2V-2

VANETにおけるネットワーク符号化通信の動的な署名検証制御

松川　智己†　　山本　泰資†　　廣友　雅徳‡　　毛利　公美††　　白石　善明†

†名古屋工業大学　　‡佐賀大学　　††岐阜大学

1　はじめに

車両台数は世界中で年々増加しており，それに伴って交通事故件数も増加している[1]．交通事故を未然に防ぐために，ITS（Intelligent Transport System）の開発分野の一つに安全運転支援がある．安全運転支援の取り組みの中に，右折車両の運転者が目視で確認することのできない対向車の挙動を画像情報として，提供するアプリケーション[2]や周囲の車両に警告メッセージを送信するアプリケーション[3]など周辺の交通情報を提供するアプリケーションの開発が行われている．

ITS は車車間で構築された VANET（Vehicular Ad-hoc Network）や道路に設置された路側機と車両間での路車間通信でデータを送受信する．このとき，電波干渉を受けるとパケットロスが発生する．パケットロスの影響を防ぐ方法としてネットワーク符号化の適用が考えられている[4]．ネットワーク符号化を適用した通信は複数のパケットを代数的に演算する符号化処理でまとめた符号化パケットを複数個送信し，欠落パケットを他の車両から受け取った符号化パケットで補間できる．

受信した複数のパケットの中に攻撃者による不正パケットが含まれていると，符号化処理で算出される符号化パケットも不正パケットとなる．符号化処理は各車両で行われるので，ネットワーク符号化を適用しない通信と比べて，ネットワーク符号化通信は不正パケットの影響が大きい．不正パケットを検出して破棄する要素技術として電子署名が挙げられる．VANET においてネットワーク符号化通信に電子署名を適用すると，各車両が受信したすべての署名を検証することで不正パケットの影響を防げる．しかしながら，交差点など車両密度が高くなる場所では，受信パケット数が増加し，署名の検証による処理時間が蓄積して通信遅延が大きくなる．通信遅延が大きくなると有効期限の切れるパケットが増加する．パケットは有効期限が切れると破棄されるので，各車両に到達するパケットの数が減少する．その結果，各車両で復号できるデータの数が減少する．

我々は，受信パケット数に応じて署名検証回数を制御することで，マルチホップ通信での検証にかかる処理時間を削減する手法を文献[5]で提案している．本稿では，ネットワーク符号化通信に電子署名を適用した代表的な通信モデルに[5]で提案した手法を適用して，各車両における到達したパケットと復号に成功した元データについてシミュレーション評価を行い，提案手法の効果を確認する．

2　VANET でネットワーク符号化通信に電子署名を適用したモデル

VANET においてネットワーク符号化通信に電子署名を適用したモデル（以下，通信モデル）は，各車両による送信処理，中継処理，受信処理の 3 種類の処理を行う Source，Forwarder，Sink で構成される．ネットワーク符号化は[5]のランダムネットワーク符号化の符号化処理に準ずるものとする．電子署名に用いる Source の検証鍵はあらかじめ PKI（Public Key Infrastructure）に登録，公開されており，署名鍵は各車両が秘密裏に所持しているものとする．Source，Forwarder，Sink にはそれぞれ次のような複数の処理パターンが存在する．Source はパケット単位に分割されたデータに対して，署名を作成する場合としない場合，署名の符号化を行う場合と行わない場合で処理フローが分岐するので計 3 種の処理フローがある（図 1）．Forwarder は，受信した符号化パケットから分割データを復号することなく署名の検証を行える場合と行えない場合，署名の符号化を行う場合と行わない場合で処理フローが分岐するので計 4 種類の処理フローがある（図 2）．Sink では，受信した符号化パケットから分割データを復号することなく署名の検証を行える場合と行えない場合で処理フローが分岐するので計 2 種類の処理フローがある（図 3）．図中の番号は，処理フローの種類を示す．これらの処理フローを組み合わせた 24 種類のフローパターンのうち，冗長なパターンを除くと表 1 のように 12 種類のフローパターンになる．本稿では，この 12 種類のフローパターンの通信モデルについて検討する．Source における分割処理は，送信する元データを N 個のパケット単位のデータに分割する．署名処理は，署名鍵を用いて，元データまたは分割データに対する署名を生成する．Source/Forwarder の符号化（A）処理はデータの符号化処理，符号化（B）処理は署名の符号化処理である．Forwarder/Sink における検証処理は，検証鍵を用いて受信した署名をすべて検証する．復号処理は N 個の符号化パケットから N 個の分割データを計算する．Sink の再構築処理は，復号して得た N 個の分割データから元データを取得する処理である．

