講演番号：43

# 低計算量で同報通信の否認を防止する方法

Non-Repudiation Methods of Broadcast Communication with Low Computational Complexity

上田 壱雅† 小川 猛志††
Ichika UEDA† Takeshi OGAWA††
† 東京電機大学工学部第二部情報通信工学科 †† 東京電機大学システムデザイン工学部情報システム工学科
† School of Engineering (Evening Division), Tokyo Denki University
†† School of System Design and Technology, Tokyo Denki University

## 1. はじめに

車両や路肩のセンサ(以下，ノードと表記)が路上の障害物の位置や速度などの情報をリアルタイムに感知し中継機を介さず直接同報しノード間で共有することで交通事故を回避する取り組みが進んでいる．10ms 程度の短い遅延時間で多数のパケットを交換できる必要があるが改ざんを防ぐためパケット毎の署名が必要である．署名には計算量の少ない TESLA の適用が望ましいが否認を防止できない課題が知られている．本稿では TTP が存在しない環境で TESLA の計算量を大きく増加させずに同報パケットの否認を防止する手法を提案する．

## 2. 既存技術の課題

同報パケット毎にデジタル署名を行うと任意の受信ノードが署名を検証できるが計算量が膨大になる．HMAC は計算量が少ないが署名鍵を事前に安全に共有しておく必要がある．TESLA は HMAC の鍵共有問題を解決し，少ない計算量で同報パケットの改ざんを防ぐ技術である[1]．TESLA では，同報サーバはランダムな値を $K_0$としてそのハッシュ値を $K_1$，更にそのハッシュ値を $K_2$として $K_n$まで $n$ 個のハッシュチェーンを生成する．通信時には図 1 に示すように $K_n$にデジタル署名して同報し，以後一定周期(例 5ms)の間同報するデータパケットには $K_{n-1}$ を共有秘密鍵として生成した HMAC 署名を付与する．その後周期が満了すると署名用の鍵を $K_{n-2}$, $K_{n-3}$と切り替えていき，遅延させて $K_{n-1}$, $K_{n-2}$, $K_0$をデータパケットに付与して公開する．$K_0$まで到達すると新しい $K_n$を生成して同報する．受信ノードは $K_{n-1}$のハッシュ値が $K_n$と一致すると $K_{n-1}$で署名され $K_{n-1}$の公開前に受信したデータパケットは当該同報サーバにより作成されたと判断する事ができる．しかし，署名鍵公開後は誰でも当該鍵を使用した署名を作成できるため，鍵公開前に作成した署名に対して署名者が事後に本人による署名ではないと偽証(否認)する可能性がある．同報データが事故の原因となる可能性もあるため，否認を防ぐ仕組みが必要である．基地局が TTP として仲介できる環境での対策の検討[2][3]があるが，本研究で目的とする，ノード間で直接通信を行い TTP が存在しない環境での検討はない．

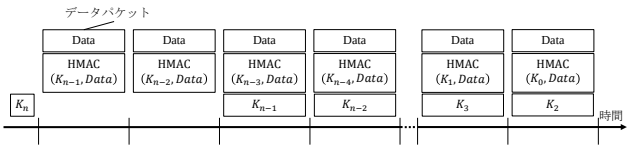


図 1 TESLA の通信手順

## 3. 提案手法

各ノードが受信した同報パケットを周期的に要約しそれらを鍵公開前に受信したことを証明するデジタル署名を付与して交換することで，TESLA と比べ計算量を殆んど増大させずに鍵公開後の否認を困難とする手法を提案する．

TESLA は周期的に $K_n$を更新しデジタル署名して同報する必要があるが，受信パケットの送信元同報サーバの ID，要約する同報パケットの通番の範囲及び Merkle tree により要約した Merkle root 値を本パケットに追加して同報する．ある同報サーバの同報パケット $P$の通番の範囲が $n-3$ から $n$ とした場合の，Merkle tree の構成例について図 2 に示す．

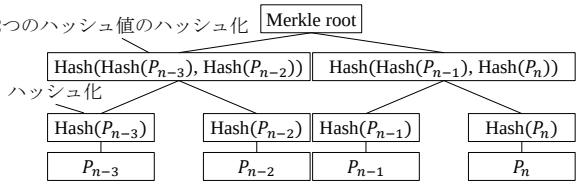


図 2 Merkle tree の構成例

ノイズの影響により一部の同報パケットを受信できない可能性があるが，各同報パケットに直前の $n$ 個の同報パケットのハッシュ値を XOR した値(32B)を付与することで，最大 $n$ 個の同報パケットが損失してもそれらを含んだ Merkle root 値の作成を可能とする．

TESLA とデジタル署名数が同じなので計算量は殆んど増加しない．通信量は $K_n$更新パケットは同報サーバの数×100B 程度，データパケットは 32B 程度増大すると見込む．

各ノードは他ノードから受信した全データを一定時間記録しておくことで，裁判などである同報サーバがある同報パケットへの署名を否認したとしても，その反証として使用することが可能となる．

## 4. まとめ

TESLA をベースとして少ない計算量で同報通信の否認を防止する手法を提案した．今後定量評価を進める．

## 参考文献

[1] IETF rfc4082.
[2] Ayan Roy-Chowdhury, John S.Baras, "Energy-Efficient Source Authentication for Secure Group Communication with Low-Powered Smart Devices in Hybrid Wireless/Satellite Nerworks", 2011
[3] Takaaki KASAI, Takeshi OGAWA, "Non-Repudiation Broadcast Authentication Methods for C-V2X Communication", 2022