モバイルコンピューティングと
ワイヤレス通信　23－15
高度交通システム 11－15
（２００２．１１．２８）

DSRC通信環境下でのSingle Sign-On技術を用いた暗号通信路確立方式の性能評価

渡邉茂道　前川貴宏　松尾真一郎　橋川善之　坂本弘章　古山俊文　田村成美
株式会社　ＮＴＴデータ

概要

安全性、快適性、効率性を向上させることを目的として、ITS の研究が盛んに行われている。しかし、ITS 実現のためのセキュリティに関する研究は少ない。そこで筆者らはこれまで情報の秘匿性の保証が要求される無線通信でかつ移動時に通信時間が限られる DSRC 通信環境下において、高速に暗号通信路を確立する方式を提案した[１]。本稿では、この提案方式のプロトタイプを開発し、DSRC 通信環境下での評価を行った結果について報告する。また、提案する暗号通信方式のアプリケーション適用領域についての検討結果についても報告する。

Evaluation of Efficient Secure Channel Constructing Scheme under DSRC Network

Shigemichi Watanabe Takahiro Maekawa Yoshiyuki Hashikawa Shin'ichiro Matsuo
Hiroaki Sakamoto　Toshifumi Furuyama　Shigeyoshi Tamura
NTT　DATA　CORPORATION

Abstract

The researches on ITS are actively carried aiming to improve safety, amenity, and efficient transportation. However the researches on ITS systems including the security are few. So we proposed the efficient secure channel constructing scheme for DSRC(Dedicated Short Range Communications) network or wireless network[1]. In this paper, we develop and evaluate this protocol under DSRC network and report these results. Moreover, the application domain of our proposal is discussed.

１．はじめに

現在、ITS サービスを実現する通信方式として、DSRC、携帯電話、無線 LAN 等様々な方式が利用され、各種情報通信サービスが実現されている。これらのサービスではいずれも無線を利用するために、情報の秘匿性を保証するには通信相手との暗号通信を実現することが必要となる。また、モバイル通信環境、特に DSRC や無線 LAN のようなスポット型通信環境では、移動速度の増加に伴い通信時間が限られるという特徴があり、限られた時間での処理が必要とされる。このような状況を踏まえ、筆者らは通信時間が限られる環境下で、高速に暗号通信路を確立する方式としてシングルサインオン技術を用いた暗号通信路確立方式を提案してきた［１］。本稿では、この提案方式のプロトタイプを開発し、DSRC システム環境下で行った評価・考察結果について報告する。

Evaluation of Efficient Secure Channel Constructing Scheme
under DSRC Network
Shigemichi Watanabe Takahiro Maekawa Yoshiyuki Hashikawa
Shin'ichiro Matsuo Hiroaki Sakamoto Toshifumi Furuyama
Shigeyoshi Tamura
NTT DATA Corporation
2-18, shiba 3-chome, Minato-ku, Tokyo 105-0014, Japan

以降、第 2 章では DSRC システム環境下での暗号通信路確立方式に対する課題をまとめ、それを実現する提案方式の概要について報告する。第 3 章では本方式の実現方式の概要について報告する。第 4 章では、本提案方式を DSRC システム環境に実装し評価を行う方法及び評価内容について報告する。さらに第 5 章では、第 4 章の評価方法に基づき評価した結果及び考察を示す。最後、第 6 章は本報告をまとめる。

２．提案方式概要

DSRC システム環境下において移動時に暗号通信を実現する場合、スポット通信であることから連続して通信可能な時間に制限がある。サービス提供に伴う一連の処理を限られた時間内で実現するためには、暗号通信路確立のための処理時間はできる限り短縮する必要がある。

一方、DSRC サービスが普及した場合、あるクライアントが複数のサービスを利用する状況が想定される。このような場合、新たなサービスを利用するたびに認証、鍵共有といった暗号通信路確立に伴う処理が必要となる。

上述の通り通信時間が限られている状況で、サービスを利用するたびに認証、鍵共有等の処理を行うのは非効率であると考えられ、これを一括して処理することができれば大幅な処理性能の向上が期待できると考えられる。この複数のサービスの認証処理を一括して行う方法として Single Sign-On(以下 SSO)技術がある。そこで、SSO 技術を利用し、認証を代行するサーバを用いて認証、鍵共有処理を集約する方式を提案する。

SSO を実現する代表的な方式として Kerberos がある。Kerberos は、共通鍵暗号方式を用いて認証および鍵共有を実現する方式であり、また、信頼できるサーバを用意し、クライアント～サーバ間のオフライン認証を可能としている。

