平成１６年度 東京大学大学院 修士論文

A thesis for a master's degree

マークパケットの統計処理による IP 経路逆探索

- サブマリンノードの検出及び正悪ユーザの判別 -

IP Traceback based on the Statistical Analysis of Marked Packets

- Detection of Submarine Nodes and Discrimination between Attackers and Legitimate Users -

平成１７ 年 １ 月 31 日

曽小川　貴裕

Takahiro Sokawa

学籍番号： 47-36312

東京大学大学院 新領域創成科学研究科 基盤情報学専攻

Dept. of Frontier Informatics,

Graduate School of Frontier Sciences, The University of Tokyo

指導教官 supervisor　　**若原 恭 教授** Professor Yasushi Wakahara

目次

第 1 章

序論

1.1 研究の背景と目的

近年のネットワーク技術の著しい発達に伴い，今日，IP ネットワークは社会的に非常に重要な役割を果たしている．しかしその一方で，コンピュータセキュリティを脅かす事件は後を絶たず，その中で不正アクセスによる情報セキュリティ侵害も実被害は減少傾向にあるものの [1]，依然として大きな社会問題となっている．

そのような不正アクセスに対する一般的な対策は，検知，追跡，防御の三つに分類される [2]．本論文で提案する手法は，その中で不正アクセスの追跡に関するものである．

追跡の主要な目的の一つは，攻撃者もしくは攻撃者に最寄のルータを特定することによって，発信源が攻撃者か正規ユーザであるかを犠牲者が判別することができないパケットフローに対し，正規ユーザの通信への被害を最小限にとどめて，攻撃者の通信のみを遮断できるようにすることである．

しかし，追跡，すなわち，IP パケットの真の送信者を特定することは容易ではない．それは，IP プロトコルでは匿名性を守るため送信ホストが自身の送信 IP アドレスを任意に決めることができるのに対し，パケットの送信元を特定する機構がないためである．つまり，攻撃者は容易に送信元 IP アドレスを偽装できるが，IP アドレスが偽装（IP Spoofing）された場合，既存の経路逆探索コマンドである Traceroute では偽装された IP アドレスに対しての経路を逆探索することになり，正しく経路を逆探索することはできないため，パケットの送信元を特定するのが困難なのである．そこで，送信元が偽造されたパケットフローから攻撃者もしくは攻撃者に最寄のルータを特定することを目的とした経路逆探索が重要となってきている．

一方で，真の攻撃者が踏み台とする多数のマシンから特定のホストに対し一斉に過剰なトラヒックを発生させることにより，WWW，FTP といったサービスを妨害する攻撃が近年社会的脅威となっている．これを，Distributed Denial of Service(DDoS) 攻撃と呼ぶ [3]．また，DDoS 攻撃では大量のトラヒックがネットワーク上を流れるため，正規ユーザに対するサービスの妨害だけではなく，帯域圧迫やルータの負荷増大といった被害ももたらされる．実際の DDOS 攻撃の被害として，2000 年 2 月に Yahoo!,Amazon.com,CNN 等の多数の米国大手商用サイト，また 2001 年 1 月には Microsoft の商用サイトが業務停止状態に追い込まれたという事例が報告されている．さらに，2003 年 8 月頃に猛威をふるったブラスターやその亜種に感染したマシンが，Microsoft の Windows Update Server に DDoS 攻撃

を行うことが確認されており，今後も DDoS 攻撃による脅威は続くと考えられる．

これに対し，最近では，DDoS の予兆を検知してトラヒックを止めてしまう技術や，膨大なトラヒックに対処できるファイアウォール製品が登場してきたため，ある程度の対策は確立されつつある．しかしながら，DDoS 攻撃は攻撃を特徴付けるパターンが存在しないため，攻撃者と正規ユーザのパケットフローを正確に切り分けることは非常に困難である．さらに，これらの対策では，帯域圧迫やルータの負荷増大といった被害を軽減することはできない．そのため，攻撃者もしくは攻撃者に最寄のルータを特定し，そこでトラヒックを遮断することが最も効果的な対策であると考えられている．しかし，DDoS 攻撃では送信元アドレスを偽装して攻撃が行われることが非常に多い．そこで，DDoS 攻撃への対策として，送信元アドレスを偽装した攻撃ホストに対する経路逆探索技術（以降，IP 経路逆探索と呼ぶ）の確立が必要となる [6]-[15]．この際，IP 経路逆探索には，できる限り多数の攻撃者もしくは攻撃者に最寄のルータを短時間に検出する能力が求められるが，実ネットワークへの導入を想定すると，機能を実装したルータへの負荷や段階的な導入が可能であるかといった点も重要である．これらの要素を考慮したとき，既存の IP 経路逆探索方式の中で最も DDOS 対策として適していると考えられるのは，確率的パケットマーキング (Probabilistic Packet Marking) 方式である [10]-[15]．

確率的パケットマーキング方式とは，マーキング機能を持ったルータが通過するパケットに対し確率的にアドレス等の経路情報をマークし，それらのマークパケットを収集した犠牲者がマーク情報を基に経路を逆探索し，その経路上で犠牲者から最も遠いルータを攻撃者に最寄のルータとして特定する方式である．この方式では，検出性能はルータがマークした情報に依存するため，従来研究ではマーク情報の中身，つまりどういった情報をマークするかという点に焦点が当てられ，様々な手法が提案されてきた．しかしながら，最寄のルータの特定にマーク情報のみを利用するという既存手法には，原理上解決することができない二つの大きな問題がある．

まず一つ目の問題は，攻撃経路が重複している場合，犠牲者に近い位置に存在する攻撃者の最寄のルータを原理的に検出できないケースが存在するということである．特に，DDoS 攻撃では数百〜数千の攻撃者が参加する可能性があり，攻撃経路の重複が頻繁に起こることが予想されるため，既存手法では最寄のルータの検出精度に限界があると言える．ただし，確率的パケットマーキング方式では検出することができないこれらのノードを本論文ではサブマリンノードと定義する．

そして二つ目の問題は，パケットマーキングは単に通過するパケットに対して行われるため，犠牲者はマークパケットの情報から送信元が攻撃者であるか正規ユーザであるか判断できないということである．そのため，特定された最寄のルータを攻撃パケットが通過するか否かを犠牲者が判別することは不可能であり，特定結果を基にパケットフィルタリングを適用すると，正規ユーザからのパケットの誤フィルタリングにつながる可能性がある．

そこで本論文では，マークパケット内に挿入された情報そのものではなく，マークパケットの統計的性質を有効利用することで，既存の確率的パケットマーキング方式の抱える二つの問題を解決する手法を提案し，その有効性をシミュレーションによって検証する．具体的には，問題 1 に対して，マークパケット数を利用することでサブマリンノードを特定し，検出精度を向上させる「マークパケット数に基づくサブマリーンノード検出手法」を提案する．また，問題 2 に対しては，マークパケットの到着間隔分布を利用して，攻撃者と正規ユーザの分別を行う「マークパケットの到着間隔分布に基づく攻撃者と正規ユーザの分別法」を提案する．

1.2 本論文の構成

本論文は以下のように構成されている.

第 2 章「IP 経路逆探索に関する先行研究」では，IP 経路逆探索に関する先行研究を概説し，送信元 IP アドレスを偽造した DDoS 攻撃への対策として確率的パケットマーキング方式（Probabilistic Packet Marking scheme : 以下，PPM 方式）が最も有望であることを示す.

第 3 章「確率的パケットマーキング方式とその問題点」では，確率的パケットマーキング方式の基本構造，動作原理，PPM 方式の代表的な手法である Edge Sample 手法について説明し，その後既存の PPM 方式が抱える 2 つの問題点を明らかにする.

第 4 章「マークパケット数に基づくサブマリンノード検出手法」では，マークパケット数を利用することで既存手法では検出することができないサブマリンノードを特定する手法を提案し，様々なネットワーク構造，条件を想定したシミュレーションにより，その有効性を示す.

第 5 章「マークパケットの到着間隔分布に基づく攻撃者と正規ユーザの分別法」では，マークパケットの到着間隔分布を利用することにより攻撃者と正規ユーザを判別する手法を提案し，シミュレーションによりその判別精度を評価し有効性を示す.

第 6 章「結論」では，本研究のまとめと今後の課題について述べる.

第 2 章

IP 経路逆探索に関する先行研究

近年，送信元を偽装されたパケットの発信源を特定するために，様々な IP 経路逆探索方式が提案されてきている．しかし，既存方式の中でも，本研究の主対象である DDoS 攻撃に有効な方式は限定される．本章では，DDoS 攻撃対策として有望な既存の IP 経路逆探策方式を説明し，その有効性を論じる．

まず 2.1 節において，既存研究を評価し本研究を進めていく上での前提条件及び評価指標について述べる．そして，2.2 節では，経路逆探索方式を体系的に説明し，各方式の概略・特性を簡単に述べ，その有効性を比較する．そして，DDoS 攻撃対策としてみたとき，確率的パケットマーキング方式が最も有効であることを示す．

2.1 前提条件及び評価指標

2.1.1 IP 経路逆探索方式を評価する上での前堤条件

IP 経路逆探索方式の有効性を評価するためには，攻撃を行う攻撃者，逆探索を行う犠牲者・ルータについての前提条件を定義する必要がある．ここでは，実ネットワークへの導入を考慮し，その 3 要素に対し以下の前提条件を定める．

攻撃者の前提条件

条件 1 攻撃者は，どのようなパケットでも送ることができる
条件 2 攻撃者は大量の攻撃パケットを送る
条件 3 複数の攻撃者が連携して動作することができる

犠牲者の前提条件

条件 1 犠牲者は DDoS 攻撃を検知・認識することはできる
条件 2 犠牲者におけるアルゴリズムは容易に変更することができる
条件 3 犠牲者はファイアーウォール等の対策を講じており，極めて短時間のうちにダウンすることはない

ルータの前提条件

条件１ ルータで使用されているアルゴリズムを変更することは困難である
条件２ ルータの計算資源 (CPU またはメモリなど) は有限であり，それほど大きくない
条件３ ルータはのっとられることはない
条件４ 必ずしもすべてのルータが経路逆探索に対応した機能を持っているわけではない
条件５ ISP 間の連携はあまり期待できない
条件６ パケットの順序逆転やパケットがロスしたりすることはある

2.1.2 IP 経路逆探索方式を評価する上での評価指標

IP 経路逆探索方式の有効性を論じるとき，最も重要となるのが検出能力である．しかしながら，実ネットワークへの導入を考慮した場合，経路逆探索を実行することでのルータや犠牲者への負荷も非常に重要な要素となる．そこで，評価指標をおおまかに検出能力と負荷と定義し，各項目を以下のように定める．

検出能力

指標１ 検出性能（検出力，正確性，迅速性）
指標２ 攻撃後の逆探索が可能であるか否か
指標３ 全てのルータが機能を実装していなくても逆探索であるか否か

指標２は，逆探索が攻撃中に制限されているか否かを判定する．DDoS 攻撃では短時間の攻撃で被害をもたらすこともあるが，攻撃中に全ての経路を特定することは困難である．また，仮に攻撃後の逆探索が可能であれば，次に同一のホストから攻撃を受けた時，対処が容易になる．

指標３は実現性という観点から着目した．なぜなら，現実的に考えると各ルータへの機能の実装は徐々に行われるため，経路を再構成するのに全てのルータが機能を実装している必要があるとすると，たとえ検出性能が優れていたとしても実際には経路を再構成することはできないことになるからである．

負荷

指標１ ルータでのオーバヘッド
指標２ ルータのデータストレージ
指標３ ISP 間の連携を必要とするか否か
指標４ 犠牲者の計算コスト
指標５ 犠牲者のデータストレージ
指標６ 帯域への負荷

指標３については，ルータの前提条件の条件５で ISP 間の連携はあまり期待できないとしたため，評価指標とした．

2.2 IP 経路逆探索の関連研究

2.2.1 経路逆探策方式の全体像

我々の研究の動機付けとなった，IP 経路逆探索方式に関する先行研究について概略を述べる．

現在 IP Spoofing の対策には，主に予防型の手法 [4, 5] と犠牲者が攻撃されてから反応する反応型の手法（IP 経路逆探索）[6]-[15] がある．予防型の手法には代表的なものとして Ingress Filtering がある．一方，反応型の手法はその特徴から, Link Testing, Logging, ICMP Traceback, 確率的パケットマーキング方式，の 4 つの方式に分類されている．Ingress Filtering は，IP 経路逆探索方式ではないが，有力なライバルであるため載せておく．

2.2.2 Ingress Filtering

Ingress Filtering とは，ネットワークの境界となる Node で，不正な送信元の IP アドレスを持ったパケットをフィルタリングする技術のことである [4]．この手法においては，IP アドレスの妥当性を確認するためにルータの負荷が大きいことや，IP アドレスの管理負荷が大きいことから，比較的規模の小さい AS 内が適用範囲と考えられる．また，同一の AS 内の別のホストに偽装された場合は，フィルタリングできないのが大きな欠点である．

2.2.3 Link Testing

Link Testing は，犠牲者が検知した DDoS 攻撃を特徴づけるシグナチャを利用して，攻撃パケットフローの経路上のルータを特定するという原理である．具体的には，シグナチャとしてパケットの宛先の IP アドレスや，統計的なパターン等を利用して逆探索を行う．代表的な手法に，Input Debugging[6], Controlled Flooding[7] がある．

しかし，いづれの手法も以下の制限／欠点がある．

- 攻撃経路上の全てのルータで，攻撃パケットと正規利用者のパケットとの識別を可能とするような固有のシグナチャが必要となる
- 攻撃中にしか経路逆探索ができない

一般的に，DDoS 攻撃において，攻撃パケットと正規の利用者のパケットを識別するためのシグナチャを検出することは非常に困難である．また，攻撃中に逆探索できない＝検出能力の指標 2 を満たしていない，ことになる．

Input Debugging

この手法は，攻撃経路上のすべてのルータが Input Debugging 機能をサポートしていることを前提条件としている．Input Debugging 機能とは，出力インタフェースで獲得したパケットがどの入力インター

フェースを通過したかを特定する機能のことである．各ルータ及び犠牲者で行われる処理は，出力インターフェースで獲得したパケットに対し攻撃のシグナチャを利用して攻撃パケットであるかを判定し，その後 Input Debugging 機能を利用して，それらの発信元の入力インターフェースを特定する．この処理を，再帰的に犠牲者から攻撃元まで繰り返す．ただし，異なる ISP 間では攻撃のシグネチャを人手を使って受け渡しする必要がある．

Controlled Flooding

Controlled Flooding は，まずリンクに対し，バースト的なトラフィックを与えることで，攻撃者からのトラフィックがどの程度不安定になるかを観測する．そして，Input Debugging と同様に再帰的に攻撃源を特定する．しかしながら，バースト的なトラフィック自体が DDoS 攻撃になってしまうため，現実的ではない．

2.2.4 Logging

Logging とは，ある特定のルータで通過する全てのパケットのデータのログをとり，犠牲者が DDoS を検知した後，疑わしいパケットのデータと各ルータで残されたログとの整合性をとり，経路を再構築していく方式である．代表的な手法に，SPIE(Source Path Isolation Engine)[8] がある．

この方式では大量のログを記録する必要があるため，データストレージの点で問題がある．また，全てのパケットに対しログを残す処理を行うことは，ルータオーバヘッドが増大する．

SPIE(Source Path Isolation Engine)

SPIE システムは，DGA(Data Generation Agent)，SCAR(SPIE Collection and Reduction Agent)，STM(SPIE Traceback Manager) という 3 つの構成要素からなっている．

DGA は，パケットのデータを保管する機能を持ったルータのことである．DGA では，通過する全てのパケットの hash を計算し，その情報を保持する．また，特定の領域に含まれるいくつかの DGA を管理しているのが SCAR であり，すべての SCAR を管理しているのが STM である．

SPIE では，DGA がハッシュ情報を基に対象パケットがその DGA を通過したかを判定し，SCAR は自領域内で管理している DGA からの判定情報により攻撃経路を再構築する．そして，STM で各 SCAR で作られた経路の木を連結させることにより完全な攻撃経路を再構築する．これにより攻撃者に最寄の DGA を特定する．よって，パケット単位での追跡が可能となる．

しかしながら，多量のパケットが通過するときに全ての情報を保持することは，hash を用いることで情報量を削減しているとはいえ，データストレージの点で負荷が大きい．また，STM-SCAR-DGA 間で高度な連携を必要としており，大規模ネットワークへの適用は現実的ではない．最後に，STM そのものが DDoS 攻撃の脅威にさらされる恐れがある．

2.2.5 ICMP Traceback

ICMP Traceback とは，経路上の各ルータが通過するパケットの一部を極めて低い確率で選択し，選択されたパケットの経路上のアドレス情報を含んだ ICMP Traceback Message を新たに生成して犠牲者に送り，その情報を元に経路を再構築する方式である．代表的な手法に iTrace 手法がある [9].

この方式は，逆探索を行うのはあくまで犠牲者であり，またルータで情報を保管するといった必要もないため，ルータへの負荷という点では優れている．しかしながら，新たにパケットを生成するため，帯域への負荷が増大する．

iTrace

iTrace 手法では，全てのルータが通過するパケットの一部を確率 $p = \frac{1}{20000}$ で選択し，選択されたパケットが通過した 1hop 上流のルータの情報を含んだ ICMP Traceback Message を新たに生成し，犠牲者に送る．犠牲者ではこれらのメッセージを収集して攻撃者までの経路を再構築する．

この手法は，新たに生成するパケットに含まれる情報は 1hop 上流のルータのものであるため，全てのルータが iTrace 機能を実装している必要がある．

2.2.6 確率的パケットマーキング (Probabilistic Packet Marking) 方式

確率的パケットマーキング方式は，通過するパケットに対してある確率 p でルータのアドレス情報等を埋め込み，犠牲者側でそれらを収集して攻撃経路を再構築する方式である [10]-[15]．代表的な手法に Edge Sample 手法 [10, 11] がある．基本原理は ICMP Traceback と同様であるため，ICMP Traceback と同様の利点を持つこととなる．しかし，ICMP Traceback が新たにパケットを生成するのに対し，この方式では通過するパケットに対し直接情報を埋め込むため，余計なトラフィックを発生することがなく，帯域に負荷をかけないという特徴がある．また，代表的 ICMP Traceback 手法である i Trace では物理的に隣接するルータが ICMP Traceback 機能を実装していなければ経路を逆探索できないのに対し，確率的パケットマーキング方式では全てのルータがマーキング機能を実装していなくても経路を逆探索できるという特徴もある．そのため，確率的パケットマーキング方式は現在最も有望な IP 経路逆探索方式と言える．

Edge Sample 手法

Edge Sample 手法では，パケットが通過した連続する二つの IP アドレスを利用する．マーキング機能を搭載したルータは通過するパケットに対しある確率 p で自分のアドレスをマークする．そして，アドレスをマーキングした場合，次に通過する機能搭載ルータはさらに自分のアドレスをマークする．犠牲者は，二つのアドレスの連結関係を利用することで経路を逆探索する．そのため，全てのルータがマーキング機能を実装していなくても逆探索可能となる．

第 3 章

確率的パケットマーキング方式とその問題点

3.1 PPM 方式

PPM 方式では，以下の二つのプロセスにより，攻撃経路を逆探索し，攻撃者に最寄のルータを特定する．

プロセス 1 マーク機能を実装したルータ（以下，CN(Co-operating Node) と呼ぶ）が，通過するパケットに対し，そのルータのアドレスやリンクを識別する情報を一定確率でマークする

プロセス 2 マークパケットを受信した犠牲者がそれらの識別情報を利用して経路を再構築することにより，攻撃者に最寄のＣＮ（以下，NCN(Nearest CN)）を特定する

本論文では，前者の処理を Packet Marking Process，後者の処理を NCN Identification Process（図 3.1)，また，マーク機能を実装していないルータをノーマルルータと呼ぶこととする．

図 3.1 の例では，CN 1，CN 2，CN 3 から回収したマーク情報 Inf.1,Inf.2,Inf.3 を用いて攻撃経路を逆探索し，CN 1 を NCN として特定している．

PPM 方式に関する既存研究について

PPM 方式における NCN の検出性能（検出数，正確性，迅速性）はマーク情報に依存するが，マーク情報を IP ヘッダ内に挿入するという制約があるため，既存研究では IP ヘッダのどのフィールドにどのような情報をマークするかということに主に焦点が当てられている．

まず，マーク情報を挿入するフィールドについては，IPV4 を対象に以下の二つのフィールドが考えられている．

- アイデンティフィケーションフィールド（利用されることが極めて少ない）
- オプションフィールド

前者のアイデンティフィケーションフィールドについては 16bit という制約があるため，PPM 方式で

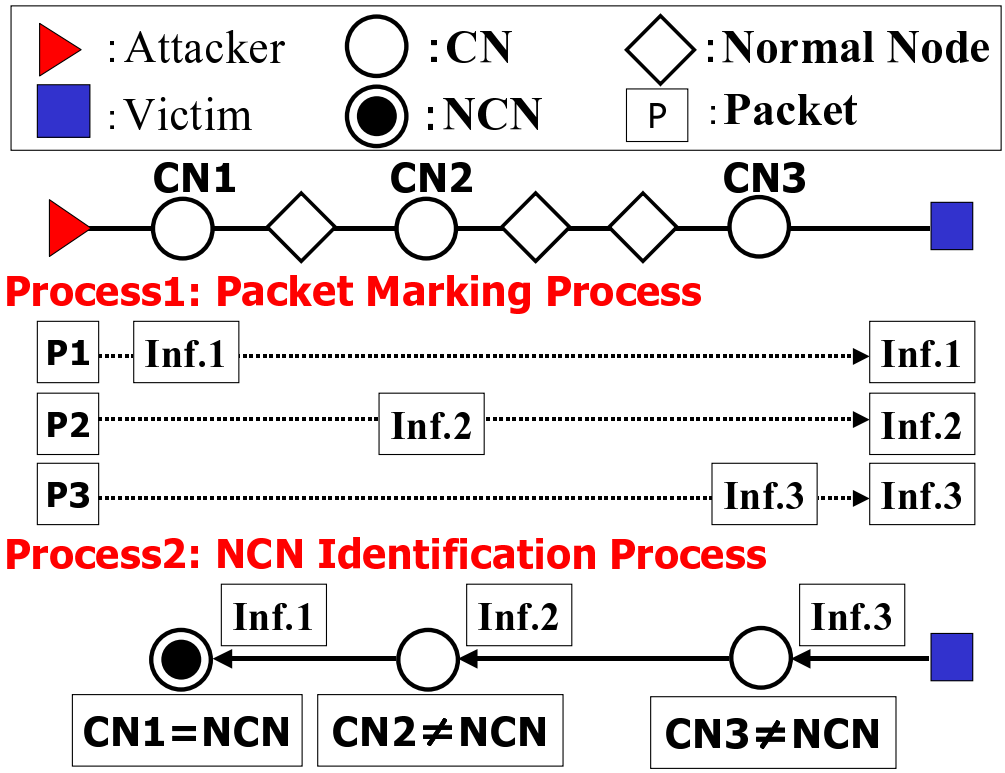

図 3.1: PPM 方式

必要な情報を全てマークすることは不可能である．そこで，マーク情報の分割，符号化を行うことで 1 パケットに挿入される情報量を削減するといった対策が採られている．しかしながら，情報の分割，符号化を行うことは，情報の復元の際に膨大な計算量を必要とし，また多数の NCN の誤検出につながる．その対策として，Song らは，ハッシュ関数を有効利用することで，計算量を減らし誤検出率を小さくする手法を提案した [11]．ところが，この手法では犠牲者は正しいインターネットマップを持たないと経路を正しく再構成することができないという別の問題が生じている．

後者のオプションフィールドについては，データサイズの厳しい制限はないため，完全なマーク情報を付与することが可能である．そのため，前者のフィールドを使用するより，検出性能という点では優れている．しかし，オプションフィールドの使用は，現実のネットワークではハードウェア処理が困難であり，ソフトウェア処理となって処理能力低下を招くことがあるため，あまり望ましくない．したがって，オプションフィールドを使用する場合にも，マークする情報量をできる限り抑えることが求められる．

次にマークする情報に関しては，既存手法は以下の 2 種類に分類することができる．

- 複数のパケットに経路情報を分散してマークする手法 [10, 11]
- 一つのパケットに連続した経路情報をマークする手法 [12, 13]

前者の代表的な手法には，当該 CN のアドレス情報のみを利用する Node Sampling[10] やパケットが通過した連続する二つの IP アドレスを利用する Edge Sample 手法 [10, 11] などがある．特に Edge Sample 手法は既存の PPM 手法の中で最も代表的な手法である．これらの手法では，一つのパケットに

マークを行うのは最大で当該 CN と次の CN の 2 つの CN だけであるため，情報量を抑えやすい傾向にある．

一方，後者の代表的な手法には，経路上の当該 CN のアドレスと以降通過した全ての入力インターフェースに対応した分岐情報を利用する Branch Label 手法 [12] などがある．これらの手法では，一つのパケットに対し，当該 CN とそれ以降に通過する CN の経路識別情報がマークされるため，NCN から 1 つのマークパケットが到達すれば，その NCN を特定することが可能となる．

前者・後者の手法はマークする情報の中身という点では異なるが，NCN の特定にマーク情報のみを利用するという点では同一である．しかしながら，NCN の特定の際にマーク情報のみを利用することでは解決することができない 2 つの問題が存在することが判明した．

以降では，まず PPM 方式の中で最も代表的な手法である Edge Sample 手法について説明し，その後 PPM 方式が抱える 2 つの問題点について述べる．

3.2 Edge Sample 手法

Savage らによって提案された Edge Sample 手法では，パケットが通過した二つの連続 CN の IP アドレス (Address Label(32bit), Next Address Label(32bit)) と犠牲者から Address Label の値をマークした CN までの距離 (step 数 (5bit)) をマーク情報 l =(Address Label, Next Address Label, Step No) として利用する [8]．ここで，step 数とはパケットが通過する CN の数を表し，それにはターゲットとなる犠牲者も含む．この手法では図 3.2 のような処理により NCN の特定を行う．

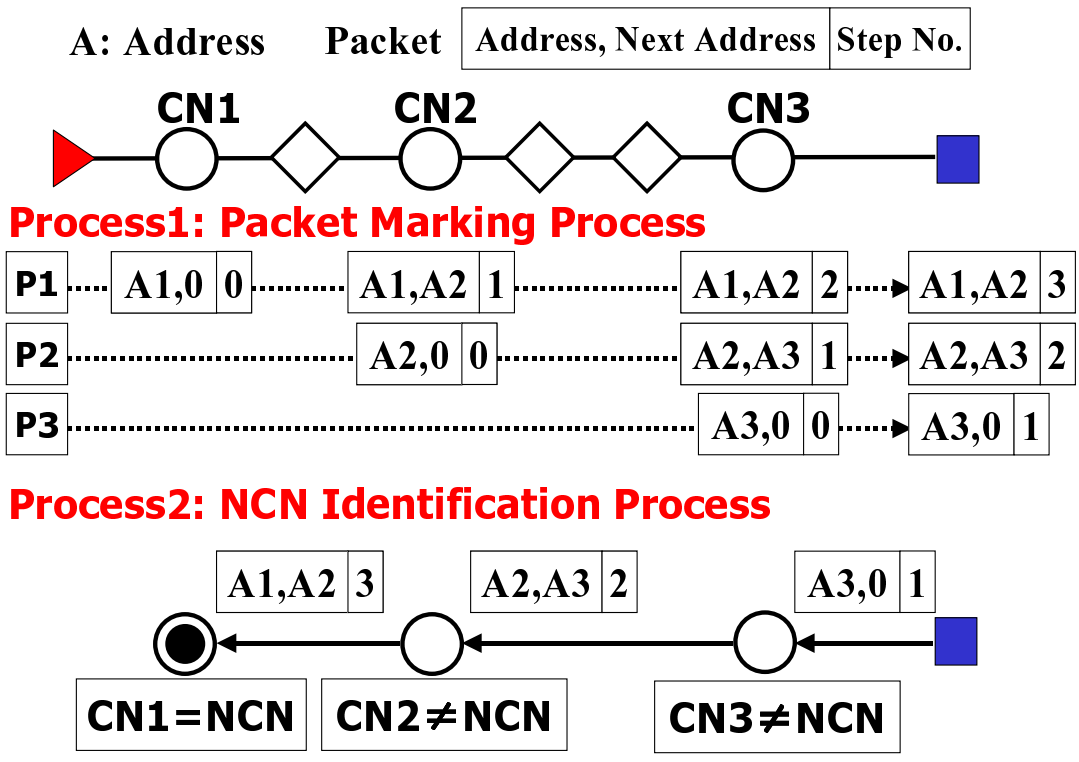

図 3.2: Edge Sample 手法

詳細な動作原理については以下に示す．ただし $l=(l^a,l^n,l^s)$ とし，各マークフィールドの初期値は，$(l^a,l^n,l^s)=(0,0,0)$ とする．また，上書きを許可する理由は，上書きを許可しない場合，攻撃者によるマークフィールドの偽造に著しく弱くなるためである．

Packet Marking Process

各ＣＮおよび犠牲者は，通過するパケットに対し下記のマーク処理を施す．

CN における処理

手順１ 一様乱数 $r(0\leq r<1)$ を生成する．
手順２ マーキング確率 p に対して $r<p$ の場合 l^a に自らのＩＰアドレスをマークし（すでに他のＣＮがマークしていれば上書き）手順３を実行する．そうでなければ手順４に進む．
手順３ $l^n=0$，$l^s=0$ にして処理を終了する．
手順４ $l^a\neq 0$ である場合，l^s を１増やす．さらに，$l^n=0$ であれば自らのＩＰアドレスをマークする．そして処理を終了する．

犠牲者における処理

手順１ 受信したパケットが $l^a\neq 0$（すでにマーク済み）である場合，l^s を１増やす．そうでなければ何もせずに処理を終了する．

NCN Identification Process

同一の (l^a,l^n,l^s) の値を持つマークの集合 $\psi^{l^a,l^n,l^s}=\{l|l^a=l'^a\cap l^n=l'^n\cap l^s=l'^s\}$ を Edge Sample Group(ESG) と呼ぶ．そして ESG によって分類した商集合を考え，それを $\Psi=\{\psi^{l^a,l^n,l^s}\}$ とする．ここで犠牲者によってマークされた場合の集合（実際にはマーク処理を行わない）である $\psi^{l^a,0,0}$ をルートとし，各ノードを CN によるマークの集合 ψ^{l^a,l^n,l^s} とするような木 $\mathcal{T}$ を考える．犠牲者はマークされたパケットを受信する毎に以下の処理を繰り返して自身をルートとする木 $\mathcal{T}$ を構築し，NCN を特定する．

犠牲者における処理

手順１ 受信したマークパケットにおいて $\psi^{l^a,l^n,l^s}=\phi$ であればマーク情報 l を ψ^{l^a,l^n,l^s} に入れ手順２に進む．そうでなければ処理を終了する．
手順２ $\Psi=\{\psi^{l^a,l^n,l^s}\}$ の l^s の最大値を l^s_{max} とすると，手順３の処理を d を 1 から 1 ずつ増加させ，l^s_{max} になるまで繰り返す．それが終了したら，手順４へ進む．
手順３ d が 1 のときは，$\psi^{l^a,l^n,1}$ を木 $\mathcal{T}$ のルートとリンク連結する．d が 1 でないときは，$(l^a=l'^n)\cap(l^s=d)\cap(l'^s=d-1)$ を満たす ψ^{l^a,l^n,l^s} と $\psi^{l'^a,l'^n,l'^s}$ をリンクで連結する．
手順４ 構成された木 $\mathcal{T}$ のリーフノードとなる ESGψ^{l^a,l^n,l^s} の要素である l が持つ l^a を NCN のアドレスとみなす．

3.3 PPM 方式の問題点

PPM 方式には，以下の２つの主要な問題点がある．

問題１ 複数の攻撃経路が重複している場合，理論上検出することができない NCN が存在する

問題２ マークパケットが攻撃パケットであるか方式内で判別することができないため，正規ユーザのパケットの誤フィルタリングを誘発する可能性がある

以降では，問題１，２の詳細について述べる．

3.3.1 問題１：理論上検出することができない NCN の存在

PPM 方式では，前述の図 3.1 のように単一の攻撃経路に対しては，逆探索に必要なマークパケットが揃えば確実に NCN を特定することができる．しかしながら，経路の一部が重複している場合，原理的に NCN を検出できないケースがある．

その具体例として図 3.3 のように，攻撃者１と攻撃者２による攻撃経路が一部重複しているケースを想定する．この例では，攻撃者１のパケットフローから Inf.1,Inf.2,Inf.3，攻撃者２のパケットフローから Inf.2,Inf.3 を挿入したマークパケットが生成される．このとき，実際には CN1（攻撃者１の NCN）と CN2（攻撃者２の NCN）が NCN となるが，NCN Identification Process において，攻撃者１からのマーク情報 Inf.1 により CN1 と CN2 が連結していると見なされるため，CN １のみが NCN として特定され，CN2 を NCN として検出することはできない．

