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 26 日現在

研究種目：若手研究（B）
研究期間：2007～2008
課題番号：19700073
研究課題名（和文）　セキュリティを保証するアドホックネットワークマルチキャスト通信

研究課題名（英文）　Secure Multicast Communications in Mobile Ad-Hoc Networks

研究代表者
野口　拓（NOGUCHI TAKU）
立命館大学・情報理工学部・講師
研究者番号：00388133

研究成果の概要：無線端末同士の相互接続によって自律的に形成されるアドホックネットワークにおいて，安全かつ確実に多地点へ配信するマルチキャスト通信を実現するために必要なネットワーク制御技術の開発を行った．送信者認証を用いた安全な経路制御技術，公開鍵を用いた端末認証技術，不正行為を抑制するマルチキャスト配送技術を開発し，アドホックネットワークにおいて安全かつ高信頼なマルチキャスト通信を実現できることを示した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	1,800,000	0	1,800,000
2008 年度	1,100,000	330,000	1,430,000
総　計	2,900,000	330,000	3,230,000

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：アドホックネットワーク，マルチキャスト，セキュア/ネットワーク，高信頼性ネットワーク

１．研究開始当初の背景

近年，基地局やアクセスポイント等のインフラを必要とせず，無線端末のみによって自律分散的に構築されるネットワークであるアドホックネットワークが注目を集めている．アドホックネットワークは災害等の緊急時におけるインフラレスな通信の手段として期待されており，例えば大地震発生時の安否情報や被災状況の通知，イベント会場での情報配信等がその具体的アプリケーションとして考えられている．これらのアプリケーションでは，同一情報を確実に多地点へ配信する機能が必須となるため，アドホックネットワークにおける多地点情報配信技術(マルチキャスト）の早急な確立が期待されている．アドホックネットワークにおけるマルチキャスト通信の潜在的な需要を受け，各国で研究開発が精力的に進められており，マルチキャスト経路制御プロトコルについては多くの提案・評価報告がなされている．しかしながら，従来研究はセキュリティ面については考慮されておらず，アドホックネットワークマルチキャスト通信のセキュリティ保証に関する研究例は世界的に見てごくわずかである．アドホックネットワークでは，送受信者以外の端末もデータの中継を行い，さらに

ブロードキャスト性を有する無線通信によりデータが伝送されることから，第三者によるデータの盗聴・改竄などが容易であり，有線ネットワーク以上にセキュリティ面で脆弱である．

２．研究の目的

アドホックネットワークにおけるマルチキャスト通信では，経路制御プロトコルによって正しく計算された経路を利用して，認証された送信元から情報が高信頼かつ安全に配信されることが求められる．

本研究の目的は，アドホックネットワークにおけるマルチキャスト通信において，データを中継する第三者によるデータの盗聴・改竄を防ぎ，高信頼かつ安全なマルチキャスト通信を実現することである．そこで，以下の 3 つの研究課題に対して具体的研究を遂行した．

(1) 送信者認証を適用したアドホックネットワーク経路制御プロトコルの開発
(2) 端末信頼度情報に基づく公開鍵を利用した端末認証技術の開発
(3) オーバレイ技術を用いた安全なマルチキャスト経路制御プロトコルの開発

２．研究の方法

(1)アドホックネットワークではネットワークトポロジの変化が激しいため，隣接端末間の情報交換に基づいてトポロジ管理と経路構築が行われる．不特定多数の隣接端末間で行われる情報交換には，暗号化が困難であるブロードキャスト通信が用いられるため，第三者によるなりすましや改竄が容易である．高信頼かつ安全なアドホックマルチキャスト通信を実現するためには，経路制御プロトコルの安全性を確保することが重要な技術課題となる．そこで，本研究では，ブロードキャスト通信の送信者認証技術である TESLA を適用した経路制御プロトコルを提案し，なりすまし送信や改竄を防ぐ安全なルーチングプロトコルを提案した．さらに，計算機シミュレーションによる性能評価を行い，提案方式の有効性を定量的に検証した．

(2) 上記(1)で開発した送信者認証技術を適用した経路制御プロトコルでは，中央サーバによる端末認証サービスの提供が不可欠である．これは，集中管理を必要とせず，無線端末による分散制御で維持・管理されるアドホックネットワークには適さない．そこで，中央サーバを必要とせずアドホックネットワーク内の端末のみで端末認証が可能となる，端末間信頼度情報に基づく公開鍵を利用した端末認証方式を提案した．さらに，計算機シミュレーションによる性能評価を行い，提案方式の有効性を定量的に検証した．