図 1 に Kerberos の処理概要と適用上の課題を示す。図に示すとおり、Kerberos を用いて暗号通信を行う場合、店舗サーバと接続する前にまず、チケット発行サーバにおいて事前認証処理を行い店舗サーバに接続するためのチケットを入手する。次に、そのチケットを用いて店舗サーバと接続し、サービスの提供を受ける。

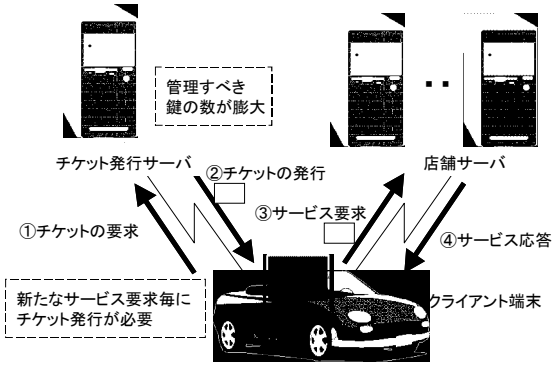

図 1　Kerberos の処理概要と適用上の課題

店舗が複数存在する場合、Kerberos のスキームを用いた方式では、サービスを利用するたびにチケット発行サーバと通信を行い、チケットを入手する必要がある。これでは通信毎にチケット発行の処理が必要となるため限られた通信時間内での処理には適さない。そこで本方式では図 2 に示す通り、サービス利用時の毎回のチケット発行処理を省略するために、Kerberos のチケット要求からサービス提供までの一連の処理をチケット発行とサービス処理の 2 つの処理に分割し、チケット発行処理において以後のサービス利用に必要となるチケットを一括して事前に発行する方式を提案する。サービスを利用する際には一括入手したチケットの中から必要なものを取り出して使用する。これによりサービスを利用する際にチケット発行サーバと毎回通信する必要がなくなるため、サービス利用時の暗号通信路確立に要する処理時間が大幅に短縮できる。

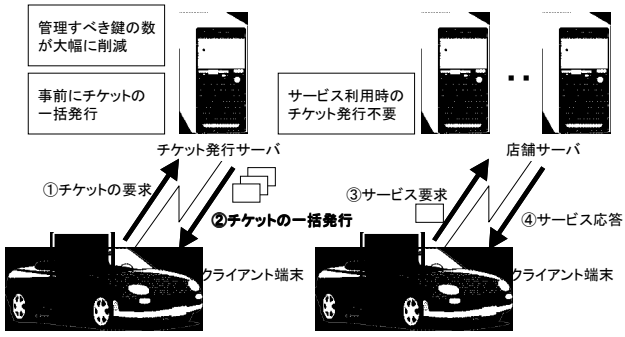

図 2　提案方式の概要

また、Kerberos ではクライアントが要求したチケットをチケット発行サーバが送信する際に、共通鍵を用いて暗号通信を行っている。共通鍵暗号方式を利用する場合、チケット発行サーバ側でもクライアントの鍵を共有し、管理する必要がある。クライアントが多数存在することが想定される ITS サービスのような場合、チケット発行サーバで管理すべき鍵の量は膨大となる。そこで本方式ではクライアント～チケット発行サーバ間で利用する暗号方式として、公開鍵暗号方式を利用する。クライアントがチケットを要求する際に公開鍵証明書を一緒に送付し、そこから公開鍵を取り出して暗号通信を行う。これによりチケット発行サーバでクライアントの暗号鍵を管理する必要はなくなり、管理すべき鍵の量は大幅に削減される。次章以降、本方式をセキュリティプロトコル(SP)と呼ぶこととする。

3．基本構成

セキュリティプロトコルを開発した際のプロトコルスタックを図 3 に示す。図に示すとおり、今回の開発においては DSRC システム以外にも流用可能とするため、通常の TCP/IP 通信上で動作するよう実装した。次にソフトウェア構成図を図 4 に示す。図に示すとおりチケット発行処理時はセキュリティプロトコルをチケット発行アプリケーションとして実装した。またサービス利用処理時は利用するサービスが様々想定されるため、ミドルウェアとして実装した。今回の評価においては、セキュリティプロトコルを評価するためのアプリケーションとして送ったデータをそのまま送り返してくるエコーバック処理と要求したデータを送り返すファイル読込み処理の二つを実装した。さらに、他のセキュリティモジュールの開発を容易にするため、暗号ライブラリと通信ライブラリに関しては共通化する形で実装した。なお、開発には C 言語を用い、基本暗号ライブラリには RSA を使用した。

