修士論文 要旨

盗聴とビザンチン攻撃に対して安全なネットワーク符号化法

数理情報学専攻 48156220　中村 渉

指導教員　平井 広志 准教授

1　はじめに

ネットワーク符号化法 [1] とは，各頂点で受信データを符号化して隣接頂点に伝送することで，送信点から受信点にメッセージ M^L を送る方法である．この方法には，より多くの情報を送信できるという利点がある．

ネットワーク符号化法に対して，伝送データからメッセージ M^L の情報を得ようとする**盗聴**や，伝送データを改変して誤ったメッセージを復号させようとする**ビザンチン攻撃**が考えられ，これらに対して安全な符号化法が重要なテーマである．盗聴に対しては安全性の基準がいくつかあり，その中でも強い基準として強 r-安全性 [2] がある．一方，ビザンチン攻撃検出可能な符号化法も研究されている ([3] など)．しかし，盗聴に対して強安全かつビザンチン攻撃検出可能な方法はない．また，盗聴に対する安全性のために用いる乱数を，送信点のみで生成できるモデルと，全頂点で生成できるモデルでは，後者のほうが同じ安全性の下で多くのメッセージを送信できるが，後者のモデルでの研究は少ない．

本論文では，以下の 2 つのテーマを扱う．1 つ目は，盗聴に対して強安全かつビザンチン攻撃検出可能なネットワーク符号化法であり，ビザンチン攻撃成功確率の下界の導出と符号化法の提案を行う．2 つ目は，全頂点で乱数生成可能なモデルでのネットワーク符号化法であり，新たな必要条件や十分条件の導出などを行う．

2　盗聴に対して強安全かつビザンチン攻撃検出可能なネットワーク符号化法

2.1　準備

有向非巡回グラフ $G = (V, E)$ において，送信点 $s \in V$ から受信点集合 $T \subseteq V \setminus \{s\}$ の全頂点に L 個のメッセージ $M^L = M_1 \cdots M_L$ を送る．ただし，$\mathcal{M}$ を有限集合とし，M^L は $\mathcal{M}^L$ 上の一様分布に従うとする．各枝では，有限集合 $\mathcal{Y}$ 上の要素 1 シンボルを伝送する．送信点 s では乱数 R_s を利用できるとし，送信点から出る各枝で伝送するデータを (M^L, R_s) の関数として定める．また，送信点以外での各頂点 v から出る各枝で伝送するデータを，v が受信するデータの関数として定める．各受信点 t では，$\mathcal{M}^L$ の要素，またはビザンチン攻撃の検出を表す記号 $\perp$ を出力する．ビザンチン攻撃がない場合には正しいメッセージ M^L を出力することが復号の条件である．

ネットワーク符号化法が**強 r-安全**であるとは，以下の条件 (i)(ii) が成り立つことである [2].

(i) r 本以下の任意の枝での伝送データと，メッセージ M^L が，確率的独立である．

(ii) 各 $1 \le j \le L-1$ に対し，$r+L-j$ 本の任意の枝での伝送データと，$M_1, \ldots, M_L$ の任意の j 個からなる組 $(M_{i_1}, \ldots, M_{i_j})$ が，確率的独立である．

また，ネットワーク符号化法が **r-安全**であるとは，上記の条件 (i) が成り立つことである．

ここで，st-枝素パスの最大本数を $\lambda(s,t)$ で表し，$k := \min_{t \in T} \lambda(s,t)$ と定める．Harada–Yamamoto [2] は，$\mathcal{M}$ が十分大きな有限体の場合に，$\mathcal{Y} = \mathcal{M}$ であり強 $(k-L)$-安全なネットワーク符号化法を与えている．

次にビザンチン攻撃のモデルを述べる．攻撃者は $k-1$ 本以下の任意の枝のデータを改変でき，改変のために，改変される枝での改変前のデータを利用できるとする[*1]．受信点 t への攻撃成功を，t で攻撃が検出されず，かつ誤ったメッセージ $\widetilde{M}^L \neq M^L$ が復号されることと定め，**攻撃成功確率** P_{success} は，t への攻撃成功の確率を，受信点 t，攻撃方法，および改変前のデータに関して最大化したものと定める．

