様式 C-19

科学研究費補助金研究成果報告書

平成２２年６月２３日現在

研究種目：若手研究（Ｂ）
研究期間：2008～2009
課題番号：20760233
研究課題名（和文）遅延量が変動するときのネットワーク符号化法の開発

研究課題名（英文）　Decodabiblity of network coding with time-variying delay

研究代表者
松本　隆太郎（MATSUMOTO RYUTAROH）
東京工業大学・大学院理工学研究科・准教授
研究者番号：１０３３４５１７

研究成果の概要（和文）：リンクにおける遅延量が変動するときに、単一の情報源を持つマルチキャストネットワーク符号化において、受信者が送信情報を復号できるための十分条件を明らかにした。

研究成果の概要（英文）：We clarified that sufficient conditions that allow the receivers to recover the transmitted information in the single source multicast network coding.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,100,000	330,000	1,430,000
2009 年度	1,300,000	390,000	1,690,000
年度			
年度			
年度			
総　計	2,400,000	720,000	3,120,000

研究分野：情報理論
科研費の分科・細目：電気電子工学　情報通信工学
キーワード：　ネットワーク符号化

１．研究開始当初の背景

（１）従来のネットワーク通信では、ネットワーク内の中継ノードは隣接ノードから受け取ったデータを改変せずにそのまま転送していた。この方式を蓄積転送方式と呼ぶ。それに対し、複数の隣接ノードから受信したデータを符号化してから転送する方式をネットワーク符号化と呼ぶ。ネットワーク符号化は蓄積転送方式と比較して、スループットの向上や消費電力の削減をはかれるため近年大きな注目を集めている。

（２）従来の蓄積転送方式では、中継ノード間のリンクにおいて、輻輳などによりデータ伝送にかかる時間が時刻と共に変動しても問題なく動作する。一方、ネットワーク符号化においては、中継ノードが複数の隣接ノードからの情報がすべて揃うまで符号化できないので、リンクにおけるデータ伝送時間が変動しているときには、単純に実装を行うと最も遅いデータの到着を待つ必要が生じ、実効的なスループットの低下を招く。そこでリンクにおけるデータ伝達時間が変動する場

合にネットワーク符号化を用いる場合には、何らかの工夫が必要となる。
（3）他方、ネットワーク符号化における消費電力削減において、従来の蓄積伝送方式と比較して削減できる電力比の上限はまだ明らかにされていなかった。削減比率の上限を解明することも理論的に重要である。

（4）近年、情報理論的セキュリティが注目を集めている。従来のセキュリティは、ある種の計算量的問題、例えば素因数分解や離散対数問題を解くために膨大な計算量が必要となることに根拠を置いている。このような安全性の根拠は、効率の高いアルゴリズムの発見や量子コンピュータの実用化で崩されてしまう。それに対して情報理論的セキュリティは、秘密に保ちたい情報と攻撃者が所有する情報が統計的に独立（統計的に関係が無い）ことを安全性の根拠としているため、安全性の根拠が他分野の研究の発展によって崩されることがない。

（5）セキュアネットワーク符号化は、情報理論的に安全なネットワーク符号化を実現する手法である。Cai らによって 2002 年に提案された最初のセキュアネットワーク符号化は、ネットワークトポロジーに依存して符号化方法を変更する必要があり、不便であった。この不便さを解消するために Silva らは、中継ノードの符号化方法も含めてどのようなネットワークでも情報理論的セキュリティを実現する、ユニバーサルセキュアネットワーク符号化を 2008 年に提案した。しかし、Cai らの方法と Silva らの方法は、安全性の基準が違っており、Silva らの手法は Cai らの基準において安全なのかどうか不明であった。Cai らのモデルにおける安全性を保証することは、以下の理由により重要であると考えられる。通常使われているインターネットプロトコル（IP）ではパケットが複数に分割され、分割された断片が別々の経路を辿って最終目的地に到達することが許されている。従って物理的に固定されたリンクを盗聴者が盗聴しているときでも、盗聴されている論理的なリンクの集合は時刻とともに変化する可能性がある。Cai らの安全性基準では盗聴されるリンクが時刻と共に変動した場合でも盗聴者に情報が漏れないことを要求していたが、Silva らのモデルでは一定の間盗聴されるリンクの集合が変化しないときに盗聴者に情報が漏れなければよいとしていた。