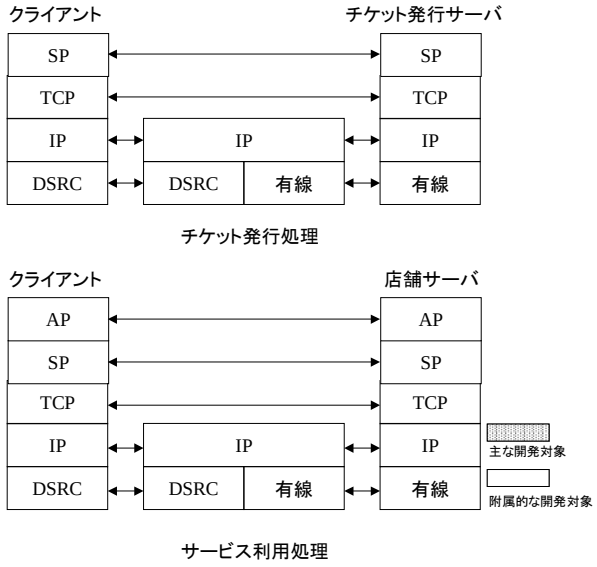

図 3　プロトコルスタック

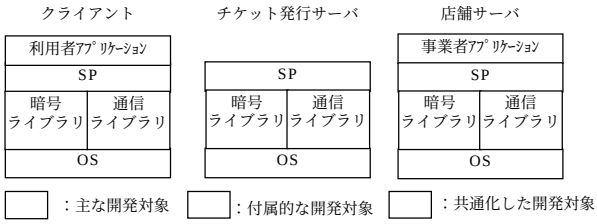

図 4　ソフトウェア構成図

４．評価

4.1 評価内容

評価はシステムの基本性能評価とセキュリティプロトコルの評価の二つを行った。具体的には以下の通りである。

①システムの基本性能評価

セキュリティプロトコルの評価を行う上で使用するシステムの性能を把握するために行う。具体的には、セキュリティプロトコルが IP をベースとして動作するよう開発されているため、ping 等を使用して IP レベルの遅延時間、パケット廃棄率及びスループットを計測し評価する。

②セキュリティプロトコルの評価

評価システム上にセキュリティプロトコルを実装し、大別すると停止時と走行時の二つの評価を行う。

停止時は、チケット発行処理時におけるチケット発行枚数の影響、同時アクセスの影響、サービス利用処理時における送受信データサイズの影響、同時アクセス数の影響をそれぞれ処理時間で評価する。

走行時は、チケット発行処理時のチケット発行可能枚数、サービス利用処理時の送受信可能データサイズのそれぞれを限界値で評価する。

4.2 評価項目

①システムの基本性能評価

システムの基本性能評価項目は以下の通りである。

（A）クライアント・サーバ間の遅延時間及びパケット廃棄率

（B）クライアント・サーバ間のスループット

②セキュリティプロトコルの評価

セキュリティプロトコルの評価項目は以下の通りである。

<<停止時>>

（A）チケット発行処理時の全体処理時間、サーバ処理時間、サーバとの通信継続時間

・全体処理時間

クライアントがチケット発行サーバへチケット要求メッセージを送信してから、チケット発行サーバよりそのチケットを受け取りチケットの内容を抽出するまでの時間

・サーバ処理時間

チケット発行サーバが、チケット要求メッセージからメッセージ内容の抽出を行い、チケットの応答内容を生成するまでの時間

・サーバとの通信継続時間

クライアントがサーバと接続している時間で、クライアントがチケット要求メッセージを送信してからチケットを受信するまでの時間（チケット発行処理を行うために継続した通信が必要となる時間）

（B）サービス利用処理時の全体処理時間、サーバでの認証処理に要する時間、サーバでのサービス利用処理に要する時間、サーバとの通信継続時間

・　全体処理時間

クライアントが認証要求メッセージを送信し、認証応答メッセージを受信し、サービス要求メッセージを送信し、サービス応答メッセージを受信するまでの時間

・サーバでの認証処理に要する時間

サーバが認証要求メッセージの内容を抽出してから認証応答メッセージの内容を生成するまでの時間

・サーバでのサービス利用処理に要する時間

サーバがサービス要求メッセージの内容を抽出してからサービス利用処理を行い、サービス応答メッセージを生成するまでの時間

・サーバとの通信継続時間

クライアントがサーバと接続している時間で、クライアントが認証要求メッセージを送信してからサービス応答メッセージを受信するまでの時間（サービス利用処理を行うために継続した通信が必要となる時間）