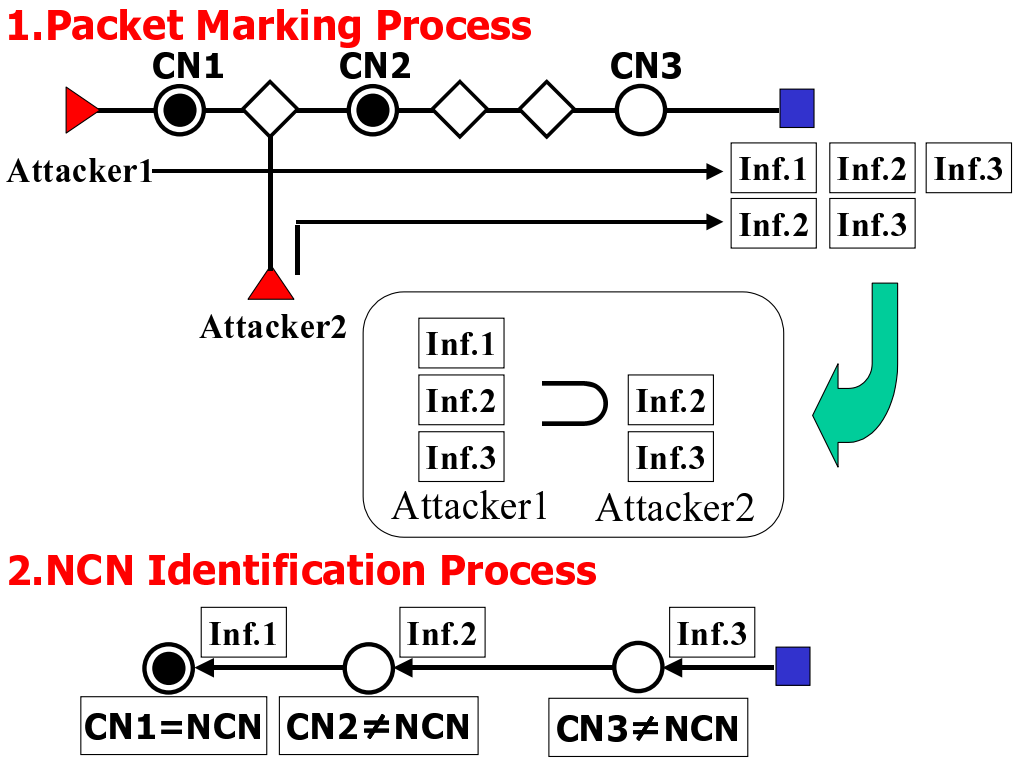

図 3.3: NCN が検出できないケース

この問題は，PPM による NCN 特定では，マーク情報を基に，犠牲者をルート，パケットが通過した CN をノードとした木 $\mathcal{T}$ を構成し，そのリーフノードとなる CN を NCN として特定するために起こる．つまり，リーフノードではない CN を NCN とする攻撃者がいた場合，その攻撃者の NCN と犠牲者間の

経路がリーフノードである別の NCN と犠牲者間の経路に包含されてしまうため，検出することができなくなるのである（図 3.4）．本論文では，PPM 方式で検出することができない NCN をサブマリンノードと呼ぶこととする．

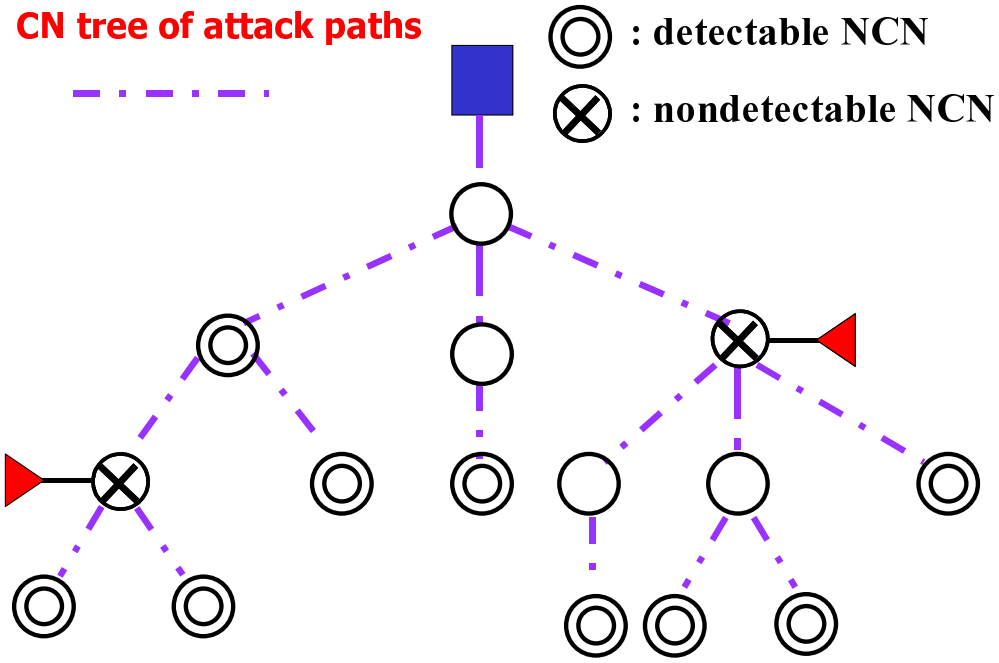

図 3.4: NCN 検出と $\mathcal{T}$ の関係

一方で，数百〜数千の攻撃者が参加する可能性がある DDoS 攻撃では，攻撃経路の重複が頻繁に起こりえるため，結果として数多くの NCN を原理的に検出できないことになる．そのため，マークパケットに挿入された情報のみを利用して経路を逆探索する PPM 手法単独では，NCN の検出精度に限界があると言える．そこで，サブマリンノードの検出が PPM 方式における大きな課題となる．

3.3.2 問題２：正規ユーザのパケットの誤フィルタリング

PPM 方式における CN の役割は，通過するパケットに対し確率的に経路情報をマークすることだけであるため，犠牲者に到達したマークパケットが攻撃パケットであるとは限らない．（ただし，一般的に正規ユーザのトータルのトラヒック量は攻撃者のものより少ないため，正規ユーザからのパケットフローに対してマーキングが行われる可能性は攻撃者に比べると低い．）

また，マークパケットには経路情報しかマークされていないため，マークパケットの情報から送信元が攻撃者であるか正規ユーザであるかを判別することはできない．さらに，DDoS 攻撃では攻撃を特徴付けるパターンが存在しないため，別の方法でもパケット単位で攻撃パケットか否かを識別することは困難である．

それゆえ，既存の PPM 手法が特定している対象は，厳密には，本来の目的である攻撃者の NCN というわけではなく，DDoS 攻撃が発生している最中のパケット送信者（攻撃者＋送信者）の NCN ということになる．よって，特定された NCN を攻撃パケットが通過するとは限らず，特定結果を基にパケット

フィルタリングを適用すると，正規ユーザからのパケットの誤フィルタリングにつながる懼れがある．

図 3.5 は，正規ユーザの CN を NCN として特定する具体例を表している．この例では，正規ユーザからのパケットフローに対し，CN4 だけしかマーキングを行ってないが，別の攻撃経路とリンクが連結されるため CN 4 も NCN として特定している．この特定結果をダイレクトにフィルタリングに反映させると，CN 4 で正規ユーザからのパケットを誤ってフィルタリングすることになる．

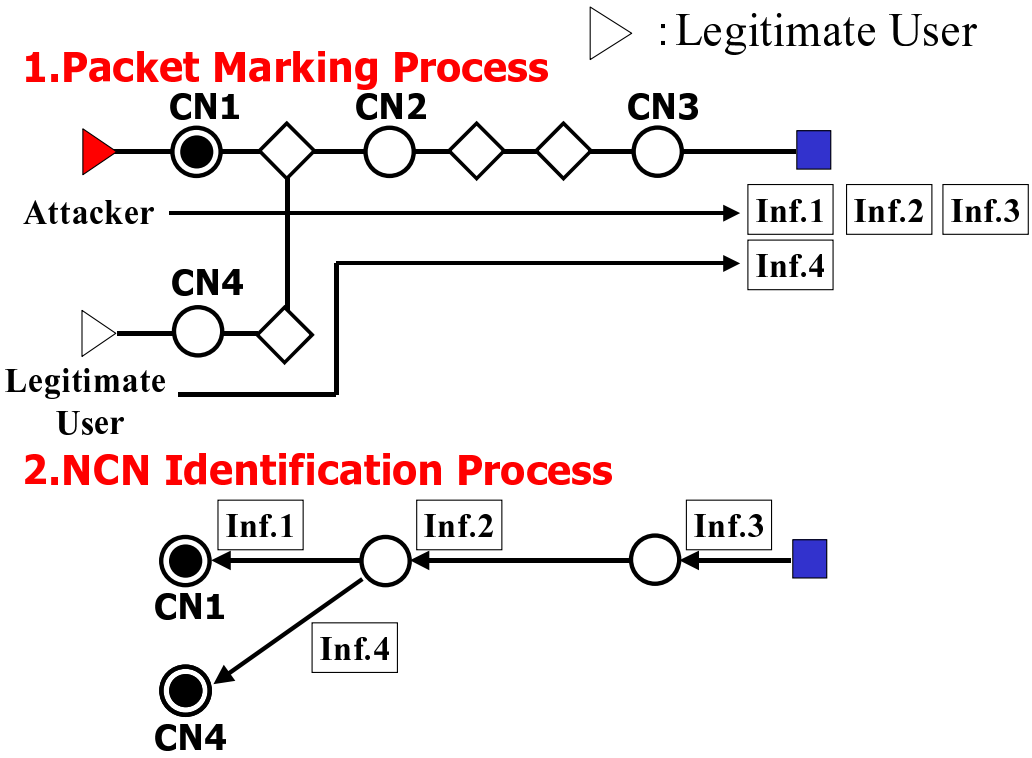

図 3.5: 正規ユーザの NCN の誤検出

現状では，マークパケットに関して PPM 手法内部で正・悪ユーザの判別ができないため，PPM 手法を実ネットワークに導入することを考えた場合，PPM 手法外部の工程，例えば特定した NCN の管理者に問い合わせ実際に攻撃パケットフローが通過しているか否かを調査してもらうといった工程が必要となる．しかし，DDoS 攻撃中の正規ユーザのトラヒック量が多いケースでは，攻撃に無関係な多数の NCN が検出されることが予想されるため，PPM 手法外部での工程を必要とすることは望ましくない．そのため，PPM 手法内部でマークパケットの送信元が攻撃者であるか否かを判別することが重要な課題となる．

第 4 章

マークパケット数に基づくサブマリンノード検出手法

第 3 章では，PPM 方式の問題を論じ，その一つとして，理論上検出することができないノードであるサブマリンノードが存在するため，検出精度に限界があることを指摘した．PPM 方式はパケットにマークされた識別情報によって NCN を特定する方式であるので，検出力をあげる方法としては，従来手法のようにマークする情報の改良，つまり，なんらかの識別情報を新たに付加することがまず考えられる．そのためには，パケットヘッダ内にそれらの情報をマークするフィールドを確保する必要があるが，3.1 節で述べたようにマークフィールドは限られており，マーク情報を増加させることは望ましくない．そこで 4 章では，パケット内に新たな情報を付加せずに犠牲者が得られる情報であるマークパケット数に着目し，その統計的性質を利用することでサブマリンノードを検出する手法「マークパケット数に基づくサブマリンノード検出手法」を提案する．そして，提案手法の有効性をシミュレーション実験を通して検証する．

4.1 マークパケット数に基づくサブマリンノード検出手法

本節では，3.3.1 節で指摘した問題 1 の解決法として，マークパケット数に基づくサブマリンノード検出手法を提案する．ただし，CNi でマークされたマークパケット数を n_{C_i} とする．またマーキング確率を p とする．

4.1.1 着眼点

PPM 方式では，一定のマーキング確率でパケットマーキングを行うため，マークパケット数はパケット数に比例して増加する数値である．したがって，攻撃経路が重複していない場合，その経路上を通過するあて先を犠牲者としたパケット数は一定であるため（パケットロスがないと仮定），経路上に存在する全ての CN から同程度マークパケットが生成されると考えられる．そのため，仮にマークパケットの上書きが不許可であるとすると（実際には許可するが），犠牲者は経路上の全ての CN から同程度のマークパケット数を得ることができる．以降では，まず上書きを許可しないと仮定して話を進め，その後上書きの影響について述べる．

一方，攻撃経路が重複していたとすると，合流するノードからトラヒック量が増加するため，合流前の CN からのマークパケット数より合流後の CN からのマークパケット数の方が多くなることが予想される．

よって，PPM 手法により構成された木 $\mathcal{T}$ のリーフノードとならない CN について，1 つ前に通過したＣＮでマークされたマークパケット数より，自ＣＮからマークされたマークパケット数が多い場合はそのノードはＮＣＮ，同程度である場合は NCN ではないとみなすことで，CN がサブマリンノードであるか否かを特定することが可能であると考えられる．

具体例を示す．例えば，単一の攻撃経路の図 4.1（a）では，n_{C_1}，n_{C_2}，n_{C_3} の関係は $n_{C_1} \approx n_{C_2} \approx n_{C_3}$ となるため，経路上には CN 1 以外の NCN は存在しないと判断することができる．一方，サブマリンノード（= CN2）が存在する図 4.1（b）では，CN 1 ～CN2 間で攻撃パケットフローが合流しトラヒックが増加するため，$n_{C_1} < n_{C_2} \approx n_{C_3}$ となり，CN 2 を NCN として特定することができる．

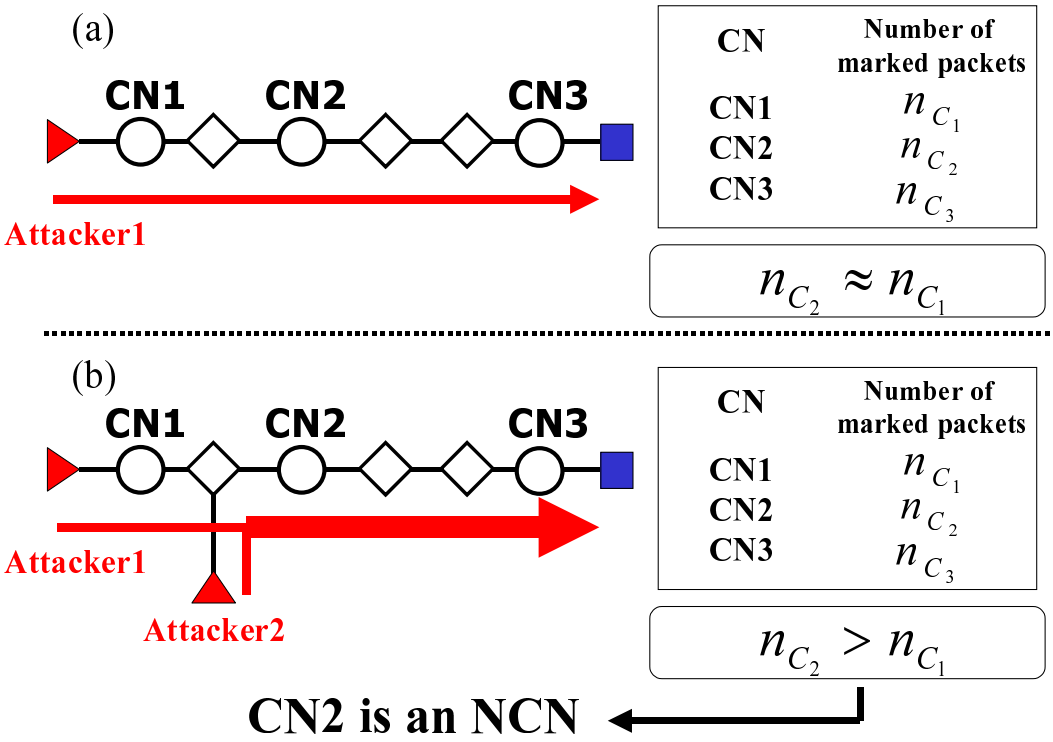

図 4.1: マークパケット数に基づく NCN 検出の例

次に，上記のアイディアに対し，上書きが与える影響について考察する．step 数 s の位置に存在する CN においてマークされたパケットが上書きされずに犠牲者に到達する確率は $p(1-p)^{s-1}$ であるため，step 数の増加に伴い上書きされる確率は上昇する．しかし，上記のアイディアでは自 CN と 1 つ前に通過した CN からのマークパケット数を比較しているため，step 数に関する上書きの影響は考慮する必要はない．なぜなら，自 CN 以降に通過する CN（自 CN と犠牲者間にある CN）において上書きされる確率は，自 CN からのマークパケットと 1 つ前に通過した CN からのマークパケットで変化がないためである．よって，1 つ前に通過した CN からのマークパケットが自 CN で上書きされない確率についての

み考慮すればよいことになる．

CN でのマーク確率は p であり，一つ前の CN でマークされたパケットが自 CN で上書きされない確率は $p(1-p)$ である．ここで，一般的にマーキング確率は小さい値（[10] では $\frac{1}{20}$，[12] では $\frac{1}{20000}$）が想定されているため，図 4.2（p の範囲を $0 < p \leq \frac{1}{20}$）で示すとおり，p と $p(1-p)$ の値はほとんど変化がない．

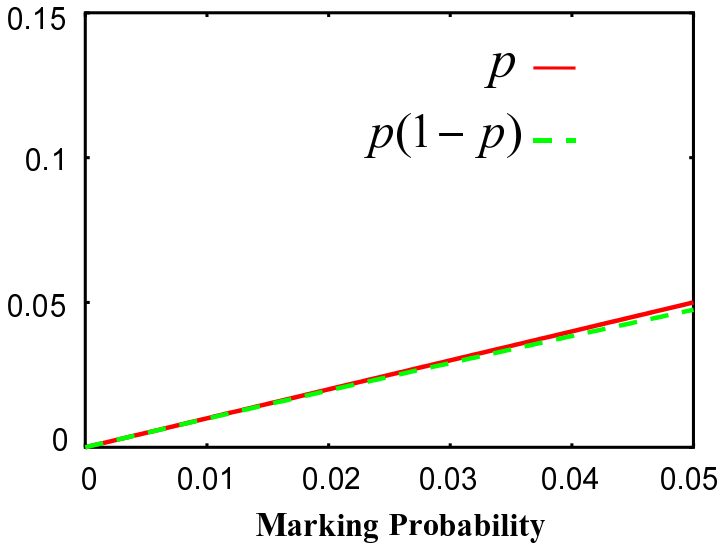

図 4.2: 上書きの影響について

よって，上書きの影響は小さいと言え，上書きが不許可の場合と同様の比較によりサブマリンノードの検出を行うことが可能である．ただし，$\frac{n_{C_1}}{(1-p)}$ と n_{C_2}（一つ前に通過した CN を CN1，自 CN を CN2）を比較すれば，上書きの影響を取り除くことができる．

以上で紹介したマークパケット数の増加を捉えることによりサブマリンノードを検出するという基本的なアイディアを，検定法を用いることにより一般化した手法を，本論文では「マークパケット数に基づくサブマリンノード検出手法」として以下で提案する．

4.1.2　マークパケット数に基づくサブマリンノード検出手法

本節で提案する「マークパケット数に基づくサブマリンノード検出手法」はサブマリンノードの検出を目的としており，PPM 手法で NCN とされなかった CN を対象として NCN 検出を行う．そのため，PPM 手法と組み合わせることで効果を発揮する．

まず図 4.3 のように，リーフノードではないある CNa に関し，1 ステップ上流の CN によりマークされた平均マークパケット数と自 CN でマークした平均マークパケット数をそれぞれ $E(\sum_{i=1}^{k} n_{C_i})$，$E(n_{C_a})$ とする．

すると，以下の式が成り立つ．

CNa が NCN である場合

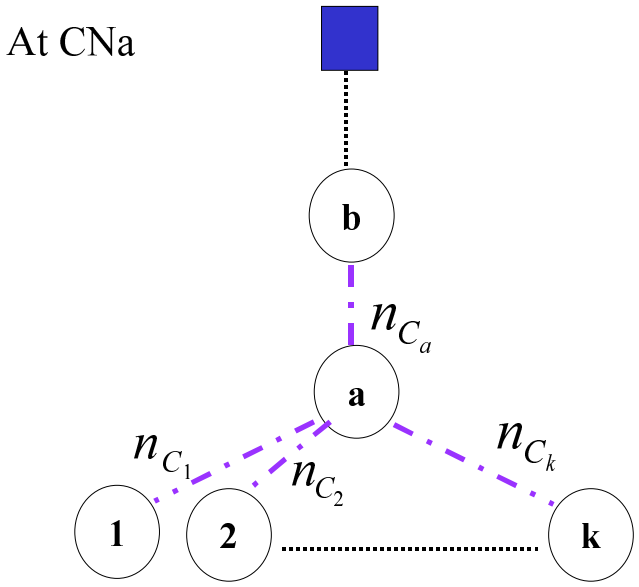

図 4.3: CNa と 1 step 前の CN から得られるマークパケット数について

$$E(n_{C_a}) = E(\sum_{i=1}^{k} n_{C_i}) \tag{4.1}$$

CNa が NCN である場合

$$E(n_{C_a}) > E(\sum_{i=1}^{k} n_{C_i}) \tag{4.2}$$

ただし，CN におけるマーキングはランダムに行われ，また経路上でパケットロスや逆転が起こる可能性があるため，マークパケットはランダムに到着する．そこで以下のような 2 つの仮説をたて，検定法を用いて式（1）もしくは（2）のどちらが成立するか判定し，CNa が NCN であるか特定する．これを，提案手法「マークパケット数に基づくサブマリンノード検出手法」とする．

- 帰無仮説：CNa が NCN でない（式（1））
- 対立仮説：CNa が NCN である（式（2））

ここで，検定法については，標本となる値としてマークパケット数 $\sum_{i=1}^{k} n_{C_i}$，n_{C_a} という 2 値しか得られないため，パラメトリック検定を用いることは難しい．また，対立仮説は適合度に関する片側（上側）検定を必要とするものなので，片側検定が可能な検定法を用いなければならない．そこで，本手法では適合度に関する代表的なノンパラメトリック検定であり，片側検定が可能な 1 標本コルモゴロフ・スミルノフ検定を用いた．また，信頼区間として，上側 95%をとることとした．

本手法における 1 標本コルモゴロフ・スミルノフ検定法では，標本についての累積相対度数と理論分布の累積相対度数との差によって仮説が判定される．すなわち，その差が棄却限界より小さい場合，帰無仮説が採択され，大きい場合，対立仮説が採択される．例えば，ある CNa に関して $n_{C_a} = 64, \sum_{i=1}^{k} n_{C_i} = 36$

であったとすると，帰無仮説として一様分布を仮定しているので，求める差は表 4. 1 のように 0.140 となる．観察度数の総数 100 に対する上側 95%信頼区間は 0.122 となるので対立仮説が採択され，この例

表 4.1: 1 標本コルモゴロフ・スミルノフ検定における数値例

累積観察度数	累積相対度数	累積理論相対度数	差
64	0.640	0.500	0.140
100	1.000	1.000	0.000

では CNa は NCN であると判定する．

また，この検定法では，1 step 前の CN からのパケット数と当該 CN から合流するトラヒックのパケット数の比から検出に必要なおおよそのマークパケット数を求めることができる．ここでは，1 step 前の CN から（合流前）のパケット数 : 合流後のパケット数の比を 1 : R_m，また，マークパケット数はその比に従って得られると仮定する．図 4.4 は，R_m を 1.0 から 3.0 まで 0.01 ずつ変化させたときの，各々の R_m における検出に必要なマークパケット数（合流後のトラヒックから生成されたマークパケット）を値を逐一代入することで求めた結果を表している．ただし，実際には，上記で述べたとおりマークパケットはランダムに到着するため，多少の増減はするものと考えられる．

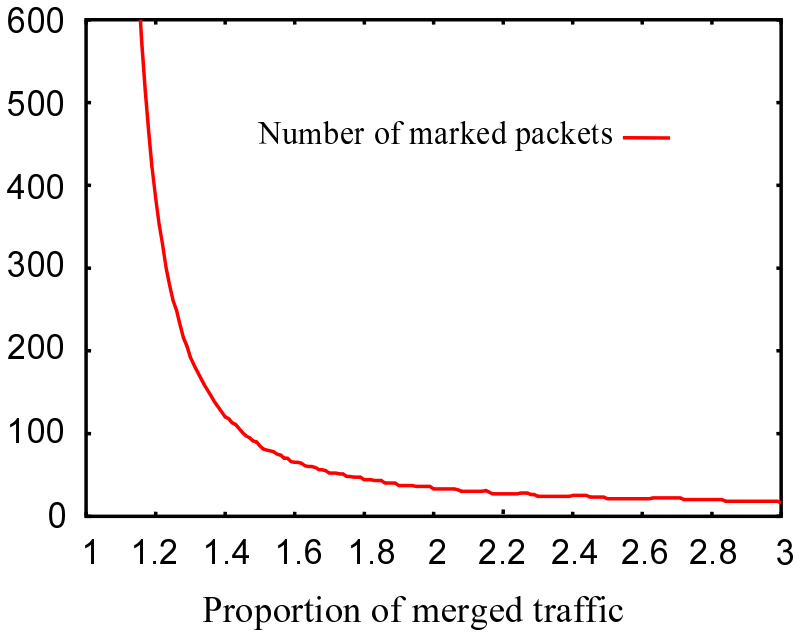

図 4.4: 検出に必要なマークパケット数

最後に提案手法の特徴をまとめる．

1. 新たにマークする情報を増やすことなく得られるマークパケット数を利用して，検出精度向上を達成することができる
2. 提案手法は PPM 手法で NCN とされなかった CN を対象として NCN 検出を行うため，PPM 手法単独の場合に比べて NCN の検出精度が低下することはない

3. 現在までに様々な PPM 手法が提案されているが，マークパケット数自体に変化はないため，多くの PPM 手法への適用が期待できる
4. 提案手法による NCN の特定は単純な処理で行われるため，犠牲者への負担増も少ない

4.2 有効性の検証

本節では，提案手法による NCN 検出の評価実験を行い，その有効性を検証する．ただし，今回提案した手法は PPM 手法と組み合わせることで NCN 検出を完成させるため，PPM 手法単独のものと提案手法を組み合わせたものとの比較により行う．また，今回の評価実験では PPM 手法として，代表的な Edge Sample 手法を用いる．

4.2.1 評価実験について

ネットワーク

PPM 方式における既存研究では，実ネットワークから収集した特定のノードを起点（犠牲者に相当）としたツリー状のトポロジーデータ [16] を基にシミュレーションを行っているが，これには 2 つの問題がある．

- 別のノードを起点とした場合に同様の結果が得られるとは限らない
- ネットワークを構成するノード数といった要因が提案法に及ぼす影響について考察することができない

そこで本論文では，実ネットワークから収集したトポロジーデータを用いるのではなく，ネットワークトポロジー生成ツールである BRITE[17] を利用しシミュレーション実験を行う．そして，DDoS 攻撃中のネットワークの特性を定める以下の項目を変数とし，次のような手順によりネットワークを構成した．

変数

- N_n：ネットワークを構成するノードの数
- $2m$： 1 ノードあたりの接続ノード数の平均値
- N_a：攻撃者の数
- R_c：全ノード数に占める CN の割合

ネットワーク構成手順

1. (N_n,m) を変数としてネットワークを生成する
2. 起点ノードを定める（起点ノードの元に犠牲者がいることとする）
3. 起点ノードから最小ホップ数基準で各ノードへのパスをはる
4. R_c の値に基づきランダムに CN を配置する（起点ノードは CN であるとする）
5. N_a の値に基づき攻撃者を配置する

ただし，接続ノード数の分布については実ネットワークにおける特徴を考慮した分布である Heavy-tailed Distribution[18] 用いた．また，PPM 手法ではある送信者からのパケットフローが一度も CN を通過しない場合，そのパケットフローの NCN を特定することは不可能であるため，犠牲者が所属する起点ノードは CN であるとした．

DDoS 攻撃，ネットワーク状態の想定

提案法の有効性の検証として，4.2.2 節で，最も単純な DDoS 攻撃，ネットワーク状態として以下のような想定を設定し，評価実験を行う．そして 4.2.3 節で，各想定が成り立たない場合の有効性について検証する．

想定１ 全ての攻撃者は同数の攻撃パケットを送出する（１攻撃者あたりのパケットレートを $N_p = 100$[packets/sec] とする）
想定２ 全ての攻撃者は同時に攻撃を開始する
想定３ 全ての攻撃者は攻撃を一定期間続ける（on,off しない）
想定４ 全ての攻撃者は同時に攻撃を終了する
想定５ 攻撃経路上でパケットロスや逆転は起こらない
想定６ 攻撃中は攻撃経路は変更されない
想定７ ネットワーク上は攻撃者のトラヒックしか流れていない
想定８ 攻撃者はマークフィールドを偽造しない

評価値

提案手法は，PPM 手法では検出することが不可能な NCN（サブマリンノード）を検出することで，NCN の検出精度（正しい NCN のうち検出することが可能な NCN の割合）を向上させることを目的としているため，評価は NCN の検出精度に主眼を置く．この値は再現率（Recall）に当たる数値である．また，再現率については，NCN に所属する攻撃者 (攻撃経路) の再現率（以下，攻撃者の再現率と略す）も評価対象とする．攻撃者の再現率を導入することで，NCN に所属する攻撃者の数を反映した評価を行うことが可能となる．

しかし，検出精度が高まったとしても，それに比例して NCN ではない CN を誤って NCN として検出することが多くなると，NCN 検出手法として望ましくない．そのため，正しい NCN の検出率（検出した NCN のうち正しい NCN を検出した割合）についても評価しなければならない．この値は適合率 (Precision) に当たる．ただし，Edge Sample 手法は確率的な処理に伴う誤検出がないため一定時間経過すれば完全に 1 となる．また，提案手法を用いた場合にも時間の経過と共に確率処理に伴うランダム性が弱くなるため，1 に近づくことが期待される．

評価実験では，全ての CN を，NCN であるか否か，NCN として検出したか否か，という 2 項目で以下の４つの状態 A,B,C,D に区分する（図 4.5）．

- A: NCN である CN を NCN として検出した（正）
- B: NCN である CN を NCN として検出しなかった（誤）
- C: NCN ではない CN を誤って NCN として検出した（誤）
- D: NCN ではない CN を NCN として検出しなかった（正）

T \ I	NCN	Non NCN
NCN	A	B
Non NCN	C	D

T : True　　I : Identification

図 4.5: CN の分類

NCN についての再現率 (Recall)，適合率 (Precision) は，状態 A,B,C に属する CN の数を N_A,N_B,N_C として導出し，$Recall_{NCN} = \frac{N_A}{N_A+N_B}$，$Precision_{NCN} = \frac{N_A}{N_A+N_C}$ とすることで求める．図 4.6 の例で，CN2,CN3,CN4,CN5,CN6,CN7 が NCN として検出されたとすると，A={4,5,6,7},B={8},C={2,3} であり，$N_A = 4$,$N_B = 1$,$N_C = 2$ となるため，$Recall_{NCN} = \frac{1}{5}$,$Precision_{NCN} = \frac{4}{6}$ と求められる．

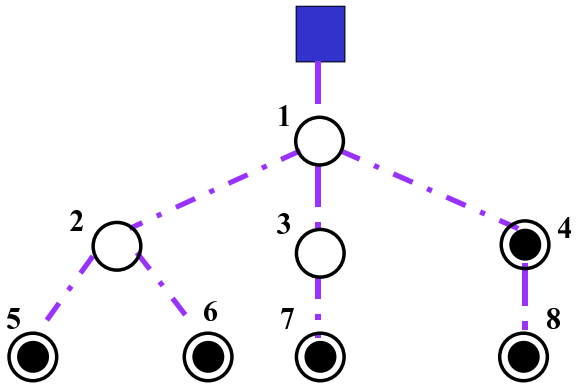

図 4.6: 再現率，適合率

また，攻撃者の再現率についても同様に求める．図 4.7 の例で，CN1 のみが NCN として検出されたとすると，検出された CN1 には攻撃者が二人，検出されなかった CN2 には攻撃者が一人であるため，攻撃者の再現率は $Recall_{Attacker} = \frac{2}{3}$ となる．このとき，NCN の再現率は $Recall_{NCN} = \frac{1}{2}$ である．

