ID ベース暗号を用いた車々間・路車間認証方式に関する研究

情報システム専攻　LE　XUAN　HIEU　　指導教員：井手口　哲夫　教授

1. はじめに

近年、自動車事故や渋滞を軽減するために、車々間・路車間通信を用いた衝突・追突防止などの安全運転支援サービスや渋滞などの交通情報を提供するサービスなどが普及されつつある。しかし、車々間・路車間通信システムにおいて様々なセキュリティ脅威が存在している。これらの脅威に対応するために、暗号技術を用いた発信元の真正性確認とメッセージの完全性や機密性を確保することは不可欠であり、車々間・路車間認証が重要となる。

本研究では、従来の公開鍵暗号より利便性が高いとされる ID ベース暗号を用いて、車々間および路車間の認証方式を提案する。実現可能性に関して交通システムの道路環境を前提に通信可能時間と処理・通信時間の割合について評価を行い、提案方式の有効性を示す。

2. ID ベース暗号

ID ベース暗号（*IBE: ID- based Encryption*）は ID 情報を公開鍵として利用できる公開鍵暗号方式ある。IBE の特徴は先に公開鍵　*(Pk: Public key)* を決めてから秘密鍵 *(Sk : Secret key)* を生成することである。秘密鍵 Sk を生成できるのは鍵発行センター*(KGC:Key Generation Center)*のみである。そのため、信頼できる KGC は必ず必要となる。

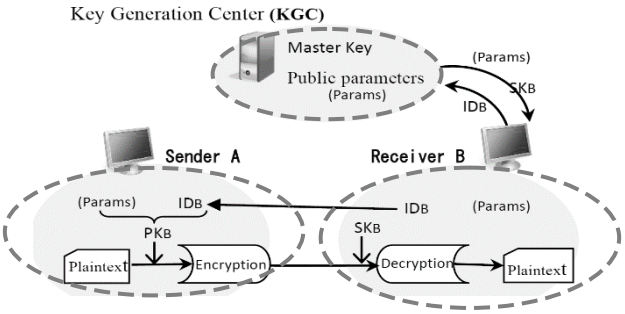

図１：ID ベース暗号

従来の公開鍵暗号に比べて ID ベース暗号は次のような利点を持っている 。

1. **公開鍵認証センターが不要**

送信者の公開鍵取得、公開鍵証明書作成、公開鍵証明書添付、公開鍵の検証などの処理が不要である。

2. **新規ユーザへの対応が容易**

新規ユーザを追加する際、ID 以外に新たに必要な情報を追加する必要はない。

3. **未登録者への送信が可能**

受信者の ID 入手できれば暗号文の作成ができるため、未登録者への送信が可能である。

運用面では、一つの KGC ですべての利用者の鍵生成を行う場合，KGC の負担が非常に大きくなるため、複数の KGC を階層的に用いて鍵生成を行う必要が生じる。階層型 ID ベース暗号(*HIDE :Hierarchical ID-Based Encryption*)は,ユーザを木構造の各ノードに対応させた ID ベース暗号で,各ノードは子ノードの秘密鍵を生成し，ノードの ID はルートノードまでのノード列となる。

3. 提案方式

階層型 ID ベース暗号を用いて、車々間・路車間の認証方式を提案する。

3.1 車両 ID

車両の ID は車両を特定するための一意的な情報であり、更新が困難である。安全性を高めるため、本論文の提案は短期限の鍵ペアを用いる。即ち、鍵ペアの有効期限が一日などの短時間であり、その期限を過ぎたら秘密鍵を更新する必要がある。そのため、固有 ID のかわりに時刻情報を追加したデータを ID データとして使う。

3.2 KGC の設置場所

鍵ペアの利用時間は短く、一定の期間中に更新する必要がある。利便性と現実性を考え、車両が走行中や休憩場所で秘密鍵を入手することができればよい。そのため、鍵発行センターは以下のような５つの場所に設置すると考えられる。

1. 高速道路の料金所(ETC ゲート)
2. 信号機
3. ガソリンスタンド
4. 充電スタンド
5. コンビニエンスストア

個々鍵発行センターの負荷を減らすために、階層型 ID ベース暗号を採用する。

3.3 処理の手順

3.3.1 車両の鍵ペア生成

鍵発行センターは５つの所に設置すると考え、５つのサーバが必要である。それらのサーバから発行した鍵ペアで認証や暗号通信を行うために、各サーバのマスターキーを同じ鍵発行センターで発行する必要である。

- **事前処理**

  各サーバ（子 KGC）はあるルート鍵発行センター (Root KGC) に自分の ID を送信し、秘密鍵生成を申請する。Root KGC は子 KGC の ID に対する秘密鍵を生成する。各子 KGC は秘密鍵をマスターキーとし、他の KGC の公開情報を取得する。ここまで、各子鍵発行センターの設定を完了する。

