マルチメディア通信と分散処理　106－19
コンピュータセキュリティ　16－19
（２００２．２．１４）

DSRC IPv6 網での位置登録要求の正当性検証機能の実装

世良田 照治
日本電気株式会社

DSRC(Dedicated Short Range Communication，狭域無線通信)を利用した DSRC IPv6 網[1]では，移動端末が網内のノードに向けて位置登録要求を送信して，IP 層でのハンドオーバを実現している．DSRC IPv6 網では，悪意を持った攻撃者が偽の位置登録要求を送信して，網内の経路制御を乱すことが可能という脆弱性がある．

そのような攻撃を防ぐため，位置登録要求に IPSec 認証ヘッダ[2]を用いた正当性検証機能を実装することにより，悪意を持った不正端末からの位置登録を排除し，網内の各ノードが持つ経路表の正当性を保持する機能を実現した．その結果，移動端末が高速に移動していても位置登録要求の正当性が検証可能であることを実証した．

A proposal for the validation function of mobile node registration process in DSRC IPv6 network

Teruharu Serada
NEC Corporation

In DSRC(Dedicated Short Range Communication) IPv6 network[1] environment, mobile nodes send registration requests to network nodes to realize IP-level handover function. In such an environment, there is a vulnerability that malicious users send bogus requests and destroy routing tables owned by each network nodes.

To mitigate this vulnerability, we propose the validation function of registration requests using IPSec AH[2]. This function protects the routing tables from unauthorized changes and keeps the routing tables sound as the result. Our implementation shows that the processing time overhead is small enough even if mobile node moves in highway speed.

1　はじめに

自動車の通信環境として利用が期待されているシステムに，DSRC がある．DSRC とは，自動車に設置された OBE(On Board Equipment，車載無線機）と道路に設置した RSU(Road Side Unit，無線基地局)の間の無線通信システムである．

DSRC IPv6 網[1]では，移動端末が位置登録要求を送信し，網側のノードが端末の位置を把握することによって，IP 層での移動サポート

を実現している．この網には，悪意を持ったユーザが不正な位置登録要求を送信すると，正当なユーザに通信が届かなくなってしまうという脆弱性があった．この脆弱性をなくすため，位置登録要求の正当性を検証する機能を実装した．また，検証の処理に必要な時間を計測し，十分に実用可能であることを実証した．

本稿では．2 節では DSRC IPv6 網の概要を述べる．3 節では DSRC IPv6 網が持つセキュリティ上の問題点を指摘し，その解決方法を述べる．4 節では，3 節の解決方法に対する具体的な実装方式について説明する．5 節では実装方式の性能評価結果を述べる．6 節では本実装方式の課題を述べ，最後に本稿の論旨をまとめる．

2　DSRC IPv6 網の概要

本節では，DSRC IPv6 網(以下 DSRC 網と省略する)を概説する．DSRC 網では，全ての車両が固定の IP アドレスを持つと仮定し，同一の IP アドレスを持つノードへの通信到達性を保持し続ける．

2.1　DSRC IPv6 網

DSRC は ETC(Electronic Toll Collection System，有料道路自動料金収受システム)で既に利用されており，車両情報，契約情報，料金所情報，車線・経路情報，料金収受情報などの送受信を路車間で行っている．また，DSRC の今後の利用形態として，駐車場，ガソリンスタンド，ドライブスルーなどでのキャッシュレスシステムへの応用や，車内でのモバイルショッピング，リアルタイム通信機能などへの展開が考えられている．

現在の DSRC は，RSU がカバーするセルの直径が 3m～30m 程度であり，例えば ETC の無線伝送方式では，OBE は 10mW 程度の低い出力で，1Mbps の通信を行うことが可能である[3]．今後，伝送速度の改良により 10Mbps 程度の通信の実現が期待されている．しかし，複数の RSU を跨ぐようなネットワーク利用が考慮されておらず，OBE と RSU の 1 対 1 のアプリケーションしか実現することができない．ETC 以外の様々なアプリケーションへの適用を可能にするためには，DSRC を利用して広域なネットワークへの接続を実現することが必要である．このような理由により，DSRC IPv6 網が開発された．DSRC 網は，Cellular IP[5]に代表されるマイクロモビリティ技術の 1 つである．この技術により，走行中でも RSU を切替えながら連続して通信を行うことが可能になった．