<<走行時>>

（A）チケット発行処理時のチケット発行可能枚数
一定速度で車両を走行させた状態で、無線通信の確立とともにチケット発行要求をかけ正常に受信できる限界のチケット枚数

（B）サービス利用処理時の送受信可能データサイズ
一定速度で車両を走行させた状態で、無線通信の確立とともにサービス要求をかけ正常に送受信できる限界のデータサイズ

4.3 評価システム
各評価を行う上で用いた評価システム構成及び機器の諸元を、それぞれ図 5、表 1 に示す。評価プラットフォームは T-75 の規格に基づき構築された DSRC 網と IPv4/v6 によるルーター網から構成されている。サーバは、チケット発行処理を行うチケット発行サーバとサービス利用処理を行う店舗サーバから構成される。また、クライアントは、計測を行う client1 とサーバへの同時アクセス数を増加させるための client2 から構成される。なお、同時アクセスの計測においては client1 からのアクセスと負荷側の client2 からのアクセスが極力同タイミングとなるようネットワークエミュレータを用いて、基本性能評価の実測値に基づき、表 2 の通り設定して計測を行った。

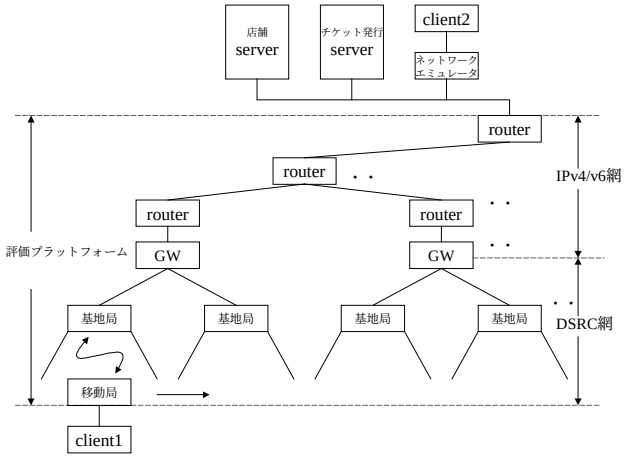

図 5　評価システム構成

表 1　評価に用いた各機器の緒元

クライアント1,2	
ホスト	PC/AT 互換機
ＯＳ	Microsoft Windows NT server4.0 SP5
ＣＰＵ	Pentium Ⅲ 1Ghz
メモリ	512 MB
ハードディスク	15GB
ネットワークカード	Intel 8255x-based PCI Ethernet Adapter
開発環境	Microsoft Visual Studio6.0(VB、VC)
暗号ライブラリ	RSA BSAFE SSL-C 2.0.1 RSA BSAFE Crypto-C 5.2.1
サーバ	
ホスト	SUN Ultra 10
ＯＳ	Solaris 2.6
ＣＰＵ	UltraSPARC-IIi, 2MB, 440MHz
メモリ	512 MB
ハードディスク	20GB
ネットワークカード	SunFastEthernet PCI Adapter 2.0
開発環境	SUN WorkShop 6.0
暗号ライブラリ	RSA BSAFE SSL-C 1.3 RSA BSAFE Crypto-C 5.0
ネットワークエミュレータ	
ホスト	PC/AT 互換機
ＯＳ	Microsoft Windows 2000 SP2
ＣＰＵ	Pentium Ⅲ 1GHz
メモリ	512M
ハードディスク	10 GB
ネットワークカード	Realtek RTL8139 Family PCI Ethernet NIC I-O DATA ET100-PCI-S Fast Ethernet Adapter
ソフトウェア	Cloud WAN エミュレータ 10Mbps

表 2　ネットワークエミュレータの設定値

パラメータ	設定値
回線速度(上り、下りそれぞれ)	Unrestricted
遅延時間	13[ms]を中心に標準偏差31[ms]の正規分布で発生
パケット廃棄率	0%

4.4 評価方法
①システムの基本性能評価方法
システムの基本性能評価は、図 5 に示すクライアント 1 に各計測ツールをインストールし、各ツールを使用して行う。システムの基本性能評価においては、次節のセキュリティプロトコルの評価結果を解釈する上で必要となるシステムの基本性能を評価する。

（A）クライアント・サーバ間の遅延時間及びパケット廃棄率の計測
計測概要を表 3 に示す。具体的には、サーバに fping コマンドをインストールし、そのコマンドを