ところが，これらの評価尺度だけでは NCN 検出の先に予定されるパケットフィルタリングがネットワークに与える効果について検証することができないため，不十分であると考えられる．つまり，NCN 特定結果をフィルタリングに適用した際にネットワークにかかる負荷をどれだけ軽減することができるのかという点での評価が必要である．そこで，各リンクを通過する攻撃トラヒック量を計る指標として hop 数×トラヒック量を定義し（ただし，攻撃者ー攻撃者が所属するノード，犠牲者が所属するノードー犠牲

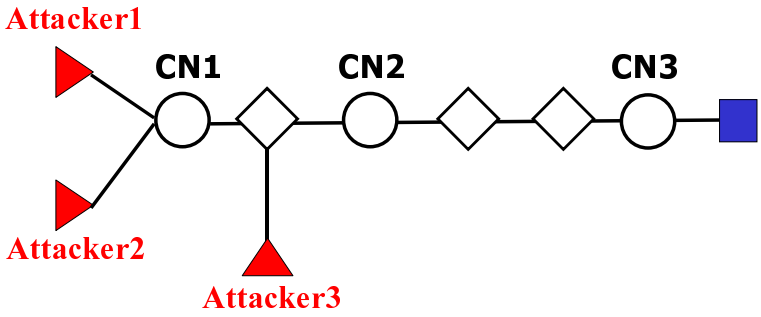

図 4.7: NCN と攻撃者の再現率の関係

者の 2hop 分はカウントしないこととした），その値のフィルタリング適用前後における減少率（以下，トラヒックの減少率と略す）を評価対象に加えることとする．

トラヒックの減少率の具体例を図 4.8 を用いて説明する．図 4.8 の例ではフィルタリングを適用しない

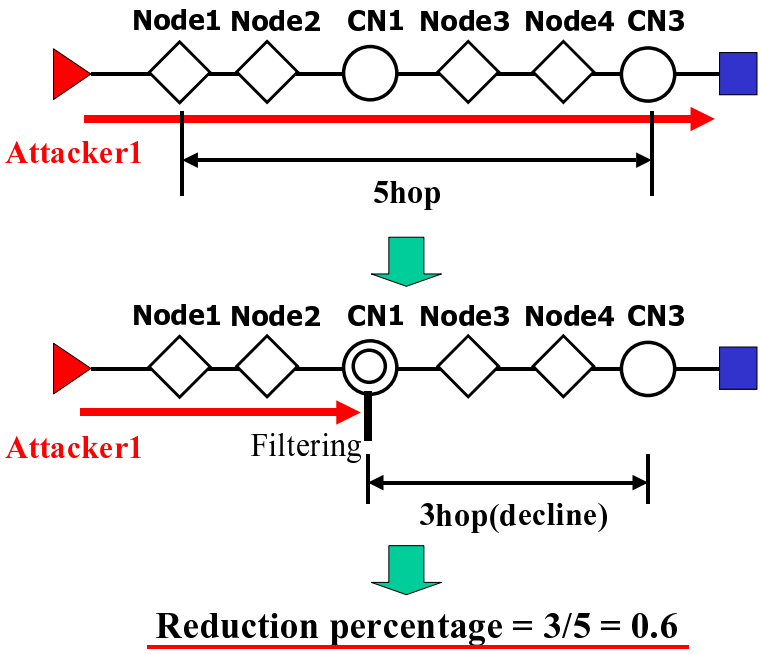

図 4.8: トラヒック減少率

場合，攻撃トラヒックは経路上にある全てのノードを通過する．つまり，攻撃トラヒックは Node1 から CN3 までの 5hop 通過することになる．一方，CN 1 が NCN として検出されフィルタリングが適用された場合，CN1 でトラヒックが遮断されるため，CN1 から CN2 までの 3hop 分トラヒックの通過を減少させたことになる．よって，hop 数×トラヒック量を基準とすると減少率は 0.6 と求めることができる．

4.2.2 有効性の検証

本節では 4.2.1 節で定めた想定でシミュレーション実験を行う．そして，NCN の再現率・適合率，攻撃者の再現率，トラヒックの減少率について Edge Sample 手法単独の場合と提案手法を用いた場合の結果を比較し，提案手法の有効性を示す．

本評価実験では，実験を進めていく上で基準となるケースを

- (N_n,m,N_a,R_c)=(5000,2,1000,5)
- $p = \frac{1}{20000}$
- 起点ノード（犠牲者が接続しているノード）を固定

とし，まず始めに，この基準となるケースについての結果を示す．次に，変数の値を同一にし起点ノードをランダムに配置したケースについての結果を，基準となるケースについての結果と比較し，提案手法の効果は起点ノードの位置に因らないことを示す．その後，(N_n,m,N_a,R_c) と p の 5 つの変数について，他の 4 つの変数を固定し，対象とした変数を変化させた場合についての評価結果を述べ，各変数の変動が提案手法の効果に及ぼす影響について考察する．また，マーキング確率 p と関連して，上書きの影響についても論じる．

基準となるケースについて

図 4.9,4.10,4.11 は，各変数を (N_n,m,N_a,R_c)=(5000,2,1000,5),$p = \frac{1}{20000}$ とし，起点ノードを固定した場合における，時間の推移と NCN・攻撃者の再現率，NCN の適合率，トラヒックの減少率（の平均値とその 95%信頼区間，以下省略する）との関係を表している．ただし，ここで与えた変数から生成されるネットワークの hop 数分布，step 数分布は図 4.12,4.13 のようになっている．

まず再現率については，Edge Sample 手法単独では，NCN で 0.75 付近，攻撃者で 0.6 付近で収束しているのに対し，提案手法を用いると NCN・攻撃者の再現率共に時間の経過に伴いゆるやかに上昇し，最終的にはほぼ 1 になる，つまり全ての NCN・攻撃者を検出できるということである．提案手法を用いると，サブマリンノードである CN については，十分な時間が経過すればマークパケット数に確実に差が生じるため，全ての NCN を検出できるのである．また，Edge Sample 手法単独のケースで，NCN の再現率が攻撃者の再現率を大きく上回っているが，これは，リーフノードに比べ，犠牲者に近い位置に存在するサブマリーンノードの方が複数の攻撃経路が合流する可能性が高いためである．そのため，この傾向は m,N_a が大きい場合，N_n,R_c が小さい場合に強く出ると推測される．このことは，N_n,m,N_a,R_c の各項で確認する．

次に適合率については，1000 秒経過したあたりでほぼ 1 になっており，提案手法は誤検出をほとんど生まないということが確認された．そこで以降の実験では，適合率については省略する．

最後に，トラヒックの減少率については，Edge Sample 手法単独では 0.6 程度になっているのに対し，提案手法では約 0.83 となっており，提案手法を用いるとリンクを通過するトラヒックを平均で 2 割以上削減できることが分かる．

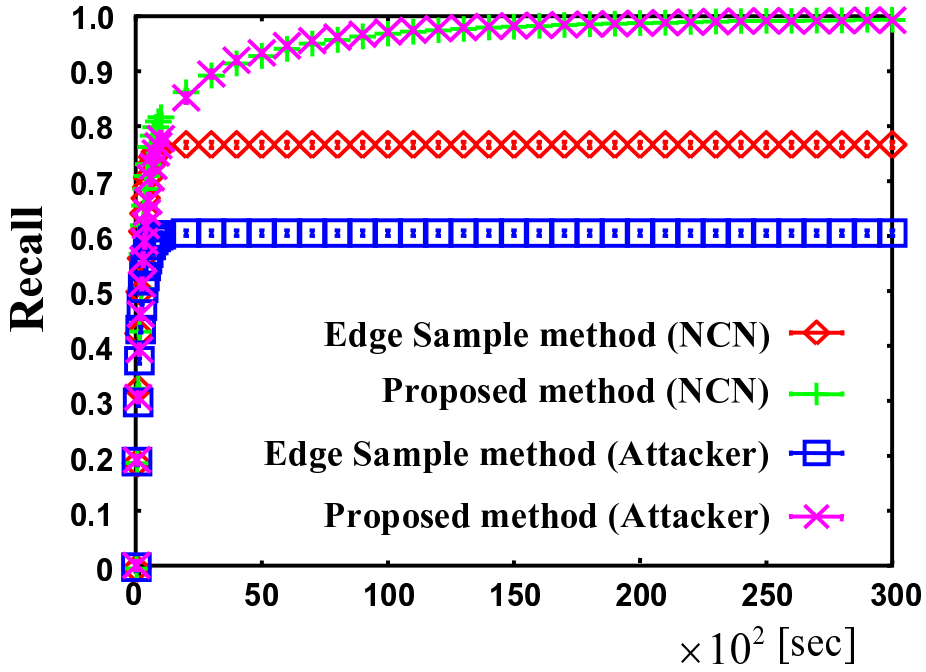

図 4.9: 基準ケースにおける時間の推移と再現率との関係

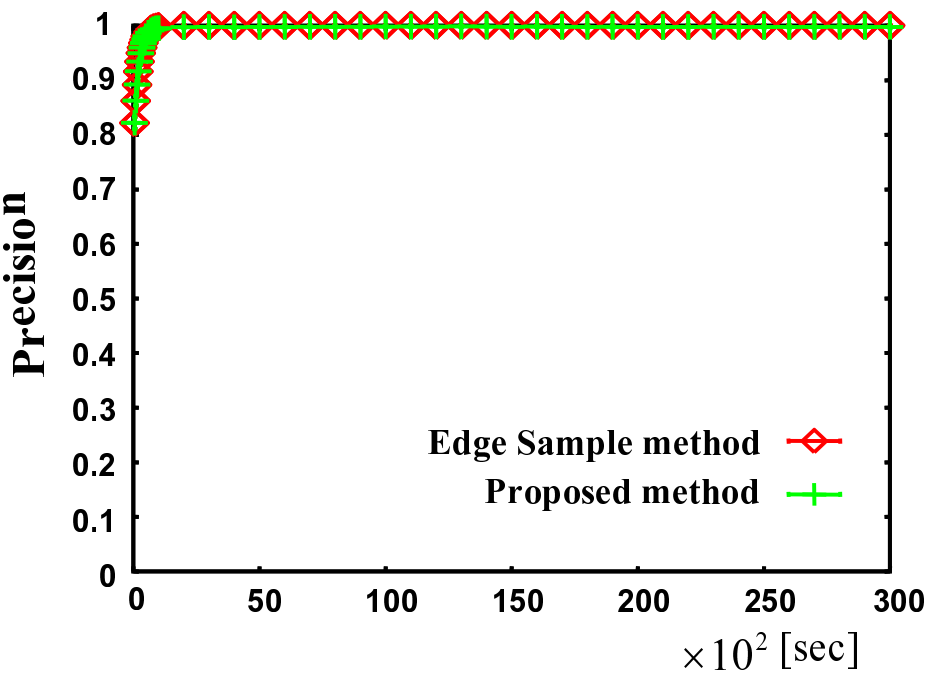

図 4.10: 基準ケースにおける時間の推移と適合率との関係

起点ノードのランダム配置について

本項では，提案手法の有効性は起点ノードの位置に因らないことを示す．そこで，基準となるケースと，そのケースと同一の変数に対し起点ノードをランダムに配置したケースについて，再現率（NCN・攻

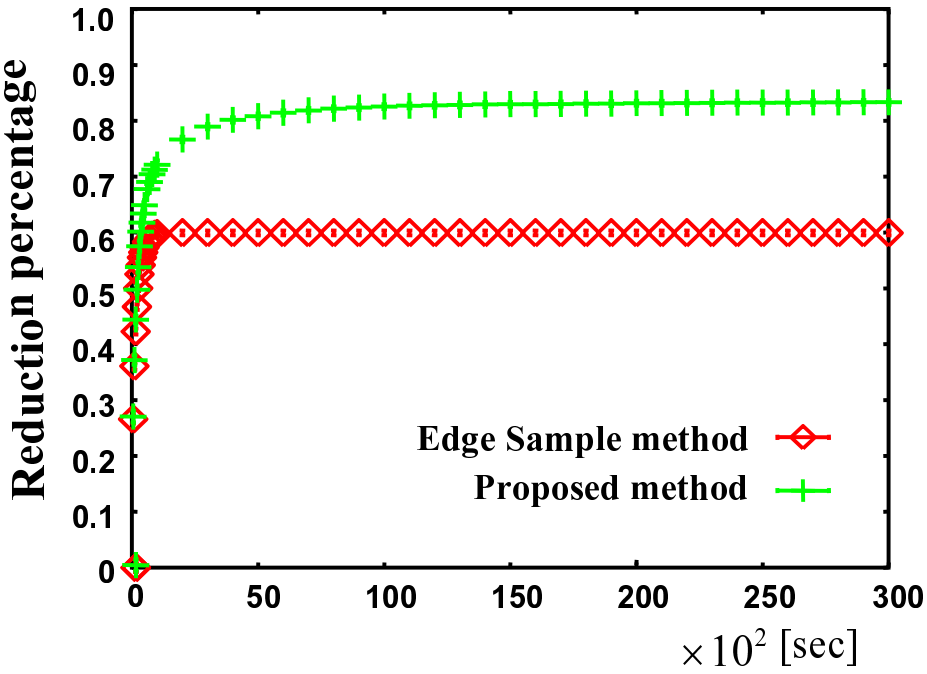

図 4.11: 基準ケースにおける時間の推移とトラヒック減少率との関係

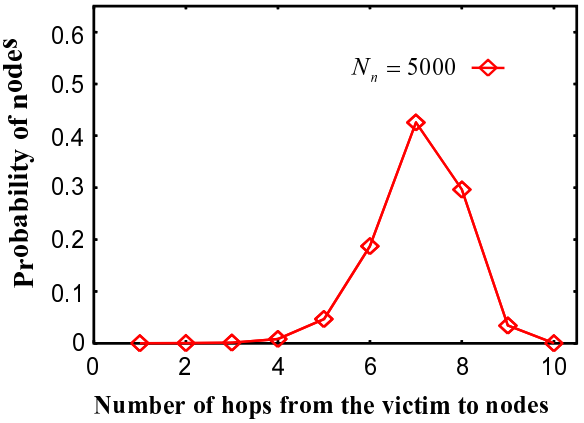

図 4.12: 基準ケースにおける hop 数分布

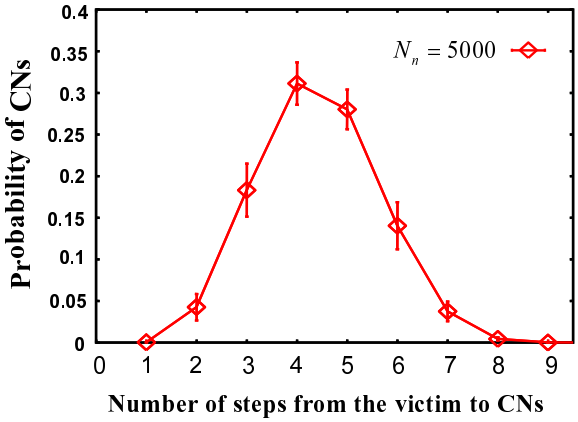

図 4.13: 基準ケースにおける step 数分布

撃者）の結果を比較する．図 4.14〜4.17 は，それぞれ，Edge Sample 手法による NCN の再現率，提案手法による NCN の再現率，Edge Sample 手法による攻撃者の再現率，提案手法による攻撃者の再現率について，基準となるケース（起点ノードを固定）と起点ノードをランダム配置したケースの比較結果を表している．また，図 4.18，4.19 は，hop 数分布，step 数分布の比較結果を表している．

図 4.14〜4.17 の全てに共通して，起点ノードを固定した場合と，ランダムに配置した場合で，ほぼ同一の再現率となっており，Edge Sample 手法，提案手法の検出精度は起点ノードの位置に因らないということが分かる．よって，提案手法は起点ノードの位置に関わらず有効であると言える．

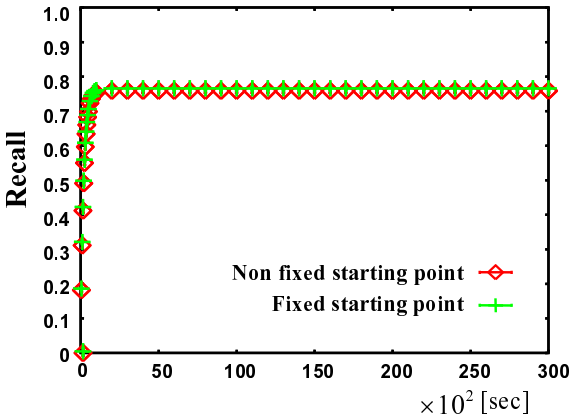

図 4.14: 基準ケースと起点ノードをランダム配置した場合との NCN 再現率の比較（Edge Sample 手法）

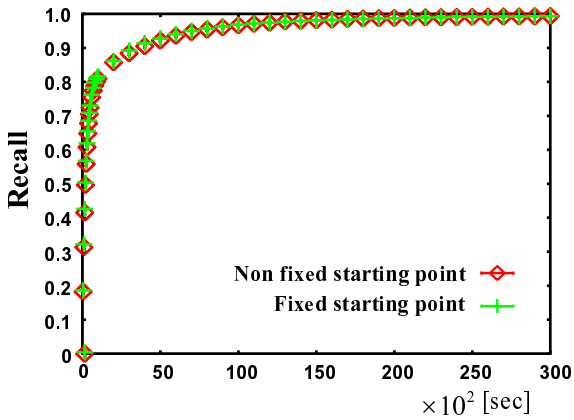

図 4.15: 基準ケースと起点ノードをランダム配置した場合との NCN 再現率の比較（提案手法）

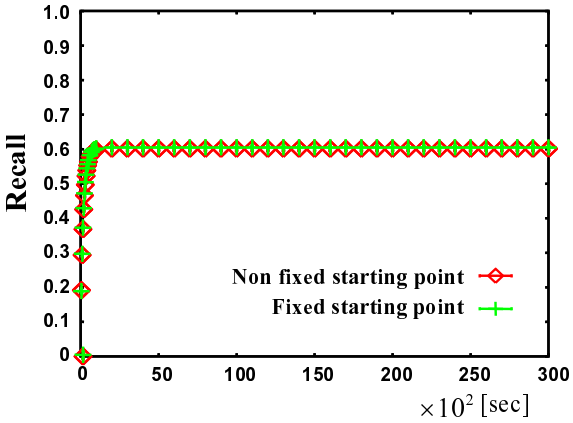

図 4.16: 基準ケースと起点ノードをランダム配置した場合との攻撃者再現率の比較（Edge Sample 手法）

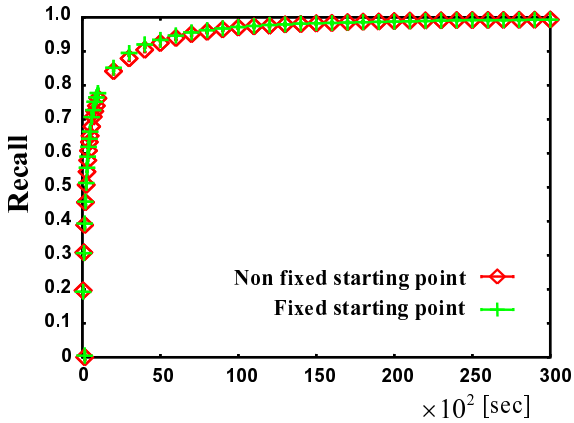

図 4.17: 基準ケースと起点ノードをランダム配置した場合との攻撃者再現率の比較（提案手法）

ネットワークを構成するノードの数 N_n について

本項では，ネットワークを構成するノードの数 N_n と各評価値との関連性を探る．まず始めに，$(m,N_a,R_c)=(2,1000,5),p=\frac{1}{20000}$ とし，N_n=1000,3000,10000,15000 とした場合における時間の推移と NCN・攻撃者の再現率，トラヒックの減少率との関係を，図 4.20〜4.27 に示す．ただし，N_n=5000 の場合は基準ケースと同一条件になるため省略する（図 4.9,4.11）．また，その際の hop 数分布，step 数分布の分布は図 4.28,4.29 のようになっている．

図 4.20〜4.27 の全てのケースで，提案手法を用いた方が Edge Sample 手法単独より再現率・トラヒックの減少率共に高くなっており，N_n の値に関わらず提案手法が有効であることが明らかである．また，基準ケースの項で推測したとおり，Edge Sample 手法において，N_n の値が小さい方が NCN の再現率と

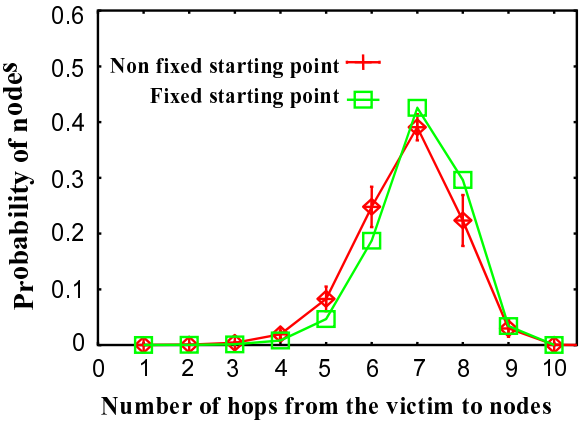

図 4.18: 基準ケースと起点ノードをランダム配置した場合との hop 数分布の比較

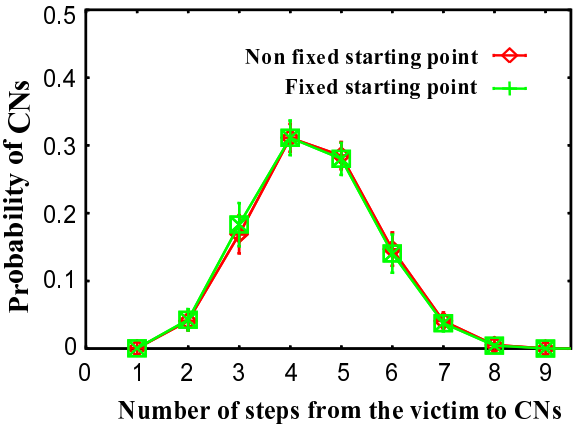

図 4.19: 基準ケースと起点ノードをランダム配置した場合との step 数分布の比較

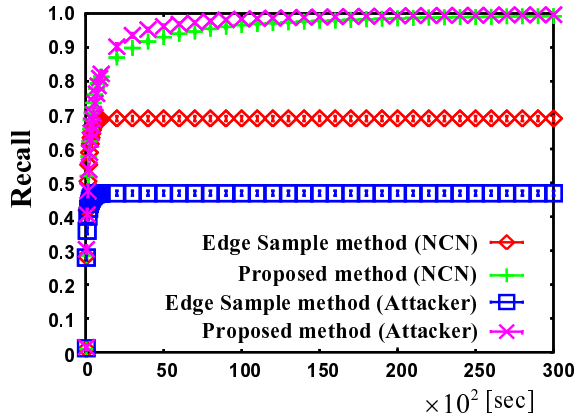

図 4.20: N_n=1000 の場合における時間の推移と再現率との関係

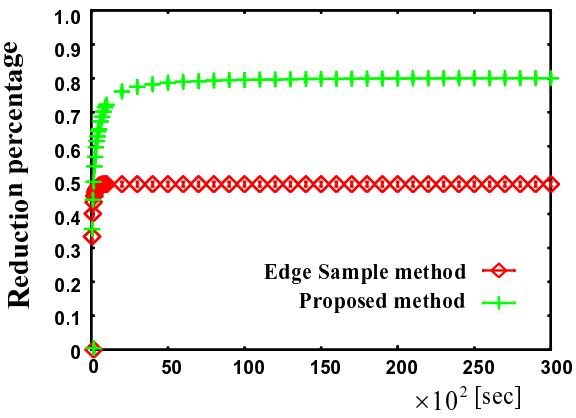

図 4.21: N_n=1000 の場合における時間の推移とトラヒック減少率との関係

攻撃者の再現率の差が大きくなっている．最後に，再現率に関しては時間の経過と共に 1 に収束していくことも併せて確認された．

次に，各々の N_n に対する実験結果から，観測時間 3000[sec] における再現率・トラヒック減少率を抽出した結果を，図 4.30,4.31 に示し，比較を行う．また，図 4.30,4.31 について，提案手法を用いた場合と Edge Sample 手法単独の場合の評価値の差分を取った結果を図 4.32,4.33 に示す．差分をとることで，提案手法による精度向上分，つまり提案手法の効果を把握することができる．

図 4.30,4.31 に共通して，Edge Sample 手法単独では N_n の減少に伴い再現率・トラヒック減少率が低下している．これは，同一の攻撃者に対しノード数が減少すると攻撃者の密度が高まり，攻撃経路が重複する可能性が増すため，Edge Samle 手法では検出できないサブマリンノードが増加することに起因する．一方，提案手法を用いると N_n の減少に伴い再現率がやや増加しているものの，N_n の値の変動による影響をほぼ受けていない．結果的に，N_n の値が小さい方が提案手法による精度向上の影響が大きいと