2.2　DSRC IPv6 網の構成

DSRC 網は高速な移動を低コストで実現するために，木構造のネットワークを採用している．葉(リーフ)の部分に DSRC 基地局を接続し，根元(ルート)の部分で外部のネットワークと接続する．ノードの部分に移動サポート機能を追加したルータを置く(図 1)．

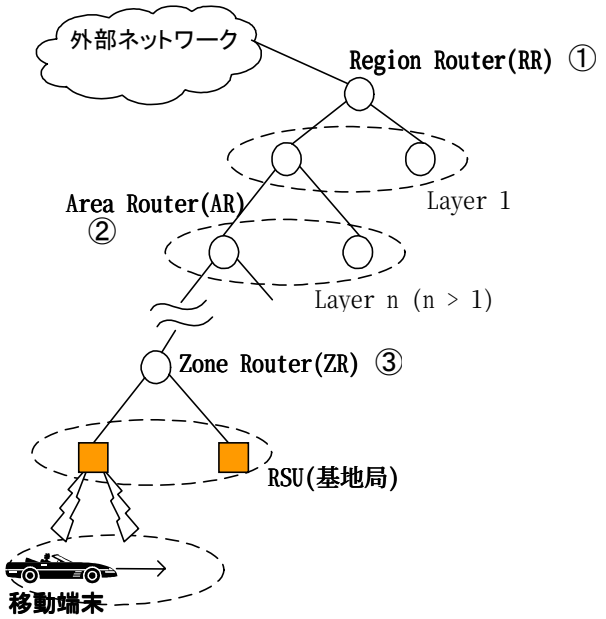

図 1. DSRC IPv6 網

木構造の根元のルータを RR(Region Router，図 1 の①)，葉の部分にある基地局の一段上の

ルータを ZR(Zone Router，図 1 の③)，それ以外のルータを AR(Area Router, 図 1 の②)と呼ぶ．

2.3 経路制御と移動管理

網内の各ルータでは，移動端末への経路を別々に保持する．つまり，移動端末が使用している基地局が接続されている ZR から RR までの経路上の全てのルータ(図 2の R1～R4)で，移動端末への経路情報を保持する．この経路情報は，移動端末毎に管理する．移動端末宛のパケットは，各ルータ上で上記経路情報を参照して，下位のルータに転送される(外部ネットワーク→R1→R2→R3→R4→移動端末)．移動端末から送信されたパケットは，上記とは逆に，各ルータの上位のルータに転送され，外部のネットワークに送信される．

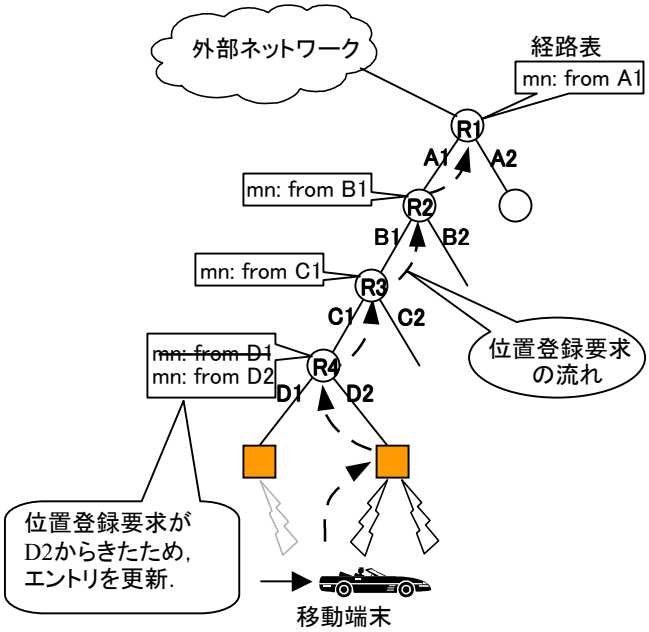

図 2. 位置登録要求の処理

移動端末への経路は，網内での基地局の移動に伴い更新される．接続する基地局が切り替わったことを移動端末が検知すると，位置登録要求という制御パケットを移動端末が送信する．位置登録要求は，ZR から RR に向けて配送される(図 2の破線矢印)．途中で中継を行うルータは，中継処理を行う際に，位置登録要求を送信した移動端末の経路を作成または更新する．図 2では，移動端末が D1 につながる基地局から D2 につながる基地局に移動したため，D1 のエントリを消去して，D2 のエントリに書き換えている．

