立命館大学研究部
2010 年　5 月　7 日

提出締切：2010 年 5 月 20 日（木）

2009 年度採択　研究推進プログラム「若手・スタートアップ」　研究成果報告書

研究代表者	所属機関・職名：	情報理工学部 情報コミュニケーション学科 助教
	氏　名：	泉 朋子
研究課題	モバイルアドホックネットワークにおける高信頼データ通信	

Ⅰ．研究計画の概要

研究の計画について、概要を記入ください。

本研究では，モバイルアドホックネットワークに代表される，移動端末機で構成されるネットワークにおいて**高い信頼性を有する通信方法の確立**を目標に研究を行った．モバイルアドホックネットワークのように多種多様なユーザが存在するネットワークでは，ユーザが安心，安全に互いの情報をやりとりできることが多くのアプリケーションを提供する上での必須である．そこで高信頼性を実現するにあたり公開鍵暗号方式に着目し，公開鍵証明書を用いた暗号化データ通信における公開鍵証明書の管理法の問題に取り組んだ．集中管理・処理を行うサーバが存在しないシステムにおいてユーザ間の通信を効率的に実現するためには，各端末機でどのように公開鍵証明書を保持・管理するのかが重要である．本研究では，ユーザ間の通信要求の特徴とネットワーク上で仮想的に構成されるオーバレイネットワークの構造の関係に焦点をあて，公開鍵証明書の維持コストを最小化する証明書の最適配置について考察した．ユーザ間の通信要求については，全ユーザ間に通信要求がある場合，ユーザがグループを構成していると想定し各グループ内で通信要求がある場合，ユーザ間で特定のグループを構成しておらず任意の通信要求が与えられる場合の 3 つの特徴を分類する．またネットワークの構造については，木やリングなどの通信経路が限定的な構造から任意の構造まで考察し，最適な証明書配置の可能性・不可能性や近似可能性について明確にし，実際の配置法の提案を行う．

Ⅱ．研究成果の概要

研究成果について、概要を記入ください。

任意のオーバレイネットワーク構造上で任意の通信要求に対応可能な公開鍵証明書の配置方法を与える問題は NP 困難であることが既に知られていた．本研究では最適配置に対する近似解を得るアルゴリズムの開発を目指したが，任意の構造と任意の通信要求に対しては近似率の下界が$\Omega(\log n)$であることを解明した（ここで n は計算機の台数である）．各ユーザが証明書を保持するシステムでは最適な証明書配置を与えることが非常に困難であることを明らかになってしまったが，一方で近似率$O(\log n)$を保証する配置法の提案にも成功した．また，全ユーザ間の通信要求を実現するよう証明書配置を行う場合に対しては，近似率 2 の手法が 2006 年に提案されていたが，本研究ではこの手法をユーザがグループを形成しており各グループに含まれるユーザ間の通信要求を実現するよう配置を行う場合に適用した．結果，この手法がグループ内通信を行う場合にも近似率 2 を保証することを定量的証明により示した．本研究ではこれらの結果を 2009 年にアメリカ・ナイアガラで開催された国際会議 The 15th International Computing and Combinatorics Conference (COCOON'09)で口頭発表を行い，当該研究分野の研究者らから我々の結果に対し評価を受けた．さらに，Elsevier 社が出版する論文誌 Theoretical Computer Science への採録が決定し，2010 年に出版されることが決まっている．

本ページはホームページに公開いたします。１ページに収めてください。