6Z-1

組み込み機器連携における端末認証機構

坂本　昂之†　　久保田　稔‡
千葉工業大学大学院工学研究科†‡

1.はじめに

昨今の組み込み機器は，センサの高性能化や無線通信機能などにより高性能化が進んでいる．我々は様々な機能を持つ組み込み機器がネットワークで結合し，機器同士が連携・動作することにより，様々なサービスを実現できるシステム（動的適応システム[1]）の開発を進めている．

ネットワークに接続された組み込み機器には外部からの不正利用や不正アクセスといった脅威が想定される．これによりユーザが要求するサービスが実現できずに停止してしまう問題がある．一方，組み込み機器は十分なリソースを持たないため，一般のセキュリティ方式をそのまま適用することは適切でない．本稿では，組み込み機器連携に適したユーザの認証機構とアクセス制御機構を提案する．

2.想定するシステムモデルと問題点

2.1. 動的適応システムモデル

本研究が対象としている動的適応システムでは，通信機能やノード上で実行されるソフトウェア単位である MSC（Micro Software Component）を持つノードを M ノード（Micro Node），それらのノードが構成する無線アドホックネットワークを M ネットワーク（Micro Network），M ネットワークを管理するノードを MNM（Micro Node Manager），複数の M ネットワークの情報を管理するノード MNGM（Micro Node Group Manager）と呼ぶ．動的適応システムモデルの概要を図 1 に示す．

M ノードは組み込み機器やセンサなどで，環境の至る所に存在するものとする．MNM はユーザが持ち歩く携帯端末を想定する．ユーザからの要求や使用環境に応じて，MNM が M ネットワーク内の M ノードの MSC を動的に組み合わせ，サービスを提供する．

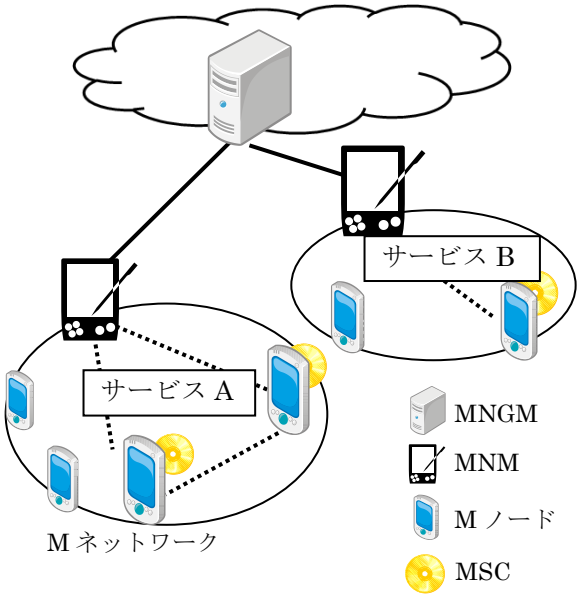

図 1. 動的適応システムの概要

2.2 動的適応システムの問題点

現在の動的適応システムの実装では，不特定多数のユーザがシステムを利用する際に十分な信頼性が保証されておらず，以下の 2 つの問題点がある．(1)悪意あるユーザが MNM を通して，なりすましや不正利用による情報漏洩を行なう可能性がある．(2)複数の MNM 間で競合する M ノードまたは不正アクセスや改竄によって不正となった M ノード，が存在することによりサービスが正常に動作しない場合がある．これらの脅威や問題に対処するため，ユーザの認証とサービスを構成する各 M ノードに対するアクセスの制御が必要となる．

3. 関連研究

ID・パスワードや Cookie 情報のような認証情報を携帯電話内に保管し，非接触 IC 通信などを利用して他端末上でも認証が行える認証システム[2]がある．端末に保管された認証情報を他端末と通信して認証を行なう手法とされているが，Wi-Fi や ZigBee 等の近距離無線通信には対応していない．また，各情報資源に対する認証とし

Authentication Mechanism for Cooperating Embedded Devices
†Takashi SAKAMOTO,‡Minoru KUBOTA
†‡Graduate School of Engineering, Chiba Institute of Technology

Copyright ©2013 Information Processing Society of Japan.
All Rights Reserved.