3 DSRC 網のセキュリティ上の問題点

DSRC 網では，移動端末は位置登録要求を RR に向けて送信する．RR までの各ルータは，その位置登録要求を見て，自身が持つ経路表を更新する．移動端末の識別子は，IP アドレスである．各ルータは位置登録要求パケットのソースアドレスを見て，経路表を更新する．

DSRC 網では，悪意を持った端末が正当な移動端末と同じ IP アドレスを使用した場合，経路表の更新が可能になってしまう．この場合，正当な移動端末にはパケットが到達せず，悪意を持った端末に通信が到達する．IP アドレスは広く公開された情報であるため，誰でも簡単に網内の経路情報を乱すことができる．

このような脅威を防ぐためには，ルータが位置登録要求パケットの受信時に，正当な移動端末からのパケットであるかどうかを検証できるようにする必要がある．そのためには，位置登録要求パケットの送信者情報として，IP アドレスだけでなく移動端末の認証データを付加すれば良い．これにより，IP アドレスを騙るだけでは位置登録要求を偽造できないようにする．

認証情報を付加する方法には，IP 層での IPSec や IP 層より上位の層に位置する TLS を使用する方法などがある．しかし，

I. 位置登録要求は ICMP で送信される．
II. 移動端末の IP アドレスは，DSRC 網内では不変である．

という 2 点に着目すると，IPSec 認証ヘッダ

[2]で移動端末のIPアドレスの正当性を検証するのが最もふさわしいと考えられる.

ただし，移動端末は1つのRSUあたり最短0.6 秒程度で通過する可能性があり，かつ40,000 台程度の移動端末が同時にネットワークを利用するという条件を満たす必要がある. 1 つのRSU を通過する時間は最短で0.6 秒程だが, データリンク層でのリンクアップなども含めた合計時間が 0.6 秒である．IP 層のセットアップは 100 ミリ秒程度に抑える必要がある. 利用者の利便性を損なわずに目的を達成するため, 正当性を検証するのに必要な時間をなるべく少なくし, かつ制御系のデータ通信量をなるべく抑えて大量の移動端末からの要求を処理できる機構が必要になる.

4 実装方式

4.1 IPSec SA の確立

通常のIP 通信でIPSec を使用する場合，通信相手との間で使用する暗号アルゴリズムや共有する鍵の集合である IPSec SA[4]の確立手段として，以下の2つの手段が考えられる.

(1) IKE を用いて動的にSA を確立する

(2) 事前にIPSec SA を交換しておく

DSRC 網の場合, 1つのRSU あたり最短0.6 秒程度で通過してしまう可能性があるため, IKE を使用した動的なSA 確立は, 時間的制約から無理である．そのため，(2)のように事前にSA を確立しておくか, 高速道路入口など移動端末が低速で走行せざるを得ない地点で動的にSA を確立する必要がある.

今回は, システムの具体的な適用形態が明確になっておらず低速で走行できる地点を仮定できないため，事前にIPSec SA を共有しておくこととした. 無論，後で具体的にシステムを設置する段階で, 移動端末が必ず低速で通過する地点があれば，そこでIPSec SA の確立を行うことができる. 今回は, 確立されたIPSec SA を路側のルータと移動端末に格納できるインタフェースだけ用意しておく.

4.2 IPSec 認証ヘッダの適用方式

4.2.1 認証ヘッダを検証するノード

移動端末からの位置登録要求は，RR に向けて送信される．そのため，通常であればRR と移動端末の間でIPSec SA を確立し，移動端末が計算した認証ヘッダを RR で検証するのが望ましいと考えられる．しかし，RR は主要高速道路につき1台程度で, その配下では40,000 台程度の移動端末が RR を利用すると想定されている．各移動端末は，RSU 切替え時の他に一定間隔(1 秒)毎に位置登録要求を送信するため，検証するRR に相当の負荷がかかる.