(3) アドホックネットワークにおけるマルチキャスト通信の実現には，導入容易性の点で，マルチキャスト専用経路制御プロトコルではなく，ユニキャスト経路制御プロトコルを利用したオーバレイマルチキャストが適している．本研究では，アドホックネットワークにおける安全なオーバレイマルチキャスト方式として，安全な 2 端末間通信リンクを連結してマルチキャスト配送木を 2 本構築し，悪意のある端末の不正行為に起因する通信リンク切断の影響を低減するマルチキャスト経路制御プロトコルを提案した．さらに，計算機シミュレーションによる性能評価を行い，提案方式の有効性を定量的に検証した．

４．研究成果

(1) アドホックネットワークにおいてオーバレイマルチキャスト技術を用いたマルチキャスト通信を行う場合，マルチキャスト配送経路の信頼性および安全性は，ユニキャスト経路制御プロトコルに大きく依存する．アドホックネットワークでは無線端末自身がルータ機能を備えているため，悪意のある端末による経路表の崩壊や消費等の不正行為が容易であり，ユニキャスト経路制御プロトコルの安全性を確保することが重要な技術課題となる．本研究課題では，高信頼かつ安全なアドホックマルチキャスト通信の実現を目指し，その要素技術となる安全なユニキャスト経路制御プロトコルの開発を試みた．

アドホックネットワークにおける経路制御では，トポロジの変化情報を含んだ制御メッセージを隣接端末同士で交換することで，トポロジの変化に対応し，正確な経路計算を実現している．しかしながら，隣接端末間の情報交換には暗号化が困難であるブロードキャスト通信を利用しているため，悪意を持った第三者によるなりすまし送信や改竄が容易に可能である．制御メッセージのなりすまし送信や改竄によってパケット配送率の低下や DoS (Denial of Service) 攻撃などが引き起こされるが，制御メッセージ送信時に送信者認証を行うことでこれらの脅威を防ぐことができる．そこで本研究課題では，メッセージ認証符号を用いたブロードキャスト通信の送信者認証技術を適用した経路制御プロトコルを提案した．提案プロトコルでは，各端末が送信する制御メッセージの重要性に応じて低遅延・高負荷認証と高遅延・低負荷認証を切り替えることで，効率的にブロードキャスト送信者認証を行い，送信者認証制御の導入に遅延の短縮を実現している．トポロジ変化の激しいアドホックネットワークにおいては，経路制御時の遅延は，経路表

の正確性を低下させる要因となる．この点を検証するため，計算機シミュレーションを行い，提案方式が既存方式と同等の配送率を実現できることを確認した．提案方式（Secure TBRPF）と既存方式（TBRPF-I）の配送率特性を図 1 に示す．なお，図 1 において縦軸はデータ配送率，横軸は移動端末の移動過程における静止時間を表している．

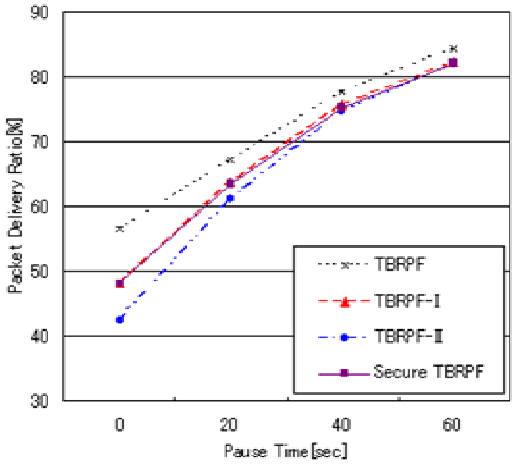

図 1：パケット配送率特性

本研究課題で開発した安全なユニキャスト経路制御プロトコルは，IETF で標準化が進められているアドホックネットワーク経路制御プロトコル TBRPF の拡張型と位置づけることができ，研究代表者の知る限り，TBRPF のセキュア化の研究例は，本研究課題が初めてである．本研究成果は，安全なアドホックネットワークユニキャスト経路制御プロトコルとして，多くのアドホックネットワークアプリケーションに応用可能である．

