マルチホップネットワークにおける
汎用ＯＳを用いたセキュリティ機構制御方式

宇野 美穂子　　(指導教員:小口 正人)

1　はじめに

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型の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．第三者が中継を行うマルチホップネットワークでは，暗号化によりデータを守ることが必須である．ただし，利用環境やアプリケーションにより認証強度や応答時間の要求は異なる．

そこで本研究では，セキュリティメカニズムのリアルタイム性に着目した．汎用 OS に既存のルーティングプロトコルやセキュリティ技術を取り入れて構築したマルチホップネットワークにおいて，OS のプリエンプション機能を有効にし，CPU に負荷を与えた場合と与えない場合の応答時間を測定して，セキュリティメカニズムのリアルタイム性を調べる．更に，その結果を基にセキュリティ実現の応答性を制御する方式を提案し，実装する．

2　実験と考察

2.1　実験概要

本研究では，2 ホップのマルチホップ通信の場合について，CPU に負荷を与える方法を変えて実験を行い，セキュアコネクション構築時間を測定する．

実験環境として，IEEE802.11b 無線 LAN 機能を持つ 3 台の端末を用い，セキュアな通信を行う実験システムを構築した [図 1]．各マシンのスペックを表 1 に示す．

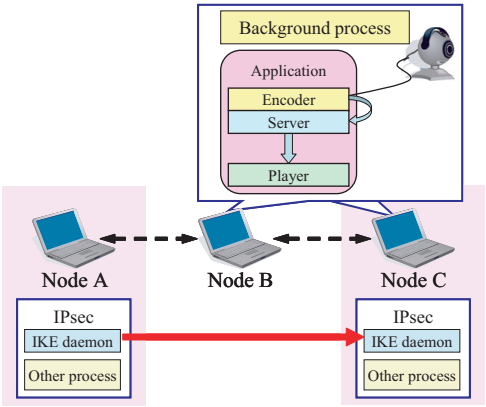

図 1: マルチホップ通信

マルチホップルーティングプロトコル OLSR(Optimized Link State Routing) によって管理されるマルチホップ通信環境を構築し，その上でデータのやり取りを行うノード間の通信データを IPsec(IP Security) により暗号化することでセキュアな通信経路を確保した．無線 LAN クライアントには BUFFALO WLI-PCM-L11GP を用いた．OLSR と IPsec の Linux における実装として，それぞれ olsrd と Openswan を使用した．この実験環境において，プロセスの実行中に割り込みが発生した際に優先度が高い他のプロセスを実行するプリエンプションの機能を取り入れるため，プリエンプティブカーネルを再構築して用いた．

表 1: 各マシンのスペック

Node	OS	CPU	メインメモリ
A	Linux2.6.11	Intel PentiumM 1.73GHz	512MB
B	Linux2.6.11	Intel PentiumM 1.73GHz	512MB
C	Linux2.6.11	Intel PentiumM 1.3GHz	512MB

本研究では，マルチホップネットワークの端末におけるアプリケーション負荷としてライブストリーミング・プロセスを使用した．ストリーミングサーバには Helix Server Basic，エンコーダには RealProducer Plus，プレイヤには RealPlayer を用いた．今回の実験では，ストリーミングの配信とその受信及び再生を各々同一ノードで行っている．以降では，このプロセスをバックグラウンドプロセスと呼ぶ．バックグラウンドプロセスの優先度は，nice コマンドで-20(高) から 19(低) の範囲で指定した．IPsec の実装である Openswan は複数のプロセスから成り立っており，デフォルトでの優先度は，IPsec の鍵交換をつかさどる IKE デーモンである PLUTO は 10，それ以外のプロセスは 0 と設定されている．また，olsrd は 0 と設定されているが，両者ともこのデフォルトの状態で実験を行った．

上記の実験環境において，中継ノード B に負荷を与えたときと宛先ノード C に負荷を与えたときの 2 つの場合について測定を行った．実験手順は，まず送信元ノード A と宛先ノード C で IPsec デーモンを起動し，IPsec 接続が可能な状態にする．次に，中継ノード B または宛先ノード C でバックグラウンドプロセスを実行し，IPsec の接続開始から IPsec コネクションの確立までに要する時間を tcpdump コマンドを利用して測定する．

2.2　実験結果と考察

図 2 は中継ノード B に負荷を与えたとき，図 3 は宛先ノード C に負荷を与えたときの実験結果である．図 2 から，中継ノードに負荷を与えても，セキュアコネクション構築時間には影響を及ぼさないということが結果が得られた．中継ノードでは IP 層におけるルーティングのみが行われており，その処理には負荷や優先度があまり影響しないためと推測される．

一方，図 3 で示されるように宛先ノードに負荷を与えた場合は，バックグラウンドプロセスの優先度によってセキュアコネクション構築時間が異なるということが分

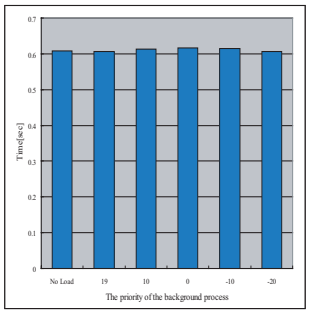

図 2: 中継ノードに負荷

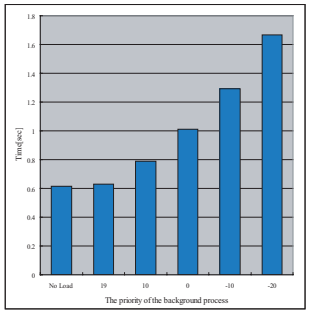

図 3: 宛先ノードに負荷

かった．バックグラウンドプロセスの優先度の指定が低いときは負荷が無いときと同程度の時間で IPsec コネクションが確立するが，バックグラウンドプロセスの優先度が高くなるにつれて構築時間が長くなる．宛先ノードでは、IKE による ISAKMP SA の確立や IPsec SA の確立が行われている．これらの処理には負荷が大きく影響し，その優先度により応答性能が決まることが確認できた．