使ってサーバからクライアント 1 に 1 秒毎に 84[byte]のパケットを送信し、その際の遅延時間及びパケット廃棄率を 1 時間計測する。計測地点はアンテナ直下から 20m 後方の地点とした。

表 3　遅延時間・パケット廃棄率の計測概要

計測時間	1 [h]
計測ツール	fping ver2.2b1
計測間隔	1[s]

（B）クライアント・サーバ間のスループットの計測

計測概要を表 4 に示す。具体的には、クライアント 1 に ftp クライントをインストールしておき、サーバに 1024[kbyte]のファイルを用意した状態で、クライアントから get 命令により、対象ファイルを取得するまでにかかる時間を計測することで、ダウンリンクのスループットを計測する。逆に、クライアントに 1024[kbyte]のファイルを用意した状態で、クライアントから put 命令により、対象ファイルをサーバ側に送信するまでにかかる時間を計測することで、アップリンクのスループットを計測する。アップリンク及びダウンリンクとも 1 分おきに 50 回続けて計測する。計測地点はアンテナ直下から 20m 後方の地点とした。

表 4　スループットの計測概要

計測時間	50[m]
計測ツール	ftp
計測間隔	1[m]

②セキュリティプロトコル評価方法

セキュリティプロトコル評価方法は、クライアント及びサーバに各セキュリティプロトコルのアプリケーションをインストールし、このアプリケーションの各設定パラメータを変更することで、処理時間を評価する。

【前提条件】

・初期起動プロセス数は 10、最大起動プロセス数は 50 とする

・同時アクセス数の計測は、クライアント 2 から複数アクセスし、サーバに負荷をかけた状態でのクライアント 1 の計測とする

＜＜停止時＞＞

（A）チケット発行処理時の全体処理時間、サーバ処理時間、通信継続時間の測定

クライアントから 100byte のチケット発行要求をかけ、当該枚数のチケットを取得するまでの各処理時間を計測する。これらの計測は鍵長 512bit、1024bit のそれぞれに対して 100 回ずつ計測し、平均値を算出する。チケット発行枚数の影響についてはチケット発行枚数を 1,2,4,6,8,10,12,14,16,18,20,30 枚に変えた場合の各処理時間への影響を計測する。

同時アクセス数の影響については、チケット発行枚数を 10 枚に固定しておき、クライアント 1,2 の合計したアクセス数が 1,2,5,10,15,20,25,30 となるようクライアント 2 からアクセス数を変えた場合のクライアント 1 の各処理時間への影響を計測する。

（B）サービス利用処理時の全体処理時間、サーバでの認証処理時間、サーバでのサービス利用処理に要する時間、サーバとの通信継続時間

クライアントから当該サイズのチケットのサービス要求をかけ、当該サイズのサービス応答を取得するまでの各処理時間を計測する。これらの計測は鍵長 512bit、1024bit のそれぞれに対して 100 回ずつ計測し、平均値を算出する。送受信データサイズの影響についてはエコーバック時には送受信データサイズを 100,500,1K,5K,10K,50K,100K に変えた場合の各処理時間への影響を、ファイル読込み時には送信データサイズを 50byte 固定とし、受信データサイズを 100,500,1K,5K,10K,50K,100K に変えた場合の各処理時間への影響を計測する。

同時アクセス数の影響については、サービス種別としてはエコーバック、ファイル読込みのそれぞれを実施した。サービス種別がエコーバック時の要求電文長は 10Kbyte、応答電文長は 10Kbyte とし、ファイル読込み時の要求電文長は 50byte、応答電文長は 10Kbyte とし、クライアント 1 のアクセス数を 1 にしておき、クライアント 1,2 の合計したアクセス数が 1,2,5,10,15,20,25,30 となるようクライアント 2 からアクセス数を変えた場合のクライアント 1 の各処理時間への影響を計測する。

＜＜走行時＞＞

（A）チケット発行処理時のチケット発行可能枚数

クライアントから 100byte のチケット発行要求をかけ、走行速度を 10,30,50km/h とした場合に発行可能なチケット発行枚数を上限を 1000 枚として計測する。これらの計測は鍵長 512bit、1024bit のそれぞれに対して 1 回ずつ計測した。なお、速度の計測においては事前にエリアの大きさを計測し、無線通信確立から切断までにかかる時間で割ることで算出した値を用いることとし、速度の揺らぎに関しては