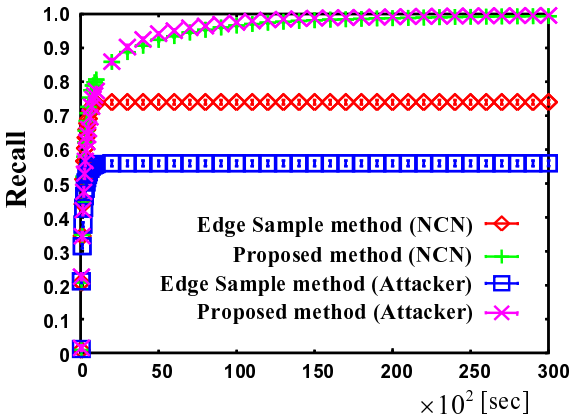

図 4.22: N_n=3000 の場合における時間の推移と再現率との関係

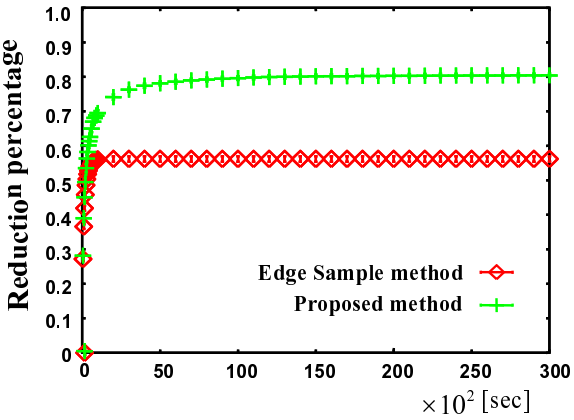

図 4.23: N_n=3000 の場合における時間の推移とトラヒック減少率との関係

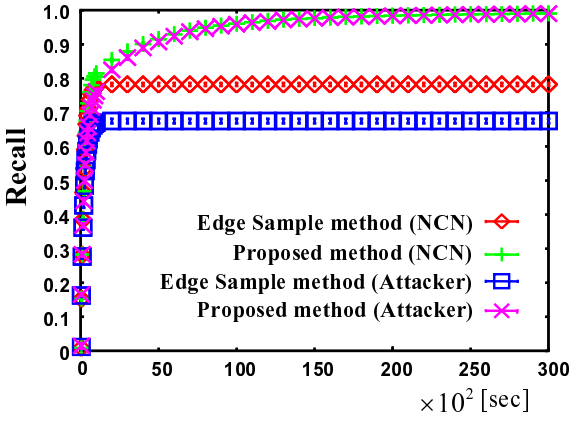

図 4.24: N_n=10000 の場合における時間の推移と再現率との関係

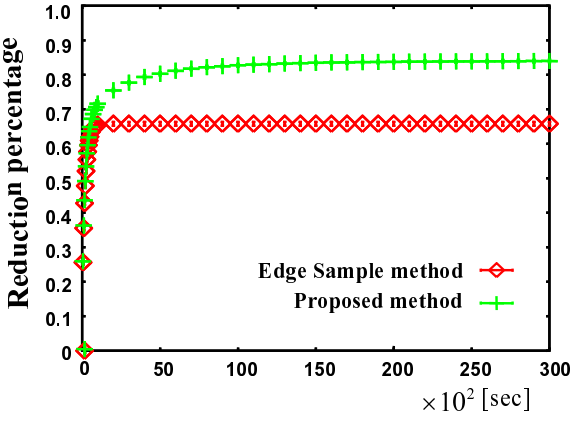

図 4.25: N_n=10000 の場合における時間の推移とトラヒック減少率との関係

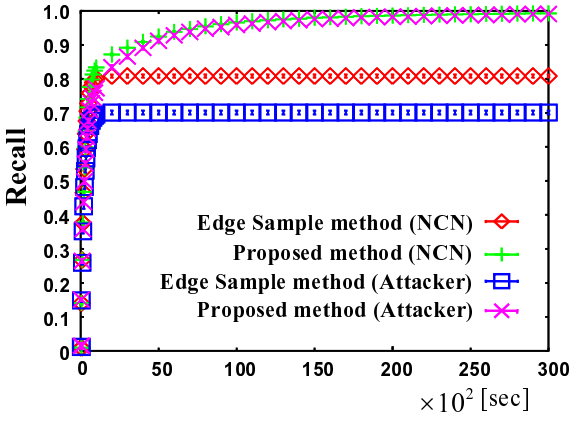

図 4.26: N_n=15000 の場合における時間の推移と再現率との関係

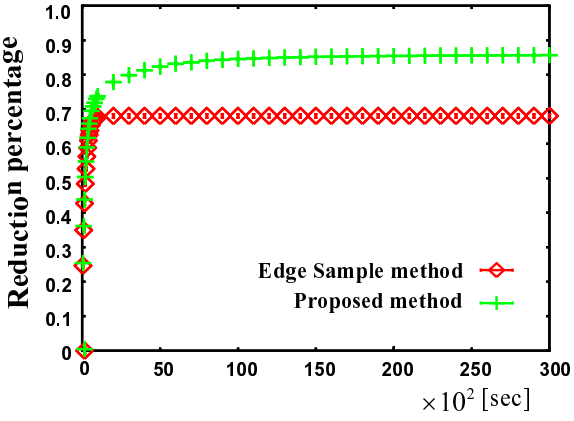

図 4.27: N_n=15000 の場合における時間の推移とトラヒック減少率との関係

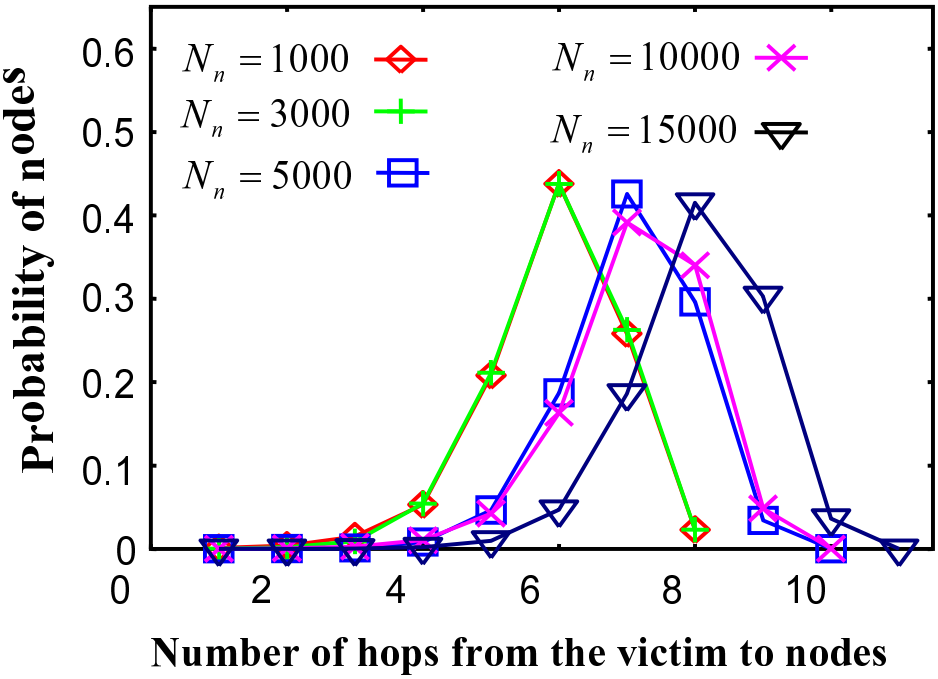

図 4.28: 攻撃者数と hop 数分布との関係

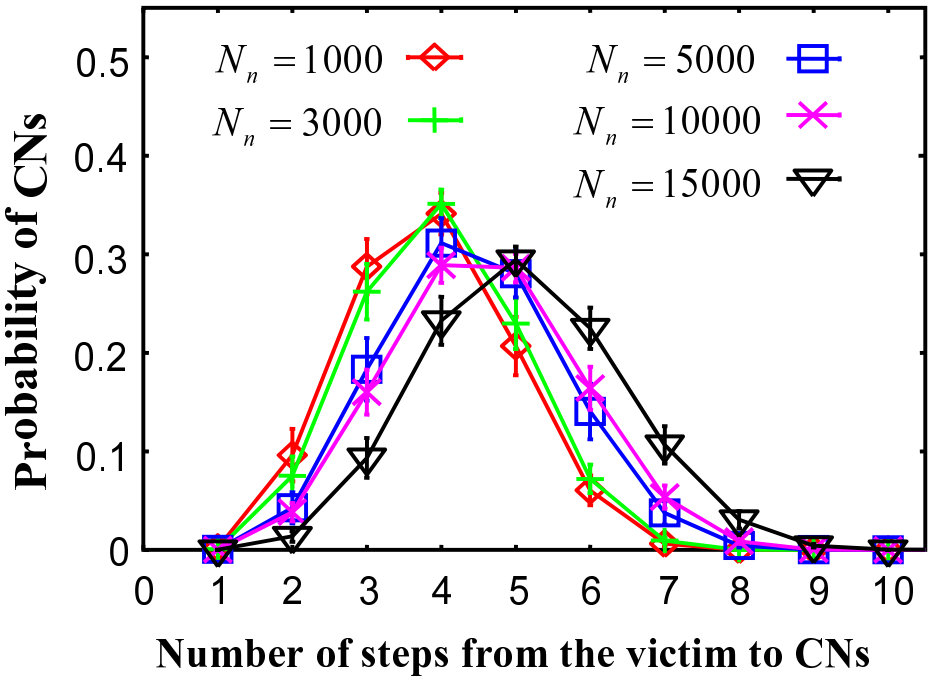

図 4.29: 攻撃者数と step 数分布との関係

いうことになる．この傾向は，評価値の差分を取った結果である図 4.32,4.33 からも明らかである．

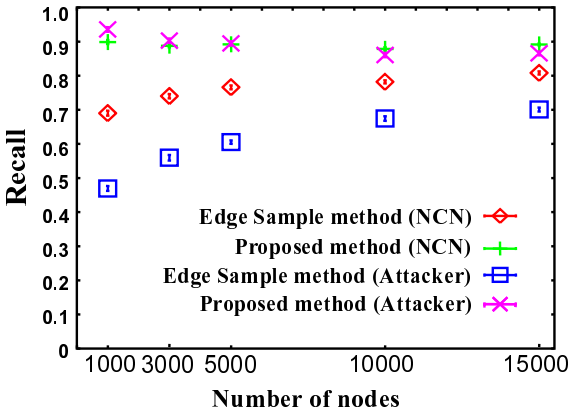

図 4.30: ノード数と再現率との関係

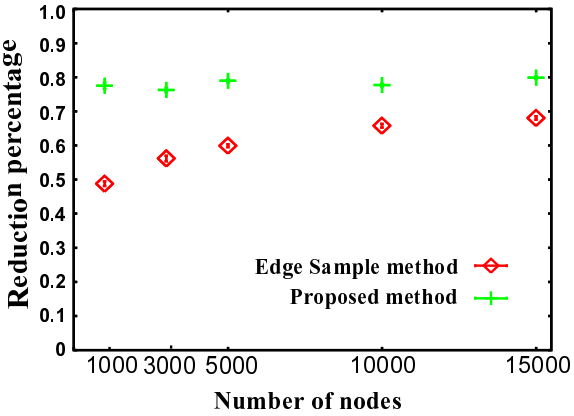

図 4.31: ノード数とトラヒック減少率との関係

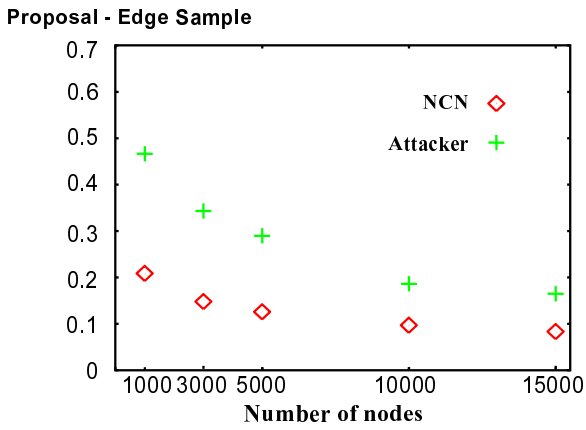

図 4.32: ノード数と提案手法の効果との関係（再現率）

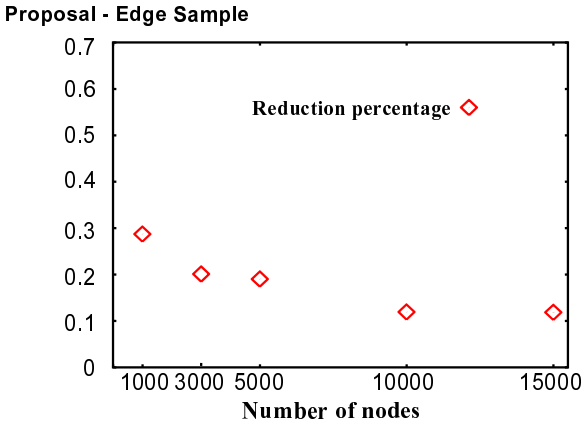

図 4.33: ノード数と提案手法の効果との関係（トラヒック減少率）

１ノードあたりの接続ノード数の平均値 $2m$ について

本項では，１ノードあたりの接続ノード数の平均値 $2m$ と各評価値との関連性を探る．まず始めに，(N_n,N_a,R_c)=(2000,1000,5),$p = \frac{1}{20000}$ とし，m=1,5,10,20 とした場合における時間の推移と NCN・攻撃者の再現率，トラヒックの減少率との関係を，図 4.34〜4.41 に示す．ただし，m=2 の場合は基準ケースと同一条件になるため省略する（図 4.9,4.11）．また，その際の hop 数分布，step 数分布の分布は図 4.42,4.43 のようになっている．

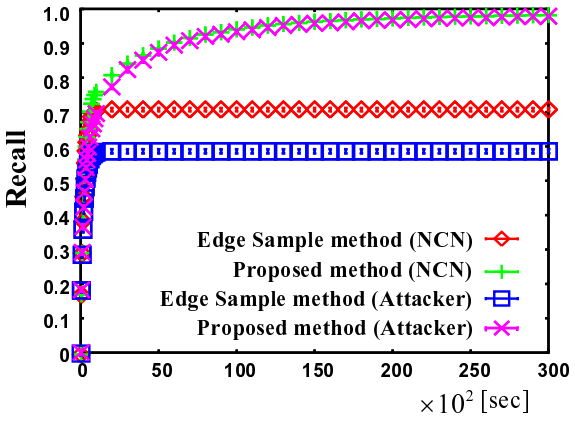

図 4.34: m=1 の場合における時間の推移と再現率との関係

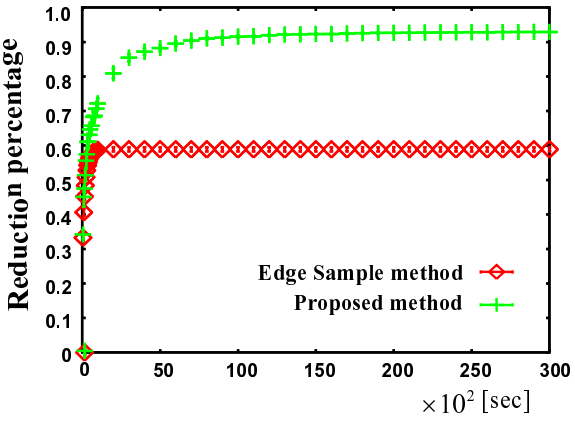

図 4.35: m=1 の場合における時間の推移とトラヒック減少率との関係

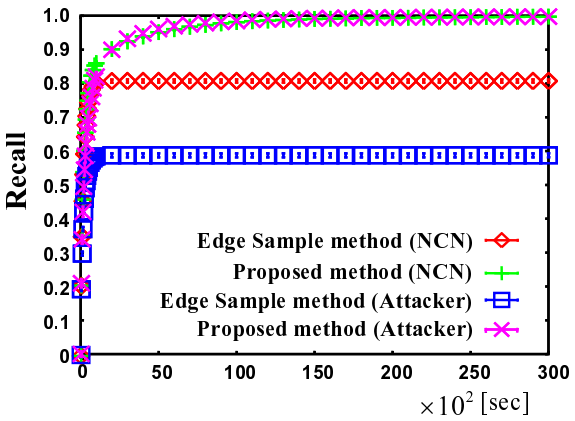

図 4.36: m=5 の場合における時間の推移と再現率との関係

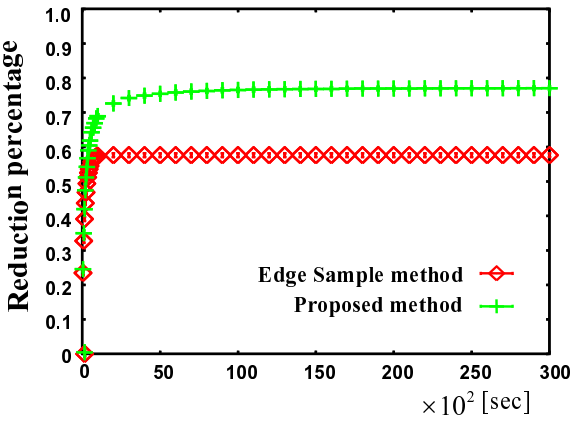

図 4.37: m=5 の場合における時間の推移とトラヒック減少率との関係

図 4.34〜4.41 の全てのケースで，提案手法を用いた方が Edge Sample 手法単独より再現率・トラヒックの減少率共に高くなっており，提案手法は m の値に関わらず有効であると言える．また，基準ケースの項で推測したとおり，Edge Sample 手法において，m の値が大きい方が NCN の再現率と攻撃者の再現率の差が大きくなっている．最後に，再現率に関しては時間の経過と共に 1 に収束していくことも併せ

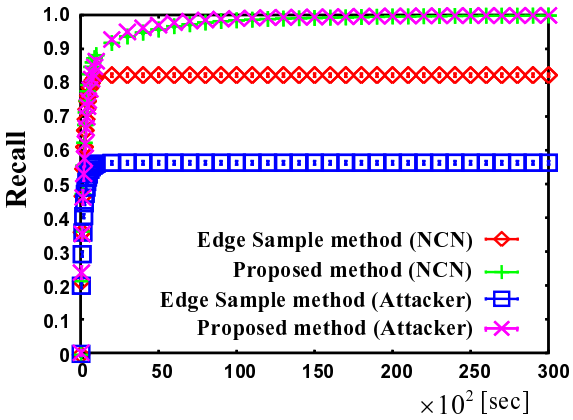

図 4.38: m=10 の場合における時間の推移と再現率との関係

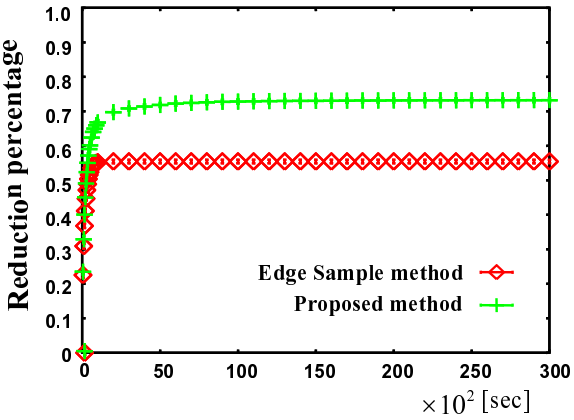

図 4.39: m=10 の場合における時間の推移とトラヒック減少率との関係

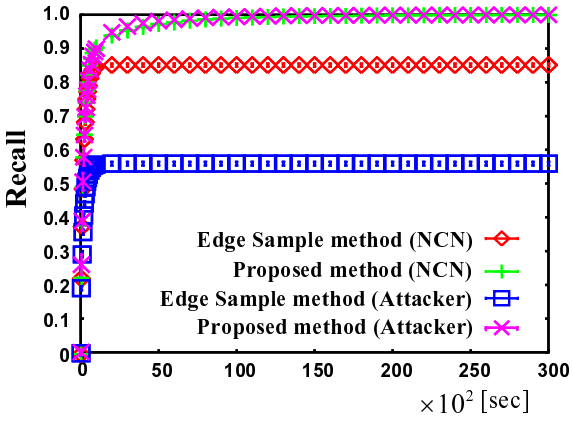

図 4.40: m=20 の場合における時間の推移と再現率との関係

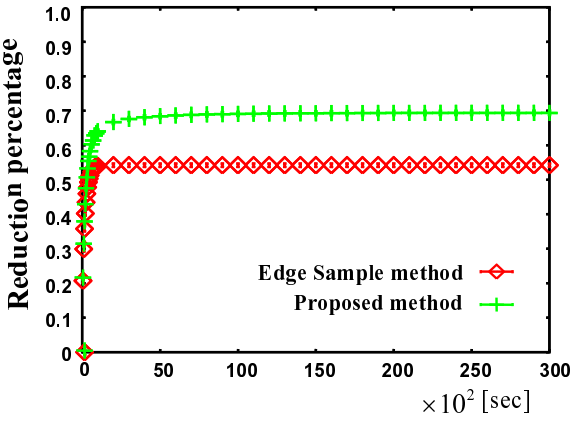

図 4.41: m=20 の場合における時間の推移とトラヒック減少率との関係

て確認された.

次に，各々の m に対する実験結果から，観測時間 3000[sec] における再現率・トラヒック減少率を抽出した結果を，図 4.44,4.45 に示し，比較を行う．また，図 4.44,4.45 について，提案手法を用いた場合と Edge Sample 手法単独の場合の評価値の差分を取った結果を図 4.46,4.47 に示す.

図 4.44 から言えることは次の 2 点である.

1. Edge Sample 手法による NCN の再現率，提案手法による再現率（NCN・攻撃者）は m の増加に伴い向上する
2. Edge Sample 手法による攻撃者の再現率は横ばい

m は，経路を再構築した木の分岐度に相関が高い数値であるため，m が増加すると，リーフノードとなる比率が高まる．したがって，m の増加に伴い Edge Sample 手法による NCN の再現率は向上し，結果的に提案手法による NCN の再現率も Edge Sample 手法に引き上げられ向上する．一方，分岐度が高まることは一つのノードに合流する経路が増加することにつながるため，1 サブマリンノードあたりの攻撃経

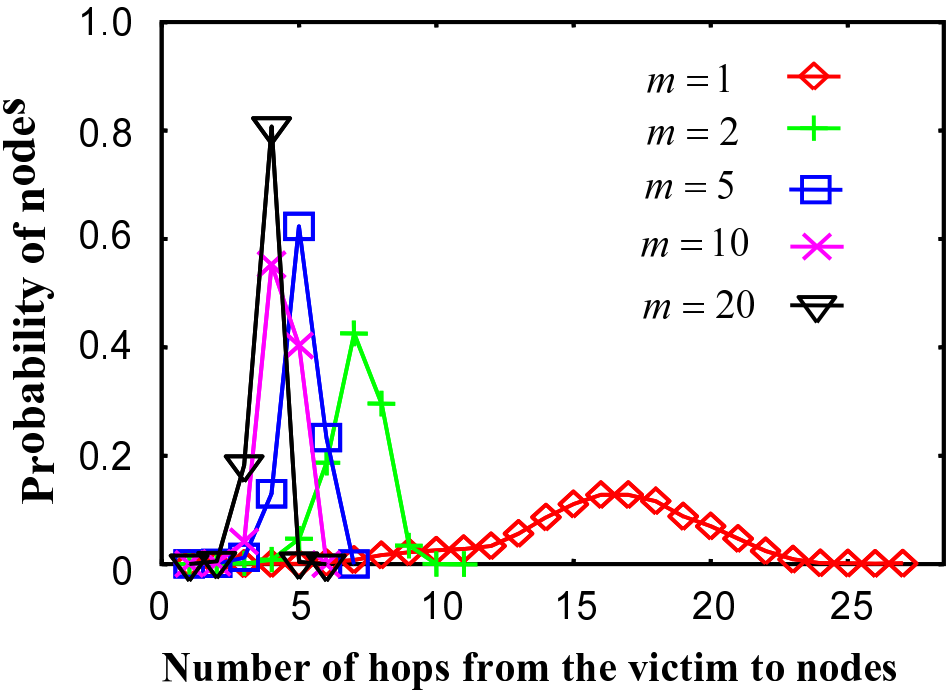

図 4.42: m と hop 数分布との関係

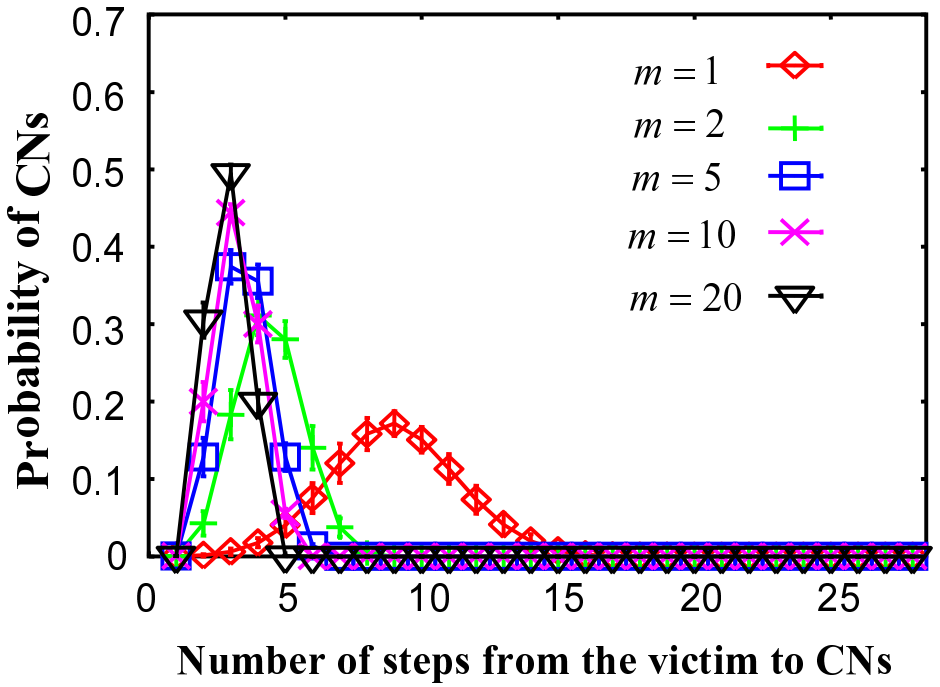

図 4.43: m と step 数分布との関係

路合流数が増加する．よって，NCN ではなく攻撃者を指標とした場合，サブマリンノードの重みが高まり，m の増加に伴う向上分を打ち消しあうため Edge Sample 手法による攻撃者の再現率は横ばいとなる．

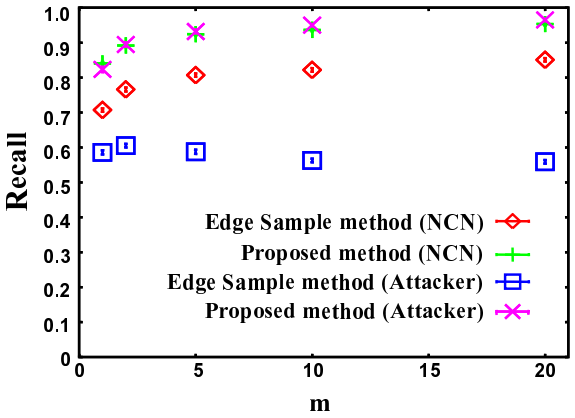

図 4.44: m と再現率との関係

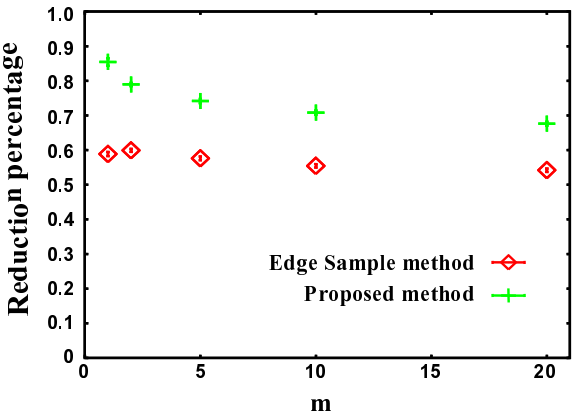

図 4.45: m とトラヒック減少率との関係

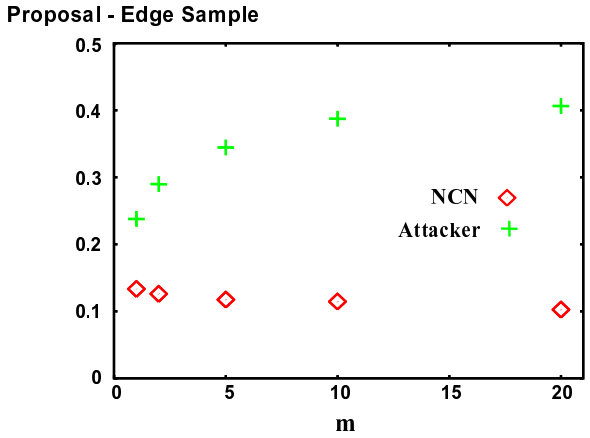

図 4.46: m と提案手法の効果との関係（再現率）

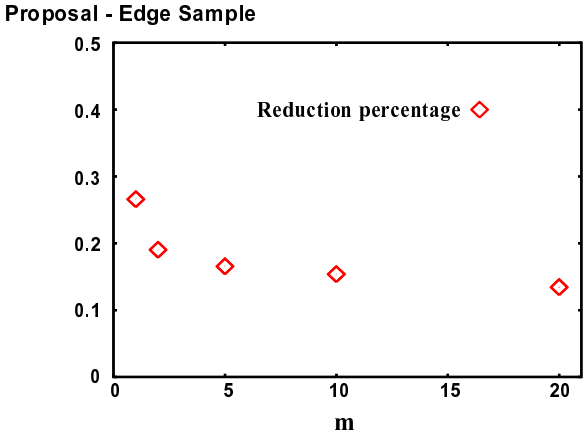

図 4.47: m と提案手法の効果との関係（トラヒック減少率）

図 4.44 については，m の増加に対し提案手法は減少，Edge Sample 手法は横ばいとなっている．しかし，m の値が増加に伴い hop 数の分布（図 4.42）が左側に偏っていくため，増加傾向にある再現率とは対照的に減少傾向にあるのはやむを得ないと考えられる．なぜなら，この評価値では hop 数×トラヒック量を指標としているため，hop 数そのものが小さくなるとトラヒックを遮断したとしても減少率はそれほど高まらないからである．特に，サブマリンノードは犠牲者に近い位置に存在するため，提案手法を用いた場合減少傾向が強くなる．

攻撃者の数 N_a について

本項では, 攻撃者の数 N_a と各評価値との関連性を探る．まず始めに, (N_n,m,R_c)=(5000,2,5),$p = \frac{1}{20000}$ とし，N_a=100,500,3000,5000 とした場合における時間の推移と NCN・攻撃者の再現率，トラヒックの減少率との関係を，図 4.48〜4.55 に示す．ただし，N_a=1000 の場合は基準ケースと同一条件になるため省略する（図 4.9,4.11）．また，N_a は hop 数分布，step 数分布を変動させる要因ではないため，それぞれの分布は図 4.28,4.29 と極めて近い分布となる．

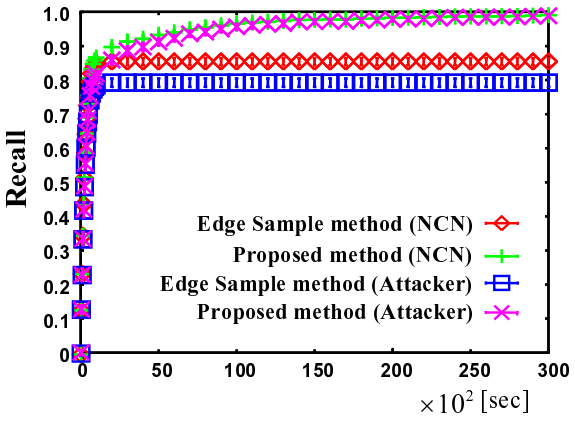

図 4.48: N_a=100 の場合における時間の推移と再現率との関係

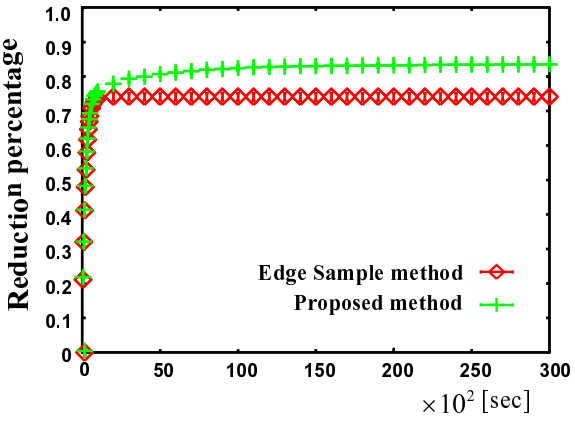

図 4.49: N_a=100 の場合における時間の推移とトラヒック減少率との関係

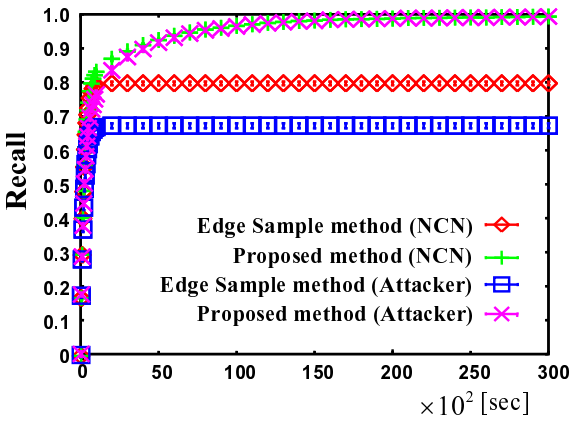

図 4.50: N_a=500 の場合における時間の推移と再現率との関係

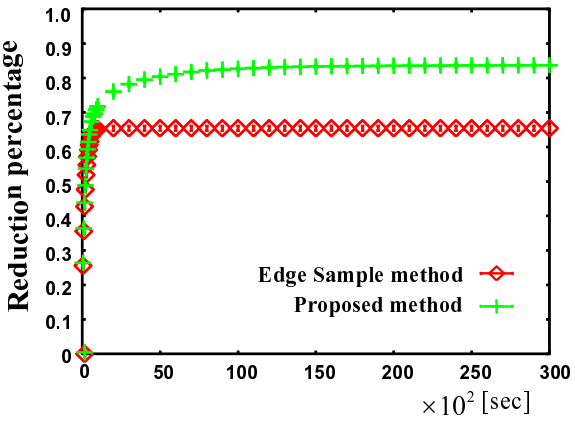

図 4.51: N_a=500 の場合における時間の推移とトラヒック減少率との関係

図 4.48〜4.55 の全てのケースで，提案手法を用いた方が Edge Sample 手法単独より再現率・トラヒックの減少率共に高くなっており，提案手法は N_a の値に関わらず有効であると言える．また，基準ケースの項で推測したとおり，Edge Sample 手法において，N_a の値が大きい方が NCN の再現率と攻撃者の再現率の差が大きくなっている．最後に，再現率に関しては時間の経過と共に 1 に収束していくことも併せ

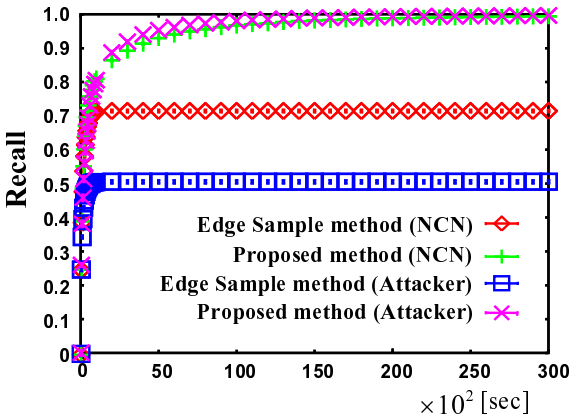

図 4.52: N_a=3000 の場合における時間の推移と再現率との関係

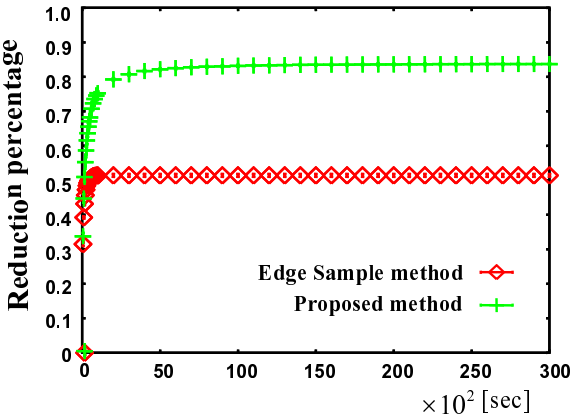

図 4.53: N_a=3000 の場合における時間の推移とトラヒック減少率との関係

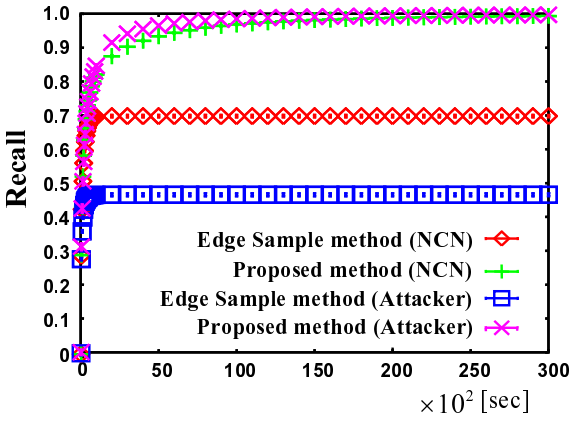

図 4.54: N_a=5000 の場合における時間の推移と再現率との関係

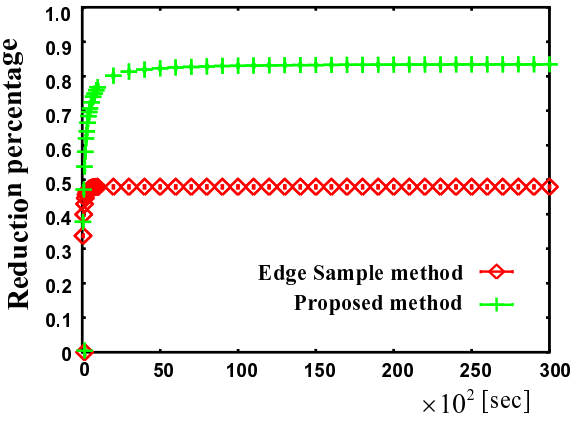

図 4.55: N_a=5000 の場合における時間の推移とトラヒック減少率との関係

て確認された．

次に，各々の N_a に対する実験結果から，観測時間 3000[sec] における再現率・トラヒック減少率を抽出した結果を，図 4.56,4.57 に示し，比較を行う．また，図 4.56,4.57 について，提案手法を用いた場合と Edge Sample 手法単独の場合の評価値の差分を取った結果を図 4.58,4.59 に示す．

図 4.56,4.57 で分かることは次の 2 点である．

1. Edge Sample 手法単独では N_a の増加に伴い全ての評価値が大幅に減少する
2. 提案手法を用いると N_a の増加に伴い全ての評価値がわずかに上昇する

結果的に，N_a の値が大きい方が提案手法による精度向上の影響が大きいということになる．この傾向は，評価値の差分を取った結果である図 4.58,4.59 からも明らかである．

次に理由について考察する．N_a は攻撃経路数と同値であるため，同一の特徴を示すネットワークに対し，N_a を増加させると，攻撃経路の重複が多くなる．したがって，サブマリンノードが増加し，Edge Sample 手法では評価値が大幅に減少することとなる．一方，提案手法を用いるとサブマリンノードを検

