待ち行列推定に基づくパケットロス攻撃検知方式のパラメータ依存性について

細井 琢朗 †　　松浦 幹太 †

† 東京大学生産技術研究所
153-8505 東京都目黒区駒場 4-6-1
{hosoi, kanta}@iis.u-tokyo.jp

あらまし ネットワーク内のルータを乗っ取って通信を操作する攻撃は、ネットワーク制御面での攻撃と、ネットワークデータ面での攻撃の二つに大別される。後者では、攻撃者は各種のパケットの送信が可能であるのみならず、転送すべき任意のパケットを廃棄することができる。このパケットロス攻撃は選択的に行うことで、廃棄パケット量の少なさに対して大きな被害を与える能力を持つ。輻輳による通常のパケット廃棄がある中でパケットロス攻撃を検知する技術が Misrak らによって提案されたが、その性能評価はまだ網羅されていない。本稿では彼らの方式における不正規パケット廃棄の検知性能について、幾つかのパラメータに対する依存性を検討する。

About Parameter Dependency of Malicious Packet Loss Detection Based on Queue Prediction

HOSOI Takurou†　　Kanta Matsuura†

†Institute of Industrial Science, The University of Tokyo
4-6-1, Komaba, Meguro-ku, Tokyo 153-8505, Japan
{hosoi, kanta}@iis.u-tokyo.jp

Abstract There are two main types of attacks which manipulate network communication by using a compromised router: subverting the network control plane, and subverting the network data plane. The attacker of the latter type can not only send any types of packets, but also drop arbitrary packets. This malicious packet loss can selectively drop packets which may lead to a severe threat compared to the amount of packet losses. Mizrak *et al.* proposed a detection method of this attack in a network with congestive legitimate packet losses, but its comprehensive evaluation has not been done yet. This paper examines the detection performance of their methods against some of its parameters.

1　はじめに

インターネットの通信は、ネットワークの結節点であるルータが正しい経路に導くことで成り立っている。ネットワークに接続された他の機器と同様、このルータもネットワークを通じた攻撃を受け、乗っ取られることがある。攻撃者に乗っ取られたルータは、そこを通過するパケットを操作することで、ネットワーク内の通信へ攻撃を仕掛けることができる。この攻撃方法には大別して、ネットワーク制御面での攻撃と、ネットワークデータ面での攻撃の二つがあ

る。前者はルータのルーティングテーブルの操作など、破壊的な影響が懸念される攻撃を含むため、それらに対する研究がこれまで多くなされてきている。一方後者は、サービス妨害攻撃や中間者攻撃、リプレイ攻撃などを含む。中でも通過する任意のパケットを廃棄するパケットロス攻撃は、選択的に行うことで廃棄パケット量の少なさに対して大きな被害を与える能力を持つ。例えば、TCP のコネクション確立のためにまず出される TCP SYN パケットをあるサーバへの分だけ廃棄することで、このサーバを利用しようとしているユーザにタイムアウトまでの比較的長い時間待たせることを強いる攻撃ができる [2] 。

このパケットロス攻撃の検知するには、あるばずのパケットが無いことを検知する必要があり、他の攻撃検知技術に比べて困難な問題になっている。また、パケットの廃棄自体は、インターネットプロトコルでも通信の混雑に対応するために正規に行われる。パケットロス攻撃はこれと区別して検知されなければならない。

初期の検知方法は、送信側から送られるパケットの送信数と実際に受け取ったパケット数の違いからパケットの廃棄を検知し、その廃棄パケット数がある閾値を超えた場合に攻撃と判断するものであった。この方式は適切な閾値の設定が難しいだけでなく、攻撃者はこの閾値未満であれば攻撃として検知されずにパケットを廃棄することができてしまう問題がある。

別の対策設計方針として、混雑によるパケット廃棄のモデルを立て、それを基に正規のパケット廃棄と攻撃を区別する方法もある。しかし、この方法では攻撃検知に十分な精度で混雑によるパケット廃棄をモデル化するのは難しいという問題があった。

