークから離脱すると，全ての通信は途絶える．このとき，新たにノード D がネットワークに参加すると，A-C 間の新たな中継ノードとして働き，経路上では引き続きノード A-C 間でやりとりされる ESP パケットが流れている．このように，OLSR により自動的に経路表の更新が行われてセキュアコネクションが再構築され，ノード A とノード C はネットワーク構成の変化に影響を受けることなく，セキュアな通信を続けていることを確認できた．

6. まとめと今後の課題

本稿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，セキュアコネクションを構築，管理するモデルを提案した．そして提案モデルの実現に向け，OLSR によって管理されるマルチホップ環境上で，送受信ノード間の通信を IPsec によって暗号化し，セキュア通信路を生成するまでの制御を実装した．今後は提案モデルが様々なシチュエーションにおいて，より現実的なモデルとなるよう検討していきたい．

謝　　辞

本研究を進めるにあたり，マルチホップネットワークの実験等について大変有用なアドバイスを頂いた芝浦工業大学工学部通信工学科の森野博章先生に深く感謝いたします．

文　　献

[1] MANET:http://www.ietf.org/html.charters/manet-charter.html
[2] Sye Loong Keoh, Emil Lupu, “ Towards Flexible Credential Verification in Mobile Ad-hoc Networks ”, POMC 2002, 2002
[3] Rajiv K. Nekkanti and Chung-wei Lee:“ Trust Based Adaptive On Demand Ad Hoc Routing Protocol ”, ACM Southeast Regional Conference, 2004
[4] 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
[5] 小早川知昭：IPsec 徹底入門，翔泳社
[6] OLSR：http://hipercom.inria.fr/olsr/
[7] TBRPF：http://www.ietf.org/rfc/rfc3684.txt

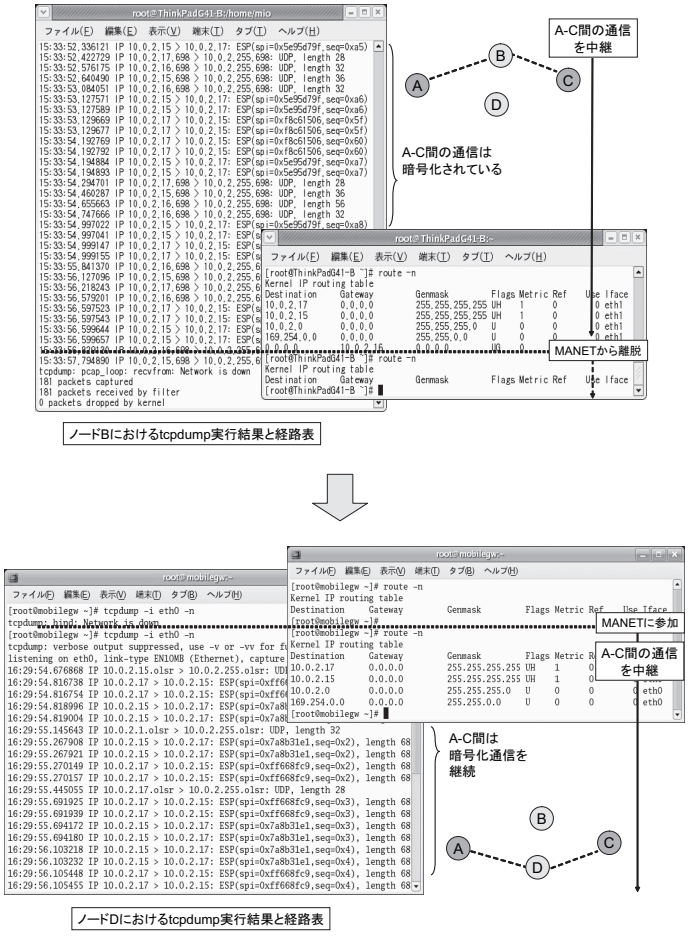

図 11　ネットワーク構成変化時の状況

[8] AODV：http://www.aodv.org/
[9] DSR：http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt
[10] olsrd：http://www.olsr.org/
[11] Linux openswan：http://www.openswan.com/
[12] 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