講演番号：60

C-V2X における否認防止可能な同報認証方式

B-15 Non-Repudiation Broadcast Authentication Methods for C-V2X Communication

河西 孝明† 小川 猛志†
Takaaki KASAI† Takeshi OGAWA†
† 東京電機大学大学院システムデザイン工学研究科
† Graduate School of System Design and Technology, Tokyo Denki University

1. はじめに

自動車や信号機などが感知した障害物等の情報を C-V2X 通信により同報しあうことで素早く危険回避できると期待されている．同報認証技術として TESLA[1]があるが，送信者が事後に送信を否認することを防止できないなどの問題があった．提案手法は，TESLA を拡張し，送信者と受信者の仲介機能を新しく定義し基地局に配備することで，それらの問題を解決した[2]．

2. TESLA の概要と問題点

(1)TESLA の概要 1:1 通信ではメッセージ認証コード(MAC)を適用することで第三者の改竄を防止できる．送信者はパケット毎に秘密鍵を用いて MAC を作成し当該パケットに付与し同報する．送受信者で秘密鍵を通信前に共有しておき受信者が受信パケットから計算した MAC とパケット内 MAC を比較することで改竄の有無を検証できる．だが同報の場合事前に秘密鍵を共有すると他受信者による改竄を防げない．TESLA は秘密鍵を一定周期で更新し遅延させて公開することで他受信者による改竄を防いでいる．なお秘密鍵は root 鍵からハッシュチェーンを作成し逆順に使用する．最初に使用する秘密鍵(以下K_{rt})にはデジタル署名が必要だが後続の鍵の本人性はハッシュの非可逆性から保証される．秘密鍵を使い切ると root 鍵とチェーンを更新する．

(2)TESLA の問題点 秘密鍵のチェーン途中から受信を開始すると次周期のK_{rt}受信まで MAC 認証できない．また秘密鍵公開後は誰でも MAC を生成可能なため送信者が送信を否認できる問題があるが未解決である[3]．

3. 提案手法

図 1 に提案手法の構成図を示す．基地局-送信者間，及び基地局-受信者間は移動網のハードウェア認証(AKA/SIM)によるセキュアパス通信ができると仮定する．また基地局は普遍的に信頼できるものとする．

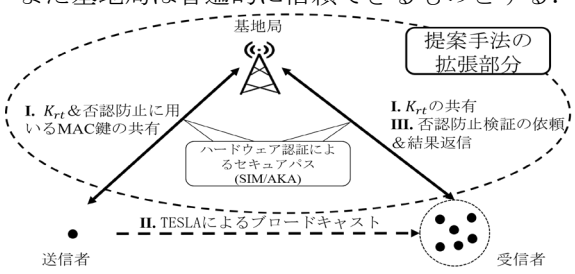

図 1．提案手法の構成図

3.1. K_{rt}の共有問題の解決

送信者はチェーン更新時に秘密鍵K_{rt} を基地局に登録し，受信者は基地局に接続時に基地局からK_{rt}を受信する．基地局は信頼できると考えているため， K_{rt}の本人性を送信者に代行して基地局が保証することができる．よって，送信者と受信者双方の TESLA のK_{rt} の検証に必要なデジタル署名の計算を省くことができる．また，必要なタイミングで基地局にK_{rt}を問い合わせることで，配布される秘密鍵の本人性を即時に確認できるため認証遅延をなくすことができる．

3.2. 否認防止問題の解決

否認防止用の MAC を新たに導入する．基地局は基地局のみが知っている一つの秘密情報と，各端末にユニークに割り振られている ID をハッシュし，送信者毎のK_{s_i}を生成し各送信者と共有する．送信者がデータを同報する際は既存の TESLA 認証で使用する MAC に加えて，各々の送信端末に配布されたK_{s_i}を使って否認防止用 MAC(NMAC)を生成し，各同報パケットに付与して送信する．基地局は全ての同報パケットの MAC と NMAC を検証し，NMAC のみ不整合の場合は送信者が事後の否認を試みたと判断し，当該送信者に割り当てていたリソースブロックを解放し，受信者に不正があったことを通知する．受信データに基づくアクションの結果事故が発生した場合など，受信者が受信データの否認を防ぐ証明書が必要な場合，受信者は当該パケットを基地局に転送する．基地局は受信パケット内の MAC と NMAC を検証し結果に基地局の署名を付けて受信者に返信する．以上により，受信者は基地局が当該パケットの送信元を保証する署名を入手できるため必要に応じて第三者に公開して送信者の否認を防止することができる．さらに，受信者は否認防止用の NMAC の生成はできないので，受信者が実際には受信していないデータを偽造し当該送信者から受信したと主張することもできない．

4. 実装と評価

C-V2X の通信形態を Wi-Fi アドホックモードで疑似し Raspberry Pi 上に実装し，送信間隔 5ms で 10 分間のパケット認証成功率と無作為抽出パケットに対する否認防止の成功回数を測定した．結果を表 1 に示す．

表 1．パケット認証成功率及び否認防止の成功回数

送信者＼受信者	認証成功数/受信パケット数/全送信パケット数 (認証成功確率/パケットロス確率)		否認防止成功数
	Ubuntu Server	Raspberry Pi 3 model B	
Raspberry Pi Zero WH	113625 / 113627/120000 (99.9%/94.7%)	119777 / 119779 /120000 (99.9%/99.8%) 119781 / 119783 /120000 (99.9%/99.8%)	100/100
Raspberry Pi 3 model B	119145 / 119147 /120000(99.9%/99.3%)	118272 / 118274 /120000 (99.9%/98.6%) 117891 / 117893 /120000 (99.9%/98.2%)	100/100

提案手法により RaspberryPiZero でも 5ms 間隔の同報通信及び否認防止可能な認証ができることを確認した．

5. まとめ

否認防止可能な同報認証技術を提案し，疑似環境での実装により有効性を示した．

参考文献

[1] IETF “rfc4082” https://datatracker.ietf.org/doc/html/rfc4082
[2] Takaaki KASAI, Takeshi OGAWA, "Non-Repudiation Broadcast Authentication Methods for C-V2X Communication," ICETC2022, IEICE.
[3] M. Muhammad, et al, "Efficient Distribution of Key Chain Commitments for Broadcast Authentication in V2V Communications," VTC2020, IEEE.