その後 Mizrak らによって、ルータ内のパケット転送の待ち行列（キュー）を推定することで、高い検知性能を持つ、現実的なパケットロス攻撃検知方式が提案された [1] 。この方式は、あるルータにおいてパケットロス攻撃が行われたかどうかを、通信混雑による正規のパケット廃棄と区別して検知する。パケットの廃棄が通信混雑による正規のものかどうかの区別は、隣接するルータでの通信の観測情報からパケット転送の待ち行列の塞がり具合を推測した結果を用いて、確率論的に行う。

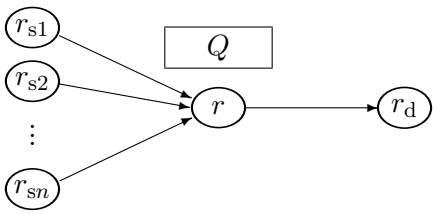

図 1: ネットワーク構成図。

この待ち行列推定に基づくパケットロス攻撃検知方式は、実際の通信に対してリアルタイムに実行可能であることが実装実験で確かめられており、少ない通信負荷増加で高い検知精度を示した。しかし実装実験のため、この方式が含む調整可能なパラメータや通信環境を表すパラメータに対する検知性能の依存性はほとんど確かめられていない。そこで本論文では、この待ち行列推定に基づくパケットロス攻撃検知方式の検知性能について、幾つかのパラメータに対する依存性を検討する。

2 攻撃検知方式

本節では、Mizrak らによって提案された待ち行列推定に基づくパケットロス攻撃検知方式について、その攻撃検知方法を大まかに説明する。

2.1 ネットワークモデル

パケットロス攻撃を行っているかどうかを調べる対象のルータを r とする。r は、隣接するルータ r_{s1} 、r_{s2} 、$\ldots$、r_{sn} から、隣接するルータ r_d へパケットを転送する。転送されるパケットは、ルータ r 内の待ち行列 Q に一旦入れられ、その先への転送が可能になると、順に取り出され、ルータ r_d へ送信される。Q が順番を待っているパケットで埋まっていると、新たに到着したパケットは入ることができず、廃棄される（混雑によるパケット廃棄）。

r_{sx} から r 、r から r_d へのパケット転送に

は、パケット長と回線の帯域幅に応じた転送時間が掛かる。

$$(\text{パケット転送完了予定時間})t_{\mathrm{c}} = t + (\text{link delay}) + \frac{(\text{パケット長})}{(\text{帯域幅})} \quad (1)$$

攻撃検知は一定時間毎に、隣接するルータでの通信の観測情報を照らし合わせて行う。そのため、各ルータの時計は全て同期していると仮定する。また、回線の帯域幅や対象とするルータの待ち行列の容量なども全てのルータが知っていると仮定する。

2.2 通信の観測情報

送信側のルータ r_{s1} 、r_{s2} 、...、r_{sn} からは、受信側のルータ r_{d} へ、送信したパケットの情報が以下の組で送られる。

$$\{\,(\text{パケットのフィンガープリント}),\ (\text{パケット長}),\ (\text{発信時刻})\,\} \quad (2)$$

この通信情報は、一定時間毎にまとめられ、各送信側ルータから揃って r_{d} へ送られる。

これに対応して、受信側のルータ r_{d} でも同様に通信を観測し、送信側と同じ時刻に同じ時間毎でまとめておく。この場合は、(2) 式の最後には（受信時間）を入れる。

元の検知手法では、これらの通信情報は署名などを施した上で送信される。それによって、この検知手法のプロトコルに従わないルータがあっても、それをネットワーク制御面での攻撃として検知できるようになっている。この部分は通信混雑によるパケット廃棄とパケットロス攻撃の区別には関係しないため、本稿では割愛する。

2.3 検知手順

受信側のルータ r_{d} で送信側の通信情報と受信側の通信情報が集まったところで、この期間における待ち行列 Q へのパケットの出入りから、Q 内に溜まっているパケットの総量の推測値 q_{pred} を以下の手順で順次計算する。