(2) 上記(1)で開発した送信者認証技術を適用した経路制御プロトコルでは，中央サーバによる端末認証サービスの提供が不可欠である．しかしながら，分散制御によりネットワークが管理・維持されているアドホックネットワークにおいて一点集中型の認証サーバーを設置することは困難であり，分散型の端末認証サービスが必要とされている．そこで，本研究課題では，既存の分散型公開鍵管理方式である証明書連鎖に信頼証明書という概念を導入することで，個々の端末の信頼度の違いを考慮した公開鍵管理方式を提案し,分散型端末認証を実現する． 提案方式では，認証局によって発行された公開鍵証明書を持たない端末を認証するための技術として，端末利用者の個人的な信頼関係をもとに発行する個人証明書を端末間で交換することで，端末認証を行う．提案方式は，個人的な信頼関係を持つ端末同士を繋ぐことで個人証明書の連鎖を形成し，自身と対象端末との間に連鎖が形成できれば認証が可能となる方式である．提案方式は，証明書連鎖の形成時に端末信頼度を考慮する事で，不正端末を証明書連鎖から排除する機構を備える．提案方式の端末認証の正確性を評価するため，計算機シミュレーションを行い，提案方式が既存方式と比較して，不正端末が存在する環境下においても誤りなく端末認証を実現できることを確認した．図 2 は，提案方式と既存方式（CKM）における正当結合率特性を表している．正当結合率とは端末認証の正確性を表す評価尺度であり，1 の場合には，誤りなく端末認証が実現できていることを表す．また，図 2 の横軸は，悪意のある端末数を示している．

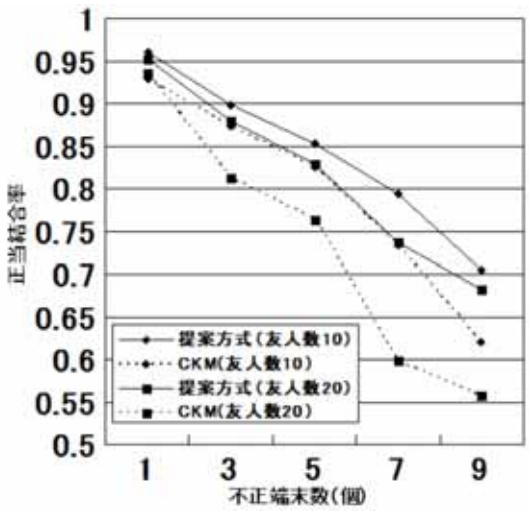

図 2：正当結合率特性

本研究課題で開発した端末信頼度に基づく端末認証技術は，安全なアドホックネットワークを構成するための基本技術であり，その応用範囲は広く，多くのアドホックネットワーク通信技術の安全化に貢献するものと考えられる．また，従来方式が考慮していない不正行為を行う端末の存在を考慮し，端末認証プロセスから不正端末を排除する本研究のアプローチは，従来にない独創的な手法である．

(3) アドホックネットワークにおいて安全なマルチキャスト通信を実現する方式として，オーバレイマルチキャスト技術を用いたマルチキャスト通信が期待されている．オーバレイマルチキャスト技術を用いた場合，既存のユニキャスト経路制御，認証技術を利用してマルチキャストを実現という利点がある．一方で，オーバレイマルチキャストネットワークを構成する端末の不正行為に脆弱であるという欠点を有する．オーバレイマルチキャストにおける端末の不正行為は，ツリ

ー状のデータ配送経路（マルチキャスト配送木）において，不正行為を行った端末の下流に位置する端末へ大きな影響を及ぼす．不正行為の影響を緩和するため，本研究課題では，接続構造の異なるマルチキャスト配送木を 2 種類構築し，一方の配送木において不正行為の悪影響を被る端末が，他方の配送木においては不正行為端末の上位に配置されるように配送木を形成する方式を提案する．これにより，悪意のある端末の不正行為に起因する通信リンク切断の影響を低減し，高信頼かつ安全なマルチキャスト通信が可能となる．さらに提案プロトコルでは，上記(1)で開発した安全なユニキャスト経路制御プロトコルおよび，上記(2)で開発した端末認証技術を利用して安全な 2 端末間リンクを構成し，このリンクを連結して連結して上述のマルチキャスト配送木を 2 本構築する．提案方式の有効性を評価するため，計算機シミュレーションを行い，提案方式が既存方式と比較して，悪意のある端末による不正行為発生時においても，スループット性能の低下を抑え安全かつ安定したマルチキャスト通信が実現できることを明らかにした．図 3 は，提案方式と既存方式における平均スループット特性を表している．また，図 3 の横軸は，総端末数に対する不正行為を行う悪意のある端末数の割合を示している．