2.2　本研究

まず，攻撃成功確率 P_{success} の限界を与える．

定理 1. 任意の強 $(k-L)$-安全なネットワーク符号化法に対して，次式が成り立つ：

$$P_{\mathrm{success}} \ge \frac{|\mathcal{M}| - 1}{|\mathcal{Y}|}. \tag{1}$$

一方，以下の符号化法を提案する．$\mathcal{M} = \mathrm{GF}(p^c)$ であり，整数 d は $1 \le d \le c$ を満たし，p は $p \ge L+2$ を満たす素数であり，p^c, p^d は十分大きいとする．

各枝 e で，以下で定義される $(W_e, U_e) \in \mathrm{GF}(p^c) \times \mathrm{GF}(p^d)$ を伝送する．W_e を，M^L に対する Harada–Yamamoto の強 $(k-L)$-安全な符号化法で枝 e で伝送するデータとして定める．一方，$x \in \mathrm{GF}(p^c)$ の下位 d 桁に対応する $\mathrm{GF}(p^d)$ の要素を $f(x)$ で表し，U_e を，$f\big(\sum_{j=1}^{L} (M_j)^{j+1}\big)$ に対する Harada–Yamamoto の強 $(k-1)$-安全な符号化法で枝 e で伝送するデータとして

[*1] このような攻撃は改ざん攻撃と呼ばれる．ネットワーク符号化法に対する改ざん攻撃の定義はいくつか考えられ，本論文では 2 通りの定義を扱っている．詳細は省略する．

定める．各受信点では，W_e からの復号結果と U_e からの復号結果が不整合なとき $\perp$ を出力する．

定理 2. 上記の符号化法は，次の条件を満たす強 $(k-L)$-安全なネットワーク符号化法である：

$$|\mathcal{Y}| = p^{c+d}, \qquad P_{\text{success}} \leq Lp^{-d}. \tag{2}$$

提案手法は，強 $(k-L)$-安全かつビザンチン攻撃検出可能な初めての符号化法である．定理 1 より，$|\mathcal{M}| = p^c$, $|\mathcal{Y}| = p^{c+d}$ の強 $(k-L)$-安全なネットワーク符号化法に対する攻撃成功確率 P_{success} の限界は，$(p^c-1)/p^{c+d} \approx p^{-d}$ であるため，提案手法は，攻撃成功確率 P_{success} が限界の L 倍程度以下である．

このテーマに対して，本研究では以下の方法を用いている．まず，強 $(k-L)$-安全なネットワーク符号化法の特殊ケースである強い (k, L, n) ランプ型秘密分散法 [4] に対して，シェアの改変を検出可能な方法の提案と，攻撃成功確率の下界の導出を行い，それらをネットワーク符号化法に拡張するという方法である．秘密分散法に対しては，シェア間の相互情報量に注目した定理や，ブロック符号化した場合の定理も与えている．

3 全頂点で乱数生成可能なモデルでの盗聴に対して安全なネットワーク符号化法

3.1 準備

本節では，全頂点で乱数生成可能とし，$\mathcal{Y} = \mathcal{M}$, $T = \{t\}$ とする．M^L を r-安全に送る符号化法の存在判定問題を，**(L, r)-Secure Unicast 問題**（**(L, r)-SU 問題**）と呼ぶ．Jain [7] は，$(1, r)$-SU 問題を線形時間で解くアルゴリズムを与えている．Huang et al. [5] は，$(L, 1)$-SU 問題が複数ユニキャスト問題以上に難しいことを示している．Huang et al. [6] は，(L, r)-SU 問題に解が存在するための必要条件を与えており，この条件を **(L, r)-HHLK 条件**と呼ぶ．$(1, r)$-HHLK 条件は十分条件でもあることが [7] より分かる．