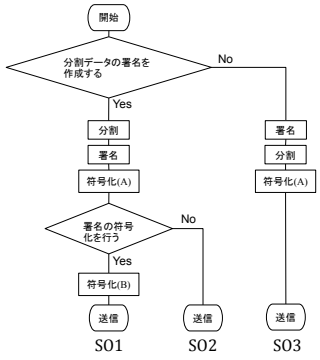

図 1 Source の処理パターン

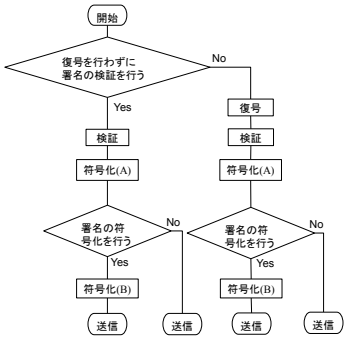

図 2 Forwarder の処理パターン

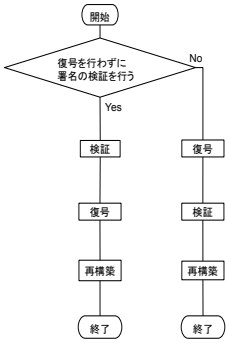

図 3 Sink の処理パターン

表 1 処理を組み合わせた通信モデル

通信モデルNo.	Source	Forwarder	Sink
1	SO1	F1	SI1
2	SO1	F2	SI1
3	SO1	F3	SI2
4	SO1	F4	SI2
5	SO2	F1	SI1
6	SO2	F2	SI1

通信モデルNo.	Source	Forwarder	Sink
7	SO2	F3	SI2
8	SO2	F4	SI2
9	SO3	F1	SI1
10	SO3	F2	SI1
11	SO3	F3	SI2
12	SO3	F4	SI2

3　署名検証回数の動的制御

VANET では車両密度が高い場所にいる車両は，そうでない

Dynamic Cotrolling Signature Verification of Network Coded Communication on VANET

† Tomoki Matsukawa, Taisuke Yamamoto and Yoshiaki Shiraishi・Nagoya Institute of Technology

‡ Masanori Hirotomo・Saga University

†† Masami Mohri・Gifu University

場所の車両に比べて，受信するパケットの数が増大する．マルチホップ通信では署名検証による処理時間が中継ごとに蓄積し，通信遅延が増加する．通信遅延の増加は，パケットの有効期限が切れる原因となる．文献[5]では受信パケット数Mに応じて，値が更新される検証確率αを各車両に導入し，受信したパケットに含まれている署名のうちV_n個だけ検証する手法を提案している．中継処理で署名検証の回数を制限することで，通信遅延を削減できる．α，V_nは以下の式で求められる．

$$\alpha = z_1 \exp\left(-\frac{M}{z_2}\right) \qquad (1 \le M) \qquad (1)$$

$$V_n = \lceil \alpha M \rceil \qquad (1 \le M) \qquad (2)$$

4 評価実験

4.1 実験内容

12 種類の通信モデルに文献[5]の提案手法を適用した通信と適用しない通信で，各車両に到達したパケットの総数のうち有効期限内に到達したパケットの割合と正確に復号することのできた元データの割合を評価する．各車両への到達パケット数の減少は元データの復号処理の失敗につながる．到達パケット数の減少は通信遅延の増加が原因であり，通信遅延は署名の検証回数と関係がある．表 1 の 12 種類の通信モデルを署名の検証回数の違いで分類すると，大きく 4 種類のカテゴリーに分けることができる．以降ではこの 4 種類を評価対象とする．対象の 4 種類の特徴は次のとおりである．

