社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

MPLS網において低帯域幅消費を実現する 複数P2MP LSPを用いたマルチキャスト電子透かし方式

松本　隼† 　高　山† 　清水　翔† 　石井　大介† 　岡本　聡†

山中　直明†

† 慶應義塾大学理工学部情報工学科
〒 223–8522 横浜市港北区日吉 3–14–1
E-mail: †matsumoto@yamanaka.ics.keio.ac.jp

あらまし　本研究では，マルチキャスト電子透かしを MPLS 網において複数の P2MP LSP を切り替えることにより実現する方式を提案する．マルチキャスト電子透かし技術は消費帯域幅の節約および流出元の特定を同時に実現する．従来の暗号化に基づく方式はネットワーク全体の消費帯域幅および追跡精度の面において問題があったが，提案では無駄なブロック転送が一切発生しないため上記を改善する．特性評価において，従来方式と比較し提案方式が消費帯域幅において優れることを示す．

キーワード　マルチキャスト電子透かし，MPLS，P2MP LSP

Low Bandwidth Consumption Multicast Fingerprinting by using Multi P2MP LSPs in MPLS Network

Jun MATSUMOTO†, Shan GAO†, Sho SHIMIZU†, Daisuke ISHII†, Satoru OKAMOTO†, and Naoaki YAMANAKA†

† Dept. of Information and Computer Science, Faculty of Science and Technology, Keio University
3-14-1 Hiyoshi, Kohoku, Yokohama, 223-8522 Japan
E-mail: †matsumoto@yamanaka.ics.keio.ac.jp

Abstract　This paper proposes the method for multicast fingerprinting by using multi P2MP LSPs in MPLS Network. Multicast fingerprinting technology achieves the saving of bandwidth consumption and the tracing traitors simultaneously. While the conventional method based on encryption has the shortcomings in bandwidth consumption on entire network and traceability for traitors, our proposed method improves those two elements since useless block transfers are not occurred at all. Computer simulations show that the proposed method excels in the bandwidth consumption.

Key words　Multicast Fingerprinting, MPLS, P2MP LSP

1. まえがき

急速なブロードバンド技術の進歩に伴い，IPTV などのマルチメディアストリーミング技術が現在広く普及している．ストリーミング配信では，マルチキャスト伝送を用いて同一データを複数のあて先に配信することにより，ネットワーク全体における帯域幅消費を抑えることが可能である．しかし一方で，配信されるディジタルコンテンツは複製が容易であるため，違法な再配布が問題となっている．著作者の権利を守るため，違法な再配布を防ぐことは必須であり，そのために流出元の特定技術が重要となる．近年，流出元の特定のため，電子透かし [1] が注目されている．電子透かしは肉眼では確認不可能な形で購入者 ID 等の情報をコンテンツに埋め込む技術であり，万が一コンテンツの不正流出が発覚した場合，埋め込まれた情報を参照することにより流出元の特定が可能となる．しかし，一般的に電子透かし技術はあて先毎に異なるデータをユニキャスト伝送する必要があるため，ネットワーク全体における帯域幅消費はあて先数に比例して増加してしまう．マルチキャスト電子透かし技術 [2]- [5] は，上記の相反する 2 つ要素を実現する．