3.2 本研究

本研究では主に $(L, r) = (2, 1)$ の場合を考える．$(2, 1)$-HHLK 条件は，$(2, 1)$-SU 問題の解が存在するための十分条件ではないことが示せる．新たな必要条件を与えるために，ネットワークに対する頂点の縮約[*2]，枝の追加，枝の細分という操作を考える．$(2, 1)$-SU 問題の解を持つネットワークは，これらの操作後も解を持つことが分かる．ここで，$(2, 1)$-HHLK 条件は以下のように書き直せる．

[*2] 縮約で生じるループは取り除くとし，縮約後も非巡回性を保つものに対してのみ行うものとし，$s \in U$ の場合は縮約後の頂点を s とし，$t \in U$ の場合は縮約後の頂点を t とする．

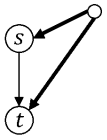

図 1. N_1

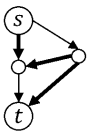

図 2. N_2

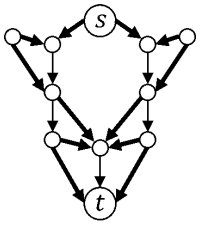

図 3. N_3

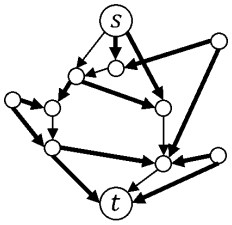

図 4. N_4

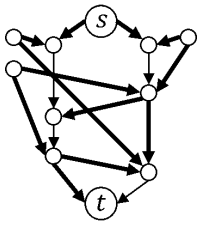

図 5. N_5

定理 3. (G, s, t) が $(2, 1)$-HHLK 条件を満たさないことは，頂点の縮約，枝の追加，枝の細分を繰り返して，N_1 または N_2 が得られることと同値である．

よって，頂点の縮約，枝の追加，枝の細分を繰り返して N_1 または N_2 が得られるネットワークには $(2, 1)$-SU 問題の解がない．このようなネットワークを新たに見つけることで，以下の定理を与える．

定理 4. ネットワーク (G, s, t) に頂点の縮約，枝の追加，枝の細分を繰り返して，図 3, 4, 5 のネットワーク N_3, N_4, N_5 のいずれかが得られたとき，(G, s, t) は $(2, 1)$-SU 問題の解を持たない．

N_3, N_4, N_5 は，どの太い枝にも 1 本以上の枝がある場合には $(2, 1)$-HHLK 条件を満たすことが示せる．

(L, r)-SU 問題に関して，上記以外に，本論文では，$(2, 1)$-SU 問題の解が存在するための十分条件と，それを満たす場合の符号化法を与えている．また，$(1, 1)$-SU 問題の解で，符号化に必要な乱数が Jain [7] よりも少なくなるような符号化法を与えている．

参考文献

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[2] K. Harada and H. Yamamoto, "Strongly secure linear network coding," *IEICE Trans. Fundamentals*, vol. E91-A, no. 10, pp. 2720–2728, 2008.

[3] Q. Guo, M. Luo, L. Li, and Y. Yang, "Secure network coding against wiretapping and Byzantine attacks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, no. 17, 2010.

[4] 山本博資，"(k, L, n) しきい値秘密分散システム，" 電子通信学会論文誌, vol. J68-A, no. 9, pp. 945–952, 1985. English Translation: *Electronics and Communications in Japan*, Part 1, vol. 69, no. 9, pp. 46–54, 1986.

[5] W. Huang, T. Ho, M. Langberg, and J. Kliewer, "On secure network coding with uniform wiretap sets," *Proc. NetCod2013*, pp. 1–6, 2013.

[6] W. Huang, T. Ho, M. Langberg, and J. Kliewer, "Reverse edge cut-set bounds for secure network coding," *Proc. IEEE ISIT2014*, pp. 106–110, 2014.

[7] K. Jain, "Security based on network topology against the wiretapping attack," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 68–71, 2004.