1Z-2

VANETでのネットワーク符号化通信の署名検証回数について

松川 智己† 山本 泰資† 毛利 公美‡ 白石 善明†
名古屋工業大学† 岐阜大学‡

1. はじめに

高度道路交通システム（ITS：Intelligent Transport System）の構成要素に，車両アドホックネットワーク（VANET：Vehicular Ad-hoc NETwork）を用いて事故や渋滞などの位置依存情報を交換してドライバーの運転支援を行うというものがある．このようにITSでは重要な情報が転送されることもあるため短時間により多くの端末がデータを受信できることが要求される．

端末がデータを符号化して転送効率を向上させるネットワーク符号化[1]があるが，悪意ある端末から汚染攻撃を受けると汚染されたデータがネットワーク内の他の端末に広がり元の情報を正しく復元できなくなる．

汚染攻撃の影響を防ぐためには符号化パケットの検証ができればよい．送信端末が電子署名を付した送信データを送り，中継端末や受信端末が検証を行い，汚染データを破棄する．例えば文献[2]のような中継端末が受け取ったデータの署名を検証するネットワーク符号化のための電子署名方式が提案されている．

しかし，VANETにおいて各中継端末が受け取った全てのデータの署名を検証すると受信遅延が発生するなど通信品質の低下が考えられる．また，無線アドホックネットワーク上ではOverhearしてデータを受け取ることもあり既に他の端末が検証したデータを再度検証する可能性もある．

本稿では，全てのデータを検証することで発生する通信品質の低下を抑えるために，各端末が受け取ったパケット数に応じて署名検証の実行回数を変動させる手法が有効であるかを確認する基礎的検討を行う．ランダムネットワーク符号化通信方式をネットワークシミュレータ上で動作させ，署名検証の実行回数に対する有効期限内の正規パケットの受信率について評価する．

2. ランダムネットワーク符号化を用いた通信方式

[通信モデル]

ランダムネットワーク符号化[3]を用いた通信方式は送信処理，中継処理，受信処理をそれぞれ行う送信端末，中継端末，受信端末の3種類の端末からなるモデルである．中継端末が受け取った複数のパケットを線形演算して一つの符号化パケットとして他端末にブロードキャストする．その結果ネットワーク使用帯域削減，パケットロスの影響が軽減されスループットの向上につながる．

送信端末は送信する元のデータを N 個に分割してから符号化して送信する．符号化処理においては自身がランダムに生成する符号化係数を用いて符号化を行う．

送信する元データを用いて N 回の符号化処理を行って N 個の線形独立な符号化データ V を生成する．なお，符号化係数は毎回異なるので同じ入力データでも出力される符号化データは常に異なる．送信端末は N 個の符号化データと復号に必要な符号化係数のペアをパケットに含みブロードキャストする．

中継端末は送信端末の符号化処理と同様に自身がランダムに生成した符号化係数を用いて受け取った複数のパケットで線形演算を行い再符号化する．再符号化データと符号化係数をパケットに含みブロードキャストする．

受信端末は送信端末が送信した N 個のパケット，中継端末が再符号化して中継したパケットを含めて N 個以上の線形独立なパケットを受信すると復号できる．

[車々間通信によるブロードキャスト通信]

ネットワーク上の全ての端末が送信処理，中継処理，受信処理を行うものとする．

ここでは，交差点での通信を考え，各端末は交差点から一定距離 R[m]内の領域に入ると送信データを用意し符号化して送信する（送信処理）．また，一定間隔ごとに複数の保持パケットを1個のパケットに再符号化して中継する（中継処理）．パケットを受信した各ノードは，受信パケットが許容遅延の範囲内であれば復号する（受信処理）．

送信処理では，送信データのタイムスタンプをパケットに含めて送信する．タイムスタンプは受信処理で受信パケットが有効期限内かを判定するのに用いる．パケットは一定の送信間隔で送信する．送信端末の符号化処理ではPET[4]を適用する．

3. 署名検証について

前述したランダムネットワーク符号化を用いた車々間通信に署名の生成，検証を追加したものを考える．具体的には次のとおりである．

事前の準備として，送信端末の公開鍵は公開鍵基盤に登録され，公開しているものとする．

[送信処理]

Step1. 送信するデータ B を N 個に分割する．

$$B=\{b_1,b_2,...,b_N\}$$

Step2. 符号化係数 C をランダムに生成する．

$$C=\{c_1,c_2,...,c_N\}$$

Step3. 符号化係数 C とデータ B で $\mathrm{GF}(2^m)$ 上で線形演算して符号化データ v を生成する．

$$v=c_1b_1+c_2b_2+,...,+c_Nb_N$$

Step4. 端末の秘密鍵を用いて符号化データの署名 $\sigma(v)$ を生成する．

On Number of Signature Verification of Network Coded Packet for Vehicular Ad-hoc Network
†Tomoki MATSUKAWA, Taisuke YAMAMOTO and Yoshiaki SHIRAISHI ・ Nagoya Institute of Technology
‡Masami MOHRI ・ Gifu University