Watercasting [2] はマルチキャストツリーの深さに応じてオ

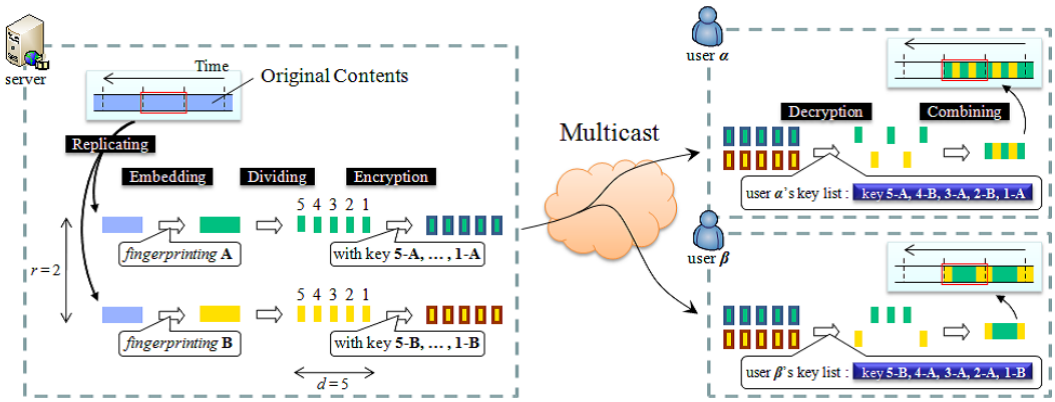

図 1　Parvianen-Parnes 方式の概要

リジナルコンテンツを複製し，わずかに異なる電子透かしを埋め込んだ後，全てのデータをマルチキャストする．マルチキャストツリー上の各分岐ルータでは受信した複数の同一コンテンツの内，転送先毎に 1 つを除いて転送し，ラストホップルータにおいてただ一つのデータをユーザに配信する．ルータ上の破棄ポリシーをパケット毎に変化させることによりコンテンツ全体を通してユーザ毎に異なる電子透かしパターンを実現する．

WHIM [3] はマルチキャストツリー上の各中継ルータにおいて受信したコンテンツを転送する際，ルータ毎にユニークな電子透かしを埋め込む．データが不正流出した際，埋め込まれた電子透かしを参照し各ルータを辿ることにより流出元の特定が可能となる．

Chameleon [4] は暗号化に基づくマルチキャスト電子透かしで，暗号化されたコンテンツを各ユーザが復号する際，わずかに異なる結果となるよう異なる鍵を配布する．

Parvianen-Parnes 方式 [5] は異なる暗号化に基づくマルチキャスト電子透かしである．本方式は，複製したオリジナルコンテンツにわずかに異なる電子透かしを埋め込んだ後，小さいブロックに分割しそれぞれ異なるキーを用いて暗号化し，全ブロックを各ユーザに配信する．そしてユーザ側において，事前に配布された復号鍵リストを用いて受信ブロックを選択的に復号化および結合しデータを復元する．その際，ユーザ毎に異なる復元結果となるよう異なる復号鍵リストを配布することにより，ユーザ間の配信コンテンツの識別化を実現する．

Watercasting および WHIM は配信サーバがネットワーク上に点在する各中継ルータを管理し，かつルータ上で特殊な処理を実行する必要がある．そのため，ネットワーク規模に応じて管理すべきルータ数が増大し運用が煩雑化してしまう．また各中継ルータは十分に信頼可能である必要がある．また Chameleon においては，ユーザ数の増加に伴い鍵サイズが増大し，かつ電子透かしの強度が弱いという問題がある．以上より上記の 3 方式が大規模なネットワークには適さない一方，Parvianen-Parnes 方式は 1000 万人規模のユーザを収容する大規模なネットワークに対して有効であり，電子透かしの強度も十分に確保可能である．以上より，我々は本研究において Parvianen-Parnes 方式を従来方式として比較対象とする．

Parvianen-Parnes 方式は大規模なネットワークに適用可能である一方，マルチキャスト経路上の全リンクにおいて，常に 2 倍以上の帯域幅が必要となる．また暗号化および復号化処理に伴う処理遅延およびセキュリティの問題がある．さらに，追跡精度および共謀攻撃耐性 [6] においても問題が残る．

本研究では，我々は上記の問題を改善するため，MPLS 網において複数 P2MP LSP(Point-to-MultiPoint Label Switched Path) を用いたマルチキャスト電子透かし方式を提案する．

本稿の構成は以下のとおりである．2 節では，従来方式である Parvianen-Parnes 方式の動作を詳解する．続く 3 節では，MPLS 網において複数 P2MP LSP を用いたマルチキャスト電子透かし方式を提案する．4 節では，コンピュータシミュレーション上で本提案方式および Parvianen-Parnes 方式を帯域幅消費において比較する．最後に 5 節で結論を述べる．