２．研究の目的

（1）研究の目的は、リンクにおけるデータ伝送速度が時刻とともに変動する場合にも使用できるネットワーク符号化方式を開発することである。これは主な研究目的であるが、その他に以下の目的も追求した。

（2）ネットワーク符号化を用いたときの消費電力が、従来方式の蓄積転送方式だけを用いたときに比べて、どの程度削減される可能性があるのか削減比率の限界を解明する。

（3）セキュアネットワーク符号化において、Silva らの提案したユニバーサルセキュアネットワーク符号化が、Cai らの提案した従来の安全性モデルにおいても安全かどうか検証する。

３．研究の方法

（1）リンクのデータ伝送時間が時刻と共に変動するときにも用いられるネットワーク符号化法の開発においては、伝送時間がどのように変動しても受信者が送信情報を復元できる十分条件を探した。

（2）ネットワーク符号化による消費電力の削減比率の上限の解明においては、具体的にネットワークおよび符号化方法を指定して比率を求めた。

（3）Silva らが提案したユニバーサルセキュアネットワーク符号化においては、Cai らの安全性モデルにおいて情報が漏れる場合がありえることを具体例を構成して確認した。

４．研究成果

（1）リンクにおけるデータ伝送時間が時刻と共に変動する場合のネットワーク符号化においては、以下の結果を得た。遅延が無くサイクルが無い有向グラフでネットワークがモデル化されるとする。また、線形ネット

ワーク符号化が用いられると仮定し、単位時間にソースノードはｎ個の GF(q)の要素を送出するとする。ネットワークのリンクの集合をＥとし、Ei をソースノードから送られるｉ番目の情報シンボルが流れているリンクの集合とする。すべてのリンクｅについて、Ei からｅに流れ込む辺の数が１以下であるという条件を考える。この条件はｉ番目の情報シンボルがネットワークの途中で合流しないことを表わしている。このとき、ソースノードから単位時間あたりに送出される情報シンボル数が２であるときに、途中のリンクにおけるデータ伝送時間がどのように変化しても、すべての受信者が送信情報を復元できることを証明した。この十分条件をソースノードから送出される情報シンボル数が３以上の場合に拡張することは自然な考え方であるが、シンボル数が３以上のときには上記の条件を満たしていても受信者が送信情報を復元できない場合があることを明らかにした。そこで、ソースノードから送出されるシンボル数が３以上の一般の場合にネットワーク符号化を構成する十分条件として、各受信者において、線形方程式を順番に解くことで常に情報を復元可能であることを保証する十分条件を提案した。

（２）消費電力の削減においては、d 次元空間においてノードが格子状に並んでいるネットワークトポロジーを考えた。これは２次元においては正方形状、３次元においては立方体状にノードが並んでいるネットワークトポロジーを一般化したものである。このネットワークにおいて、格子の端面にある各ノードが向かい側のノードに向かって情報を送ることを考える。これは送信者と受信者がそれぞれのデータストリームについて一つだけ存在するユニキャスト通信が複数並行して行われるものである。例えば、２次元の正方形状のネットワークの場合には、上下左右の４方向にデータが流れることになる。ここで、各ノードはブロードキャスト通信によって、隣接ノードに同時に情報を送れるものとする。また、消費電力を最小限に抑えることを目標としているので、各ノードが送信信号が干渉して受信失敗しないように、時刻をずらせて情報を送信するものと仮定する。ここで、従来の蓄積伝送方式では、ｄ次元のネットワークにおいては 2d 個の方向に情報が流れているので、ネットワーク内部のノードは 2d 回情報を送信する必要がある。それに対して、ネットワーク符号化を用いる方式では、隣接ノードからの受信信号を適切に線形結合した信号を１回送出するだけで、2d 方向にデータを流せることを明らかにした。このことによりｄを大きくすると、蓄積転送方式による消費電力のネットワーク符号化法に比べた比率は無限に大きく成りえることを示した。なお、実際に指定されたネットワーク構造に対して消費電力を少なく抑える符号化方法を構成するアルゴリズムの開発は今後の課題となっている。

