5G－4

ホームネットワークをターゲットとした複数端末でのマルチメディアサービスにおける認証方式の検討

益崎　将一†　中西　智則†　桐本　直樹‡　小菅　昌克‡　蓮池　和夫‡
†富士通関西中部ネットテック株式会社　‡㈱エイ・ティ・アール環境適応通信研究所

1. はじめに

ホームネットワークを想定し、適応的ＱｏＳ制御方式[1][2]に基づいた複数端末を利用したマルチメディアサービスの実現方法を検討してきた。複数端末でのマルチメディアサービスを実現する場合に、利用ユーザの要求により複数端末へのサービスの分割が考えられる。その際の端末の不正利用や、サービスの横取りなどの不正行為を防ぐ為にセキュリティ面での考慮が必要である。そこで上記の特性に適したサービス利用認証方式の検討を行った。

2. ホームネットワークの課題

将来、家の中で人々がマルチメディア通信端末を携帯装着して生活するようになることで、自分の好きな時間を過ごしながらも家族とコミュニケーションをとることが可能となる。この携帯端末で個人間のコミュニケーションを行う為のアプリケーションとして、画像、音声、動画、音楽などを組み合わせたマルチメディアサービスを提供する。しかし、現在の携帯端末では限られたリソースしか利用できず、サービス内容によっては満足を得られない場合がある。そこで、ユーザが移動した場合に、近くにある利用可能なリソースの多い端末がそれぞれの音声、動画などの品質や優先度をより高いレベルに制御する仕組みがあれば、より充実したサービスを提供できる。例えば、ユーザが携帯端末で動画をみながらコミュニケーションをしていた場合、近くに大きなモニターがあれば、ユーザの選択により、大きな画面で表示する（図１）。

このようなサービスをホームネットワークで実現する場合にいくつかの問題点が考えられる。複数端末にサービスの分割や移動を行う場合に、移動先の端末は、共用端末であるが為に誰でも操作が可能となってしまう。しかし、家庭内においてもプライバシーが必要であり、端末の不正利用やなりすまし行為を防ぐ必要がある。そのような仕組みとして、多くの認証方式が提唱されているが、今回はKerberos[3]を利用することで実現する。

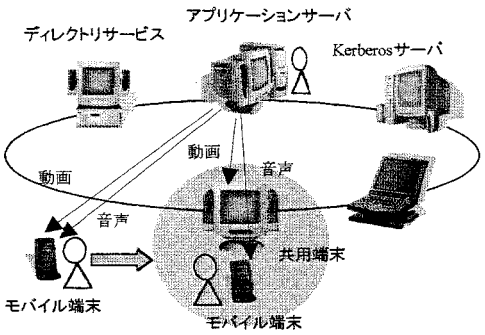

図１サービス提供イメージ

3. 認証方式

3.1. Kerberos

Kerberosは、ネットワーク上で提供されている各種サービスに対して、ユーザの認証を行う認証方式である。Kerberosは、共通鍵暗号方式を使用し、信頼のおける第三者機関の条件下で認証を行う。信頼できる第三者機関として、ユーザの認証を行う認証サーバ（AS）とサービス利用の認証を行うチケット配布サーバ（TGS）と、サービスを利用するユーザ端末から構成される。ASは、ユーザの認証を行い、そのユーザにTGSに提示する為のTGTを発行する。TGSは、ユーザからのTGTを検証し、ユーザに対してサービスの利用許可書であるチケット

A Study of Authentication System Using Multimedia Service on Multiple Terminals
Masakazu MASUZAKI†, Tomonori NAKANISHI†, Naoki KIRIMOTO‡, Masakatsu KOSUGA‡, Kazuo HASUIKE‡
†FUJITSU KANSAI-CHUBU NET-TECH LIMITED
‡ATR Adaptive Communications Research Laboratories

を発行する。ユーザは、このチケットをサービスに提示してはじめて、サービスを受けることが出来る。

3.2. 権限の代理行使

複数端末を利用したマルチメディアアプリケーションでは、複数端末を利用したサービス分割の利用が発生する。その際に、端末とサービスの不正利用を防止する必要がある。

上記アプリケーションのサービス分割のように、ユーザの代わりに、サービスが他の操作を実行できるように許可する必要がある場合、サービスはユーザの権限を、ある目的で利用できなくてはならない。しかし、ユーザのすべての情報（ユーザパスワード、共通鍵情報など）をサービスに渡し、操作を実行させることは、サービスが利用する特定の目的以外の権限を持ち、ユーザになりすますことが出来てしまう為、望ましくない。そこで、Kerberos の代理可能チケットを利用した権限の代理行使を利用する。ユーザはサービスに代理行使を与えることで、ある特定の目的でサービスがユーザの権限を利用できるように許可することができる。

現在、ユーザが、モバイル端末でアプリケーションサーバから音声と動画のサービスを受けている。(この時点で、ユーザがアプリケーションサーバからの音声、動画のサービスを利用する認証は終了している。)このうち動画サービスだけをモニターの大きい共用端末に移したいとする。この際は、ユーザが共用端末を利用し、アプリケーションサーバの動画サービスを受けることになる。つまり、アプリケーションサーバの動画サービスが共用端末を利用する為の認証が発生する。そこで、アプリケーションサーバの動画サービスにユーザの代理権限を与えることで、動画サービスがユーザに成り代わり認証を受け、共用端末を利用することができる。

4. 実現の方式

本提案を検証するために、図２のような構成を持ったフレームワークを検討している。

本フレームワークは適応的ＱｏＳ制御方式の検討[2]時に作成したフレームワークを拡張（拡張部分は、網掛け部分）することで実装する。

このフレームワークは、２つの部分から構成されている。１つ目の端末制御は、端末内に唯一存在し、端末内で実行される様々なサービスを管理する機能を提供する。管理機能には、実行されるサービスに対してのユーザ認証機能、サービス移行時には代理可能チケットを利用した権限の代理行使を使う機能等が含まれる。２つ目は、個々のサービス内に実装され、ユーザの要求するサービス品質で実際のサービスを提供する部分である。また本フレームワーク内に実装されている Kerberos 暗号化通信機能を利用し、ネットワーク内に流れるデータを暗号化することも可能である。

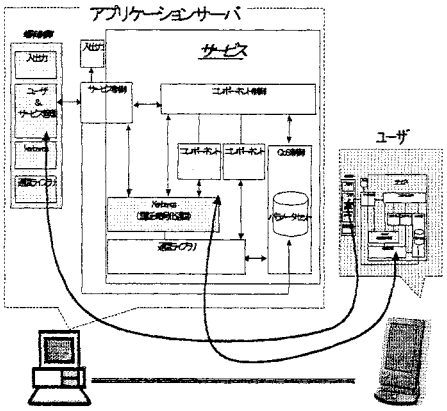

図２フレームワーク構成図

5. おわりに

現在、図２のフレームワークを用いたマルチメディアアプリケーションを実装中であり、今後実機上での評価を行う予定である。

【参考文献】

[1] 小菅，山崎，荻野，松田，“マルチエージェントによる適応的ＱｏＳ制御方式”，信学会論文誌，Vol. J82-B No. 5, pp. 702-710, 1999

[2] 益崎，小菅，蓮池 “適応的ＱｏＳ制御方式に基づく複数端末でのマルチメディアサービスの検討”，情報処理学会　第６１回全国大会　2G-2, Oct. 2000

[3] J. Kohl and C. Neuman : The Kerberos Network Authentication Service (V5), RFC1510, Sept. 1993.