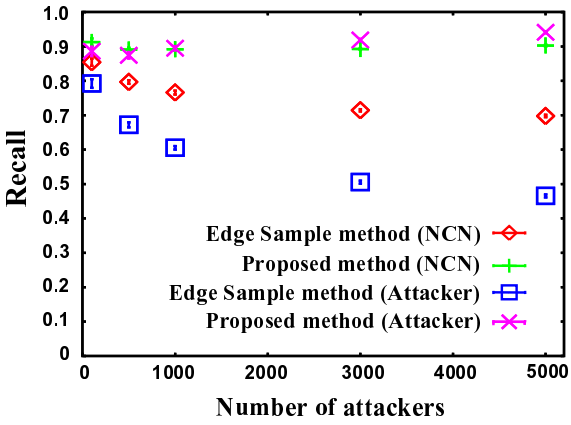

図 4.56: 攻撃者数と再現率との関係

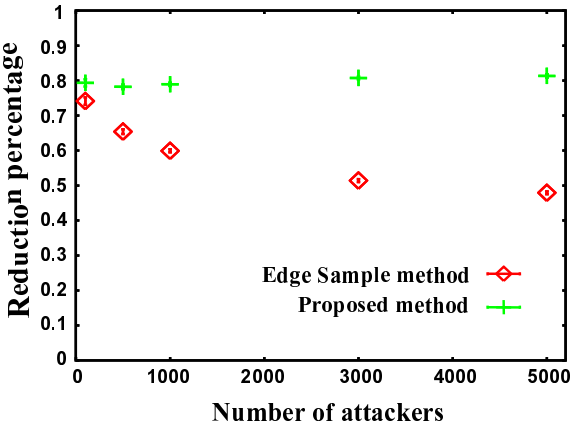

図 4.57: 攻撃者数とトラヒック減少率との関係

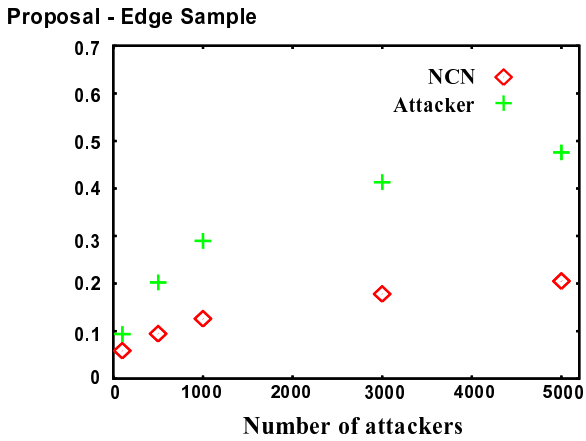

図 4.58: 攻撃者数と提案手法の効果との関係（再現率）

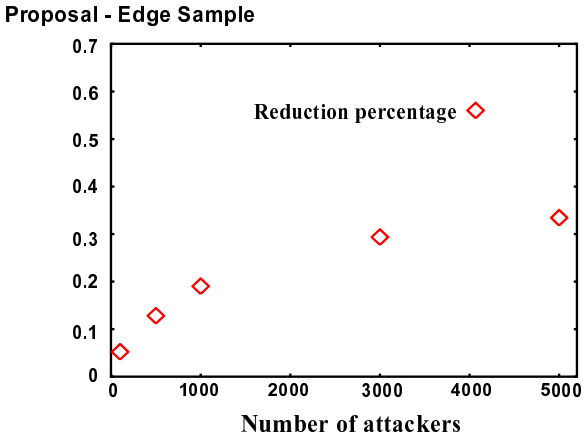

図 4.59: 攻撃者数と提案手法の効果との関係（トラヒック減少率）

出することが可能であるため，評価値は減少しない．また，N_a が増加すると，提案手法の検定における標本値である 1 NCN あたりのマークパケット数も増加するが，検定法は標本値が多くなるに従い閾値が低下するため，サブマリンノードの検出に要する時間が短縮され，提案手法による評価値がわずかに上昇することとなる．

全ノード数に占める CN の割合 R_c について

本項では，全ノード数に占める CN の割合 R_c と各評価値との関連性を探る．まず始めに，(N_n,m,N_a)=(5000,2,1000),$p = \frac{1}{20000}$ とし，R_c=0.1,0.3,0.7,0.9,1.0 とした場合における時間の推移と NCN・攻撃者の再現率，トラヒックの減少率との関係を，図 4.60〜4.69 に示す．ただし，R_c=0.5 の場合は基準ケースと同一条件になるため省略する（図 4.9,4.11）．また，step 数分布を図 4.70 に示す（hop 数分布は R_c の値では変動しない）．

図 4.60〜4.69 の全てのケースで，提案手法を用いた方が Edge Sample 手法単独より再現率・トラヒッ

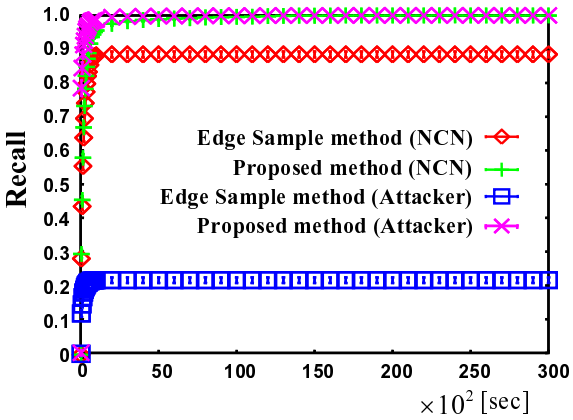

図 4.60: R_c=0.1 の場合における時間の推移と再現率との関係

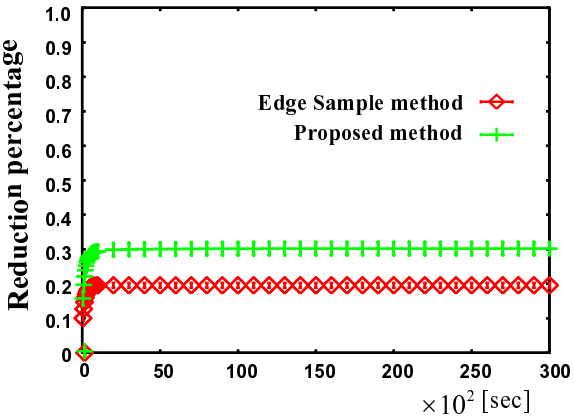

図 4.61: R_c=0.1 の場合における時間の推移とトラヒック減少率との関係

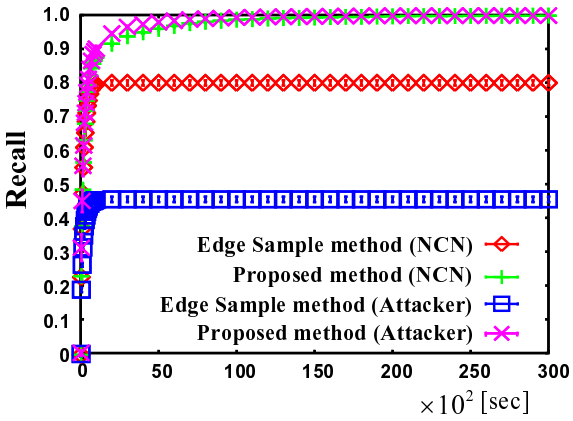

図 4.62: R_c=0.3 の場合における時間の推移と再現率との関係

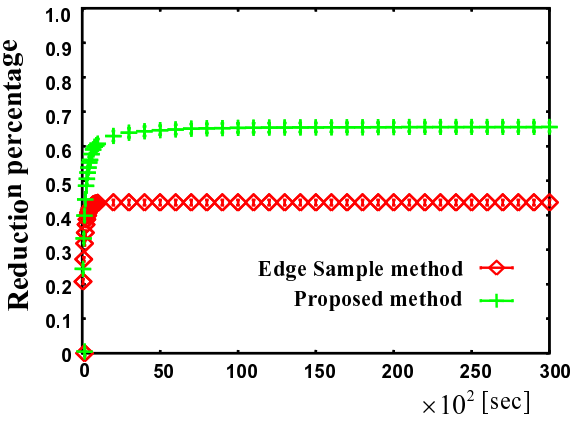

図 4.63: R_c=0.3 の場合における時間の推移とトラヒック減少率との関係

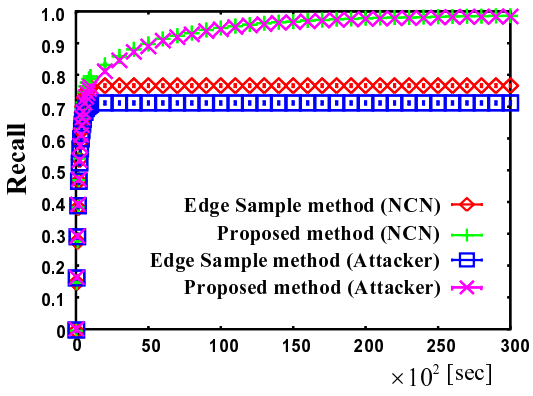

図 4.64: R_c=0.7 の場合における時間の推移と再現率との関係

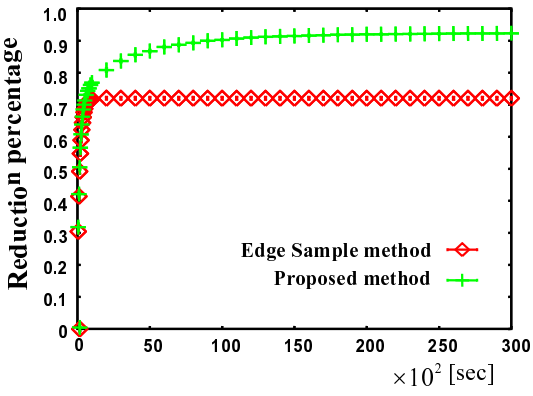

図 4.65: R_c=0.7 の場合における時間の推移とトラヒック減少率との関係

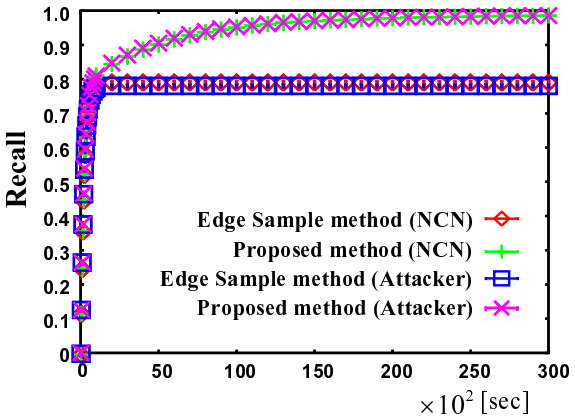

図 4.66: R_c=0.9 の場合における時間の推移と再現率との関係

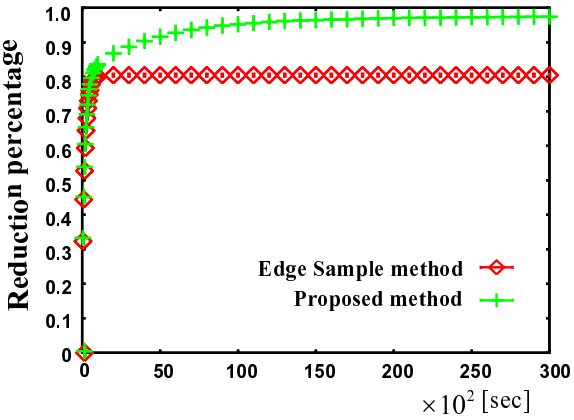

図 4.67: R_c=0.9 の場合における時間の推移とトラヒック減少率との関係

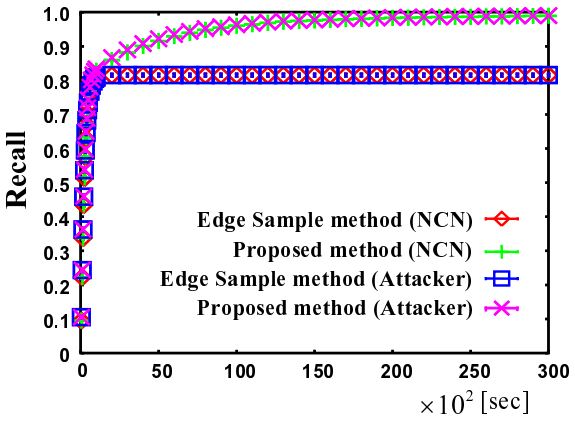

図 4.68: R_c=1.0 の場合における時間の推移と再現率との関係

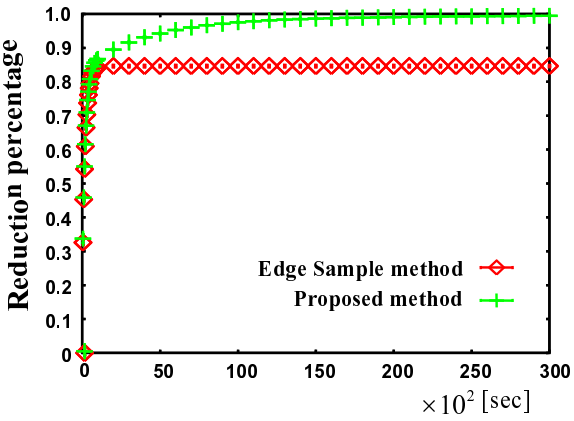

図 4.69: R_c=1.0 の場合における時間の推移とトラヒック減少率との関係

クの減少率共に高くなっており，提案手法は R_c の値に関わらず有効であると言える．そして，基準ケースの項で推測したとおり，Edge Sample 手法において，R_c の値が小さい方が NCN の再現率と攻撃者の再現率の差が大きくなっている．また，提案手法によるトラヒックの減少率については R_c=1.0 の場合には NCN 検出を確実に行えば攻撃トラヒックを攻撃者の根元で遮断することが可能となるため，十分に時間が経過すれば減少率はほぼ 1 .0 となっている．最後に，再現率に関しては時間の経過と共に 1 に収束していくことも併せて確認された．

次に，各々の N_a に対する実験結果から，観測時間 3000[sec] における再現率・トラヒック減少率を抽出した結果を，図 4.71,4.72 に示し，比較を行う．また，図 4.71,4.72 について，提案手法を用いた場合と Edge Sample 手法単独の場合の評価値の差分を取った結果を図 4.73,4.74 に示す．

図 4.71 からは次の 2 点が分かる．

1. Edge Sample 手法による NCN の再現率，提案手法による再現率（NCN・攻撃者）は，R_c の増加に伴い初めは緩やかに減少し，R_c=0.5or0.7 の付近から緩やかな上昇に転じる

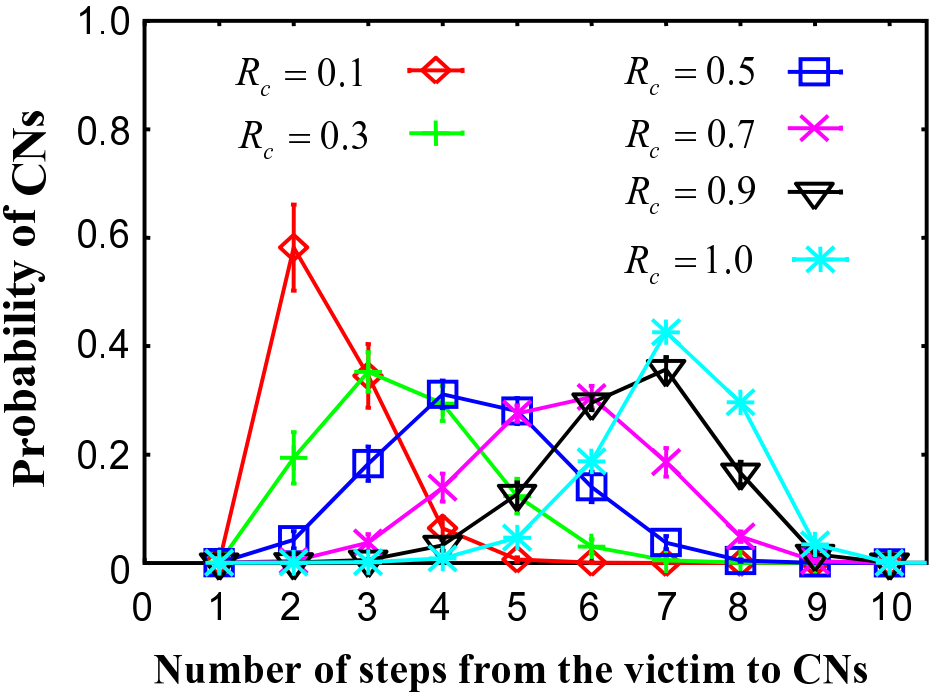

図 4.70: CN の割合と step 数分布との関係

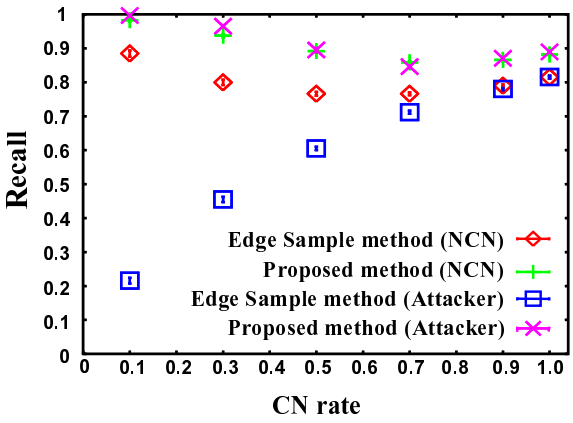

図 4.71: CN の割合と再現率との関係

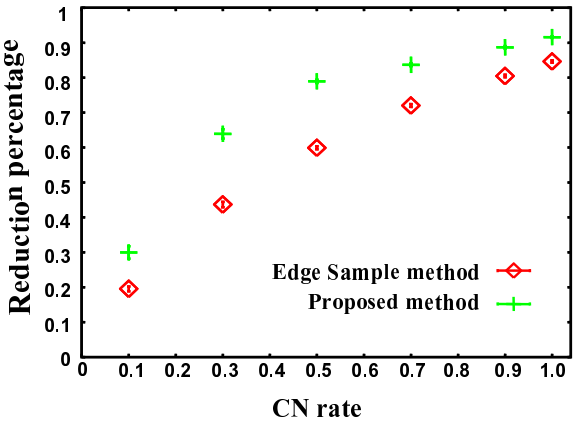

図 4.72: CN の割合とトラヒック減少率との関係

2. Edge Sample 手法による攻撃者の再現率は，R_c の増加に伴い大幅に上昇する

ここでは， 1 について，一次関数的な特徴を示さない原因を図 4.75 を用いて説明する．図 4.75 は，あるトポロジーに対し，CN を増加させていったときの Edge Sample 手法で検出することができる NCN の比率の変遷を表している．例えば，図 4.75(a) では検出比率は $\frac{1}{2}$ であるが，Node1 が CN（CN3）となることによって（図 4.75(b)），$\frac{2}{2}$ となり検出比率は増加することとなる．一方，さらに Node2 が CN（CN4）となると（図 4.75(c)），検出比率は $\frac{2}{3}$ となり逆に低下することとなる．つまり，CN が増える（= R_c が増加する）ことで，検出可能な NCN が増える場合もあれば減る場合もあるということである．し

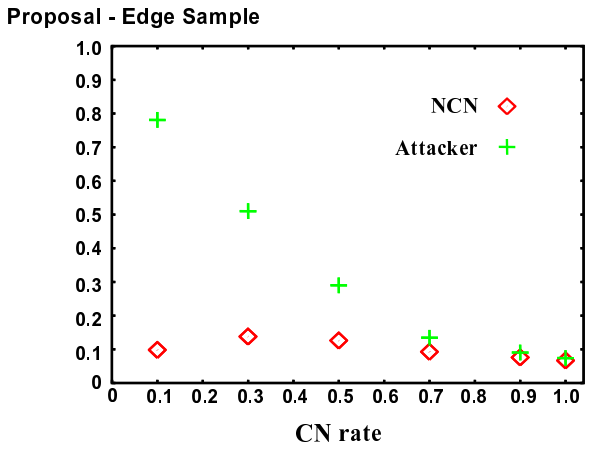

図 4.73: CN の割合と提案手法の効果との関係（再現率）

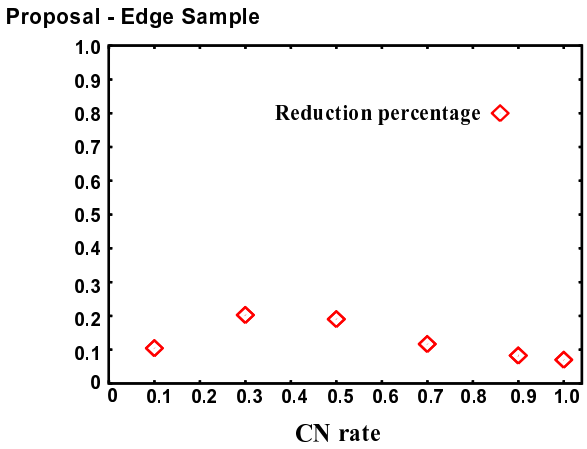

図 4.74: CN の割合と提案手法の効果との関係（トラヒック減少率）

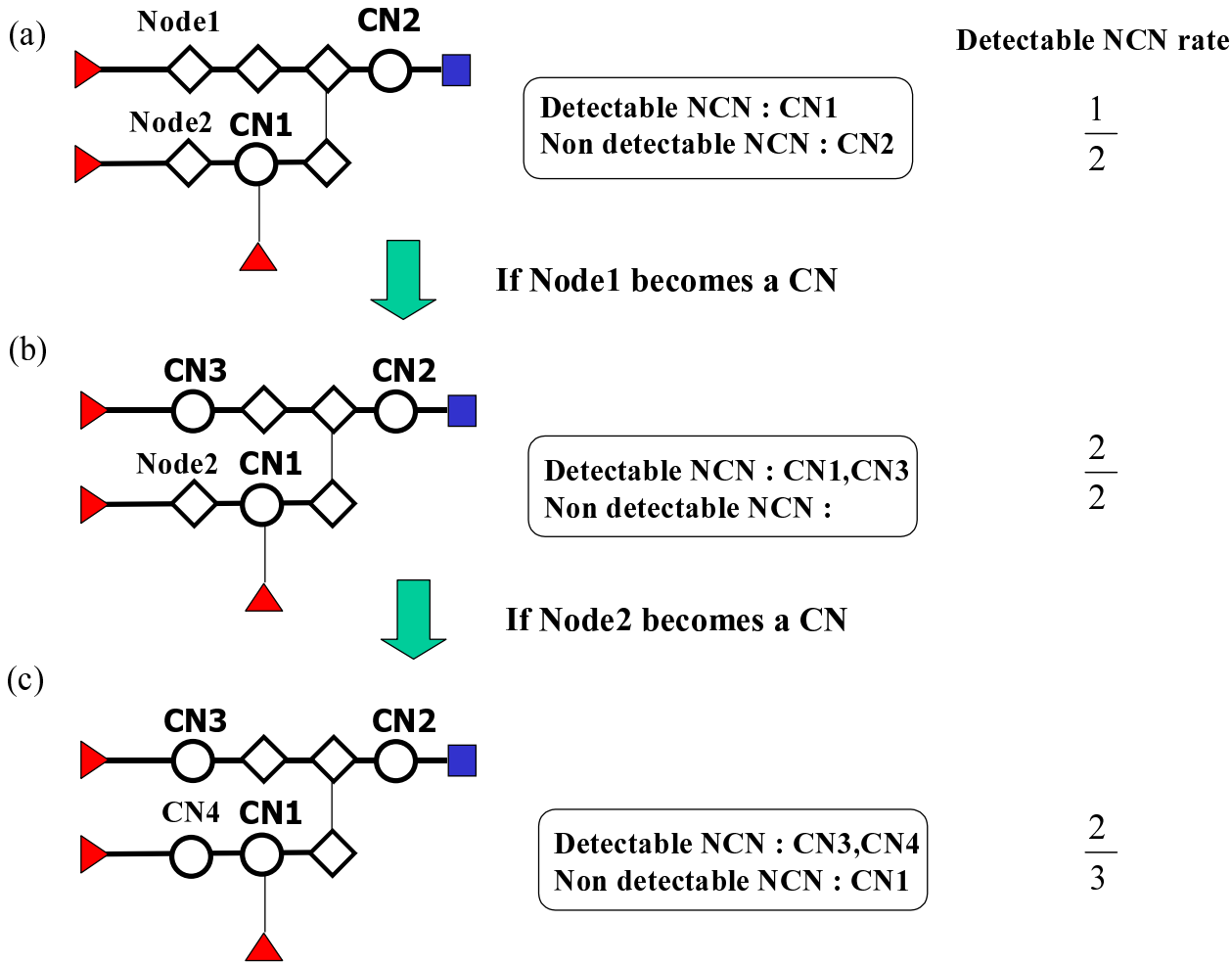

図 4.75: Edge Sample 手法において検出可能な NCN の変遷

たがって一次関数的な特徴を示さないのである．

次に，２については R_c が小さくなると，サブマリンノードに合流する攻撃経路数が増加することが原因である．

最後に，図 4.72 では，R_c の増加に伴い大幅にトラヒック減少率が上昇している．これは，R_c が小さい場合，攻撃者から NCN までの hop 数が大きくなるため，NCN を検出したとしても，減少率が抑えられてしまうからである．

マーキング確率 p について

本項では，マーキング確率 R_c と各評価値との関連性を探る．提案手法は，マークパケット数の統計的性質を利用して NCN 検出を行うため，マーキング確率 p に比例して NCN を検出するために要する時間が増減すると考えられる．そこで，基準ケースと同一の条件でマーキング確率 p を p=$\frac{1}{2000}$（観測終了時間：3000[sec]），$\frac{1}{200}$（観測終了時間：300[sec]），$\frac{1}{20}$（観測時間：30[sec]）と変動させた場合の，時間の推移と NCN・攻撃者の再現率，トラヒックの減少率との関係を図 4.76～4.81 に示し，各評価値との関連性を考察する．

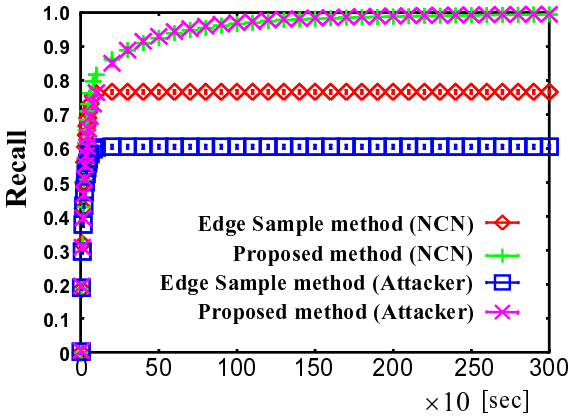

図 4.76: $p = \frac{1}{2000}$ の場合における時間の推移と再現率との関係

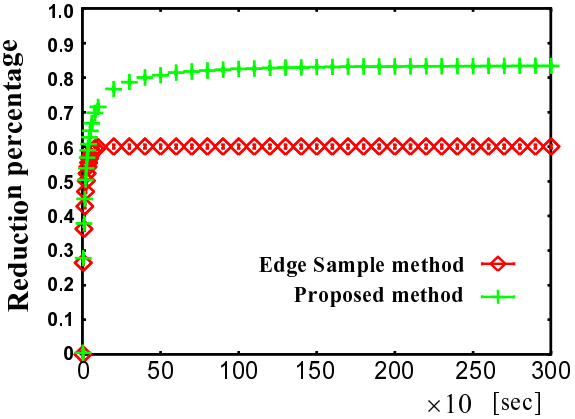

図 4.77: $p = \frac{1}{2000}$ の場合における時間の推移とトラヒック減少率との関係

図 4.76～4.81 の全てのケースで，提案手法を用いた方が Edge Sample 手法単独より再現率・トラヒックの減少率共に高くなっており，提案手法は p の値に関わらず有効であると言える．また，それぞれの評価値は図 4.9,4.11 の例と酷似しており，マーキング確率 p と検出に要する時間は比例関係にあることが明らかとなった．

上書きの影響について

.4.1.1 節では，上書きはマークパケットの比較にほとんど影響を与えないことを示し，式 (3.1),(3.2) を用いた検定による提案手法を提案した．本節では，上書きの影響を取り除くために以下の式を導入して NCN 検出を行い，その結果を式 (3.1),(3.2) を用いた従来の実験結果を比較することで，上書きの影響が

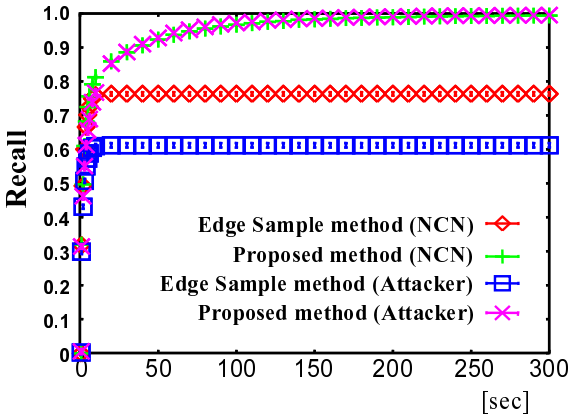

図 4.78: $p = \frac{1}{200}$ の場合における時間の推移と再現率との関係

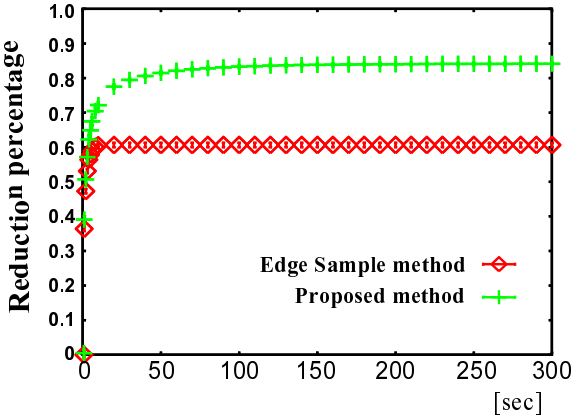

図 4.79: $p = \frac{1}{200}$ の場合における時間の推移とトラヒック減少率との関係

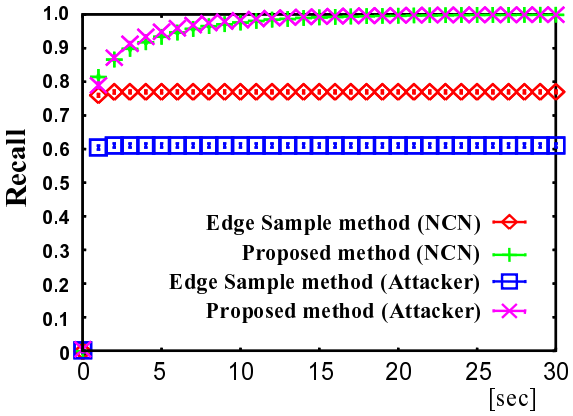

図 4.80: $p = \frac{1}{20}$ の場合における時間の推移と再現率との関係

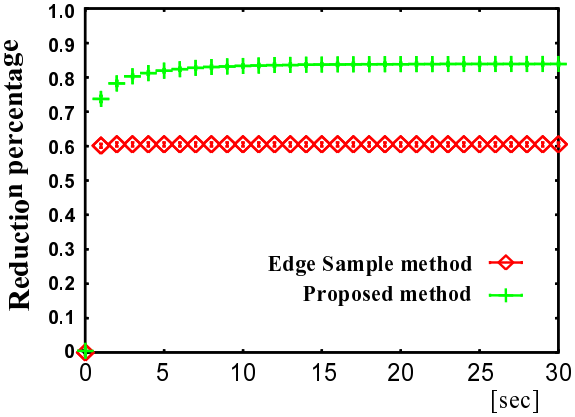

図 4.81: $p = \frac{1}{20}$ の場合における時間の推移とトラヒック減少率との関係

寡少であることを示す．ただし，ここでは，比較する評価値として NCN の再現率・適合率を用い，上書きの影響がある提案手法のみの結果を比較する．

CNa が NCN でない場合

$$E(n_{C_a}) = \frac{E(\sum_{i=1}^{k} n_{C_i})}{1-p} \tag{4.3}$$

CNa が NCN である場合

$$E(n_{C_a}) > \frac{E(\sum_{i=1}^{k} n_{C_i})}{1-p} \tag{4.4}$$

(N_n,m,N_a,R_c)=(2000,2,1000,5)，マーキング確率 p=$\frac{1}{20000}$,$\frac{1}{2000}$,$\frac{1}{200}$,$\frac{1}{20}$ に対し，式 (3.1),(3.2) を用いた場合と式 (3.3),(3.4) を用いた場合の，時間の推移と NCN の再現率・適合率との関係を比較した結果を図 4.82〜4.89 に示す．

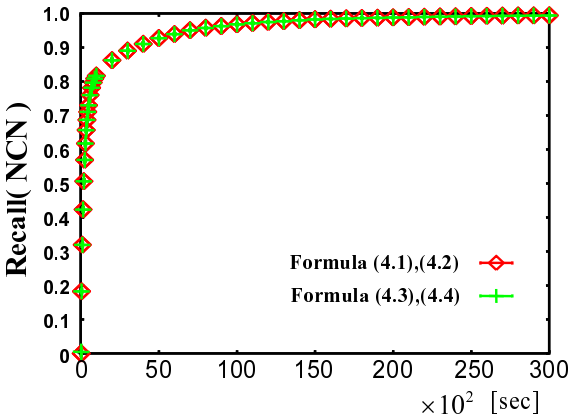

図 4.82: $p = \frac{1}{20000}$ において式 (4.1),(4.2) を用いた場合と式 (4.3),(4.4) を用いた場合の再現率の比較 (x 軸:時間)