2. Parvianen-Parnes 方式

図 1 にストリーミング配信における Parvianen-Parnes 方式の概要を示す．まずサーバ側においてオリジナルコンテンツを一定間隔毎に区切り r 複製した後，異なる電子透かしを各コンテンツに埋め込み d ブロックに分割する．そして，全ブロックをそれぞれ異なる鍵を用いて暗号化した後，全ユーザに配信する．ユーザ側では，受信したブロックを復号化および結合し，コンテンツを復元する．その際，各ユーザ間において異なるブロックの組み合わせとなるように復号鍵リストを各ユーザに事前配布することにより，配信ユーザ間におけるコンテンツの識別化を実現する．可能識別数は r^d であり，万が一動画の不正流出が発覚した場合，埋め込まれた電子透かしパターンを参照することにより流出元の特定が可能となる．

Parvianen-Parnes 方式は中継ルータ上に特殊な処理を実装する必要がなく，既存の IP ネットワークに適用可能であり汎用性に優れる．しかし，本方式は以下に挙げる問題点を有する．

- 帯域幅消費

  異なる電子透かしが埋め込まれた r の複製コンテンツの全ブロックを全ユーザに配信するため，オリジナルコンテンツのみを全ユーザにマルチキャストする場合と比較し r 倍の帯域幅が要求される．そのため，ネットワーク全体の帯域資源の冗長な消費のみならず，アクセスネットワークにおいて他のデータトラヒック等で帯域幅がひっ迫した場

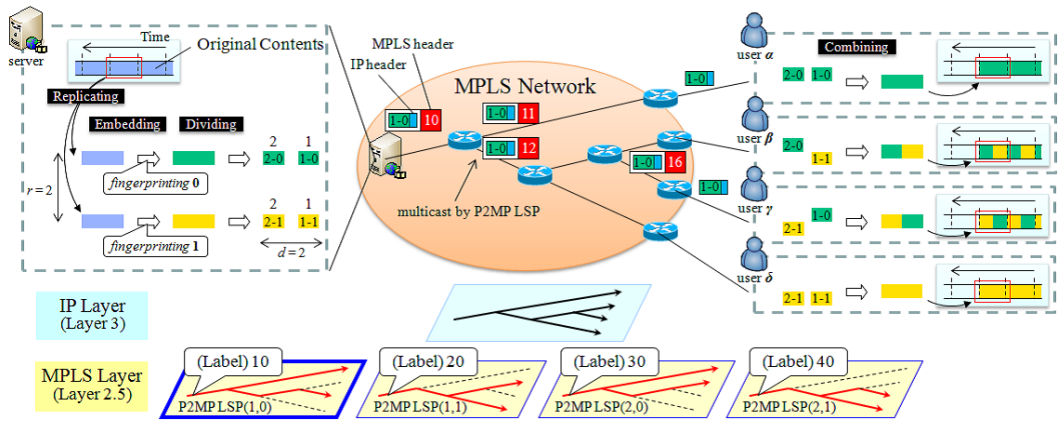

図 2　提案方式の概要

合，リアルタイムな視聴が困難となる可能性がある．また，同時に視聴可能なチャネル数も半減する．

- 遅延

  Parvianen-Parnes 方式は暗号化および復号化処理が必要である．そのため，復号化に伴う処理遅延が発生し，リアルタイムな視聴が困難となる可能性がある．また，各ユーザ側に設置されるデバイスに復号化処理を行うための専用エンジンが必要となり，生産コストの高騰や規格統一に関する問題の発生が予想される．

- セキュリティ

  全ブロックを全ユーザに配信するため，悪意のあるユーザによって暗号の破壊や鍵の漏洩が発生した場合，任意の電子透かしパターンが生成され流出元の特定が不可能となる．

- 追跡精度

  ユーザ数が増加した場合あるいは共謀攻撃耐性 [6] を向上させる場合，可能識別数 r^d を増加させる必要があるが，必要な帯域幅が r 倍となるため r の増加は制限され，d を増加させる必要がある．しかし，d の増加に伴い区切り間隔が長くなるため，短い動画については流出元の特定が困難となる．すなわち，Parvianen-Parnes 方式は帯域幅消費の抑制および追跡精度の向上を同時に達成することが不可能である．