1割の揺らぎまで許容することとした。

（B）サービス利用処理時の送受信可能データサイズ

エコーバックもしくはファイル読込みの要求をかけ、走行速度を 10,30,50km/h とした場合に送受信可能なデータサイズを計測する。これらの計測は鍵長 512bit、1024bit のそれぞれに対して 1 回ずつ計測した。

5．評価結果・考察

5.1 システムの基本性能評価結果

本評価システムの各計測における平均往復遅延時間及び標準偏差を表 5 に、パケット廃棄率を表 6 に示す。各表より、平均往復遅延時間は 25.3[ms]、標準偏差は 61.4[ms]、パケット廃棄率は 0%であり、遅延時間が短くパケット廃棄率が無いものの、遅延時間の標準偏差が大きいことから、比較的システムの揺らぎが大きいことがわかる。

表 5　平均往復遅延時間と標準偏差

平均往復遅延時間[ms]	25.3
標準偏差[ms]	61.4

表 6　パケット廃棄率

パケット廃棄率[%]	0.0

次に、本評価システムのアップリンク、ダウンリンクそれぞれの平均スループット及び標準偏差を表 7、表 8 に示す。各表より、平均スループットがそれぞれ 497.0kbps、461.9kbps であり、アップリンクとダウンリンクとも 450kbps 以上のスループットが確保されていることがわかる。なお、アップリンクとダウンリンクで値が異なるのは今回測定に使用した ftp クライアントの仕様によるものである。

表 7 平均スループットと標準偏差(アップリンク)

平均スループット[kbps]	497.0
標準偏差[kbps]	6.2

表 8 平均スループットと標準偏差(ダウンリンク)

平均スループット[kbps]	461.9
標準偏差[kbps]	1.6

5.2 セキュリティプロトコルの停止時の性能評価結果

5.2.1 チケット発行処理時のチケット発行枚数の影響

チケット発行枚数の影響を図 6 に示す。横軸はチケット発行枚数を示しており、縦軸は各処理時間を示している。チケット発行枚数の増加に伴い、各処理時間が増加している。全体処理時間には鍵長の違いが大きく現れているが、サーバ処理時間及びサーバとの通信継続時間については鍵長の違いはわずかであり、30 枚のチケット発行においては鍵長が 1024bit でも 350ms 程度の通信継続時間があればチケット発行可能であることがわかる。

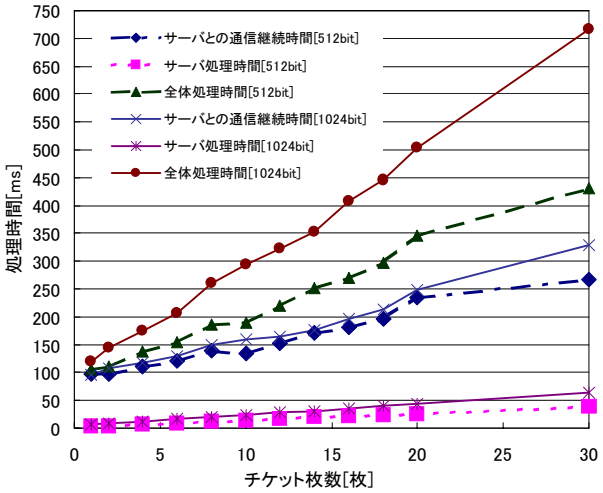

図 6　チケット発行枚数の影響

5.2.2 チケット発行処理時の同時アクセス数の影響

同時アクセス数の影響を図 7 に示す。横軸は同時アクセス数を示しており、縦軸は各処理時間を示している。同時アクセス数の増加に伴い、各処理時間が増加している。全体処理時間には鍵長の違いが大きく現れているが、サーバ処理時間及びサーバとの通信継続時間については鍵長の違いはわずかであり、同時アクセス数が 30 程度であれば鍵長が 1024bit でも 300ms 程度の通信継続時間があればチケット発行可能であることがわかる。全体処理時間、サーバとの通信継続時間に揺らぎがあるが、これは、基本性能評価結果に現れている値の範囲内のため得られた結果は妥当と考えられる。