（３）Silva らの提案したネットワーク符号化法においては、以下の結果を得た。Silva らの方法では、ソースノードは単位時間あたりにｎ個の GF(q)のシンボルをｍ時刻にわたって送出する。従ってソースノードは mn 個のシンボルを送出する。盗聴者はμ本のリンクを単位時間あたりに盗聴して内容を知ることができるとする。従って盗聴者は mμ個のシンボルを盗聴により得る。Silva らのオリジナルの盗聴者のモデルでは、m 時刻の間盗聴されるリンクの集合は不変であると仮定されていた。これを Cai らのモデルにならって時刻毎に変更できる場合について検討した。このとき、各時刻におけるソースノードにおける情報シンボルと、盗聴者が得られるシンボルの間の関係は行列で表現することができる。セキュアネットワーク符号化がユニバーサルセキュアであるためには、この行列がどのようなものであっても、盗聴者が情報を得られないことが必要である。情報が得られないということは、相互情報量が０であることによって表現できる。また、ソースノードはｍｎ個のシンボルのうちｍｋ個に送信情報を含め残りにはランダムに生成したシンボルを含めることで秘密にしたい情報を隠している。本研究では、まず補題として、ユニバーサルセキュアであることと、盗聴された情報が同じでネットワークに送出された mn 個のシンボル列が異なるときには、対応する秘密情報が必ず異ならなければいけないことを示した。次に、実際に正規送信者に対して都合の悪い盗聴者の行列を実際に構成することによって、正規送信者がどのような情報の送り方をしても、上に述べた補題の条件を満たせないから、Cai らによる時刻

毎に盗聴するリンクの集合が変わることを許す盗聴モデルではSilvaらの方式ではユニバーサルセキュリティを実現できないことを証明した。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）
〔雑誌論文〕（計２件）
①J.Goseling,, Ryutaroh Matsumoto, Tomohiko Uyematsu,他
“Lower Bounds on the Maximum Energy Benefit of Network Coding For Wireless Multiple Unicast” Eurasip Journal on Wireless Communications&Netwoking, 印刷中

②T.Tateno. R.Matsumoto 他
Decodability of Network Coding with time-variyiing delay IEICE Transacitons on Fundamentals 査読あり vol. E92-A, pp. 2141-2145, 2009

〔学会発表〕（計 3件）
①Eitaro Shioji, R.Matsumoto 他
Vulnerability of MRD-Code-Based Uniervsal Secure Network Coding against Stronger Eavesdroppers
ISIT 2010 Austin, Texas, USA, 2010年6月14日

②E.Shoji, R.Matsumoto 他
Vulnerability of MED-code-based universal Network coding
電子情報通信学会情報理論研究会, 信州大学, 2010年3月5日

③J.Goseling, R.Matsumoto 他
On the energy benefit of network coding for wireless multiple unicast
IEEE Intl. Symp. On Information Theory
韓国ソウル, 2009年7月3日

〔その他〕
ホームページ等
http://www.rmatsumoto.org/research.html

６．研究組織
(1)研究代表者
松本 隆太郎 (MATSUMOTO RYUTAROH)
東京工業大学・大学院理工学研究科・准教授
研究者番号：１０３３４５１７

(2)研究分担者
なし

(3)連携研究者
なし