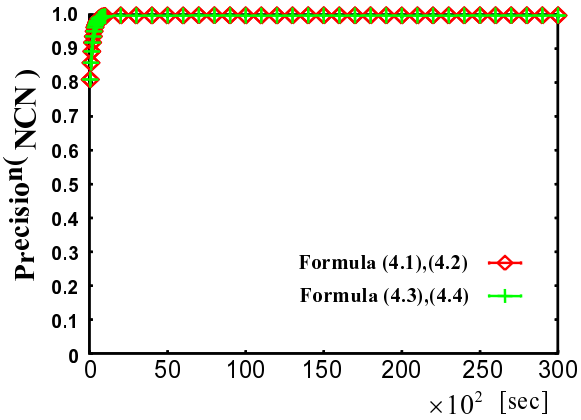

図 4.83: $p = \frac{1}{20000}$ において式 (4.1),(4.2) を用いた場合と式 (4.3),(4.4) を用いた場合の適合率の比較 (x 軸:時間)

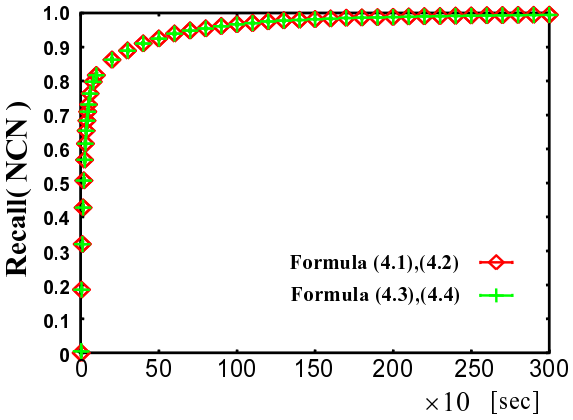

図 4.84: $p = \frac{1}{2000}$ において式 (4.1),(4.2) を用いた場合と式 (4.3),(4.4) を用いた場合の再現率の比較 (x 軸:時間)

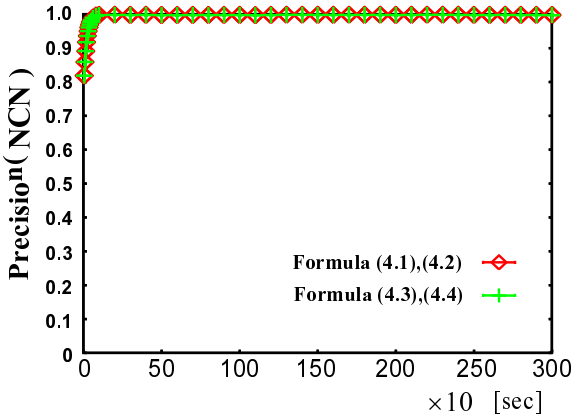

図 4.85: $p = \frac{1}{2000}$ において式 (4.1),(4.2) を用いた場合と式 (4.3),(4.4) を用いた場合の適合率の比較 (x 軸:時間)

図 4.82〜4.89 の全てについて，式 (3.1),(3.2) を用いたものと式 (3.3),(3.4) を用いたもので結果の違いはほぼない．よって，マーキング確率が $p \leq \frac{1}{20}$ である場合，上書きの影響はほぼないと言える．

4.2.3 提案手法に対して各想定が及ぼす影響について

4.2.2 節では 4.2.1 節で提示した 8 つの想定で実験を行った．しかし，これらの想定が成り立つことは実ネットワークでは考えられない．本節では提案手法の実ネットワークへの適用を考慮し，各想定への頑健性の検証を行う．

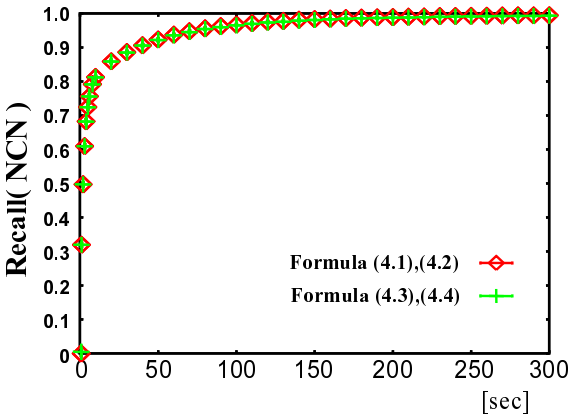

図 4.86: $p = \frac{1}{200}$ において式 (4.1),(4.2) を用いた場合と式 (4.3),(4.4) を用いた場合の再現率の比較（x 軸：時間）

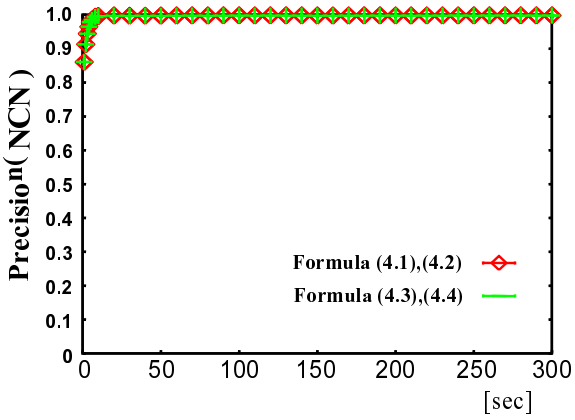

図 4.87: $p = \frac{1}{200}$ において式 (4.1),(4.2) を用いた場合と式 (4.3),(4.4) を用いた場合の適合率の比較（x 軸：時間）

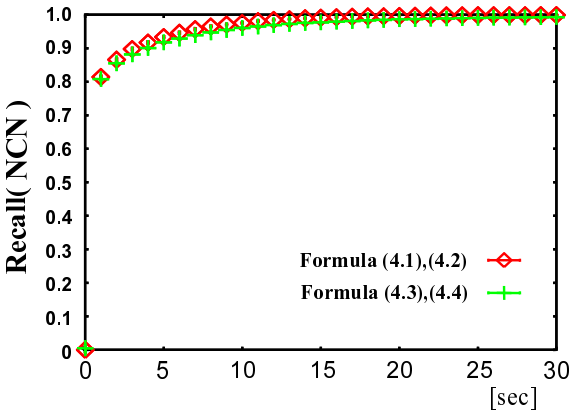

図 4.88: $p = \frac{1}{20}$ において式 (4.1),(4.2) を用いた場合と式 (4.3),(4.4) を用いた場合の再現率の比較（x 軸：時間）

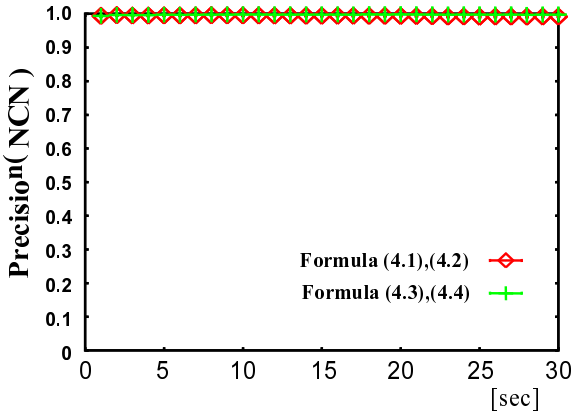

図 4.89: $p = \frac{1}{20}$ において式 (4.1),(4.2) を用いた場合と式 (4.3),(4.4) を用いた場合の適合率の比較（x 軸：時間）

想定１～５について

想定１ 全ての攻撃者は同数の攻撃パケットを送出する
想定２ 全ての攻撃者は同時に攻撃を開始する
想定３ 全ての攻撃者は攻撃を一定期間続ける（on,off しない）
想定４ 全ての攻撃者は同時に攻撃を終了する
想定５ 攻撃経路上でパケットロスや逆転は起こらない

想定１～５は，１攻撃経路あたりのマークパケット数，マークパケットの発生間隔を揺るがす想定である．しかしながら，これらの想定の成否は本質的に提案手法による効果を妨げるものではない．なぜなら，NCN である CN に攻撃パケットが合流することに変わりはなく，マークパケットの差は確実に生じ

るからである．ただし，マークパケット数はパケット数に比例するため，想定１～５を覆すことで特定するまでにかかる時間は変動すると考えられる．

ここでは，想定１～５の成否が提案手法の有効性を妨げる要素にはならないことを示すため，各想定についてそれを覆す DDoS 攻撃のモデルを設定し，実験を行う．ただし，想定４については，想定３についての実験で説明可能であるため，省略する．また，想定５については以下の要因から提案手法の効果にほぼ影響を与えないことが明白であるため，これについても省略する．

- パケットの逆転は，マークパケット数の変化をもたらさない
- パケットロスについては，マークパケットの喪失という点でマークパケットの上書きと影響は同じであり，ネットワーク全体のパケットロス率が $\frac{1}{20}$ を上回ることはないと考えられるため，影響は限定的である

以下の各項で，各想定を覆すための攻撃モデルを説明し，そのモデルを用いた場合の実験結果を示し，想定１～４に対する提案手法の頑健性を確認する．また，その他の条件については節の基準ケースと同一（(N_n,m,N_a,R_c)=(5000,2,1000,5),$p = \frac{1}{20000}$）とし，評価値については提案手法の主目的である再現率を用いる．

想定１について

想定１　全ての攻撃者は同数の攻撃パケットを送出する

4.2.2 節における実験では，全ての攻撃者 (攻撃者数 : 1000) はパケットレート $N_p = 100$[pps] で行っている．本節では攻撃者のパケットレートを５種類設定し，均等に配分して攻撃を行った結果を示す．具体的には，パケットレート $N_p = (20, 60, 100, 140, 180)$[pps] の５種類を用意し，各パケットレートに対し攻撃者数２００ずつ配置した．図 4.90 はその条件下での再現率の結果（x 軸 : 時間）を表している．

図 4.90 は，基準ケースである図 4.9 とほぼ同一の結果となっているが，観測終了時点で提案手法の再現率が 1.0 になっていない．これは，パケットレートが低い攻撃者の NCN が検出されていないためであると推測される．

その確認のため，提案手法による各パケットレートごとの攻撃者の再現率の結果を図 4.91 に示す．NCN の再現率としなかった理由は，一つの NCN に異なった種類のパケットレートの攻撃経路が合流している可能性があるためである．ただし，図 4.91 ではパケットレートごとの再現率の違いを分かりやすく表示するため，y 軸の範囲を $0.7 \leq y \leq 1.0$ としてある．

図 4.91 を見ると，パケットレートが $N_p = (100, 140, 180)$[pps] の攻撃者の再現率はほぼ 1.0 となっているのに対し，$N_p = (20, 60)$[pps] の攻撃者の再現率は観測終了時点で 1.0 になっているとは言えない．そのため，全体の検出率も観測終了時点で 1.0 とならない．

想定２について

想定２　全ての攻撃者は同時に攻撃を開始する

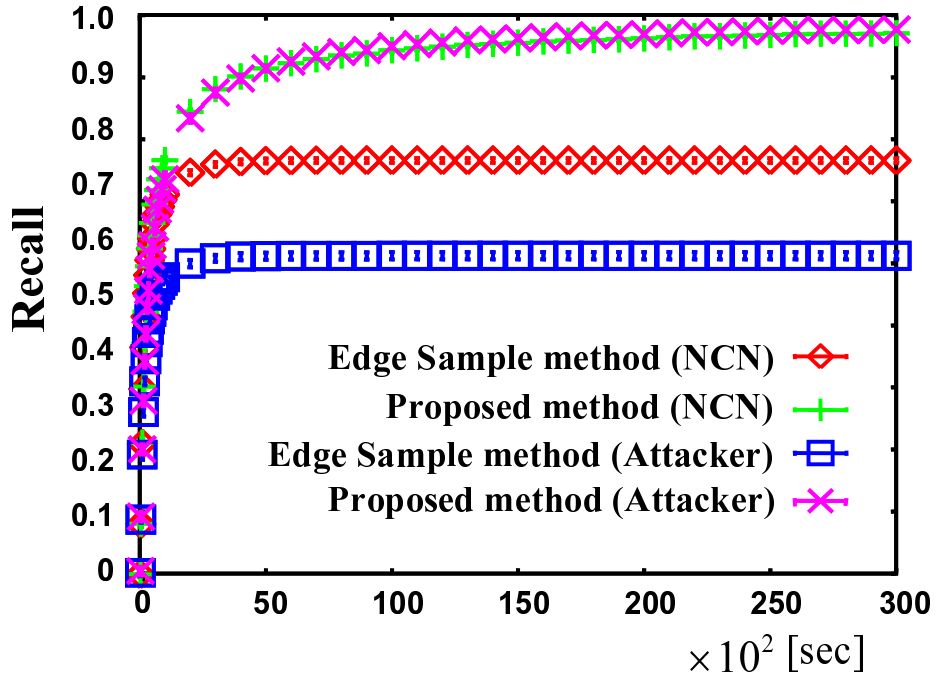

図 4.90: $N_p = (20, 60, 100, 140, 180)$[pps] とした場合における時間の推移と再現率との関係

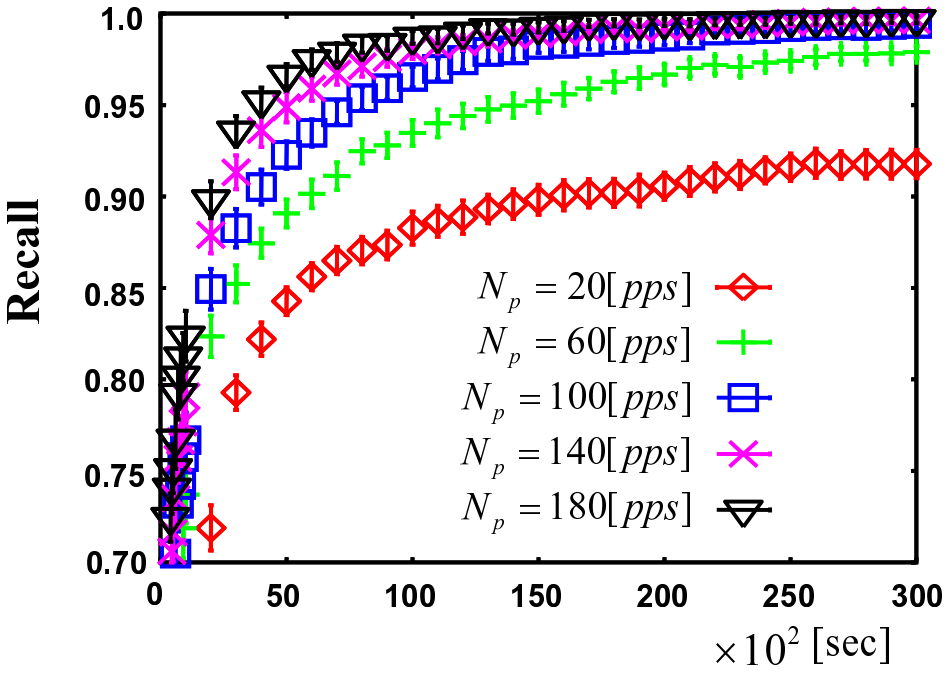

図 4.91: 各パケットレートにおける攻撃者再現率の比較（x 軸：時間）

本項では，想定 2 を覆す攻撃モデルとして，以下の攻撃モデルを用いる．

- 攻撃開始時の攻撃者数を 1 とする

- 毎秒ごとに $\frac{1}{t_i}$ の確率で攻撃者数を 1 増加させる（平均 t_i 秒で攻撃者 1 増加する）
- 攻撃者数の最大値を 1000 とする

図 4.92〜4.97 は上記の攻撃モデルを用い t_i=2,5,20 とした場合の，NCN・攻撃者の再現率と攻撃者・NCN の出現率（x 軸：時間）を表している．ただし，NCN の出現率については，ある NCN について複数の攻撃者がいる場合，1 攻撃者が出現した時点で，その NCN は出現したとみなした．

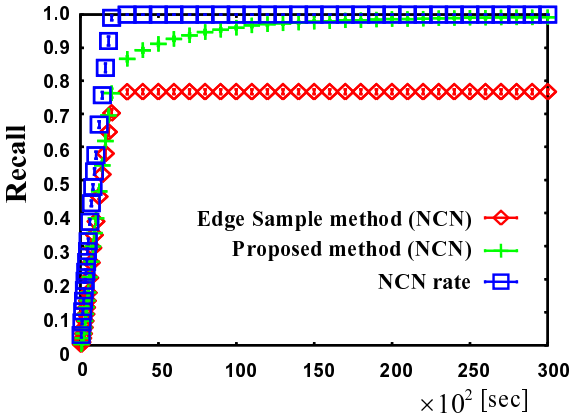

図 4.92: 攻撃を同時に開始しない場合（t_i=2）における時間の推移と NCN 再現率との関係

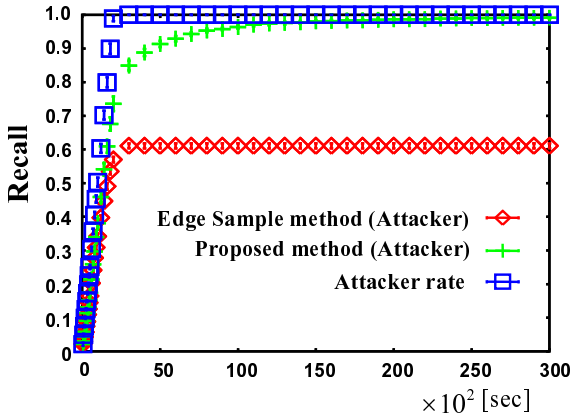

図 4.93: 攻撃を同時に開始しない場合（t_i=2）における時間の推移と攻撃者再現率との関係

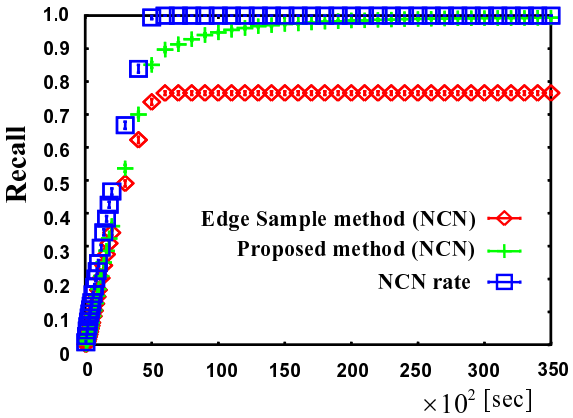

図 4.94: 攻撃を同時に開始しない場合（t_i=5）における時間の推移と NCN 再現率との関係

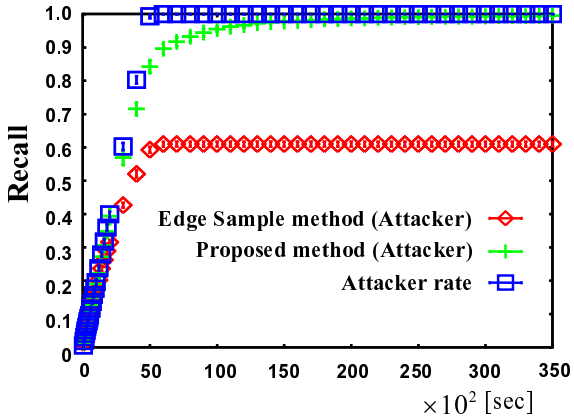

図 4.95: 攻撃を同時に開始しない場合（t_i=5）における時間の推移と攻撃者再現率との関係

図 4.92〜4.97 では，提案手法による再現率は NCN・攻撃者の出現率を追走する形で上昇しており，攻撃が同時に開始されない場合でも，提案手法が有効であることが明らかとなった．

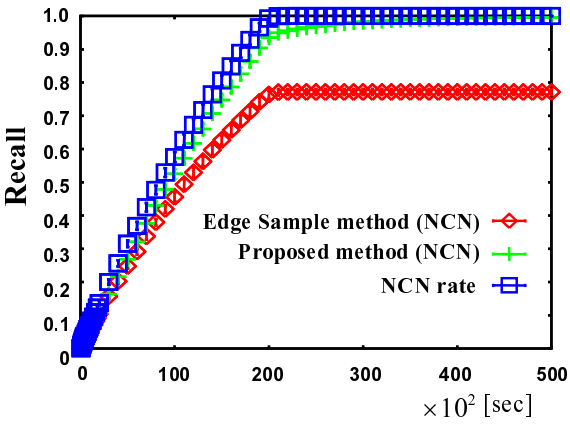

図 4.96: 攻撃を同時に開始しない場合（t_i=20）における時間の推移と NCN 再現率との関係

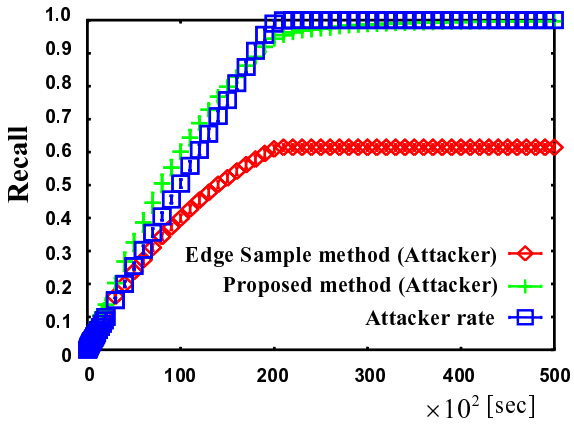

図 4.97: 攻撃を同時に開始しない場合（t_i=20）における時間の推移と攻撃者再現率との関係

想定３について

想定３　全ての攻撃者は攻撃を一定期間続ける（on,off しない）

本項では，想定３を覆す攻撃モデルとして，常に一定のパケットレートで攻撃を行うのではなく，パルス的にオン・オフを繰り返しながら攻撃を行うモデルを設定する．ここでは，High パルス幅（攻撃がオンの状態）を T_{on}[sec]，パルスのデューティー比を R_d と定義し，全ての攻撃者はこの値に従い攻撃をオンオフすることとする．また，攻撃が行われている最中のパケットレートは全て $N_p = 100$[pps] とする．ただし，全ての攻撃者が同時に攻撃を開始すると，オンオフ状態が全て重なるため，単純にオフの部分をカットした結果が出ることが明白である．そこで，各攻撃者の開始時間を変え，オンオフの位相をずらすことにする．具体的には，想定２の攻撃モデルを用いることで順次攻撃参加させ，開始後は上記のオンオフモデル（攻撃開始時はオン）に従って攻撃を行う．

図 4.98～4.102 は，それぞれ (T_{on}, R_d) =(100,5),(1000,5),(10000,5),(1000,2),(1000,10) とした場合の再現率の結果（x 軸：時間）を表している．

図 4.98～4.102 において，再現率は良好な値をとっていることが分かる．ただし，T_{on},R_d の値の増加に伴い，平均パケットレートが低下するため，検出に要する時間は増大している．

そこで，次にパケットレートを完全に平均化した（$N_p = 100R_d$[pps]）結果と上記で提示したオンオフモデルによる結果を比較する．このとき，１攻撃者からのパケット数を比較すると，オンが終了してオフに切り替わる時に差は最大（オンオフモデルによるおパケット数の方が多い）となり，その差は $100T_{on}(1 - R_d)$ で求められる．よって，(T_{on}, R_d) =(100,5),(1000,5),(10000,5),(1000,2),(1000,10) に対し，差が最大となるのは (T_{on}, R_d) =(10000,5) の場合であり，平均化した結果とオンオフモデルによる結果に最も違いが生じることとなる．そこで，このケースについての比較を行う．図 4.103 は NCN の検出の比較結果（x 軸：時間）を表している．

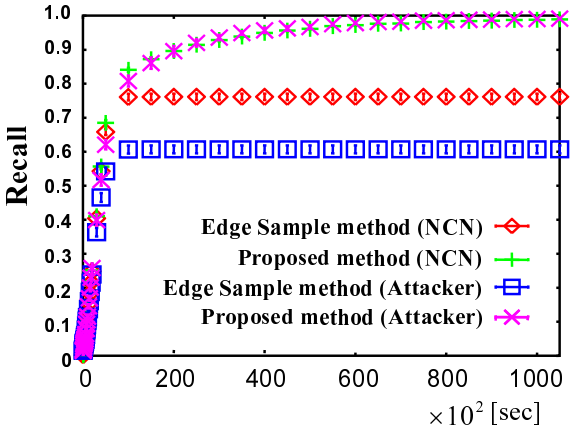

図 4.98: (T_{on}, R_d) =(100,5) の場合における時間の推移と再現率との関係

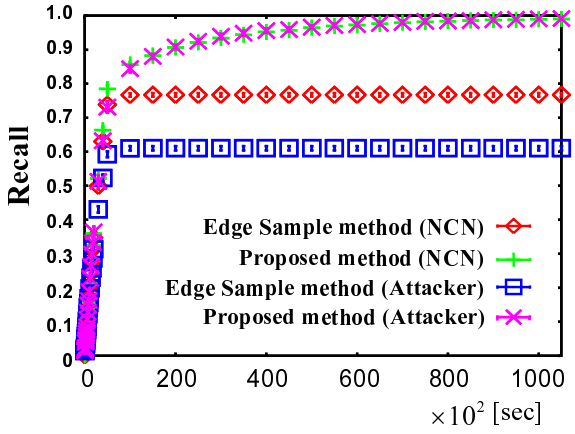

図 4.99: (T_{on}, R_d) =(1000,5) の場合における時間の推移と再現率との関係

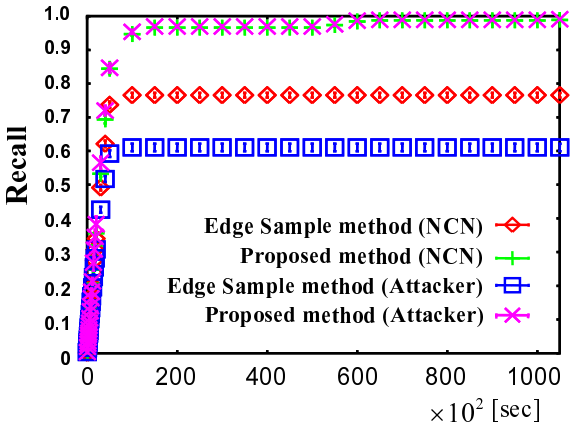

図 4.100: (T_{on}, R_d) =(10000,5) の場合における時間の推移と再現率との関係

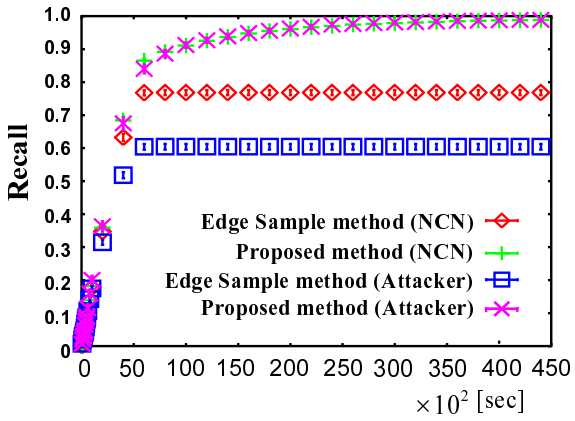

図 4.101: (T_{on}, R_d) =(1000,2) の場合における時間の推移と再現率との関係

図 4.103 では，特に 20000[sec] 以下の時，提案手法の結果において，オンオフモデルが上回っている．この結果の差は，図 4.104 で示す通り，総パケット数の差がもたらすものである．

したがって，x 軸に時間ではなく，総パケット数をとると図 4.105 のようになり，平均化したものとオンオフモデルの結果の差はほぼなくなる．

また，本項の実験ではオンオフの位相がずれているため，終了は同時とならない．よって，想定 4 についても問題にならないと考えられる．

想定 6 について

想定 6　攻撃中は攻撃経路は変更されない

この想定の成否も提案手法による効果を妨げないと考えられる．なぜなら，提案手法は入り側と出側のマークパケット数の差を捉えることにより NCN であるか特定する手法であるため，攻撃経路が変更され

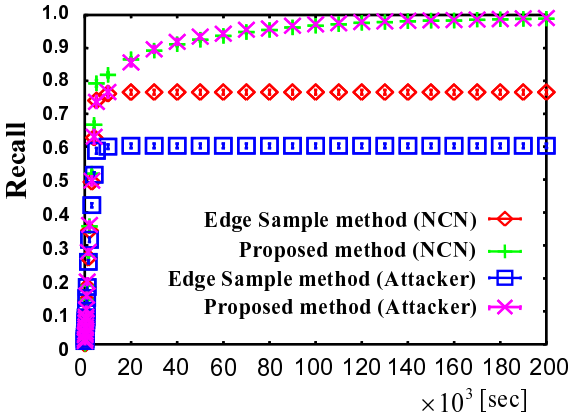

図 4.102: (T_{on}, R_d) =(1000,10) の場合
における時間の推移と再現率との関係

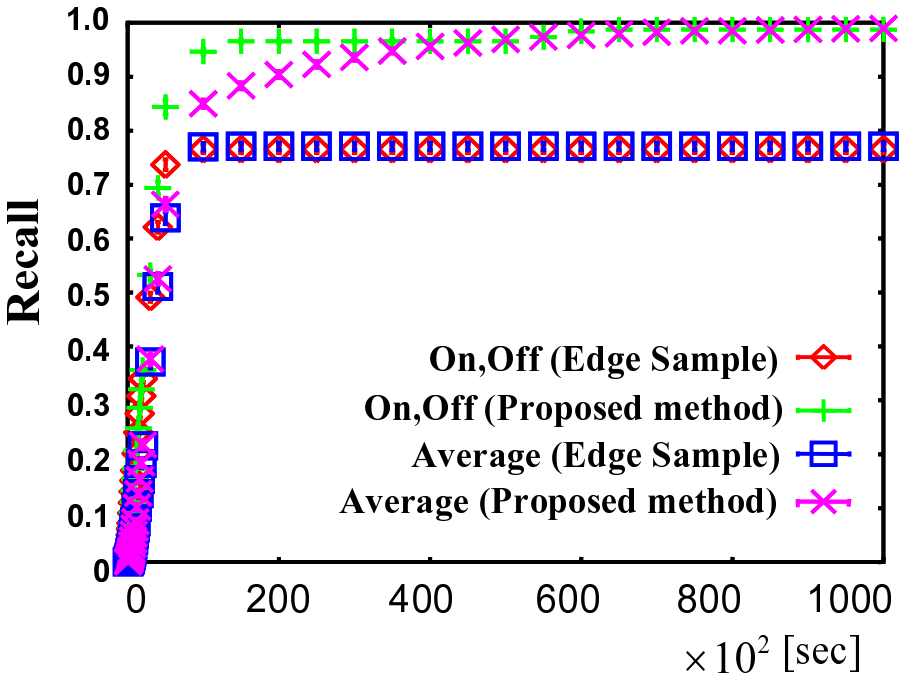

図 4.103: オンオフモデル ((T_{on}, R_d) =(10000,5)) と平均化した場合との NCN 再現率の比較（x 軸：時間）

て攻撃パケットが通過する出力インターフェースが変わったとしても，出側のマークパケット数には変わりはないからである．

その例として，図 4.106 のように攻撃経路が変更されたケースを想定する．

このとき，出側のマークパケット数を $n_{C_{a,b}} + n_{C_{a,d}}$ としてカウントすれば，入り側と出側のマークパケット数の比較になんら支障はない．そのため，経路が変更されるケースについても，提案手法を変化させることなく適用できる．