Step5. 符号化データ v，符号化係数 C，署名 $\sigma(v)$，タイムスタンプを含めたパケット P を構築する．
Step6. Step2～Step5 を繰り返して，N 個の線形独立なパケットを生成する．

$$\{P_i \mid i = 1,2,...,N\}$$

Step7. パケットを一定の送信間隔でブロードキャストする．

[中継処理]
Step1. 一定間隔内に受信したパケットのタイムスタンプが有効期限内かどうか調べる．有効期限内のタイムスタンプを含むパケットは受理し，期限外のパケットは破棄する．
Step2. 公開鍵を用いてパケットの署名を検証する．不正パケットが検出されたら破棄する．
Step3. ランダムに生成した符号化係数を用いて受理したデータを再符号化する．
Step4. 再符号化データ，符号化係数，署名，タイムスタンプを含めたパケットを構築する．
Step5. パケットを一定の送信間隔でブロードキャストする．

[受信処理]
Step1. 受信したパケットのタイムスタンプが有効期限内かどうか調べる．
Step2. 公開鍵を用いてパケットの署名を検証する．
Step3. パケットが N 個集まったらパケットに含まれている符号化係数を用いてデータ B を復号する．

各端末が受け取った全てのパケットの署名を検証すると通信品質が低下すると考えられる．そこで，署名検証を行う前に各端末は，検証確率 α に応じて中継間隔の間に受けとったパケットを検証する数を決める．つまり，中継処理の Step2 で M 個のパケットが検証対象となったときに，$q(\alpha) = \alpha M \quad (0 \le \alpha \le 1)$回だけ署名検証する．

4. 評価

α の値によって決まる検証実行回数は署名検証にかかるコストを調節するものである．この手法の効果を確認するために，以下のシミュレーションを行う．

【シミュレーションモデル】

図 1 のような交差点付近での自動車の動作を想定したシミュレーションを行う．

道路は片側 3 車線あり，歩道側から左折車両・直進車両・右折車両とする．直進車両は時速 60[km]，車頭距離 40[m]で速度を落とさずに交差点を通過するとする．右左折車両は交差点が混み合っている状況を想定して時速 20[km]，車頭距離 20[m]とする．送信データは 1500[byte]のパケットで送信されるものとし送信端末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文献[5]の ITS での安全運転支援システムの通信要件に対応して 1000[ms]とする．送信端末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．

有効期限内に送信端末はパケットを 10 個まで送信することができる．符号化・復号は $GF(2^8)$で演算する．送信データサイズを 3,6,9,12,15,18[KB]として評価する．なお，中継および受信処理での署名検証に要する時間は 15[ms]としている．

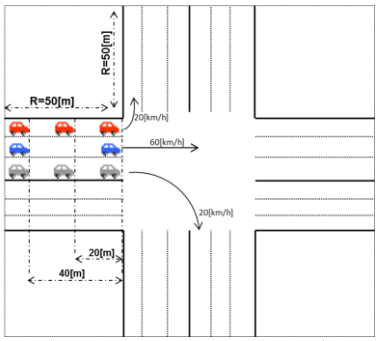

図 1 シミュレーションモデル

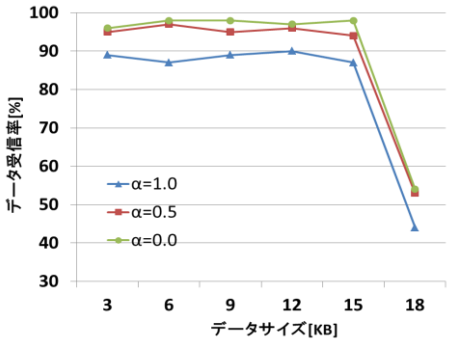

図 2 評価結果

【シミュレーション内容と結果】

検証確率 α が 0.0，0.5，1.0 のときの送信データサイズに対するデータ受信率を調べた．その結果を図 2 に示す．α=0 は署名機能がない通常の通信で，α=1 はすべてのパケットを検証する通信である．すべてのパケットを検証すると，中継端末や受信端末で検証処理による遅延が累積していき，有効期限を過ぎて破棄されるパケットが増えると考えられる．α=0.5 のとき，すなわち，中継端末で受信パケットの半分だけを検証するときにはデータ受信率がほとんど低下しないことがわかった．

5. おわりに

本研究では，全てのデータを検証することで発生する通信品質の低下を抑えるために，各端末が受け取ったパケット数に応じて署名検証の実行回数を変動させる手法を検討している．本稿では，その基礎的検討として，署名検証回数を変動させることでデータ受信率が変わることを確認した．

参考文献

[1] R. Ahlswede, N. Cai, S.-Y.R. Li and R.W. Yeung, “Network Information Flow”, IEEE Transactions on Information Theory, vol.46, no.4, pp.1204-1216, July 2000
[2] Y. Jiang, H. Zhu, M. Shi, X. Shen, and C. Lin, “An efficient dynamic-identity based signature scheme for secure network coding”, Computer Networks, vol.54, pp.28-40, 2010
[3] T. Ho, R. Koetter, M. Medard, D.R. Karger, and M. Effros, “The Benefits of Coding over Routing in a Randomized Setting”, ISIT 2003, Yokohama, Japan, June29 - July4, 2003
[4]P.A. Chou, Y. Wu, and K. Jain, “Practical Network Coding”, in Allerton Conference on Communication, Control, and Computing, Moniticello, IL, Oct. 2003
[5]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