3. 提 案 方 式

本研究では，MPLS 網において複数の P2MP LSP を用いてブロック毎にあて先を切り替えることにより，マルチキャスト電子透かしを実現する方式を提案する．

図 2 に提案方式の概要を示す．従来方式と同様，まずサーバ側においてオリジナルコンテンツを一定間隔毎に区切り r 複製した後，異なる電子透かしを各コンテンツに埋め込み d ブロックに分割する．そして，ブロックをユーザ間で異なる組み合わせとなるように選択的に転送を行う．その際，各ブロックのあて先を含む P2MP LSP をブロック数分確立し，ブロック毎に利用する P2MP LSP を選択することにより，選択的なブロック転送を実現する．可能識別数は r^d であり，万が一動画の不正流出が発覚した場合，本コンテンツの電子透かしパターンを参照することにより流出元ユーザの特定が可能である．

本方式では IP 層 (レイヤ 3) の下位にあたる MPLS 層 (レイヤ 2.5) に複数の P2MP LSP を確立する．そのため，IP 層以上においては本方式の動作は不可視であり，単一のマルチキャスト IP アドレスでマルチキャスト電子透かしが実現可能である．具体的には，各ブロック毎に，用意された P2MP LSP に対応するラベルを IP ヘッダの前に付加する．そのため，サーバには一つのフローに対し複数のラベルを切り替えて付加するための特殊な機能を実装する必要性がある．すなわち Layer 2.5 から 7 まで及ぶプログラムを作成する必要がある．

提案方式は Parvianen-Parnes 方式と比較し以下の点において優れる．

- 帯域幅消費

  提案方式では無駄なブロック転送が一切発生しないため，常に r 倍の帯域幅消費が発生する Parvianen-Parnes 方式と比較し帯域幅の面で優れる．

- 遅延

  MPLS は高速なラベル転送が可能であり，加えて暗号化および復号化処理に伴う処理遅延が発生しないため，低い遅延を実現する．

- セキュリティ

  提案方式では暗号化および復号化処理を行わないため，暗号の破壊や鍵の漏洩に伴うリスクの回避が可能である．また共謀攻撃に対する耐性も向上している．共謀攻撃耐性については後ほど詳解する．

- 追跡精度

  ユーザ数が増加した場合あるいは共謀攻撃耐性を向上させる場合，可能識別数 r^d を増加させる必要がある．Parvianen-Parnes 方式が帯域幅消費の点より r の増加が制限されたのに対し，提案方式では r を増加させた場合もネットワーク全体の消費帯域幅はほぼ変化しないため，r を増加させることが可能となる．そのため d を増加させる必要が無く，短い区切り間隔を実現し追跡精度が向上する．すなわち，提案方式は帯域幅消費の抑制および追跡精度の向上を同時に実現可能である．

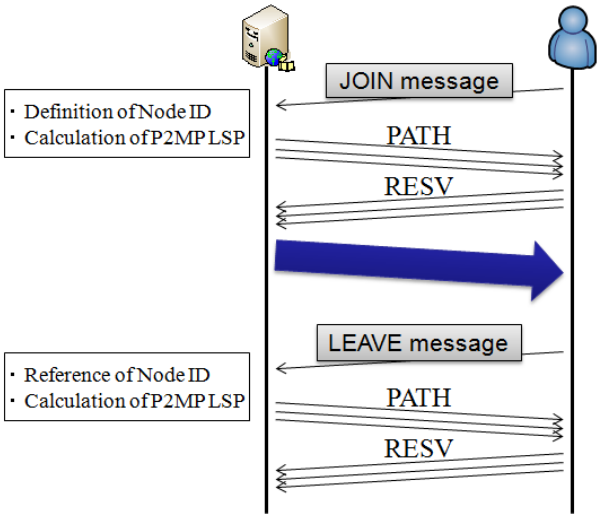

図 3　提案方式における視聴の開始から終了までのシーケンス図.