3 セキュリティ機構の応答性制御方式

3.1 提案手法

上記の実験結果に基づき，環境によって認証強度やレスポンスタイムを選択できる様，セキュリティ機構の応答性制御方式を検討する．宛先ノードでアプリケーションを使用している場合は，バックグラウンドプロセスの優先度によってセキュアコネクション構築時間が異なる．そこで，バックグラウンドプロセスの優先度が高くなるとセキュアコネクション構築時間が長くなるという点に着目し，環境やユーザの希望により優先度を変更することが可能な制御方式を考案することにした．具体的には，IPsec 起動後にアプリケーションプロセスと IPsec プロセスの優先度を比較し，アプリケーションの優先度が IPsec の優先度よりも高い場合には，IPsec の優先度がアプリケーションの優先度よりも高くなるように，プロセスの優先度を変更する．そして，その状態で IPsec 接続コマンドを実行し，セキュアコネクションを構築することが可能となる制御方式の枠組みをツールとして実装する．

3.2 制御方式の実装

提案した制御方式を図 1 と同じ実験環境に実装した場合を紹介する．ノード A を送信元ノード，ノード C を宛先ノードとし，IPsec 接続に関わる全ての処理は，ノード A で一元的に制御する．

図 4 は，ノード A で IPsec 接続プログラムを実行したときの様子である．まず，ノード A，ノード C のそれぞれで IPsec が起動される．次に，ノード C におけるプロセス情報を取得する．バックグラウンドプロセスの優先度が IKE デーモンの優先度よりも高いとき，つまり，バックグラウンドプロセスの NICE 値が 10 よりも小さいとき，それらのプロセス優先度を全て 10 に再設定する．そして，IPsec 接続を開始し，ノード AC 間でセキュアコネクションが構築される．なお，優先度の再設定には，renice コマンドを使用した．この制御スクリプトにより，IPsec の方がアプリケーションより優先度が高くなるようプロセス優先度の再設定を行うことができた．

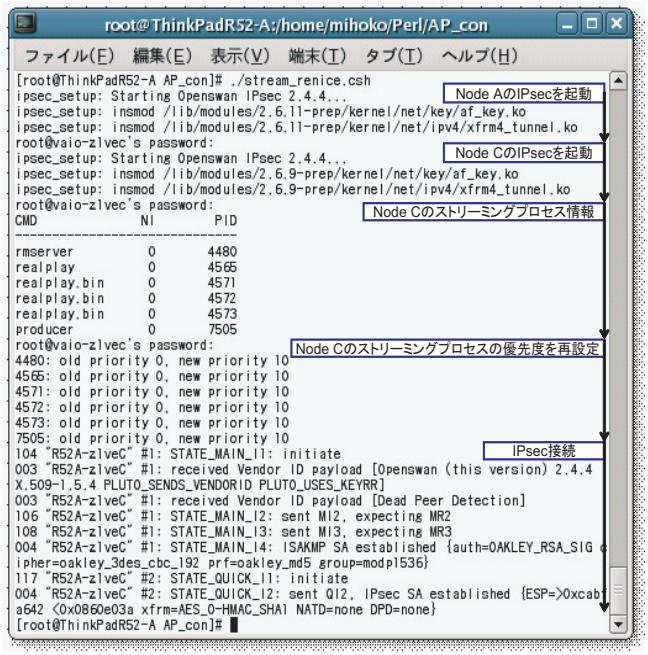

図 4: IPsec 自動接続プログラムの実行例

4 まとめと今後の課題

本稿では，汎用 OS を用いて構築されたマルチホップネットワークにおいて，ライブストリーミングにより負荷を与えた際のセキュアコネクション構築時間を測定して比較した．その結果，中継ノードにおいて CPU に負荷を与えた場合には影響はほとんどないが，宛先ノードにおいて負荷を与えた場合は，バックグラウンドプロセスの優先度が高くなるにつれてセキュアコネクション構築時間も長くなることが確認された．この実験結果を踏まえ，環境によって認証強度やレスポンスタイムを選択できるセキュリティ機構の応答性制御方式を提案し，実装した．IPsec プロセスの優先度とバックグラウンドプロセスの優先度を比較し，IPsec プロセスの方が優先度が高くなる様，バックグラウンドプロセスの優先度を再設定して IPsec コネクションを確立する自動制御方式を実装した．

今後は，ホームネットワークや ITS など様々な状況下での使用を検討し，更なる制御方式の提案と実装を目指す．

参考文献

[1] 宇野 美穂子，小口 正人：“ MANET における汎用 OS を用いたセキュリティメカニズムの応答性評価 ”，マルチメディア，分散，協調とモバイル (DICOMO2008) シンポジウム，7E-4，pp.1644-1650，札幌，2008 年 7 月

[2] Mihoko Uno and Masato Oguchi：“ An Evaluation of Response Time of a Security Mechanism Using a General-Purpose OS for a Multi-hop Network ”，In Proc. International Conference on Intelligent Pervasive Computing (IPC2008)，Sydney，Australia，December 2008

[3] 宇野 美穂子，小口 正人：“ マルチホップネットワークにおける汎用 OS を用いたセキュリティ機構の応答性制御方式 ”，コンピュータシステム研究会 (CPSY)，京都，2008 年 12 月