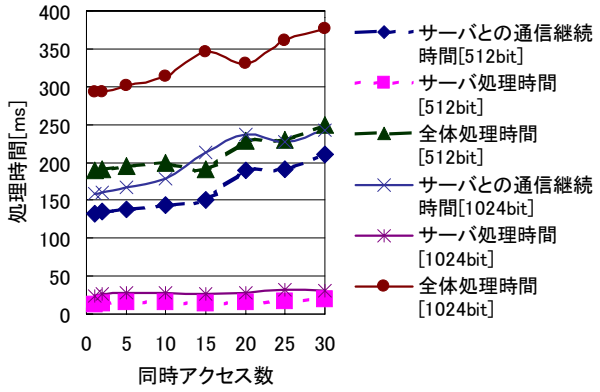

図 7　同時アクセス数の影響

5.2.3 サービス利用処理時の送受信データサイズの影響

エコーバック時及びファイル読込み時それぞれの送受信データサイズの影響を図 8、図 9 に示す。横軸はデータサイズを示しており、縦軸は各処理時間を示している。データサイズの増加に伴い、各処理時間が増加している。共通鍵での処理が主となるため、ここでは鍵長による違いがほとんど無いことがわかる。またグラフに示していないが、認証処理時間は今回の計測においては 1ms 程度であり、認証処理は十分高速に処理できることがわかる。

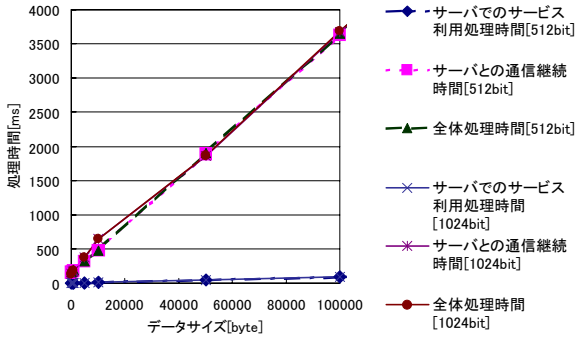

図 8　送受信データサイズの影響(エコーバック)

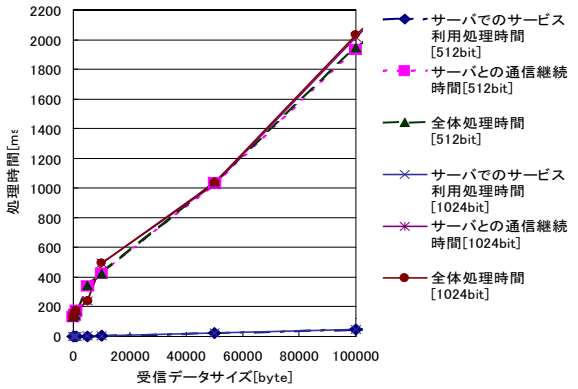

図 9　送受信データサイズの影響(ファイル読込み)

5.2.4 サービス利用処理時の同時アクセスの影響

エコーバック時及びファイル読込み時それぞれの同時アクセス数の影響を図 10、図 11 に示す。横軸は同時アクセス数を示しており、縦軸は各処理時間を示している。同時アクセス数の増加に伴い、各処理時間が増加している。全体処理時間、サーバとの通信継続時間に揺らぎがあるが、これは、基本性能評価結果に現れている値の範囲内のため得られた結果は妥当と考えられる。またグラフに示していないが認証処理時間は、今回の計測においては最大で 3ms 程度であり、認証処理は十分高速に処理できることがわかる。

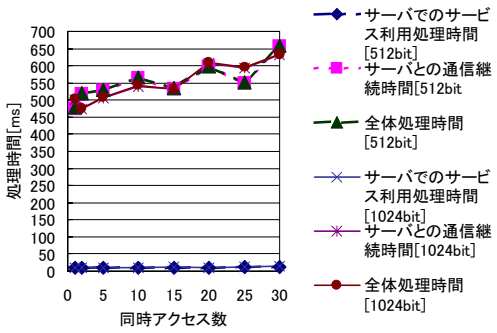

図 10　同時アクセス数の影響(エコーバック)

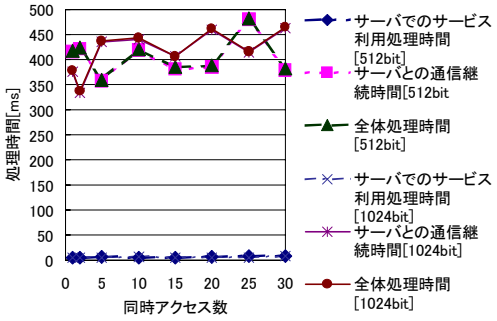

図 11　同時アクセス数の影響(ファイル読込み)