次節において，具体的な P2MP LSP の管理および運用手法について詳しく説明する．

3.1　管理・運用

提案方式ではブロックおよびそのブロック転送に用いられる P2MP LSP が 1 対 1 で対応する．そのため，複製数 r およびブロック分割数 d に対し，$r \times d$ の P2MP LSP が必要となる．これらの P2MP LSP を体系的に管理する手法について説明する．

サーバ側において複製したコンテンツに埋め込む電子透かしをそれぞれ $R = 0, 1, \ldots, r$ とし，分割されたブロックを前から順に $D = 1, 2, \ldots, d$ とする．ここで，各ブロックを”$D-R$”と表記する．すなわち，電子透かし 0 が埋め込まれたコンテンツの先頭から 2 番目のブロックは”2-0”と表記する．以上の表記規則に基づき，各ブロックに対応する P2MP LSP の表記を以下のように定義する．

$$\mathrm{P2MP\_LSP}(D, R) \tag{1}$$

また，各参加ユーザにはそれぞれ異なる Node ID(=0,1,...,$r^d - 1$) を割り当て，Node ID を d 進数表記した際の各桁および値を受信すべきブロックと対応付ける．例えば複製数 $r = 2$，ブロック分割数 $d = 6$ のとき，Node ID：5=$(000101)_2$ のユーザには 6-0,5-0,4-0,3-1,2-0,1-1 のブロックが配信される．すなわち，式 (1) の P2MP LSP の表記に基づき，本ユーザは以下の P2MP LSP にあて先として登録されていることを示す．

$\mathrm{P2MP\_LSP}(6, 0)$

$\mathrm{P2MP\_LSP}(5, 0)$

$\mathrm{P2MP\_LSP}(4, 0)$

$\mathrm{P2MP\_LSP}(3, 1)$

$\mathrm{P2MP\_LSP}(2, 0)$

$\mathrm{P2MP\_LSP}(1, 1)$

3.2　JOIN 処理

図 3 に提案方式における視聴の開始から終了までのシーケンス図を示す．本節では新規ユーザの加入を扱う JOIN 処理について説明する．

まず参加するユーザはストリーミングサーバに対して，JOIN メッセージを送信する．JOIN メッセージを受信したサーバは，$[0, r^d - 1]$ の範囲で未使用の Node ID をユーザに対して割り当てる．そして先述した体系化規則に基づき，割り当て Node ID より計算された各 P2MP LSP のあて先に本ユーザを登録する．各 P2MP LSP のあて先登録には RSVP-TE プロトコル [7] を用いる．該当する P2MP LSP が既に確立されている場合は Graft 処理が行われ，まだ確立されていない（すなわちあて先が空である）場合は確立が行われる．本処理は d 本について実行されるが，並列に実行することにより高速に処理が完了する．各 P2MP LSP のあて先への登録処理が全て終了すると，JOIN 処理が完了しストリーミング配信が開始される．

