ITS サービスのための路車間認証方式の提案

2T－6

卯木 輝彦　降旗 智樹　八木 正和
技術研究組合 走行支援道路システム開発機構 沖電気研究室

1. はじめに

走行支援システム(AHS)は、スマートカー(知能化された自動車)とスマートウエイ(知能化された道路)が協調して、ドライバーに対する情報提供、警報、操作支援を行い、安全で安心な走行を実現し事故の削減を図るシステムである[1]。このような AHS を含む高度道路交通システム(ITS)では、システムの安全性を確保するために高いセキュリティレベルの情報通信システムが必要であり、車載器とサービスの間の認証は不可欠である。路車間通信を利用する場合、路車間通信データ量が少なく、より短時間で可能な認証方式が要求される。RADIUS[2]や SSL[3]では、車が移動し路側アクセスサーバが替わったときに、認証手続きを再度行う必要がある。第三者認証のKerberos[4]は、複数のチケットが転送されるため、路車間通信データ量が多い。

本研究では、チケットを用いた第三者認証方式において、路車間通信を削減することを試みた。路側システム内に個別の車に対応するエージェントを導入し、エージェントがチケットを保持することにより、安全性を損なわずに、路車間のチケット転送が不要になった。本稿では、路車間の認証シーケンスを中心に、方式の概要について述べる。

2. システムモデル

ITS の路車間通信には、国際標準として検討されている狭域通信 DSRC (Dedicated short range communications)が使われる。システム導入当初、局所的なサービスゾーンが不連続に配置され、車は、一つのサービスゾーンを短時間で通り抜ける。図 1 は、本方式を適用した ITS システムの構成例である。

ログインサーバは、Kerberos における KDC に相当する。クライアントである車載器を通してユーザを認証し、車載器とサービスサーバを接続するためにチケットを発行する。

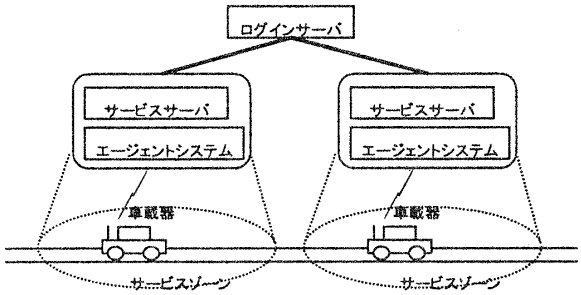

図1 ITSシステムの構成

エージェントシステムは、ログインサーバの要求に応じて、エージェントの生成を行う。エージェントは、車載器ごとに作られ、ログインサーバが発行したチケットを保持する。エージェントは、対応する車載器が存在するエリアのエージェントシステムに置かれ、車載器の移動とともにエージェントシステム間を移動する。

サービスサーバには、ITS サービスを提供するプロセスが置かれる。実際は、サービス内容に応じて適当な階層構造が構成されるが、この例では、サービスエリアごとにローカルな一つのサービスサーバを配置した。

3. 認証プロトコル

プロトコルは、Kerberos をベースにした第三者認証方式である。クライアント(車載器)とサーバの間にエージェントを導入することにより、クライアントのメッセージ交換を削減した。また、認証要求時に公開鍵暗号方式を用いることにより、ユーザが匿名のままサービスを利用することを可能とした。サービスサーバの認証は必須であるが、車載器の認証はプライバシー保護の観点からオプションである。

図 2 は、認証に関するシーケンスである。ログインサーバ(LS)とサービスサーバ(S)、および LS とエージェントシステム(AS)は、各々、事前に安全な方法で交換した秘密鍵 Kls、Kla を共有している。また、LS は車載器(C)を利用しているユーザの公開鍵 PKu

---

Trusted Third Party Authentication for ITS Services.
Teruhiko UNOKI, Tomoki FURIHATA , Masakazu YAGI
unoki@okilab.oki.co.jp, { furihara275,yagi300}@oki.co.jp
Advanced Cruise-Assist Highway System Research Association,
Oki Electric Industry Laboratory.
10-3, Shibaura 4, Minato-ku, Tokyo, 108-8551, Japan.