  車両は ETC セットアップのように車両 ID 管理センターに登録する。

- **車両の鍵生成**

  車両はいずれかの子 KGC へ自分の ID データを送信し、秘密鍵生成を申請する。子 KGC はその ID データに対する秘密鍵を生成する（図 2)。

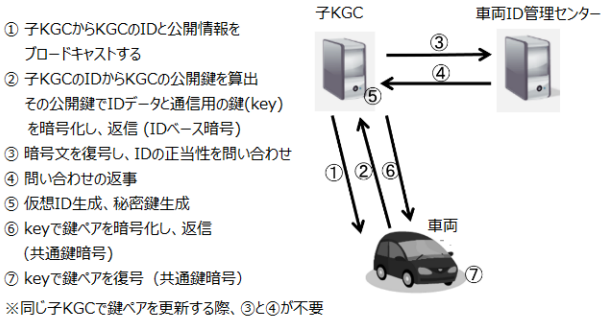

図 2：車両の鍵生成

3.3.2 車々間・路車間認証

走行する際、他の車または路側機と通信する時、先に認証を行う必要がある。図 3 に認証の手順を示す。X,Y は自動車または路側機である。

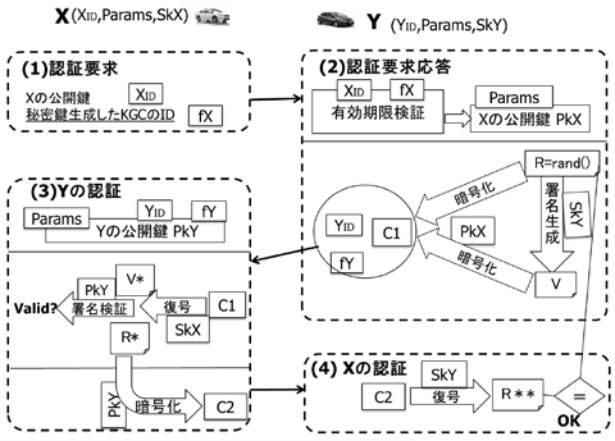

図 3：認証処理

(1) **認証要求**

送信側 X は自分の公開鍵（vID）データ(XID)と秘密鍵生成したサーバ ID (fX)を送信し、認証を要求する。

(2) **認証要求応答**

Y では、X と fX の有効期限を確認し、送信側の公開鍵 PkX を計算する。次に、ランダムにチャレンジデータ R を生成し、R の署名を作成し、送信側の公開鍵 PkX で暗号化する。Y の情報と暗号文と共に送信側 X に返信する。

(3) **受信側 Y の認証**

X では、まず YID と fY の有効期限を確認し受信側の公開鍵 PkY を計算する。次に、暗号文を復号し、R*と V*を得る。また、Y の公開鍵 PkY と R*で署名 V* を検証する。署名の検証ができれば、受信側 Y の認証が成功する。その後、Y の公開鍵 PkY で R*を暗号化し、Y に送る。

(4) **送信側 X の認証**

Y では、秘密鍵 SkY で暗号文を復号し、元のチャレンジデータ R と一致すれば、送信側 X の認証が成功である。

4. 評価

4.1 機能条件

- **車両の鍵生成**

  ID ベース暗号で安全に車両 ID データと key を送信することができる。KGC と ID 管理センターのやり取りで車両 ID の正当性を確認できる。key を秘密に交換できたため、車両の秘密鍵も安全に配布される。

- **認証ステップ**

  機器同士がお互いに正当性が確認でき、暗号通信で、不正行為が防止できる。鍵ペアの利用時間は短いため、安全性が高い。

4.2 処理時間の評価

① 条件導入:各ステップの通信可能時間の理論値を算出
② 処理時間測定:プログラムの実行時間で各ステップの処理時間を測定
③ 通信時間計算:通信方式のパケットフレームに基づいて通信時間を計算

処理・通信時間は通信可能時間に比較し、評価を行う。

表 1　処理・通信時間と通信可能時間の比較

処理	鍵ペア生成	車々間認証	路車間認証
通信可能時 A(ms)	1800	43200	8600
処理時間 B(ms)	1035.0	190.6	
通信時間 C(ms)	12.4	4.84	1.66
合計:D=B+C(ms)	1047.4	195.44	192.26
比例:D/A	58.2%	0.5%	2.2%

5. おわりに

階層型 ID ベース暗号を用いて、車々間(路車間)認証方式を提案し、評価を行った。提案方式で、安全に車両の鍵生成申請と取得することができる。認証処理で機器同士がお互いに正当性も確認できる。認証後、暗号通信でなりすましやデータ改竄の不正行為も防止される。また、高速度路と一般道において通信可能時間の理論値から条件を導入し、処理時間と通信時間を計算し、比較した結果により、秘密鍵生成のステップにおいて通信可能時間内に鍵生成と鍵配布が完了できる。車々間および路車間の認証のステップにおいて、処理・通信時間は通信可能時間の僅かな時間(3%以下)を占め、残り時間で十分に暗号通信を行うことができると考えられる。故に、道路において ID ベース暗号を用いる車々間および路車間の認証方式を適用することができると確認した。

参考文献

[1] LE XUAN HIEU、「高速道路における車々間通信システムへの ID ベース暗号の適用に関する研究」、平成 24 年度愛知県立大学情報科学部卒業論文、(2013/2)

[2] C. Gentry and A. Silverberg,“Hierarchical ID Based Cryptography” in Proceedings of Advances in Cryptology Asiacrypt 2002, Lecture Notes in Computer Science 2501, pp.548–566, 2002