てシングルサインオン（SSO）を用い，ルールベースに基づいて認可されたサービスを変更させるシステム[3]がある．SSO は Web アプリケーションを対象に認証を行なうため，複数の組み込み機器を連携したサービスに対しての認証に利用した研究はされていない．

本システムでは，組込み機器に対応した近距離無線通信（M ネットワーク）と，MNM による認証，それに伴い生成された証明書を利用することで，組み込み機器連携に適した認証と複数のサービスの実行が可能となる．

4.提案手法

4.1.認証機構

2.2 で述べた問題(1)に対し，以下の特徴をもつ認証機構を提案する．システム利用開始（ログオン）時に MNM で 1 回の認証を行うことで，以後は使用環境が変化しても追加の認証無しに複数のサービスを利用可能とする．本認証により，なりすましによる悪意あるユーザのアクセスを制限し，不正アクセスや情報漏洩等の脅威を低減することができる．ログオン認証の仕組みを図 2 に，手順を以下に示す．

1. ユーザは MNM でシステムを起動する．
2. MNM はユーザが MNM の所有者であるか端末が記憶する認証情報（ユーザ ID・パスワード）を基に認証を行なう．
3. MNM の認証機構によって認証が成功すれば，当該ユーザの正当性を保証する情報を含む認証証明書を生成する．
4. 認証証明書は MNGM とユーザが利用するサービスに必要な MSC を持つ M ノードへ送信され，サービス実行中それぞれで管理される．

サービス変更時やログアウトする際，M ネットワークの切断やタイムアウト処理とともに認証証明書は破棄される．

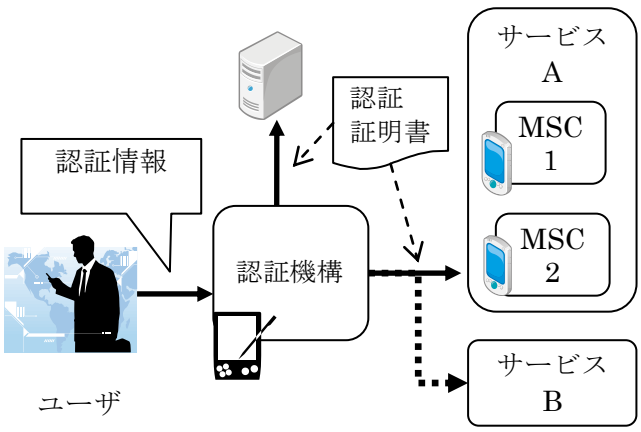

図 2.ユーザと端末間のログオン認証

認証証明書は，認証機構によってユーザが認証された際に，システムに対して MNM の正当性を示す情報となる．MNGM は，生成された認証証明書を受け取り，これを基にユーザ ID と利用しているサービス等の状態を管理する．これにより，MNM による不正アクセスの脅威に対してアクセスの制限を行なうことが可能となる．

4.2.アクセス制御機構

2.2 で述べた問題(2)に対してサービスを構成する各 MSC に役割（ロール）を割り当て，必要な M ノードへのアクセスを制御する RBAC（Role Based Access Control）方式のアクセス制御機構を提案する．このため MNGM で管理するすべての M ノードの IP アドレスや MSC をリストとしてまとめたファイルを使用する．このファイルから，ユーザが利用できるサービス毎に必要な MSC を持つ M ノードにロールを割り当てる．あるサービスに必要なロールを割り当てた複数の M ノードの集合をサービスロールとする．

MNM では認証証明書とサービスロールを組み合わせ，どのユーザが要求するサービスに必要な M ノードの MSC を使用しているかを各 M ノードへ送信する．これにより，利用しようとする他の MNM に対してアクセス制限を持つようになるため，M ノードに対する競合や不正アクセスや改竄などを防止し，サービス利用時の安全性を高めることが可能となる．

5.まとめ

端末認証機構のプロトタイプを作成し，MNM（Android 端末）と M ノード（Sun SPOT）へ実装し，動作することを確認している．本稿で提案した手法によって，想定される外部からの脅威に対処することができるため，ユーザは安全にシステムを利用することができる．今後，提案手法であるアクセス制御機構の実装を進める．

参考文献

[1]久保田稔, “動的適応性をもつモジュラー型基盤ソフトウェアの提案,” 信学技報(CPSY), Vol.105, No.670, pp.19-24, 2006.
[2]梅澤克之, 萱島信, 手塚悟, “携帯電話を認証情報の保管庫として用いる端末連携認証システムの提案,” 信学技報（MoMuC）, Vol.110, No.290, pp.73-78, 2010.
[3]田中美里, 廣安知之, 三木光範, “条件に基づく認可を実現するシングルサインオンシステム,” 第 70 回情処全大(3), pp.425-426, 2008.

Copyright ©2013 Information Processing Society of Japan.
All Rights Reserved.