ここでは，検証実験としてノード故障に伴い経路変更が発生するネットワーク状況での NCN 特定結果

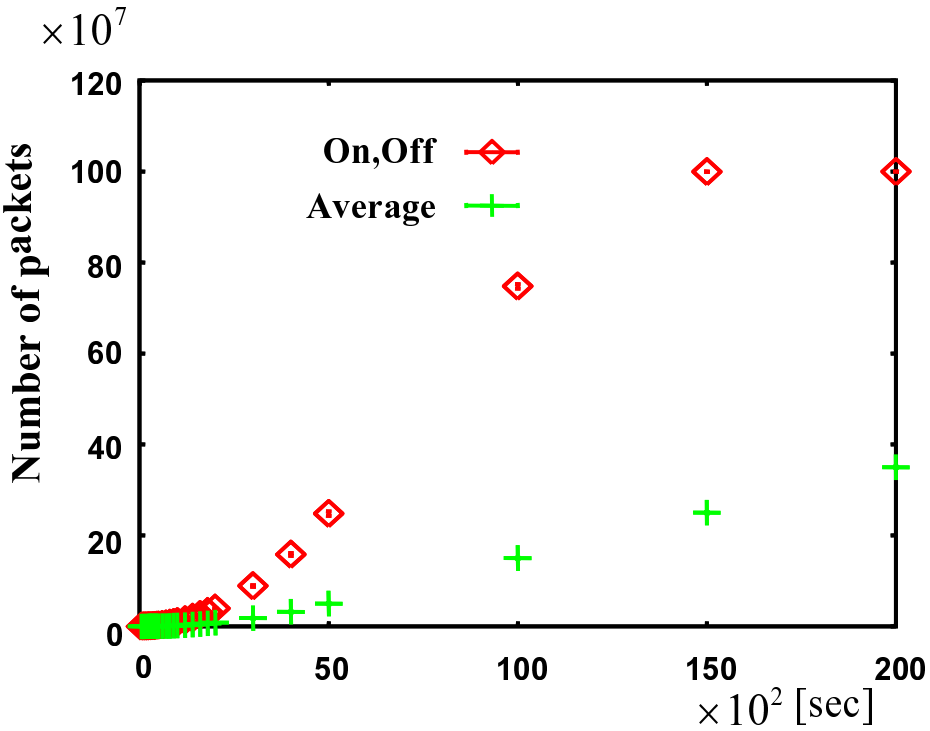

図 4.104: オンオフモデル ((T_{on}, R_d) =(10000,5)) と平均化した場合と総パケット数の比較

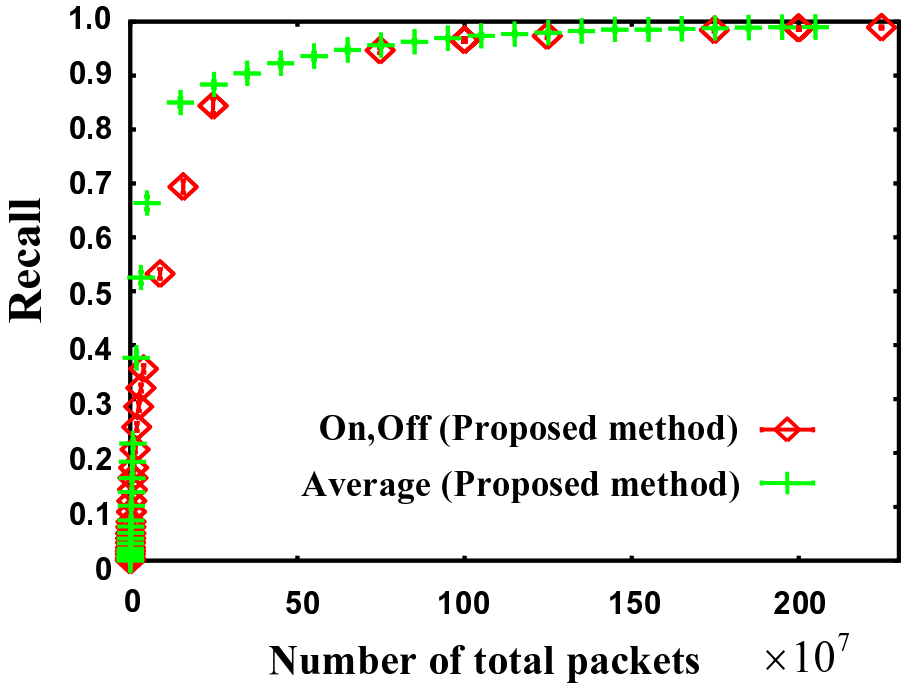

図 4.105: オンオフモデル ((T_{on}, R_d) =(10000,5)) と平均化した場合との NCN 再現率の比較（x 軸：総パケット数）

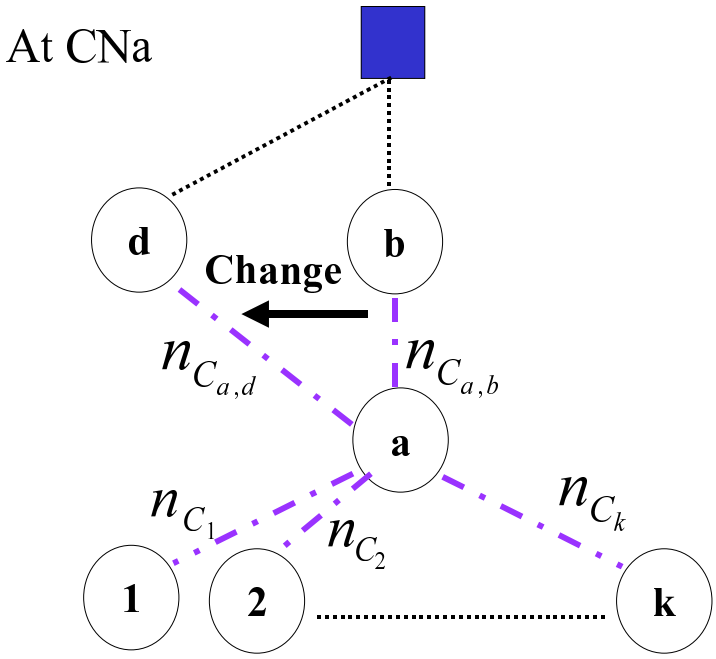

図 4.106: 経路変更に伴うマークパケット数の得られ方の変化

を示す．ただし，毎秒ごとの故障発生確率を $\frac{1}{t_b}$（平均 t_b[sec] に 1 ノード故障する），修理時間を∞とする．また，経路変更により NCN ではなくなった CN については，犠牲者側でそのことを検知できないため，NCN としてカウントする．

図 4.107〜4.112 は t_b=10,30,60 とした場合の NCN の再現率の結果（x 軸：時間）と，経路変更に伴う NCN とリーフ NCN（Edge Sample 手法で検出可能な NCN）の数の推移（x 軸：時間）を表している．

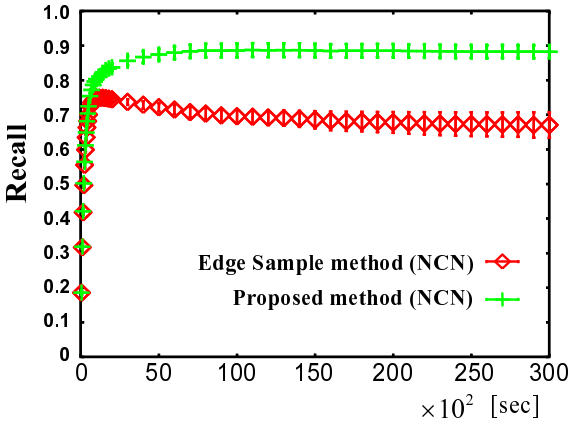

図 4.107: 経路変更が起こる場合（t_b=10）における時間の推移と NCN 再現率との関係

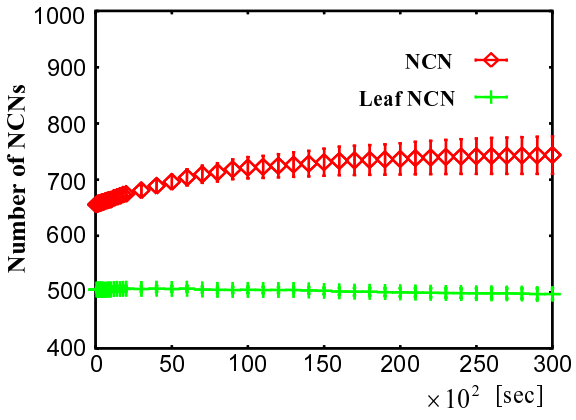

図 4.108: 経路変更が起こる場合（t_b=10）の NCN とリーフ NCN の数の推移（x 軸：時間）

図 4.107,4.109,4.111 を見ると，Edge Sample 手法単独では経路変更に伴い再現率が低下しているのに対し，提案手法を用いた場合，Edge Sample 手法による再現率の低下を提案手法が補っているため，再

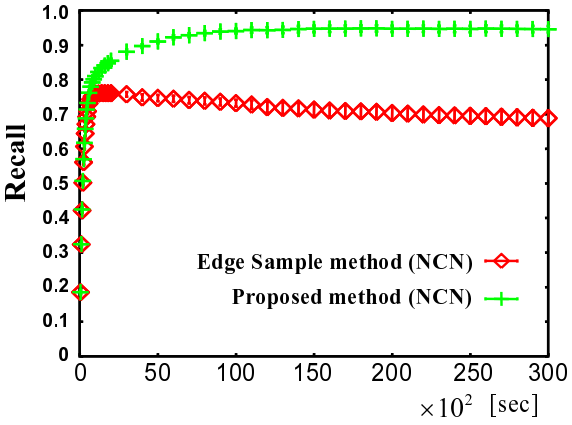

図 4.109: 経路変更が起こる場合(t_b=30)における時間の推移と NCN 再現率との関係

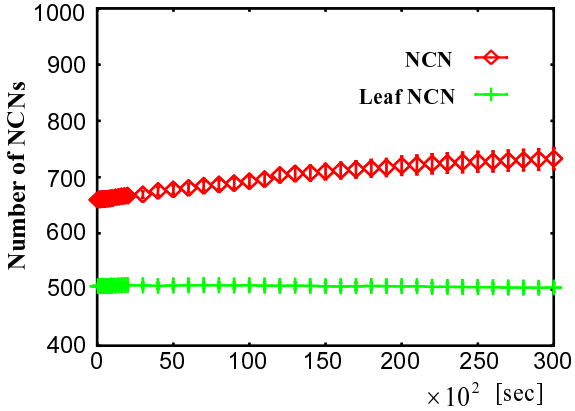

図 4.110: 経路変更が起こる場合(t_b=30)の NCN とリーフ NCN の数の推移（x 軸：時間）

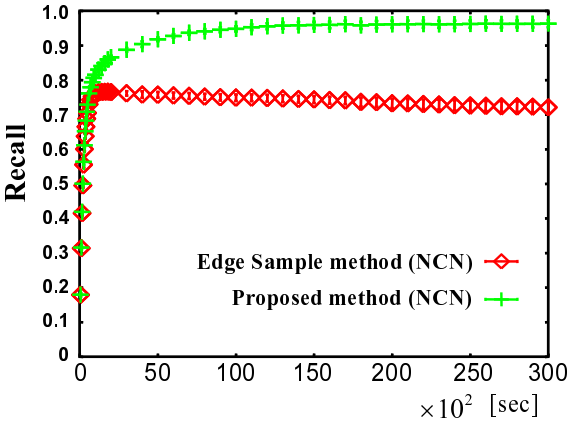

図 4.111: 経路変更が起こる場合(t_b=60)における時間の推移と NCN 再現率との関係

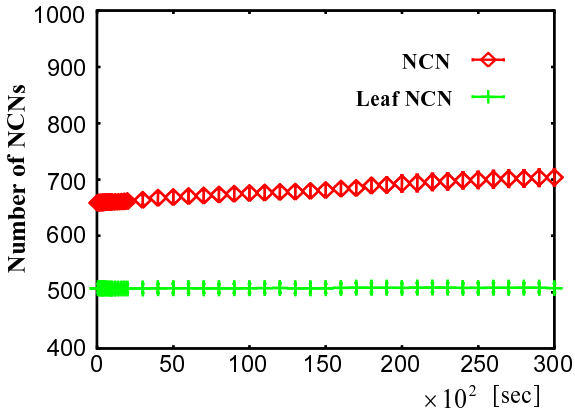

図 4.112: 経路変更が起こる場合(t_b=60)の NCN とリーフ NCN の数の推移（x 軸：時間）

現率の低下は見られない．ただし，故障するノードによっては，犠牲者に到達する経路が著しく少なくなるといった事態を引き起こすため，信頼区間の幅は大きくなっている．

また，図 4.108,4.110,4.112 を見ると，NCN の数は増加しているのに対し，リーフノードの数は僅かながら減少している．つまり，経路変更の影響で全体の NCN に占めるリーフ NCN の割合が低下し，逆にサブマリンノードの割合は増加することになるのである．例えば，図 4.113 の例では Node1 が故障することによって，CN3 が NCN（リーフ NCN）となるが，その影響で CN2 がサブマリンノードとなる．そのため，リーフ NCN は増加せずに NCN のみが増加していることになる．また，図 4.114 の例では Node2 が故障することによって，CN 1 がサブマリンノードとなる．そのため，NCN は増加しないが，リーフ NCN の数が低下することになる．

したがって，時間の経過と共に Edge Sample 手法による再現率は低下し，一方提案手法を用いると新たに誕生したサブマリンノードを検出することによって再現率を維持していると言える．

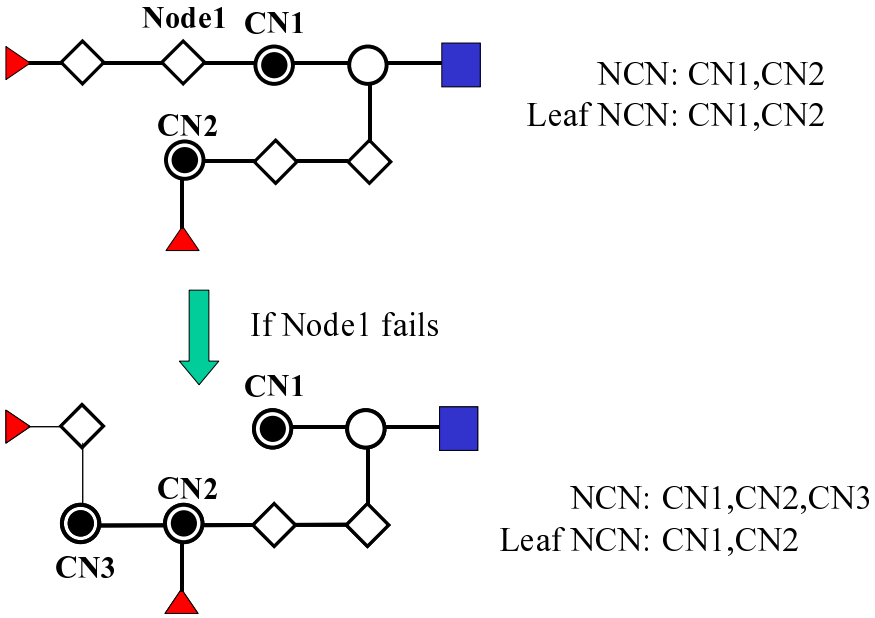

図 4.113: 経路変更に伴う NCN とリーフ NCN の数の変化 1

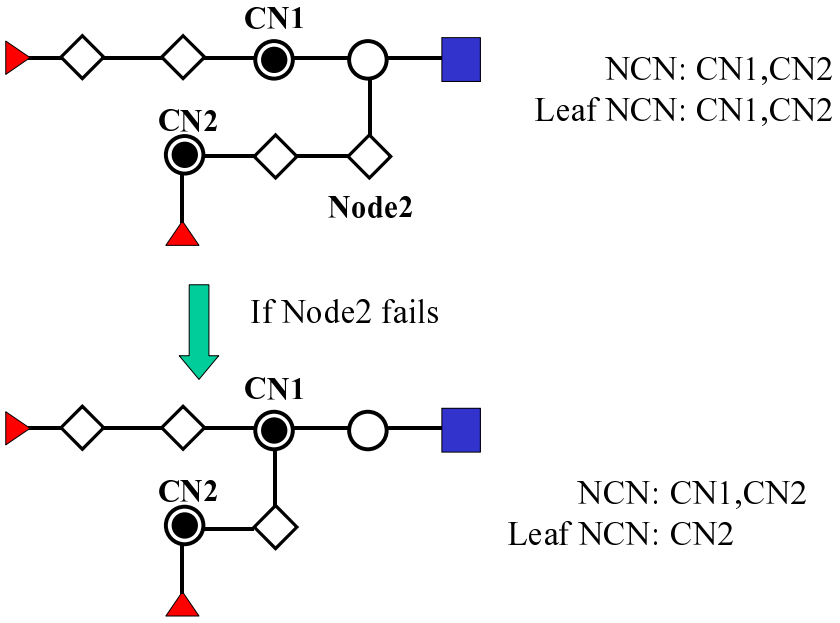

図 4.114: 経路変更に伴う NCN とリーフ NCN の数の変化 2

想定 7 について

想定 7　ネットワーク上は攻撃者のトラヒックしか流れていない

この想定を覆したときに引き起こす問題は，節で提示した PPM 方式における問題 2 そのものである．

問題２に対する解決法は次節で提案するため，ここでの言及は避ける．

想定８について

想定８ 攻撃者はマークフィールドを偽造しない

Edge Sample 手法（その他の PPM 手法も含む），提案手法は共にマークフィールドが偽造されるとその情報によって誤った検出を行ってしまう．そのため，マークフィールドの偽造は提案手法だけではなく PPM 手法そのものの問題であると言える．しかし，仮にマーク情報を保護することができる手法が提案されれば，提案手法の適用も可能となる．

第 5 章

マークパケットの到着間隔分布に基づく攻撃者と正規ユーザの分別法

第 3 章では，PPM 方式の問題を論じ，その一つとして、マークパケットが攻撃パケットであるか方式内で判別することができないため，正規ユーザのパケットの誤フィルタリングを誘発する可能性があることを指摘した．５章では，この問題を解決するため，攻撃者と正規ユーザから発生する犠牲者向けのトラヒックのトラヒックパターンの違いに着目し，犠牲者側で得られるマークパケットの到着時間間隔の分布が攻撃者，正規ユーザで異なるという性質を利用することにより，特定された NCN を攻撃パケットが通過するか判別する手法「マークパケットの到着間隔分布に基づく攻撃者と正規ユーザの分別法」を提案する．

5.1　目標

本手法では，特定された NCN において，（送信元 IP アドレス，送信先 IP アドレス）＝（攻撃パケットで使われている送信元 IP アドレス，犠牲者の IP アドレス）であるパケットをフィルタリングすることを視野に入れ，PPM 手法とサブマリンノード検出手法で特定された NCN とそのアドレスがマークされたパケットの送信元アドレスを一組（NCN,SA(Source Address)）とし，その NCN を通過し SA を送信元アドレスとするマークパケットが攻撃パケットを含むか否かを判別することを目標とする．

複雑なケースとして，例えば，NCN1 を NCN とする組み合わせとして (NCN1,SA1(正規ユーザ)), (NCN1,SA2(攻撃者)) の 2 組が得られた場合，後者のみを攻撃パケットを含むものとして判別する（図 5.1）．

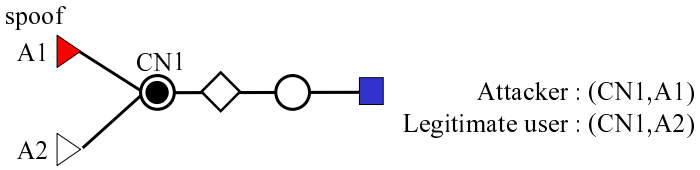

図 5.1: (NCN,SA) の判別例 1

また，組み合わせ (NCN1,SA1(正規ユーザ)) に対し，(NCN1,SA1(正規ユーザ))，(NCN 1 ,SA1(攻撃者：偽造)) の 2 種類が存在する場合には，この組み合わせは攻撃パケットを含むものとして判定する（図 5.2）.

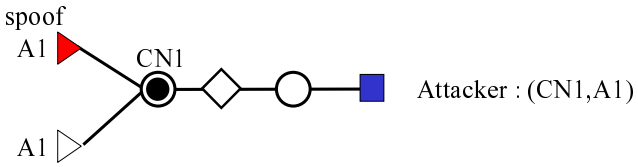

図 5.2: (NCN,SA) の判別例 2

そして，攻撃者が送信元アドレスを偽装したために同様に，(NCN1,SA1(正規ユーザ))，(NCN2,SA1(攻撃者)) の 2 組が得られた場合にも後者のみを攻撃パケットを含むものとして判別する（図 5.3）.

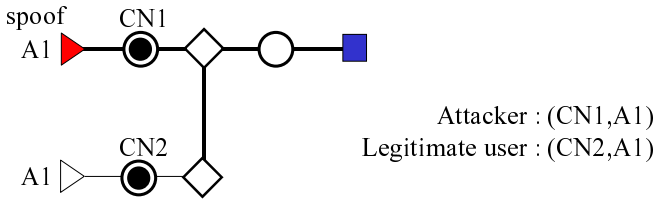

図 5.3: (NCN,SA) の判別例 1

つまり，提案手法の効果は，（NCN,SA）が正規ユーザのみである場合は攻撃パケットを含まない，攻撃者のみ，もしくは攻撃者と正規ユーザが混在する場合は攻撃パケットを含むと判別できることが鍵となる.

5.2　マークパケットの到着間隔分布に基づく攻撃者と正規ユーザの分別法

第 3 章の問題提起の箇所で述べたように，マークパケットが攻撃パケットであるか否かをパケット単位で判別することは現状では不可能である．そのため，各（NCN,SA）についてその情報を持つグループ単位で判別を試みることとなるが，攻撃者が偽造する送信元 IP アドレスを頻繁に変更した場合，その都度異なったグループを構成することになるため判別を行うことは容易ではない．そこで，提案手法は，攻撃者が偽造 IP アドレスの変更をほぼ行わない，もしくは一つのアドレスを使用し続ける場合を対象とする．ただし，ある NCN について構成されるグループ数が極端に多くなった場合，それ自体が攻撃を特徴付けるシグネチャとなるため，その NCN を攻撃パケットが通過すると判別することが可能である.

DDoS 攻撃では，一般的に攻撃者は継続してパケットを送出し続ける．また，実際の DDoS 攻撃を想定するとパケットサイズはほぼ同一となることが推測される．なぜなら，代表的な DDoS 攻撃である Syn Flood 攻撃等では，特定のパケットを用いるため（Syn Flood 攻撃では Syn パケット），攻撃パケットは同一のサイズであるし，またパケットサイズが大きい場合には一般的な MTU である 1500byte に経路上

のルータでならされるためである．よって，DDoS 攻撃では，ほぼ等間隔でパケットが伝送されることが予想され，この性質を持つパケットフローに対し確率 p でパケットにランダムにマークすると，マークパケットはポアソン到着となり，その到着間隔の分布は指数分布となる．

一方，正規ユーザとあるサーバ（今回の場合では犠牲者）との 2 点間通信においては，On 期間（1 セッションの接続時間）と Off 期間（休止時間）はそれぞれ非常に大きな分散を持っていることが顕著な特徴として知られている [19]．そのため，攻撃者のパケットフローによるマークパケットの到着間隔は指数分布とはならない．

そこで，各（NCN，SA）の組み合わせに対し，到着間隔が指数分布に従うか否かを検定することにより，攻撃者が存在するかを判別することとし，これを，マークパケットの到着間隔分布に基づく攻撃者と正規ユーザの分別法と呼ぶこととする．

本論文では，具体的な検定法として，理論分布（指数分布）への適合検定（検定法 1）と分散値に関する検定（検定法 2）を用いる．

理論分布への適合検定では，まず，以下のように仮説を立てる．

- 帰無仮説：母分布は指数分布でないとはいえない（攻撃者）
- 対立仮説：母分布は指数分布ではない（正規ユーザ）

そして，標本値の平均値から推定される理論分布（指数分布）と標本値との適合度を求め，その有意確率を基に上記の二つの仮説の内一つを採択する．

次に，分散値に関する検定について説明する．正規ユーザのトラヒックは上記の通り，Off 期間が非常に多きな分散を持っているため，そのパケットフローから得られるマークパケットの到着間隔分布も指数分布に比べ分散値が大きくなる．そこで，標本値の平均値を基に指数分布である場合の分散値を推定し，その分散値について以下の片側検定を行うことで仮説の内の一つを採択する．

- 帰無仮説：母分散が指数分布に従う値である（攻撃者）
- 対立仮説：母分散が指数分布に従う値より大きい（正規ユーザ）

5.3 有効性の検証

本節では，マークパケットの到着間隔分布に基づく攻撃者と正規ユーザの分別法の有効性を評価実験を通して検証する．

5.3.1 評価実験について

今回の評価実験では，4.2.2,4.2.3 節のように大規模ネットワークを用いるのではなく，送信者－犠牲者間に 1 CN が存在するトポロジーを用い，1 CN についての正悪の判別を行う．これは，1 CN の結果から大規模ネットワークへ適用した場合の結果を推測できると考えられるからである．その理由を以下に記す．

攻撃者が正規ユーザ-犠牲者間の通信を盗聴できないと仮定すると，異なるネットワークに存在する正規ユーザ，攻撃者の IP アドレスが一致することは偶然一致する場合しかなく，その可能性は IPv4 にお

いて $\frac{1}{2^{32}}$ であるため，このケースは極めて少ない．そして，盗聴対策は本研究の対象外であるため，本研究では異なるネットワークに存在する攻撃者，正規ユーザの IP アドレスが一致することは事実上ないとする．つまり，IP アドレスが合致する可能性は同一ネットワークに存在する攻撃者，正規ユーザについてのみ考慮すればいいということである．したがって，ある一つの NCN の（NCN，SA）の組み合わせに対し正悪の判別が可能となれば，全体のネットワークに適用した場合も同様の結果を得ることができると推測される．そこで，今回の評価実験では単純なトポロジーデータを用いることとした．

本評価実験では，攻撃者のみのケース，正規ユーザのみのケース，混在するケースについて判別を試みる．そして，正規ユーザのみのケースでは攻撃パケットを含まない，攻撃者のみ・混在するケースについては攻撃パケットを含むと判別可能であるかを見ることで，提案手法の有効性を論じる．

正規ユーザのトラヒックモデルについては文献 [19]（LAN トラヒックの観測データから 2 点間のトラヒックモデルを確立）を基に，On 期間，Off 期間共に Pareto 分布に従う On-Off トラヒックを用いた．ただし，Pareto 分布とは分布関数が次のように与えられる分布のことを言う．

$$F(t) = 1 - (\frac{k}{t})^{\alpha} \qquad t \in [k, \infty) \tag{5.1}$$

また，パレート分布における平均値は $\frac{\alpha k}{\alpha - 1}$ であるため，α が小さいほど大きくなる．

On,Off それぞれの間隔 t_{on},t_{off} は以下の Pareto 分布に従い求められる．

$$F(t_{on}) = 1 - (\frac{k_{on}}{t_{on}})^{\alpha_{on}} \tag{5.2}$$

$$F(t_{off}) = 1 - (\frac{k_{off}}{t_{off}})^{\alpha_{off}} \tag{5.3}$$

文献 [19] では，t_{on},t_{off} を定める α_{on},α_{off},k_{on},k_{off} について，観測結果から以下のように求めている．

$$1.6 \leq \alpha_{on} \leq 1.8 \tag{5.4}$$

$$1.1 \leq \alpha_{off} \leq 1.3 \tag{5.5}$$

$$k_{on} = 2.0 \tag{5.6}$$

$$k_{off} = 2.0 \tag{5.7}$$

また，今回の評価実験における重要な要素として，標本数があげられる．一般的に検定法は，標本数が多くなればなるほどその検定精度は向上するが，多くの標本数を必要とすることはそれだけ多くの時間を要することになる．

以上のことを踏まえ，本評価実験は以下の順序で進めていく．その際，α_{on},α_{off},k_{on},k_{off} と標本数の基準値として，(α_{on},α_{off},k_{on},k_{off})=(1.7,1.2,2.0,2.0)，標本値を 1000 とした．また，各送信者は等間隔に 100[pps] のレートでパケットを送出するものとし，それぞれの試行回数を 2000 とし，検定法における有意水準を 1%とした．

1. 攻撃者のみのケース
2. 正規ユーザのみのケース
3. 混在するケース
4. α_{on},α_{off} について
5. 標本数について

表 5.1: 正規ユーザのみのケースにおいて攻撃パケットを含まないと判別した確率

正規ユーザ数	検定法 1	検定法 2
1	0.989	1.000

5.3.2 有効性の検証

攻撃者のみのケース

図 5.4 は，(攻撃者数, 正規ユーザ数)=(1,0),(2,0),(3,0),(4,0) である場合に，攻撃パケットを含むと判別した確率を表している．図 5.4 を見ると，特に検定法 1 を用いた場合，精度良く攻撃者の判別が可能であ

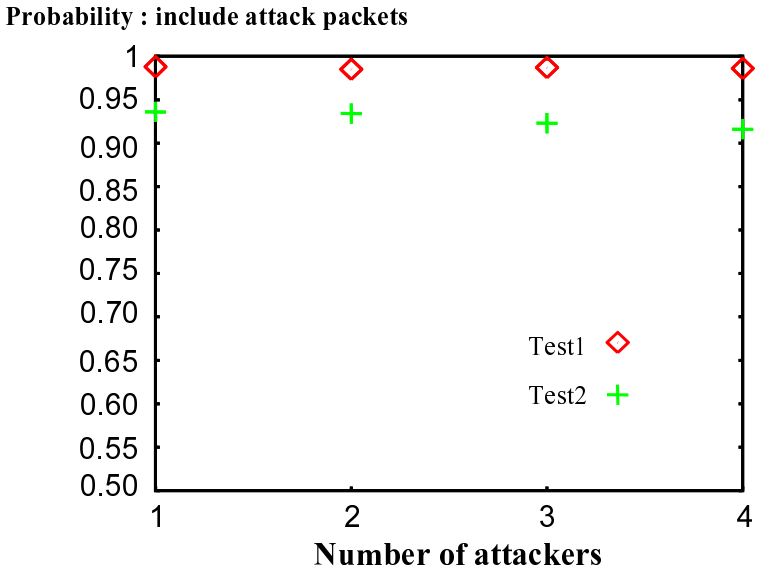

図 5.4: 攻撃者のみのケースにおいて攻撃パケットを含むと判別した確率

ることが分かる．また，検定法 1，2 に共通して，攻撃者数の変化した場合でもほぼ同様の判別精度が得られているが，これは，複数のポアソン到着を重ね合わせてもポアソン到着になるという性質のためである．

正規ユーザのみのケース

同時刻に同一の IP アドレスを持った正規ユーザは一人であるため，正規ユーザのみのケースは正規ユーザが一人である場合についてのみ判別を行う．表 5.1 は，(攻撃者数, 数正規ユーザ数)=(0,1) である場合に，攻撃パケットを含まないと判別した確率を表している．表 5.1 を見ると，両検定法に共通して高精度に判別が可能であることが分かる．特に，検定法 2 では 100%の判別が可能となっている．

混在するケースについて

本項では，攻撃者と正規ユーザが混在するケースについて評価実験を行う．正規ユーザの項で述べたとおり，正規ユーザ数は最大で 1 人であるため，混在するケースとして，(攻撃者数, 正規ユーザ数)=(1,1),(2,1),(3,1),(4,1) を想定する．図 5.5 は，それぞれの場合に，攻撃パケットを含むと判別した確率を表している．

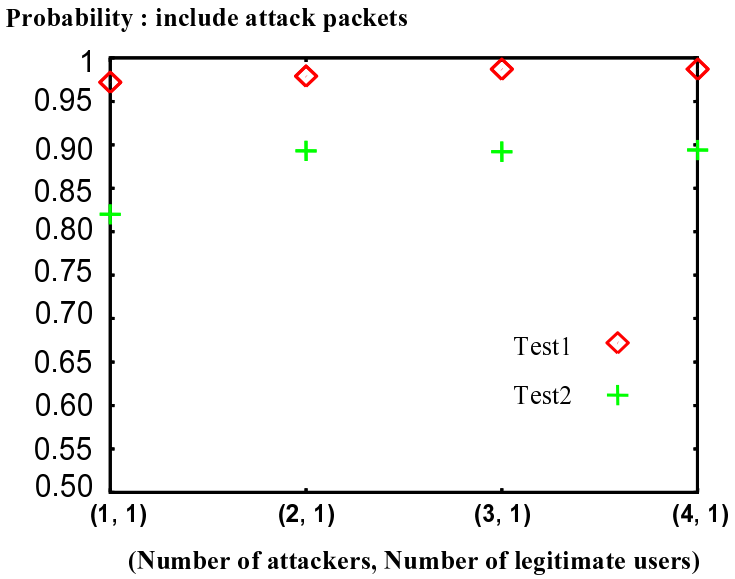

図 5.5: 混在するケースにおいて攻撃パケットを含むと判別した確率

図 5.5 を見ると，検定法 1 を用いた場合，精度良く攻撃者の判別が可能であることが分かる．一方，検定法 2 では攻撃者数の増加に伴い，判別精度が向上している．これは，攻撃者数が増えることで，正規ユーザのトラヒックの影響を緩和することができるためだと考えられる．

α_{on},α_{off} について

本項では，正規ユーザのトラヒックパターンを決める変数である α_{on},α_{off} についての検討を行う．文献 [19] において，α_{on},α_{off} はそれぞれ $1.6 \leq \alpha_{on} \leq 1.8$,$1.1 \leq \alpha_{off} \leq 1.3$ としているため，α_{on}=1.6,1.7,1.8,α_{off}=1.1,1.2,1.3 を候補とする．そして，そこから作られる 9 つの組み合わせに対し，攻撃者のみのケース，正規ユーザのみのケース，混在するケースにおける判別実験を行う．

まず，各 α_{on},α_{off} の組み合わせに対し，攻撃者のみのケースとして (攻撃者数, 正規ユーザ数)=(1,0) とした場合における判別結果（攻撃パケットを含むと判別した確率）を図 5.6,5.7,5.8 に示す． 図 5.6,5.7,5.8 を見ると，全てのケースにおいて両手法共通してほぼ同様の判別精度が得られていることが分かる．つまり，$1.6 \leq \alpha_{on} \leq 1.8$,$1.1 \leq \alpha_{off} \leq 1.3$ の範囲内では，攻撃者のみのケースの判別精度は α_{on},α_{off} の変動に左右されにくいということである．