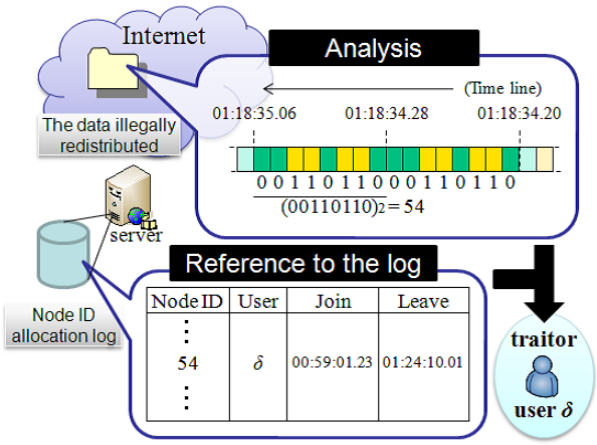

図 4　流出元発見手続き

3.3　LEAVE 処理

本節では既存ユーザの離脱を扱う LEAVE 処理について説明する．まず離脱するユーザはストリーミングサーバに対して，LEAVE メッセージを送信する．LEAVE メッセージを受信したサーバは，先述した体系化規則に基づき，Node ID より計算された各 P2MP LSP のあて先から本ユーザを削除する．JOIN 処理と同様，各 P2MP LSP のあて先削除には RSVP-TE プロトコルが用いる．該当する P2MP LSP に本ユーザ以外にもあて先メンバが登録されている場合は Prune 処理が行われ，本ユーザ以外にあて先メンバが登録されていない（すなわち本処理によってあて先が空となる）場合は本 P2MP LSP は削除される．各 P2MP LSP のあて先からの削除処理が全て終了すると，LEAVE 処理が完了する．

3.4　流出元発見手続き

流出元発見手続きの全体図を図 4 に示す．

まずコンテンツの不正流出を発見した著作権者あるいは監査機関は本コンテンツを解析し，電子透かしパターンを検出する．そして検出された電子透かしパターンより，Node ID を計算する．図 4 の例では区切り毎に電子透かしパターン (00110110) が検出されており，本動画が Node ID:54 に配布された動画であることが解析される．次にサーバに保存されている Node ID

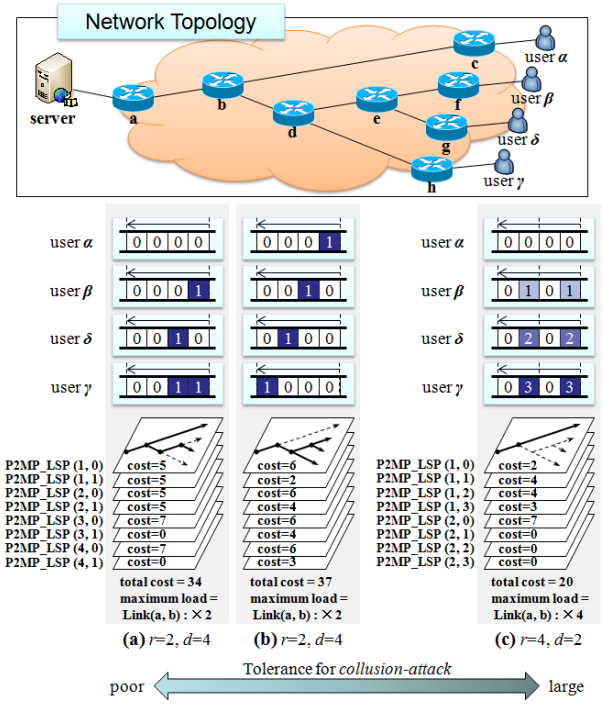

図 5　共謀攻撃耐性および消費帯域幅の関係

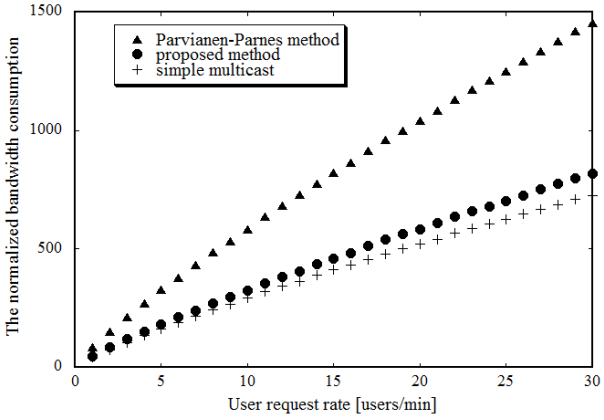

図 6　ユーザ生成頻度の増加に伴う消費帯域幅の変化

割り当てログを参照することにより，本動画が配布されていた時間に Node ID:54 を利用していたユーザ δ が割り出され，ユーザ δ が流出元であると特定される．