また，RR で認証ヘッダを検証する場合，以下の手順となる.

① ZR が移動端末からの位置登録要求を受信.
② 上位のノード(AR ないし RR)に位置登録要求を転送.
③ ②を繰り返してRR が位置登録要求を受信.
④ RR にて認証ヘッダを検証．経路表更新要求を送信.
⑤ 上位のノードからの経路表更新要求を下位のノードに転送して，経路表を更新.
⑥ ⑤を繰り返して，ZR 内の経路表を更新.

この手順では，情報がZR からRR までを往復するため，AR が何段も重なっていた場合，経路表を更新するために必要な時間が，1 つのRSU を通過する時間を越えてしまうという問題点がある.

そこで, 位置登録要求の正当性検証と経路表の更新を短くするために，ZR で認証ヘッダの検証を行うこととした．この場合，手順は以下のようになり, より少ない手順で正当性を検証し経路表を更新することが可能である.

① ZR が移動端末からの位置登録要求を受信.
② ZR で認証ヘッダを検証する．検証した結

果が正しい要求のみ上位に転送する.

③ 上位のノードに位置登録要求を転送し, 経路表を更新する.

④ ③を繰り返し，最後に RR の経路表を更新する.

4.2.2 IPSec SA の配布方式

4.1節で述べたように, IPSec SA は事前に確立しておく. 認証ヘッダの検証を可能にするために，SA を網内にある ZR に配布する必要がある．その方式について考える.

最も単純な方法は，全ての ZR に IPSec SA を配置する方法である．IPSec SA の確立が終った時点で，網内の全ての ZR に IPSec SA を送信する．この方式をとった場合, 全ての移動端末が全ての ZR を使用するわけではないため無駄が多く, かつ移動端末の台数により大量の通信が発生する可能性がある．また，SA を更新した場合，全ての ZR に保存されている SA を更新する必要があるため, 運用管理コストもかかる．つまり，使用される可能性が高い ZR にのみ SA を配布することで網全体の通信の中で制御系通信が占める割合を抑え，かつ SA を管理する場所を減らして運用管理にかかるコストを低減できるような方式が必要となる.

IPSec SA の配布方式について考慮すべき点は，以下の 2 つである.

1. 網内のノードに IPSec SA を配布するか(push 形式)，網内のノードが必要に応じて IPSec SA を取りに行くか(pull 形式).
2. IPSec SA を分散させて管理するか，1 箇所で管理するか.

網内の制御用トラフィックを抑えるという観点では pull 形式が良く，管理コストを考慮すると 1 箇所で管理するのが良い. そこで, 今回は最初に RR に IPSec SA を保存しておき, 位置登録要求を受信した ZR が RR に向かって IPSec SA を要求する方式を採用した.

しかし，ZR が RR に向かって IPSec SA を要求する方式では，AR が何段も重なっていた場合，要求と応答に必要な時間が，移動端末が 1 つの RSU を通過する時間を越えてしまう可能性がある. そこで, ネットワークが木構造である点に着目し, 各ノードで IPSec SA を一時的に保存しておき, 処理時間を短縮させることとした．RR が ZR に SA を送信する時，途中にある AR が SA を保持しておく．使用する ZR が切り替わり ZR が RR に向かって SA を要求したとき, 途中の AR が当該移動端末の SA を持っていれば, その SA を送信する. AR と ZR での SA 保存は一時的なものであり, 移動端末がそれぞれの管理下を通過する時間が経過したら，SA を削除する．これにより，SA の配布に必要な通信量を必要最小限に抑え，かつ RR のみで SA を管理するため，運用管理コストも減らすことが可能になる(図 3).

