論文審査の結果の要旨

氏名　林　素娟

本論文は「ユビキタスコンピューティング環境における認証プロトコルと安全なサービス発見に関する研究」と題し，セキュリティレベルの低いデバイス間でサービスを切り替えるサービスモビリティの実現に向け，安全なサービスハンドオーバー機構とサービス発見のための認証プロトコルの2つについて論じている．

本論文は全5章からなり，ユビキタス環境におけるサービスモビリティ実現に向けた要件を明らかにし，その中でも特にサービスハンドオーバーとサービス発見におけるセキュリティ確保の重要性について論じ，それを実現するために Key-insulated 型と Identity-based 型の認証プロトコルを利用したセキュアなサービスハンドオーバーとサービス発見の手法を提案し，その設計・評価について包括的に論じている．

第1章は「序論」であり，本論文の目的と全体構成について述べている．

第2章は「背景」であり，ユビキタスコンピューティング環境におけるサービスのあり方について議論し，ユビキタスコンピューティングにおける要素技術の一つとしてサービスモビリティに着目し，その実現手法について従来技術を含めて議論している．さらに，サービスモビリティの実現においてはセキュアなサービスハンドオーバーとサービス発見が重要となることに触れ，従来研究ではサービスモビリティにおけるセキュリティが十分に検討されていないことを指摘している．また，これを受けて，セキュアなサービスモビリティ実現に向けた課題を明らかにし，認証プロトコルの必要性とそれを評価する形式検証技術である BAN 論理について概要を説明している．

第3章は「サービスモビリティを支援する認証プロトコル」と題し，セキュアなサービスハンドオーバーを実現する認証プロトコルについて，その詳細を述べている．本章ではモビリティサポートを実現する従来技術である Mobile IP，SIP(Session Initiation Protool)，mSCTP(Mobile Stream Control Transmission Protocol)などのプロトコルとサービスハンドオーバーとの関係について議論を行い，これら従来技術では，特にセキュリティ的な観点から十分なサービスモビリティを実現することが困難であることを指摘している．これを受けて，セキュアなサービスモビリティを実現するための要求用件を明確にし，多様なデバイスに跨ってセキュアなサービスハンドオーバーを行う際にはサービス ID（あるいはセッション ID）のセキュアな共有を行うユーザ認証と，ユーザのプライベート鍵漏洩問題への対策を行うデバイス認証が必要であることを述べている．次いで，それら問題を具体的に解決するために，Key-insulated 型の公開鍵暗号化方式を用いる認証

プロトコルと Identity-based 型公開鍵暗号化方式を用いる認証プロトコルの 2 つのプロトコルを提案し，BAN ロジックによりそれらプロトコルの検証を行っている．加えて，それら 2 つのプロトコルの比較を行い，実際的な課題についても議論を行っている．

第 4 章は「セキュアなサービス発見」と題し，サービスモビリティにおいてサービスのハンドオーバー先のデバイスを発見するためのサービス発見プロトコルについて述べている．本章では，ユビキタスコンピューティング環境ではディレクトリサービス等の集中型のサービス発見プロトコルがサービスモビリティを十分にサポートすることが困難であることを指摘し，その場で動的にサービス発見が可能なプロトコルの必要性を述べている．これを受けて，アドホックなサービス発見をサポートする Bluetooth SDP(Service Discovery Protocol)，GSD(Group based Service Discover protocol)，DEAPspace などのサービス発見プロトコルについて議論を行い，これら従来技術ではシームレスなサービスモビリティをセキュアに実現することが困難であることを指摘している．次いで，アドホックなサービス発見プロトコルのセキュリティ要件を明らかにし，Identity-based 型の公開暗号化方式を用いたサービス発見プロトコルによりそれら用件を満足するプロトコルが実現できることを示している．

第 5 章は「結論」であり，本論文の成果をまとめるとともに，セキュアなサービスモビリティ実現に向けて残された課題，および今後の研究の方向性について述べている．

以上これを要するに，本論文はユビキタスコンピューティング環境におけるセキュアなサービスモビリティを実現するための認証プロトコル群を設計し，その有効性を検証したものであり，情報学の基盤に貢献するところが少なくない．したがって，本論文は博士（科学）の学位論文として合格と認められる．