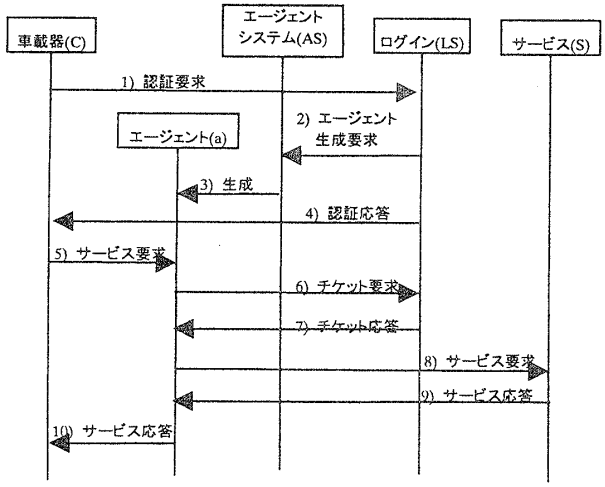

図2 認証シーケンス

を、C は LS の公開鍵 PKl を含む証明書を事前に入手しているものとする。各メッセージの概要を次で説明する。

1) 認証要求：C は、LS に、PKl で暗号化したユーザ名 uid およびユーザの署名を送る。LS は、署名により正規ユーザからであることを確認する。ただし、匿名ユーザの場合には、ユーザ名の代わりに適当な乱数 R を送り、ユーザ確認は行わない。
2) エージェント生成要求：LS は、AS に、Kla で暗号化したセッション鍵、およびチケット交付チケット(TGT)を送る。KSca は、C とエージェント(a)間で使われる。TGT には、LS の親鍵で暗号化したセッション鍵 KSla が含まれる。KSla は、LS と a 間で使われる。
3) エージェント生成：AS は、エージェントのインスタンス a を生成する。このとき、TGT を a に保存する。a は、C によって使われる。
4) 認証応答：LS は、C に、KSca と uid を PKu で暗号化して送る。匿名ユーザの場合は、R を鍵として共有鍵暗号方式により暗号化する。
5) C－a 間サービス要求：C は、a に、利用したいサービス名 sid および適当な文字列 r1 を KSca で暗号化して送る。
6) チケット要求：a は、LS に、TGT と sid を送る。
7) チケット応答：LS は、TGT から KSla を取り出し、a に、KSla で暗号化したセッション鍵 KSas、および sid を利用するためのサービスチケット T を送る。T には、Kla で暗号化した KSas が含まれる。KSas は、a と S 間で使われる。
8) a－S 間サービス要求：a は、S に、T と KSas で暗号化した適当な文字列 r2 を送る。
9) a－S 間サービス応答：S は、T から KSas を取り出し、a に、r2 を加工した文字列 r2'を KSas で暗号化して送る。a は、r2'により S が KSas を知っていることを認識する。
10) C－a 間サービス応答：a は、C に、r1 を加工した文字列 r1'を KSca で暗号化して送る。C は、r1'により a が KSca を知っていることを認識する。

以上のメッセージ交換により、車載器とサービス間の認証ができる。認証要求から認証応答までは、車載器起動後に一度だけ実行すればよい。エージェントが保持するチケットが有効期限内であれば、チケット要求／応答も省略できる。車の移動に伴ってエージェントが移動するため、サービスゾーンが変わって再接続する際の手順が少ない。また、チケットが路車間で転送されないため、Kerberos と比較して、路車間通信が少ない。

4. まとめ

AHS を始めとする ITS に適した認証方式として、エージェントを導入した第三者認証を提案した。これにより、比較的少ない路車間通信で、ユーザとサービスの相互認証が可能となる。ITS のセキュリティは、ITS 情報通信プラットフォームの共通の枠組である分散オブジェクト環境上に構築されることが望まれている。この認証方式についても、今後、そのための精緻化を行い、Jini[1] や CORBA などの分散オブジェクトで実装および評価を行う予定である。

なお、本研究は建設省土木研究所の委託を受けて実施しているもので、引き続きご指導を仰ぎながら研究を進めて行く。

参考文献

[1] 技術研究組合走行支援道路システム開発機構：第 3 回 AHS 研究報告会資料、1999.
[2] C.Rigney *et al.*: Remote Authentication Dial In User Service(RADIUS), *Internet RFC2138*, 1997.
[3] A.O.Freier *et al.*: The SSL Protocol Version 3.0, *Internet-Draft*,1996.
[4] R.M.Needham *et al*:Using encryption for authentication in large networks of computers. *Comm. of ACM*, 1978.

1. Jini は、米国 SunMicrosystems,Inc.の商標である。