様式 C-19

科学研究費補助金研究成果報告書

平成　21 年　6 月　1 日現在

研究種目：基盤研究（C）
研究期間：2007～2008
課題番号：19500067
研究課題名（和文）　安全性と柔軟性を両立させるフレキシブルプライベートネットワークの実現
研究課題名（英文）　Realization of “Flexible Private Network” that can provide both security and flexibility.
研究代表者
渡邊　晃（WATANABE AKIRA）
名城大学・理工学部・教授
研究者番号：50360235

研究成果の概要：移動透過性とアドレス空間透過性の機能を統合し実装を完了した．FreeBSD で開発済みの GSCIP の基本部分を Windows へ移植し，安定動作することを確認した．管理装置の実装を行い基本部分の動作を検証した．CVS (Concurrent Versions System)を用いて管理を実施中であり，ソースコード公開に向けての準備をほぼ完了した．国内学会の口頭発表 13 件，国際会議口頭発表 2 件，論文誌掲載 2 件を達成した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	1,700,000	510,000	2,210,000
2008 年度	1,400,000	420,000	1,820,000
年度			
年度			
年度			
総　計	3,100,000	930,000	4,030,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム･ネットワーク
キーワード：情報ネットワーク

１．研究開始当初の背景

ユビキタスネットワークにおいてセキュアな通信を実現するために，共有ネットワーク環境の中に通信グループを構築することは有効な手段である．しかしこれまでの通信グループ構築方法ではサブネットワーク単位の通信グループと個人単位の通信グループを混在させたり，ネットワーク構成の変化に動的に対応させようとすると管理負荷が増大し実現が難しかった．そこで我々は柔軟性とセキュリティを兼ね備えたネットワークとして，フレキシブルプライベートネットワーク（FPN；Flexible Private Network）と呼ぶ概念を提案している．また，FPNを実現するための技術として，GSCIP (Grouping for Secure Communication for IP；ジースキップ) と呼ぶ一連のプロトコルを提案している．GSCIPは，IPv4とIPv6の両者での実現が可能である．当面はIPv4によるネットワークが一般であることから，まずはIPv4による実現を目指している．

２．研究の目的

FPN とはユビキタス社会に向けたネットワークのあるべき姿を示したもので，サブネ

ットワーク単位と個人単位の要素が混在する環境において，容易に通信グループの定義ができる．同一通信グループに属する端末間の通信は，暗号化によりその安全性が保証され，グループ外の端末からのアクセスを拒否することができる．サブネットワークが階層的に構築されている場合や，サブネットワーク内に異なるグループに属する端末が存在するような環境（多段構成ネットワーク）であってもかまわない．

本研究では，FPNを実現するための一連のプロトコルGSCIP (Grouping for Secure Communication for IP)を開発し，それらのプロトコルを統合することを目的としている．

３．研究の方法

研究代表者の他に，大学院博士課程学生１名，大学院修士課程学生５名を研究協力者とする．

統合に向けての検討は H19 年度より最優先で実施する．実装のベースは FreeBSD においてすでに確立している．FreeBSD においては IP 層より GPACK モジュール（GSCIP の機能を実装したモジュール）を呼び出し，処理を終えたら差し戻す．この方式は既に確立しており，カーネルを改造することが可能である．

Windows ではカーネルがブラックボックスであるが，外部に公開された NDIS (Network Driver Interface Specification)インタフェースを用いて FreeBSD で実現していたことと同等のことを実現できる．ただし，バッファ管理の方法が異なるので改造が必要である．移動透過性の実現においては，アプリケーション層から Windows 内のルーティングテーブルを操作する必要があることが判明している．

管理装置はLINUXまたはWindowsのアプリケーション上で開発を行う．実現上の制約はない．グループ鍵をあらかじめ各 GE に埋め込んでおくことにより事前のフィールド試験を行う．

４．研究成果

(1)NAT 越え

インターネット利用形態の多様化により，IP 電話やマルチメディア通信など個人間を主体とした P2P 通信の需要が高まっている．しかし通信相手ノードが NAT 配下に存在する場合，インターネット側から通信を開始することができない．このため NAT 配下のノードとコネクションを確立する NAT 越え技術が要求されている．これまでの NAT 越え技術は，特有の装置を導入し，パケットのカプセル化や中継転送を行うなどの方式が提案されているが, P2P 通信の特徴を大きく損なうなどの課題がある．そこで，外部ノードから NAT に対してマッピング処理を指示する外部動的マッピング方式を提案した．これを実現するためのプロトコルとして NAT-f（NAT-freeprotocol）を定義した．提案方式は，外部ノードが NAT 配下のノードに通信を開始する際, NAT とネゴシエーションを行うことにより, NAT にマッピング処理を行わせる．外部ノードはカーネルにおいて，NAT でマッピングされた情報に一致するようにアドレス／ポート変換を行うことにより，NAT 越え通信を実現する．プロトタイプシステムの実装を行い，エンドノード間の初期遅延およびスループットを評価した結果，通信開始時の遅延増加は 1ms 以下であり，スループットは提案方式を実装しない場合と比べ，同等であることを確認した．