[カテゴリーA] Source は元データを分割した N 個の分割データに対して署名する．Forwarder/Sink は分割データを復号せずに署名を検証できる．通信モデルは表 1 の No.1，2，5，6 が該当する．この評価では No.1 を実装した．

[カテゴリーB] Source は元データを分割した N 個の分割データに対して署名する．Forwarder/Sink は分割データを復号してから署名を検証する．通信モデルは表 1 の No.3，4，7，8 が該当する．今回の評価では，No.3 を実装した．

[カテゴリーC] Source は元データに対して署名する．Forwarder/Sink は分割データを復号せずに署名を検証できる．通信モデルは表 1 の No.9，10 が該当する．この評価では No.9 を実装した．

[カテゴリーD] Source は元データに対して署名する．Forwarder/Sink は分割データを復号してから署名を検証する．通信モデルは表 1 の No.11，12 が該当する．この評価では No.11 を実装した．

4.2 実験方法

ネットワークシミュレータ OMNeT++4.0[6]を用いて評価を行う．OMNeT++4.0 の無線移動体通信用フレームワーク MiXiM1.1[7]を使用する．シミュレーションモデルは図 4 のような交差点を用いる．道路は歩道側から左折車両・直進車両・右折車両とする．元データのサイズは 7500[byte]で 1500[byte]に分割されて送信されるものとする．Source のデータ送信間隔は 100[ms]としてシミュレーションを行う．送信パケットの有効期限は安全運転支援システムの通信要件[8]に対応して 1000[ms]として，有効期限が切れたパケットは破棄する．Source が交差点から情報取得距離 R=50[m]以内の領域に入ったときにデータの送信処理を開始する．各車両が中継処理を行う間隔は 300[ms]として 1 つの署名を検証する処理時間は 100[ms]とする．500[ms]周期で不正パケットを送信する攻撃車両を 1 台配置する．MAC 層プロトコルは IEEE802.11b を用いた．通信帯域幅は 11[Mbps]とし，送信パケットは 10[mW]の送信電力で送信する．この評価では，提案手法を適用した通信で検証確率 α を求めるときに用いるz_1，z_2は 5.0，3.0 とする．シミュレーション時間は 2000[ms]である．シミュレーション時間内で各車両に到達したパケットのうち，有効期限内に到達したパケットの割合をパケット到達率とし，復号に成功した元データの割合をデータ受信率として測定する．そして，検証処理による通信遅延の蓄積に対する提案手法の効果を確認するために基準値を測定する．検証による通信遅延の増加が原因で有効期限切れパケットが発生しない通信でのパケット到達率とデータ受信率を基準値とする．基準値は検証処理時間を 0[ms]として測定した．

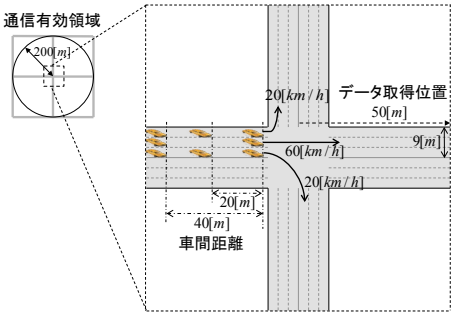

図 4 シミュレーションモデル

表 2 シミュレーション実験結果

	パケット到達率(%)			データ受信率(%)		
	提案手法を適用していない通信	提案手法を適用した通信	基準値	提案手法を適用していない通信	提案手法を適用した通信	基準値
カテゴリーA	42.1	60.4	86.1	41.5	56.9	84.6
カテゴリーB	63.1	65.3	84.3	58.8	60.3	79.8
カテゴリーC	39.2	56.9	86.3	37.9	53.7	83.1
カテゴリーD	63.3	64.5	85.4	61.1	62.3	81.4