3.5　共謀攻撃耐性

複数の悪意のあるユーザがそれぞれに配信されたデータから新たなデータを生成することを共謀攻撃 [6] と呼ぶ．Parvianen-Parnes 方式および提案方式はユーザ間で共通するデータが多いため，共謀攻撃に対する耐性が低い．ただし，ユーザ可能識別数 r^d を増加させることにより，共謀攻撃に対する耐性を向上させることが可能である．例えばユーザ数 $n = 100000$，共謀攻撃者数 $p = 10$，複製数 $r = 2$，ブロック分割数 $d = 10000$ のとき，99.9%の確率で少なくとも一人の攻撃者を特定することが可能である [5]．

しかし Parvianen-Parnes 方式はネットワーク全体の帯域幅消費の点より複製数 r の増加が制限されており，ブロック分割数 d の増加により追跡精度が低くなるという問題がある．一方，提案方式ではネットワーク全体の帯域幅消費がほとんど変化しないため，ブロック分割数 d だけでなく複製数 r も増加させることが可能である．複製数 r の増加に伴い，ユニキャスト伝送と同等の共謀攻撃耐性が得られる．

ただし，共謀攻撃耐性および消費帯域幅は負の相関関係にある．図 5 に提案方式を用いてマルチキャスト電子透かしを実現する 3 つの例を示す．(a)-(c) は全て同じ可能識別数である．本図において，(b) は各ユーザを特定可能なブロックを有するため (a) と比較し共謀攻撃耐性が高い．例えば不正流出した動画の電子透かしパターンが (0001) であった場合，(b) は少なくともユーザ α が攻撃者の 1 人であることが解析可能である．ただし，ホップ数をコストとした場合，(b) の総コストは 37 となり，(a) の総コスト 34 と比較し大きい．また，(c) は各ユーザを必ず特定可能なブロックを有するためもっとも共謀攻撃耐性が強い．例えば不正流出した動画の電子透かしパターンが (0000) であった場合，(b) は共謀攻撃の発生は検知可能であるが攻撃者の特定は不可能である．本図の場合，ユーザ数と複製数が等しいためユニキャストと同等の共謀攻撃耐性を有する．ただし，(c) は最も負荷のかかるリンクが 4 倍の帯域幅消費となる．そのため，サーバ付近のリンクの利用可能帯域幅に応じて共謀攻撃耐性には限界がある．

しかし，共謀攻撃に対して実際に攻撃者を特定可能かどうかはあまり重要ではなく，攻撃者を追跡可能であることを攻撃者に対して示唆することが重要である．すなわち一部の共謀攻撃が実際に追跡不可能であったとしても，攻撃者は追跡可能か不可能かを知る術がないため，心理的な抑止効果が働く．特に提案方式は Parvianen-Parnes 方式と異なり，ユーザが明確に複製数 r を把握しないため，攻撃者は追跡可能か不可能かより一層判断しにくい．

4.　特 性 評 価

4.1　シミュレーションモデル

Barabási-Albert モデルに基づくランダムネットワーク上でシミュレーションを行った．ルータ数は 10000 で，各ルータには 1 ユーザが接続する．平均視聴時間は 10[min] とし，指数分布に基づく．またマルチキャストルーチングはスパニングツリーに基づく．JOIN 処理において割り当てる Node ID はランダムとする．1000 分間のシミュレーションにおける平均値の測定を 100 のランダムネットワーク上で行い，その平均値を測定した．

4.2　シミュレーション結果

図 6 にユーザ生成頻度の増加に伴うネットワーク全体の消費帯域幅のシミュレーション結果を示す．横軸にポアソン分布に基づくユーザ生成頻度の平均を，縦軸にストリーミング動画の帯域幅により正規化したネットワーク全体の消費帯域幅を示す．ただし，複製数 $r = 2$，ブロック分割数 $d = 20$ とする．

Parvianen-Parnes 方式が単純なマルチキャスト伝送の 2 倍の帯域幅を常に消費するのに対し，提案方式は約 1.2 倍の帯域幅のみ消費し，Parvianen-Parnes 方式と比較し約 44%の消費帯