(2)パケットロスレスハンドオーバ

ユビキタスネットワークの環境では，通信中に端末が移動してもコネクションを切断することなく通信を継続できる移動透過性が要求される．これまで移動透過性の研究はIPv6 を前提とした研究が多かったが, IPv6 が完全に普及するにはまだ時間が必要であり, IPv4 での移動透過性も重要な課題である．そこで，我々はIPv4 においても移動透過性を実現できるMobile PPC を提案してきた．しかしながらIPv4 の世界では, ハンドオーバ時の通信切断時間が非常に長く, 仮にIP レベルで移動透過性を実現できても実用的ではない．そこで，端末に2 枚の無線LAN カードを搭載し，Mobile PPC を用いてこのような課題を解決する方法について検討した．提案方式を実装し評価を行った結果，パケットロスがほとんど発生しないこと，通信に与える負荷は十分に小さく，消費電力もほとんど増加せずに実現できることがわかった．

(3)移動端末の認証

通信中に移動しても通信を継続できる移動透過性技術は，今後のユビキタスネットワークに必須の技術である．このとき移動後のエンドノード間で相互認証を行い，通信の横取りを防ぐことは重要な機能である．このため一般に通信に先立ち認証鍵を共有する方法が取られる．これまで認証鍵をエンドノード間で共有する方法として，乱数を 2 つの経路に分割して交換する Return Routability が提案されていた．しかし，この方法では情報が平

文であるため，盗聴に対して完全な解決策とはなっていなかった．そこで，Diffie-Hellman 鍵交換を採用し，さらにこの鍵交換を 2 つの経路に分割して実行する鍵共有方式 Split DH (Split Diffie-Hellman key sharing method)を提案した．Split DH は，盗聴による攻撃を完全に防止するとともに，より高度な攻撃となる中間者攻撃に対しても高いセキュリティを保つことができる．提案方式の基本機能を Mobile PPC（Mobile Peer-to-Peer Communication）へ実装して処理時間の測定を行なった．その結果，実装の工夫により通信に影響を与えるようなオーバヘッドをほとんど発生させず実現できることがわかった．

(4)NAT 越えと移動透過性の統合
外出先ノードからホームネットワーク内の情報家電機器などと自由に通信を行いたいという要求が高まっている．このような新たな通信スタイルにおいて，移動ノードが通信中に移動しても通信を継続できる移動透過性が実現できると有用性が更に高まる．従来の移動透過性プロトコルは，移動ノードが通信相手ノードと通信を開始できることを前提としている．しかし，IPv4 ネットワークにおいては通信相手ノードがプライベートネットワークに存在するとグローバルネットワーク側から NAT を越えて通信を開始することができない．そこでこの問題を解決するために，NAT 越え技術として提案済みのNAT-f（NAT-free protocol）を既存の移動透過性プロトコルと融合した．移動ノードは通信開始時にNAT-f によりプライベートネットワーク内の通信相手ノードと通信を開始し，移動時は既存の移動透過性プロトコルを用いて通信を継続する．NAT-f と移動透過性プロトコルは異なるタイミングで処理を行うため，互いに独立性を保持しつつ，かつ容易に組み合わせることができる．NAT-f とMobile PPC を実装したシステムを評価した結果，所定の機能を実行できること，かつ通信開始時のオーバヘッド及びスループットの低下は十分に小さいことを確認した．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　4　件）
① 瀬下正樹，鈴木秀和，伊藤将志，渡邊晃：「分割 Diffie-Hellman 鍵交換による移動ノードの鍵共有方式の提案」，情報処理学会論文誌，Vol.50，No.7，掲載決定，(2009-7)
② 鈴木秀和，渡邊晃：「プライベートネットワーク内のノードを通信相手とした移動透過性の実現方式」，電子情報通信学会論文誌 B，Vol.J92-B，No.1，pp109-121，（2009-1）
③ 金本 綾子，鈴木 秀和，伊藤 将志，渡邊晃：「IPv4 移動体通信システムにおけるパケットロスレスハンドオーバの提案」，情報処理学会論文誌，Vol.50，No.1，pp133-143，(2008-1)
④ 鈴木 秀和，宇佐見　庄五，渡邊 晃：「外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装」，情報処理学会論文誌，Vol.48，No.12，pp3949-3961，(2007-12)

〔学会発表〕（計　35　件）
①H. Suzuki and A. Watanabe, “Design of NAT Traversal for Mobile PPC Applying Hole Punching Technology.” TENCON 2008, Nov. 2008.
②Miyazaki, H. Suzuki and A. Watanabe, “Proposal of a NAT traversal system independent of user terminals and its implementation.” TENCON2008, Nov. 2008.
③ Suzuki, Y. Goto and A. Watanabe, “External Dynamic Mapping Method for NAT Traversal.” ISCIT2007, Oct. 2007.
④Y. Goto, H. Suzuki and A. Watanabe,” Researches on Extended Dynamic Process Resolution Protocol that Can Traverse NAT”, TENCON2007, Oct.2007.
⑤Y. Miyazaki, H. Suzuki and A. Watanabe, “A Proposal for a NAT Traversal System that Does Not Require Additional Functions at Terminals.” TENCON2007, Oct.2007.
⑥K. Imamura, H. Suzuki and A. Watanabe, “A Proposal for a Remote Access Method using GSCIP and IPsec.” TENCON2007, Oct.2007.
⑦C. Shu, H. Suzuki and A. Watanabe, “Proposal of an Authentication Method “SPAIC” using a Non-contact Type IC Card.” ISCIP2007, Oct. 2007.

他 28 件

〔図書〕（計　0　件）

〔産業財産権〕
○出願状況（計　0　件）

○取得状況（計 0　件）

〔その他〕
ホームページ
http://www.wata-lab.meijo-u.ac.jp/

６．研究組織
(1)研究代表者
渡邊　晃（WATANABE　AKIRA）
名城大学・理工学部・教授
研究者番号：50360235

(2)研究分担者
なし
(3)連携研究者
なし