5.3 セキュリティプロトコルの走行時の性能評価結果

5.3.1 チケット発行処理時のチケット発行可能枚数

車両速度とチケット発行可能枚数の関係を示したグラフを図 12 に示す。横軸は車両速度を示しており、縦軸はチケット発行可能枚数を示している。

車両速度の増加に伴い、チケット発行可能枚数は減少している。また、鍵長が長くなることによりチケット発行可能枚数は減少している。これは図 6 のチケット発行枚数が少ない状態ではわずかであったサーバとの通信継続時間の差が、チケット発行枚数の増加に伴い、大きくなったために現れた結果と考えられる。

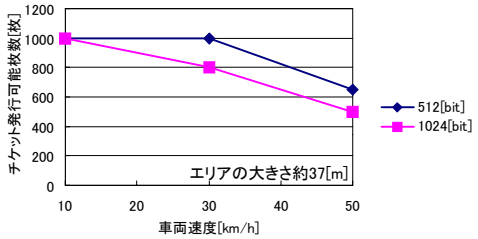

図 12　発行可能枚数への車両速度の影響

5.3.2 サービス利用処理時の送受信可能データサイズ

車両速度と送信可能データサイズの関係を図 13、図 14 に示す。横軸は車両速度を示しており、縦軸は送信可能データサイズを示している。車両速度の増加に伴い、送信可能データサイズは減少している。また、静止時の結果同様、鍵長による影響はほとんど見られないことがわかる。

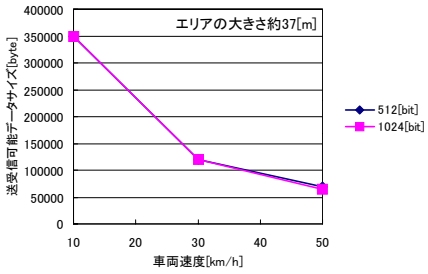

図 13　送受信可能データサイズへの車両速度の影響(エコーバック)

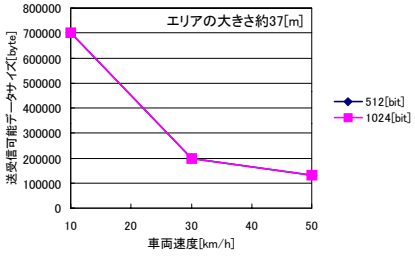

図 14　送受信可能データサイズへの車両速度の影響(ファイル読込み)

5.3.4 アプリケーション提供領域に関する考察

チケット発行処理に関しては走行試験の結果から 50km/h 以下の一般道を走行するような場合、鍵長が 1024bit の場合でも 500 枚以上のチケット発行が可能であることから、様々なアプリケーションへの適用が検討できると考えられる。また、停止時の試験結果から、仮に 90km/h で高速走行していたとした場合(通信時間では 1200ms)でも、30 枚程度のチケットであれば十分発行可能であることがわかる。したがって高速走行時においてはチケット発行枚数が 30 枚程度のアプリケーションに対して適用できると考えられる。

サービス利用処理に関しては走行試験の結果から 50km/h 以下の一般道を走行するような場合、鍵長が 1024bit の場合でも 65kbyte 程度のデータの送受信もしくは 130kbyte 程度のデータの受信が可能であることから、テキストレベルのＷＥＢブラウジング等のアプリケーションへの適用が考えられる。また、停止時の試験結果から、90km/h で高速走行していたとした場合(通信時間では 1200ms)でも、25kbyte 程度のデータの送受信もしくは 50kbyte 程度のデータの受信であれば可能であることがわかる。したがって高速走行時においては送受信データが 20Kbyte 程度のアプリケーションに対して適用できると考えられる。

6．まとめ

本稿では、ITS サービス特に DSRC 通信システムを用いた際に必要となる高速な暗号路生成のための一方式として提案したシングルサインオン方式を用いたセキュリティプロトコルを DSRC プラットフォーム上に実装して評価を行った。その結果、提案した方式が有用であり、多くのアプリケーションへの適用が可能であることが示された。今後は、本方式を実サービスに適用した場合の課題や改良点等明らかにし、さらに適した方式への改良を行っていく予定である。

謝辞

本研究は、通信・放送機構 (TAO) の委託研究「走行支援システム実現のためのスマートゲートウェイ技術の研究開発」の一環として実施されています。この場をお借りしまして、御礼申し上げます。また本評価を進めるにあたり、協力頂きました関係各位に感謝いたします。

参考文献

[1]前川他：“Single Sign-On技術を用いたモバイル通信における暗号通信路確立のための一方式の検討”情処　第62回　全国大会

[2]The Kerberos Network Authentication Service (V5)　RFC1510