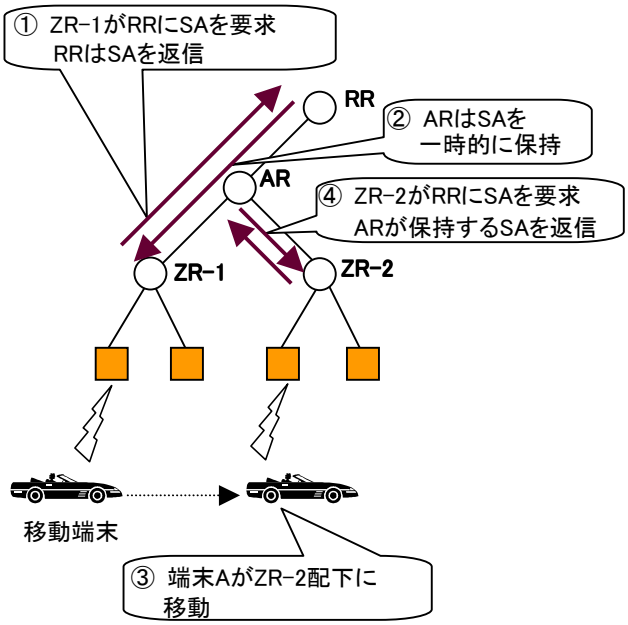

図 3. IPSec AH の適用方式

5 評価

前節で述べた方式が有効であるかどうか判断するために, 正当性検証の処理に必要な時間

を計測し, 処理時間をどれくらい削減しているか測定し，評価を行った.

以下の条件において, 正当性検証の所要時間を測定した.

- システム全体の移動端末台数: 1 台
- AR: 1 段

(1)ZR が SA を持っていてすぐに検証を行うとき, (2)上位に SA を要求し AR が返答した場合, (3)RR が返答した場合の 3 つの場合で, 検証が完了するまでの時間を計測した. 結果は，表 1 の通りである.

表 1. 認証ヘッダの検証が終了するまでの時間

(1)ZR が SA を持っていた場合	0.8 ミリ秒
(2)AR が SA を持っていた場合	3.6 〃
(3)RR が SA を持っていた場合	6.0 〃

移動端末 1 台で 5 ミリ秒程度時間を短縮し，検証の所要時間を 1 ミリ秒以下にすることが可能である．また，この方式では ZR が検証を行うため, 移動端末の台数が増えても RR での処理が輻輳しない．この結果により，本方式が十分に実用可能であることが実証できた.

6 課題

本方式では, IPSec 認証ヘッダを検証するノードが時間によって変化し, 認証ヘッダ内のシーケンス番号を管理するノードが存在しない. そのため, IPSec 認証ヘッダが持つ再送防止機能を使用することができない. 位置登録要求にはタイムスタンプが含まれるため, 最終更新時刻を管理することで同一ZR内での再送攻撃を防ぐことは可能である．しかし，ZR を跨ぐような再送攻撃については, 現時点では防ぐことができない．これについては，今後更なる検討が必要である.

7 おわりに

本稿では，DSRC 網に IPSec 認証ヘッダを適用して，位置登録要求の正当性を検証する機構について述べた.

DSRC 網では

- 1 つの RSU を通過する時間が極端に短いため，正当性検証に時間をかけられない.
- 多数の移動端末の移動をサポートする必要があるため, 制御系で必要な通信量を抑える必要がある.

という要求があるため，IPSec SA をノード毎に一時保存する方式を実装した. 実際に処理時間の計測を行った結果, 移動端末 1 台あたり 5 ミリ秒程度時間を軽減でき，1 ミリ秒以下で検証を行うことができた．これにより，本方式が有効であることが実証された.

今後は, 課題となる再送攻撃防止の機構についての検討を行うと同時に, 大規模シミュレーションで本方式の有効性を検証する予定である.

なお，本研究は，通信・放送機構からの委託研究である「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」の一部として行われた.

参考文献

[1] 水越,守屋, “DSRC IPv6 網による車両位置追跡機構の実現”, 情報処理学会 IPSJ ITS&MBL Vol.2000, No.112, pp.105-112, Nov 2000.

[2] S. Kent, R. Atkinson, “IP Authentication Header”, IETF RFC2402, Nov 1998.

[3] ARIB, “有料道路自動料金収受システム”, ARIB STD-T55, Nov 1997.

[4] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, IETF RFC2401, Nov 1998.

[5] Cellular IP
http://comet.ctr.columbia.edu/cellularip/