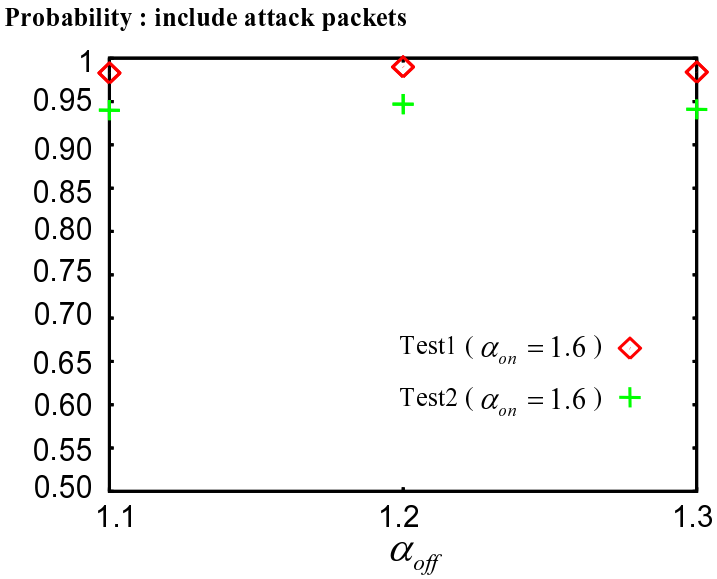

図 5.6: (α_{on},α_{off})=(1.6,1.1),(1.6,1.2),(1.6,1.3)，(攻撃者数, 正規ユーザ数)=(1,0) に対し，攻撃パケットを含むと判別した確率

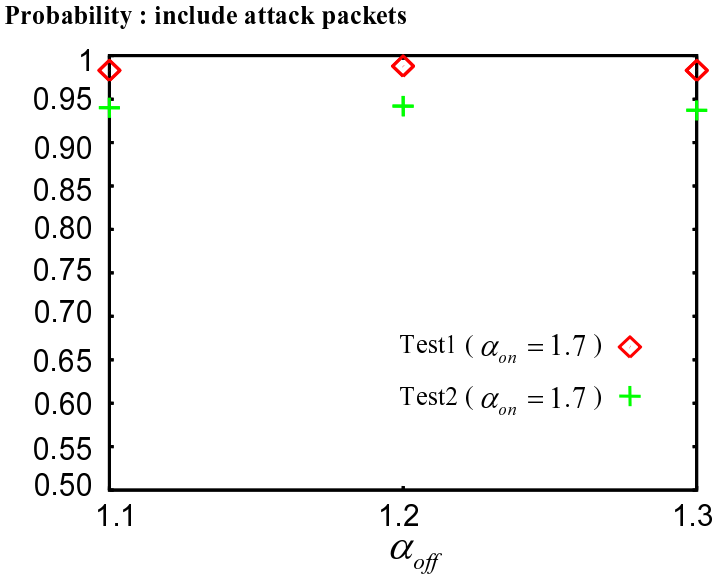

図 5.7: (α_{on},α_{off})=(1.7,1.1),(1.7,1.2),(1.7,1.3)，(攻撃者数, 正規ユーザ数)=(1,0) に対し，攻撃パケットを含むと判別した確率

次に，各 α_{on},α_{off} の組み合わせに対し，正規ユーザのみのケースとして (攻撃者数, 正規ユーザ数)=(0,1) とした場合における判別結果（攻撃パケットを含まないと判別した確率）を図 5.9,5.10,5.11 に示す． 図 5.9,5.10,5.11 を見ると，検定法 2 では全てのケースで高精度に判別できていることが分かる．一方，検定法 1 は $\alpha_{off} = 1.3$ の場合，極端に精度が落ち込んでいる．

pareto 分布では α の値が増加すると平均値が低下する．よって，$\alpha_{off} = 1.3$ のケースでは他のケース

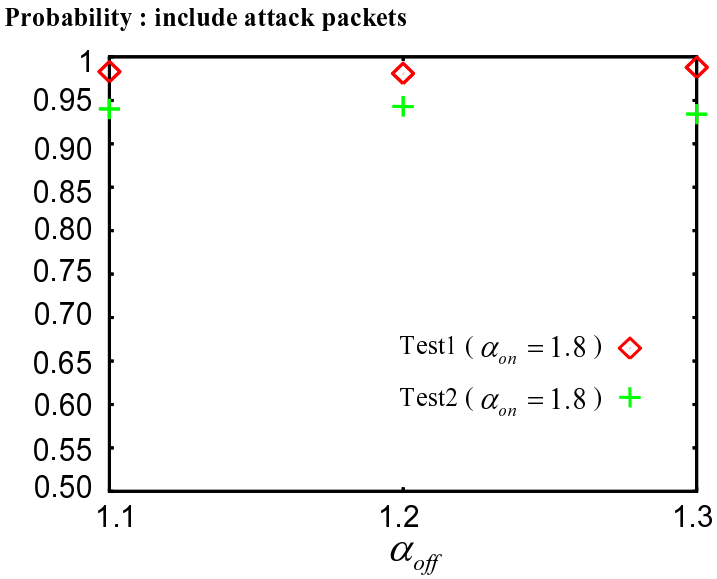

図 5.8: (α_{on},α_{off})=(1.8,1.1),(1.8,1.2),(1.8,1.3)，(攻撃者数, 正規ユーザ数)=(1,0) に対し，攻撃パケットを含むと判別した確率

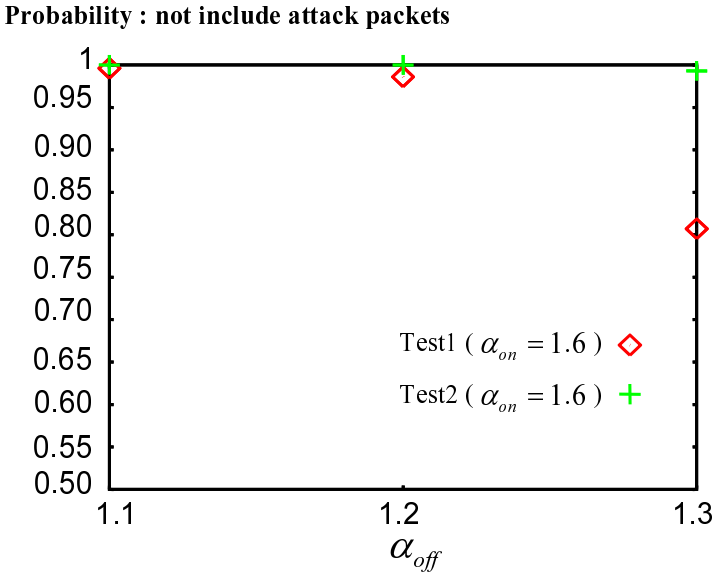

図 5.9: (α_{on},α_{off})=(1.6,1.1),(1.6,1.2),(1.6,1.3)，(攻撃者数, 正規ユーザ数)=(0,1) に対し，攻撃パケットを含まないと判別した確率

に比べ，Off 期間が短くなり，その影響で判別が難しくなり検定法 1 における判別精度が低下したと考えられる．

最後に，各 α_{on},α_{off} の組み合わせに対し，攻撃者のみのケースとして (攻撃者数, 正規ユーザ数)=(1,1) とした場合における判別結果（攻撃パケットを含むと判別した確率）を図 5.12,5.13,5.14 に示す．

図 5.12,5.13,5.14 を見ると，全てのケースにおいて両手法共通してほぼ同様の判別精度が得られている

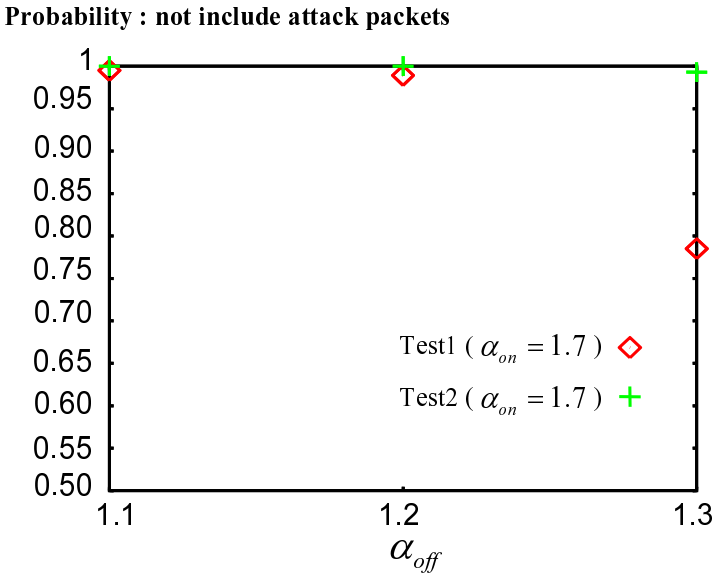

図 5.10: (α_{on},α_{off})=(1.7,1.1),(1.7,1.2),(1.7,1.3)，(攻撃者数, 正規ユーザ数)=(0,1) に対し，攻撃パケットを含まないと判別した確率

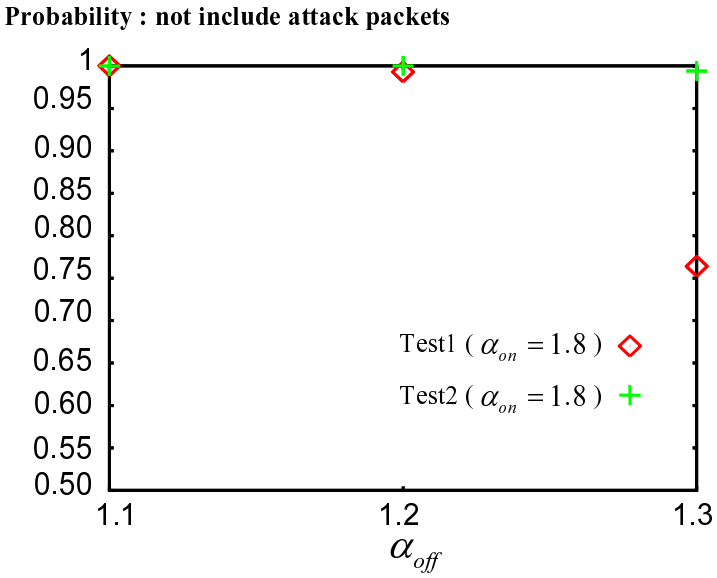

図 5.11: (α_{on},α_{off})=(1.8,1.1),(1.8,1.2),(1.8,1.3)，(攻撃者数, 正規ユーザ数)=(0,1) に対し，攻撃パケットを含まないと判別した確率

ことが分かる（図 5.6,5.7,5.8 と同様である）．つまり，$1.6 \leq \alpha_{on} \leq 1.8$,$1.1 \leq \alpha_{off} \leq 1.3$ の範囲内では，混在するケースの判別精度は α_{on},α_{off} の変動に左右されにくいということである．

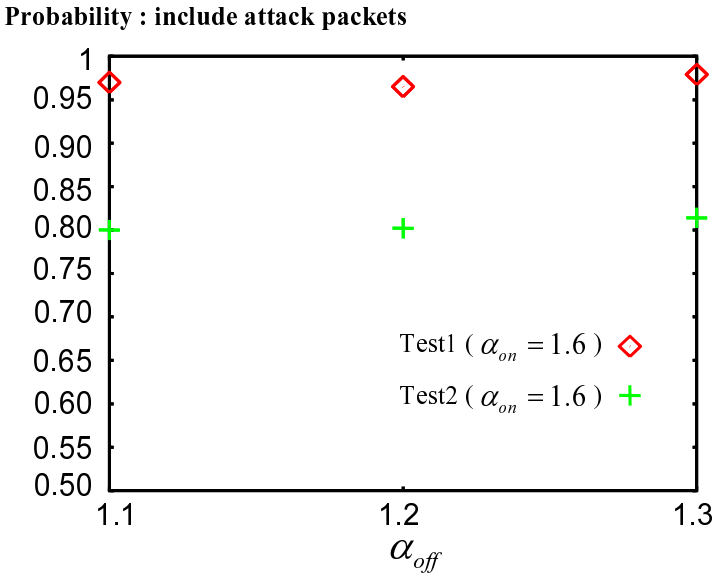

図 5.12: $(\alpha_{on},\alpha_{off})$=(1.6,1.1),(1.6,1.2),(1.6,1.3)，(攻撃者数, 正規ユーザ数)=(1,1) に対し，攻撃パケットを含むと判別した確率

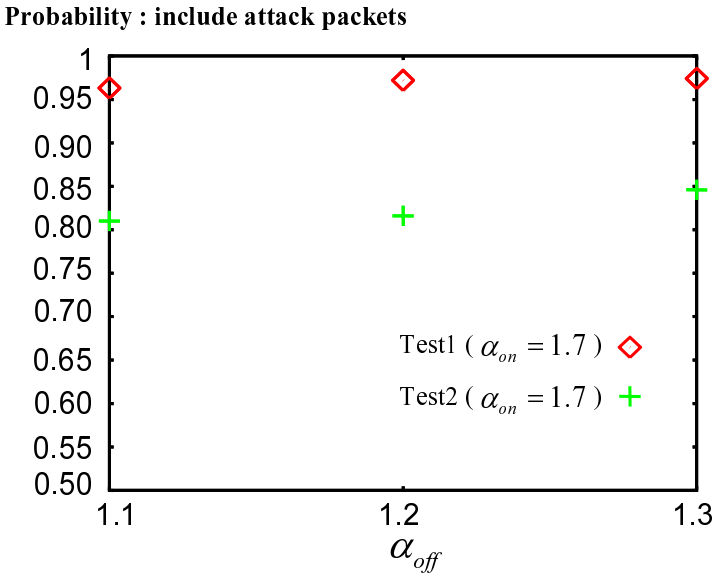

図 5.13: $(\alpha_{on},\alpha_{off})$=(1.7,1.1),(1.7,1.2),(1.7,1.3)，(攻撃者数, 正規ユーザ数)=(1,1) に対し，攻撃パケットを含むと判別した確率

標本数について

これまでの項では，標本数（マークパケット数-1）を 1000，つまり 1001 のマークパケット数を収集した時点での判別結果を提示してきた．しかしながら，マーキング確率 $p = \frac{1}{20000}$，(攻撃者数, 正規ユーザ

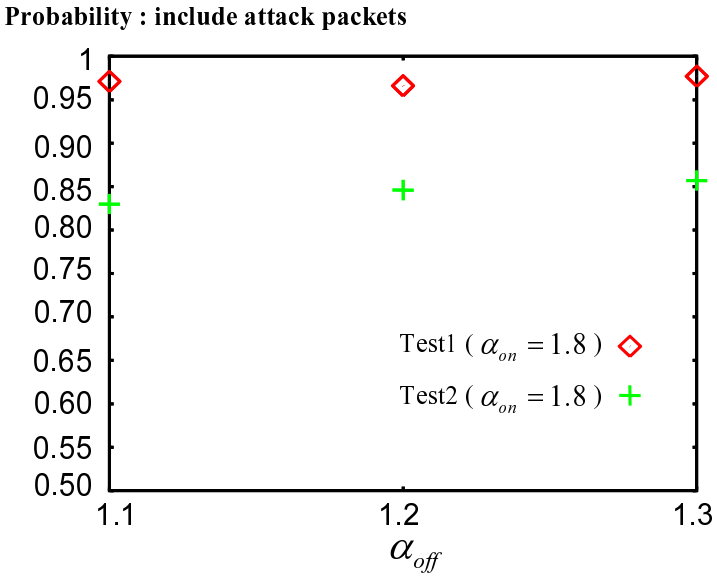

図 5.14: $(\alpha_{on},\alpha_{off})$=(1.8,1.1),(1.8,1.2),(1.8,1.3)，(攻撃者数, 正規ユーザ数)=(1,1) に対し，攻撃パケットを含むと判別した確率

数)=(1,0), パケットレート N_p =100[pps] とした場合，マークパケット数を回収するために約 200000[sec] もの時間を要することとなる．判別はできる限り短時間に行われることが望ましいため，標本数が少ない場合に良好な判別精度を維持することができるかということが重要となる．そこで，本項では標本数についての検討を行う．具体的には標本数=100,200,300,400,500,600,700,800,900,1000 に対し，攻撃者のみのケース，正規ユーザのみのケース，混在するケースにおける判別実験を行う．

まず，各標本数に対し，攻撃者のみのケースとして (攻撃者数, 正規ユーザ数)=(1,1) とした場合における判別結果（攻撃パケットを含むと判別した確率）を図 5.15 に示す．図 5.15 では，全ての標本数に対し

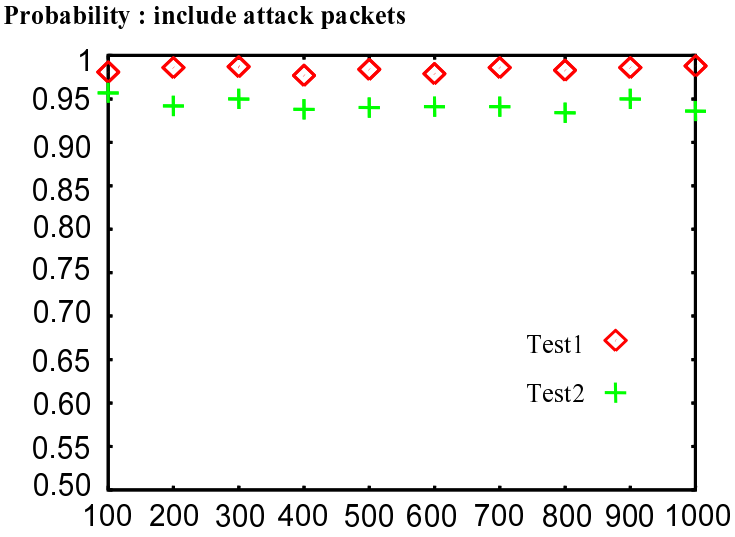

図 5.15: 標本数を変動させ，(攻撃者数, 正規ユーザ数)=(1,1) とした場合に攻撃パケットを含むと判別した確率

両検定法でほぼ同一の判別精度となっている．よって，攻撃者のみのケースの判別では標本数が少ない場合でも，高精度に判別可能であると言える．

次に，各標本数に対し，正規ユーザのみのケースとして (攻撃者数, 正規ユーザ数)=(0,1) とした場合における判別結果（攻撃パケットを含まないと判別した確率）を図 5.16 に示す．図 5.16 では，標本数が少

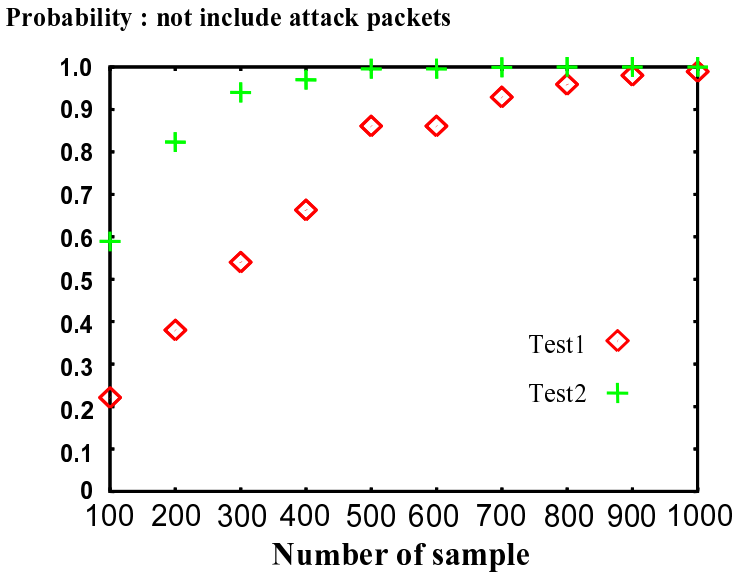

図 5.16: 標本数を変動させ，(攻撃者数, 正規ユーザ数)=(0,1) とした場合に攻撃パケットを含むと判別した確率

ない場合両検定法共に判別精度が低下している．特に，検定法 1 では標本数の増加と共に極端に落ち込んでいる．正規ユーザのみのケースで，攻撃パケットを含まないと判別しない（＝攻撃パケットを含むと判別する）ことは正規ユーザのパケットの誤フィルタリングにつながる恐れがあり，望ましくない．そのため，標本数が少なく，正規ユーザのみのケースについては更なる改善が必要だと言える．

最後に，各標本数に対し，攻撃者のみのケースとして (攻撃者数, 正規ユーザ数)=(1,1) とした場合における判別結果（攻撃パケットを含むと判別した確率）を図 5.17 に示す．図 5.17 では，検定法 1 を用いた場合全ての標本数に対しでほぼ同一の判別精度となっている．よって，検定法 1 によって判別を行えば，標本数が少ない場合でも，高精度に判別可能であると言える．一方，検定法 2 では標本数が少ない場合の方が判別精度が高いという逆転現象が起こっている．この現象は，正規ユーザの Off 期間の性質に起因する．正規ユーザの Off 期間は分散の大きい Pareto 分布に従うが，平均値より非常に長い Off 期間をとることはまれである（ただし，指数分布よりは可能性が高い）．そのため，標本数を多くした方が非常に長い Off 期間を含む可能性が高い．結果，標本数が多い場合は，その Off 期間の影響で分散値が大きくなることがあり，攻撃パケットを含まないと判別する可能性が高くなる．

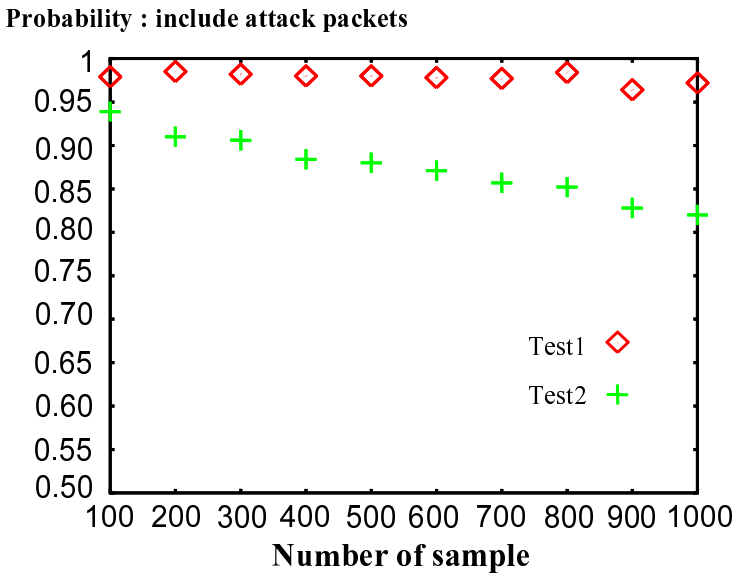

図 5.17: 標本数を変動させ，(攻撃者数, 正規ユーザ数)=(1,1) とした場合に攻撃パケットを含むと判別した確率

第 6 章

結論

本論文では，DDoS 攻撃対策として有望な，確率的パケットマーキング（PPM）方式が抱える 2 つの問題に対する解決法としてマークパケットの統計的性質を利用する「マークパケット数に基づくサブマリーンノード検出手法」及び「マークパケットの到着間隔分布に基づく攻撃者と正規ユーザの分別法」を提案した．

現在社会的脅威になっている DDoS 攻撃は，多量なトラヒックによりネットワーク全体に被害をもたらすため，攻撃者に最寄のルータでトラヒックを遮断することが最も有望な対策法となる．しかしながら，攻撃者は送信 IP アドレスを任意に決めることができるため，そのルータを特定することは困難である．そのため，送信元が偽造されたパケットフローから，攻撃者に最寄の真のルータを特定する技術である IP 経路逆探索が近年重要となってきている．そして，PPM 方式は現在最も有望な IP 経路逆探索方式である．

確率的パケットマーキング方式とは，マーキング機能を持ったルータ（CN）が通過するパケットに対し確率的にアドレス等の経路情報をマークし，それらのマークパケットを収集した犠牲者がマーク情報を基に経路を逆探索し，その経路上で犠牲者から最も遠いルータを攻撃者に最寄のルータ（NCN）として特定する方式である．この方式では，検出性能はルータがマークした情報に依存するため，従来研究ではどういった情報をマークするかという点に焦点が当てられ，様々な手法が提案されてきた．しかしながら，既存の PPM 方式では原理上解決することができない二つの大きな問題があることが判明した．

まず一つ目の問題は，攻撃経路が重複している場合，原理的に検出することができない NCN(サブマリンノード) が存在するということである．これは，確率的パケットマーキング方式のおける NCN 特定では，マーク情報を基に，犠牲者をルート，パケットが通過した CN をノードとした木を構築し，そのリーフノードとなる CN を NCN として特定するために起きる．つまり，リーフノードではない CN を NCN とする攻撃者がいた場合，その攻撃者の NCN と犠牲者間の経路が，リーフノードである別の NCN と犠牲者間の経路に包含されてしまうため，検出不可能となってしまうのである．

この問題に対し，本研究では攻撃経路が合流するノードではパケット数の増加に伴いマークパケット数も増加することに着目した．これは，マークパケット数の増加を捉えることができればサブマリンノードの検出が可能であることを意味する．本論文では，このアイディアを検定法を用いることで一般化した「マークパケット数に基づくサブマリーンノード検出手法」を提案した．

提案手法では，既存の PPM 手法でリーフノードとされた CN を対象に， 1 step 前に存在する CN か

らのマークパケット数と当該 CN からのマークパケット数を検定法を用いて比較し，サブマリンノードを検出する．そのため，PPM 手法と組み合わせることで効果を発揮するが，検出の対象としている CN が PPM 手法と異なるため，検出精度の向上が確実に見込める．また，時間が経過すればマークパケットの差は確実に生じるため，最終的には全ての NCN を検出することが可能であると推測される．

提案手法の有効性を検証するため，既存の PPM 手法として Edge Sample 手法を用い，様々なネットワーク構造，条件を設定した状況でシミュレーション実験を行った．その結果，推測したとおり，提案手法を用いると全てのケースで Edge Sample 手法単独より，検出精度，トラヒック減少率共に優れていること，また，時間が経過すれば検出精度が 1 に近似することが確認された．

次に二つ目の問題は，マークパケットは攻撃パケットであるとは限らないのに対し，犠牲者はマークパケットの情報から送信元が攻撃者であるか正規ユーザであるか判断できないということである．つまり，特定された NCN を攻撃パケットが通過するとは限らない．そのため，特定結果を基にパケットフィルタリングを適用すると，正規ユーザからのパケットの誤フィルタリングにつながる恐れがある．

この問題に対し，攻撃者と正規ユーザかから発生するトラヒックのトラヒックパターンは異なることに着目した．攻撃者は DDoS 攻撃の最中パケットを送出し続けるが，正規ユーザのトラヒックは On 期間（1 セッションの接続時間）と Off 期間（休止時間）共にそれぞれ非常に大きな分散を持っている．そのため，攻撃パケットフローにマーキング処理を施すとその到着間隔分布は指数分布に従うのに対し，正規ユーザのパケットフローからのマークパケットの到着間隔分布は指数分布とならない．そこで本論文では，この違いを指数分布に関する検定法を用いて捉え，攻撃パケットを含むか否かを判別する手法「マークパケットの到着間隔分布に基づく攻撃者と正規ユーザの分別法」を提案した．提案手法では，検定法の候補として適合検定と分散に関する検定をあげている．

提案手法の有効性を検証するため，送信者－ CN －犠牲者という単純なトポロジーを用いた評価実験を行った．この評価実験では，攻撃者数や標本数など様々な変数に対し，各検定法の判別精度を求めた．その結果，標本数が十分多い場合，両検定法共良好に判別を行うことができることが判明した．

今後の課題は大きく分けて二つ考えられる．まず，一つ目の課題は「マークパケットの到着間隔分布に基づく攻撃者と正規ユーザの分別法」の改良である．この手法では，標本数が多い場合には良好に判別可能であるが，標本数が少なくなると，正規ユーザしかいないケースに対し攻撃パケットが含まれると判別する可能性が高くなることが評価実験により実証された．そのため，現在の手法では判別するのに多くの時間を必要とすることになる．DDoS 攻撃は短時間で被害をもたらすこともあるため，これは望ましくない．また，攻撃者はソースアドレスを定期的に変えることで標本数の回収を妨害する可能性もある．したがって，実ネットワークへの導入標本数が少ない場合でも高精度な判別を行うことができる手法についての検討が重要となる．

二つ目の課題は，マーク情報そのものの偽造への対策である．4 章で述べたとおり，PPM 手法，提案手法共にマーク情報の偽造に対して非常に弱い．しかしながら，攻撃者がこれらの手法の存在を認知しているとしたら，マーク情報の偽造を行う可能性が非常に高い．その対策として，ルータ間で連携して偽造されたマークパケットのネットワークへの流入を防ぐ仕組みを導入することや，署名方式や公開鍵暗号方式の利用などが考えられるが，十分に検討する必要がある．

謝辞

本研究を進めるにあたり、定期的に議論の場を設け、終始熱心に御指導を頂きました、東京大学大学院新領域創成科学研究科若原恭教授に心から感謝致します。また同議論の場において、数々の貴重な御指摘を頂き、さらに、実験環境の構築等、非常に多岐にわたって御指導頂きました、同研究科中村文隆助手に深く感謝致します。折に触れ、研究に関する御助言を頂きました、同研究科中山雅哉助教授に深く感謝致します。

また、貴重な御意見を頂いた若原・中山研究室の皆様に心から御礼申し上げます。

参考文献

[1] コンピュータウィルス・不正アクセス届出状況について
http://www.ipa.go.jp/security/txt/2005/01outline.html.

[2] 白井　雄一郎，白濱　直哉，又江原　恭彦，柳岡　祐美,”インターネットセキュリティー不正アクセスの手法と防御” SOFT BANK, 2001

[3] Paul J. Criscuolo, ”Distributed Denial of Service” CIAC-2319, Feb. 2000.

[4] P.Fergusson and D.Seine, ”Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,” RFC2827, May. 2000

[5] Kihong Park, Heejo Lee, ”On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets” In Proceedings of SIGCOMM’2001, Aug. 2001

[6] J. Glave. (1998) Smurfing cripples ISPs. Wired Technology News.http://www.wired.com/news/technology/ 0,1282,9506,00.html

[7] Hal Burch and Bill Cheswick, ”Tracing Anonymous Packets to Their Approximate Source”, In Proceedings of the 2000 USENIX LISA Conference, pages 319-327, New Orleans, LA, December. 2000

[8] Alex C. Snoeren, Crig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Beverly Schwartz, Stephen T. Kent, and W. Timothy Strayer, ”Single-Packet IP Traceback”, IEEE/ACM Trans. Networking, vol.10, no.6, Dec, 2002

[9] Steven M. Bellovin. ICMP traceback massage, March 2000. Internet Draft: draft-bellovin-itrace-00.txt (expires September 2000)

[10] Stefan Savage , David Wetherall, Anna Karlin, and Tom Anderson, ”Network Support for IP traceback” IEEE/ACM transaction on networking, vol.9, no.3,pp.226-239, JUN. 2001.

[11] Dawn X. Song and Adrian Perrig,” Adcvanced and authenticated marking schemes for IP traceback” In Proc. IEEE INFOCOM, Jan 2001

[12] Toshiaki OGAWA, Fumitaka NAKAMURA and Yasushi WAKAHARA: ”Branch Label based Probabilistic Packet Marking for IP Traceback” Trans. IEICE Vol.E87-B, No.7, July 2004

[13] M. Adler, ” Tradeoffs in Probabilistic Packet Marking for IP Traceback”, University of Massachusetts, Amherst, MA, 2001

[14] Fu-Hau Hsu, Tzi-cker Chiueh, ”A Path Information Caching and Aggregation Approach to Traffic Source Identification,” 23rd IEEE International Conference on Distributed Computing

Systems (ICDCS), May 2003,

[15] Michael T. Goodrich, "Efficient Pcket Marking for Large-Scale IP Traceback" In Proceedings of the 9th ACM conference on Computer and communications security, Nov. 2002.

[16] Wolfgang Theilmann and Kurt Rothermel, "Dynamic Distance Maps of the Internet", In proceedings of the 2000 IEEE INFOCOM Conference, Tel Aviv, Israel, March 2000

[17] http://www.cs.bu.edu/brite/

[18] A.Medina, I.Matta, and J.Byers, "On the Origin of Power-laws in Internet Topologies" ACM Computer Communication Review, pp.160-163, Apr. 2000

[19] Willinger W., Taqu M., Sherman R., Wilson D., "Self-Similarity through High-Variability: Statistical Analysis of Ethernet LAN Traffic Modeling", IEEE/ACM Transactions on Networking,5(1), pp. 1-16, 1997