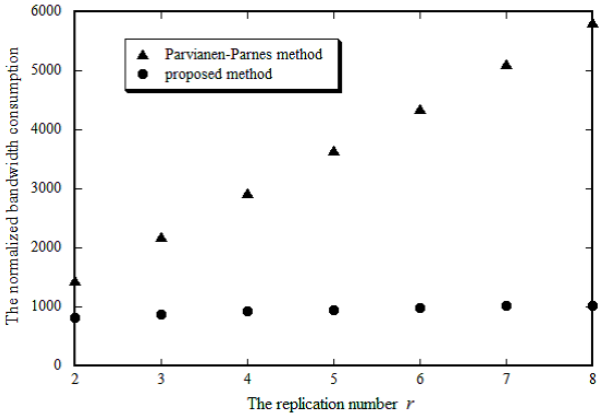

図 7　複製数の増加に伴う消費帯域幅の変化

域幅の削減を実現する．すなわち，提案方式の方がネットワークに対して少ないトラヒック負荷で運用可能なことがわかる．

また，図 7 に複製数 r の増加に伴うネットワーク全体の利用帯域幅のシミュレーション結果を示す．横軸に複製数 r を，縦軸にストリーミング動画の帯域幅により正規化したネットワーク全体の消費帯域幅を示す．ただし，ブロック分割数 $d = 10$ とし，ポアソン分布に基づくユーザ生成頻度の平均を 3[ユーザ/分] とする．Parvianen-Parnes 方式が複製数 r に比例し消費帯域幅が増加するのに対し，提案方式の消費帯域幅は複製数 $r = 8$ の場合でも約 23.8%の増加に抑えられている．すなわち，ユーザに近いリンク上のトラヒック負荷はほとんど変化しないことがわかる．

以上 2 つのシミュレーション結果より，サーバ付近のリンク上の利用可能な帯域幅の制限にのみ基づき，複製数 r を増加させることが可能であることがわかる．複製数 r の増加は追跡精度の向上をもたらす．

5. む す び

本研究では，MPLS 網において複数の P2MP LSP を用いたマルチキャスト電子透かし方式を提案した．本提案では暗号化および復号化処理を排除し，選択的なブロック転送によりユーザ間のコンテンツの識別化を図ることにより，消費帯域幅の抑制および追跡精度の向上を実現する．コンピュータシミュレーションにより，Parvianen-Parnes 方式と比較し約 44%の消費帯域幅を実現し，複製数 $r = 8$ の場合でも約 23.8%の増加に抑えることが可能であることを示した．今後の課題としては，共謀攻撃に対する具体的な追跡方法の検討および実ネットワークへの実装による検証が必要である．

文　献

[1] N. Wagner, “Fingerprinting”, in *Proc. of the 1983 IEEE Symposium on Security and Privacy*, Oakland, pp. 18-22, 1983.

[2] I. Brown, C. Perkins and J. Crowcroft, “Watercasting: distributed watermarking of multicast media”, in *Proceedings of the First International Workshop on Networked Group Communication*, pp. 286-300, 1999.

[3] P. Judge and M. Ammar, “WHIM: Watermarking multicast video with a hierarchy of intermediaries”, in *Proc. of NOSSDAV 2000*, Chapel Hill, NC, Jun. 2000.

[4] R. J. Anderson and C. Manifavas, “Chameleon - A new kind of stream cipher”, in *Fast Software Encryption-FSE ’97, LNCS 1267*, pp. 107-113, 1997.

[5] R. Parviainen and P. Parnes, “Large scale distributed watermarking of multicast media through encryption”, in *Proc. of IFIP Communications and Multimedia Security 2001*, Norwell MA: Kluwer Academic Publishers, pp. 149-158, 2001.

[6] J. Domingo-Ferrer, F. Sebé and Antoni Martinez-Balleste, “On multicast fingerprinting and collusion security”, in *AXMEDIS International Conference 2005*, pp.153-159, Nov. 2005.

[7] R. Aggarwal, D. Papadimitriou, S. Yasukawa, “Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)”, RFC4875, May 2007.