4.3 実験結果

表 2 に実験結果を示す．提案手法をカテゴリーA，C に適用することで，パケット到達率とデータ受信率を基準値に近づけることができた．これは検証回数を制御することで検証の処理遅延を削減して，有効期限切れパケットの増加を抑えたことを示している．

ある Forwarder が M 個のパケットを受信したとすると，提案手法を適用していないときの A，C の検証回数 V_Mは V_M=M となる．Source が元データを N 個に分割していたとすると，M≧Nのとき，B，D の検証回数 V_Nは V_N=N となるので V_M≧V_Nとなる．M<N のとき，B，D は復号ができず署名の検証をしないので，V_M>V_Nである．ゆえに，A，C の方が B，D より検証回数が多くなるので，検証の処理遅延が大きくなり，A，C のパケット到達率とデータ受信率は B，D のそれらより小さくなる．

提案手法を適用しているとき，式(1)，式(2)より，V_Mは M 以下，V_Nは N以下となる．このとき，提案手法の適用による A，C と B，D の検証回数の減少数は，それぞれ M-V_M，N-V_Nになる．M≧N のとき，V_nは単調減少関数であるので，M-V_M≧N-V_Nが成立する．M<N のときは，B，D は検証できないので N=V_N=0 となり，M-V_M>N-V_Nが成立する．つまり，A，C は B，D に比べて提案手法の適用による検証回数の減少数が多くなる．検証回数の減少数が多いと検証の処理遅延が小さくなり，B，D に比べて A，C の方がパケット到達率，およびデータ受信率の増加量が大きくなる．

5 おわりに

本稿では，文献[5]の提案手法を各種の通信モデルに適用し，パケット到達率とデータ受信率を評価した．Forwarder/Sink で復号してから検証する通信より，分割データを復号せずに署名を検証できる通信の方が提案手法の効果が高いことがわかった．

参考文献

[1] R. Miller, Q. Huang, “An Adaptive Peer-to-Peer Collision Warning System”, IEEE Vehicular Technology Conference, pp.317-321, 2002.
[2] H. Sakai, M. Koyamaishi, K. Toyota, “Experiment of Safety Drive in an Intersection by Visual Assistances based on HIR System”, IEEE Intelligent Vehicles Symposium, pp.265-270, June 2003.
[3] R. Tatchikou, S. Biswas, F. Dion, “Cooperative Vehicle Collision Avoidance using Inter-vehicle Packet Forwarding”, Proc. IEEE Global Telecommunications Conference, pp.5, Dec. 2005.
[4] R. Ahlswede, N. Cai, S.-Y. R. Li and R.W. Yeung, “Network Information Flow”, IEEE Transactions on Information Theory, pp.1204-1216, July 2000.
[5] T. Matsukawa，T. Yamamoto, Y. Fukuta, M. Hirotomo, M. Mohri, Y. Shiraishi, “Controlling Signature Verification of Network Coded Packet on VANET”, Proc. the 12th International Conference on ITS Telecommunications, pp.679-683, Nov. 2012.
[6] OMNeT++，＜http://www.omnetpp.org/＞（参照 2013-0103）
[7] MiXiM，＜http://sourceforge.net/projects/mixim/＞（参照 2013-0103）
[8] ITS 無線システムの高度化に関する研究会作業班(第 4 回会合)資料 4-4，“アンケートとりまとめ結果 I ～利用イメージの明確化のためのアンケート～”，総務省事務局，2009 年 1 月．