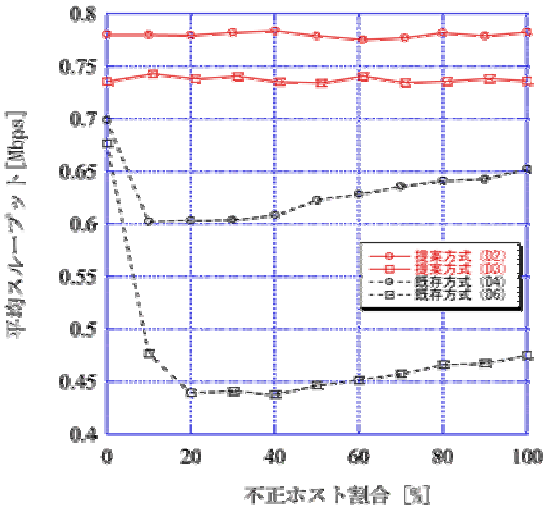

図 3：平均スループット特性

本研究課題で開発した不正端末を考慮した安全なオーバレイマルチキャスト技術は，安全なアドホックマルチキャスト通信を実現する上で必要不可欠な技術であり，多くの一対多通信アプリケーションに応用可能である．また，2 本の配送木を利用して不正行為対策を行う本研究課題のアプローチは，従来にない独創的な手法である．

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 5 件）

① Taku Noguchi, Miki Yamamoto, ``Cheatproof Dual-tree Application-level Multicast For Bulk Data Distribution'', IEICE Transactions on Communications, Vol.E91-B, No.12, pp.3872-3881, 2008, 査読有.

② Takahiro Matsuda, Taku Noguchi, Tetsuya Takine, ``Broadcasting with Randomized Network Coding in Dense Wireless Ad Hoc Networks'', IEICE Transactions on Communications, Vol.E91-B, No.10, pp.3216-3225, 2008, 査読有.

③ 南圭祐, 野口拓, 松田崇弘, 滝根哲哉, ``無線ブロードキャストのためのマルチソースネットワークコーディング”, 信学技報, Vol. 108, No. 204, IN2008-54, pp. 63-68, 2008 年, 査読無.

④ Nyein Aye Maung Maung, Taku Noguchi, Makoto Kawai, ``Maximizing Aggregate Throughput of Wireless Ad Hoc Networks Using Enhanced Physical Carrier Sensing”, IEEE International Conference on Distributed Computing Systems (ICDCS 2008), pp. 132-137, 2008, 査読有.

⑤ 中井隆幸, 野口拓, 松田崇弘, 滝根哲哉, ``ネットワークコーディングを用いたアプリケーションレベルマルチキャストのための経路構築法”, 信学技報, Vol. 107, No. 525, IN2007-160, pp. 7-12, 2008 年, 査読無.

〔学会発表〕（計 5 件）

① 大籔良祐, 野口拓, 川合誠, ``エージェント数制御を行う Ant 型アドホックネットワークルーチング”, 情報処理学会第 71 回全国大会, 2U-1, pp. 3-95-96, 2009 年, 査読無.

② 立山崇之, 野口拓, 川合誠, ``アドホックネットワークにおける端末の信頼度を考慮した分散型公開鍵管理方式”, 情報処理学会第 71 回全国大会, 5W-9, pp. 3-385-386, 2009 年, 査読無.

③ 上村哲也, 野口拓, 川合誠, ``アドホックマルチキャストネットワークを用いた分散型ホワイトボードシステム”, 2008 年電子情報通信学会総合大会, B-21-13, p. 614, 2008 年, 査読無.

④ 星野豊, 野口拓, 川合誠, ``ネットワークコーディングを用いたアドホックマル

チキャストネットワーク”, 2008 年電子情報通信学会総合大会, B-21-14, p. 615, 2008 年, 査読無.
⑤ 河内洋介, 野口拓, 川合誠, ``送信者認証を用いたアドホックネットワークルーチングプロトコルのセキュア化”, 2007 年電子情報通信学会ソサエティ大会, B-21-7, p. 409, 2007 年, 査読無.

６．研究組織

(1)研究代表者

野口　拓（NOGUCHI　TAKU）
立命館大学・情報理工学部・講師
研究者番号：00388133