1. 通信情報を一つの配列にまとめ、送受信時間の早い順に並べる。
2. (1) の配列から順に一つずつパケット情報を取り出し、以下の方法で q_{pred} を更新する。
   (a) このパケット情報が受信側のものなら、
   $q_{\mathrm{pred}}(t_{\mathrm{current}}) = q_{\mathrm{pred}}(t_{\mathrm{prior}}) - (\text{パケット長})$
   (b) このパケット情報が送信側のもので、受信側にも対応するパケット情報があるなら、
   $q_{\mathrm{pred}}(t_{\mathrm{current}}) = q_{\mathrm{pred}}(t_{\mathrm{prior}}) + (\text{パケット長})$
   (c) このパケット情報が送信側のもので、受信側には対応するパケット情報がないなら、
   $q_{\mathrm{pred}}(t_{\mathrm{current}}) = q_{\mathrm{pred}}(t_{\mathrm{prior}})$
   これがパケット廃棄の検知にあたる。

(2.2c) のパケット廃棄が通信混雑による正規のものか、パケットロス攻撃によるものかは、Q が満杯かどうかを q_{pred} で推測して判定する。これば単純な比較

$$(Q \text{ の容量}) < q_{\mathrm{pred}} + (\text{パケット長}) \quad (3)$$

でも判定できるが、その場合 q_{pred} の推定の不正確さから来る判定間違いが多く出てきてしまう。これを抑えるため、文献 [1] では確率論に基づいた判定を行う。

$$\mu = (q_{\mathrm{pred}} \text{ の真値からのずれの平均}) \quad (4)$$
$$\sigma = (q_{\mathrm{pred}} \text{ の真値からのずれの標準偏差}) \quad (5)$$

この期間内に n 個のパケット廃棄が見つかったとする。各廃棄パケットについての判定は、

$$y = \frac{(Q \text{ の容量}) - q_{\mathrm{pred}} - (\text{パケット長}) - \mu}{\sigma} \quad (6)$$

$$c = \frac{1 + \mathrm{erf}(y/\sqrt{2})}{2} \quad (7)$$

$c < s_{\mathrm{single}}$ ならば、混雑による廃棄 (8)

$c >= s_{\mathrm{single}}$ ならば、パケットロス攻撃 (9)

個々の廃棄パケットについての判定ですべて攻撃でないと判定された場合は、それに続けて、この期間内の n 個のパケット廃棄全体についての判定を以下の通り行う。

$$z = \frac{(Q \text{ の容量}) - (q_{\text{pred}} \text{ の平均}) - (\text{パケット長の平均}) - \mu}{\sigma\sqrt{n}} \tag{10}$$

$$c = \frac{1 + \mathrm{erf}(z/\sqrt{2})}{2} \tag{11}$$

$c < s_{\text{multi}}$ ならば、
全て混雑による廃棄 (12)

$c \leq s_{\text{multi}}$ ならば、
パケットロス攻撃を含む (13)

これにより、この期間内に対象とするルータ r がパケットロス攻撃をおこなったかどうかが判定できる。

3 調査方法

Mizrak らは、提案した待ち行列推定に基づくパケットロス攻撃検知方式の性能を、実機への実装を使った実験で評価した。この評価方法は実時間での処理の検証が可能であるなどの利点を持つが、方式が含むパラメータに対する振る舞いを検証するのは多くの場合、困難である。そこで本稿では、シミュレーション実験により性能評価を行い、いくつかのパラメータについてその依存性を検討した。

Mizrak らの実装実験において、通信混雑による正規のパケット廃棄を発生させるため、大きなデータのダウンロードを主な通信にしたところ、ほとんどのパケットが最大パケット長のものになることが分かった。そこで今回のシミュレーションでは、全てのパケットは同一のパケット長を持つものとする。

送信側からのパケットの送信は、凡そ一定間隔で行い、その間隔の分だけ乱数により揺らいだ時刻に送信することとした。これにより、対象とするルータ r での待ち行列が偶然によりときどき満杯になることがあるようにした。

パケットロス攻撃としては、対象とするルータ r で適宜適当なパケットをその先へ送らずに廃棄した。これを見逃さずに、通信混雑による正規のパケット廃棄と区別して発見できれば検知成功である。一方、これを見逃すと偽陰性発生となる。また、これ以外で検知したと判定すると偽陽性となる。

4 結果

本節では、検討したパラメータ依存性の実験結果について述べる。

4.1 期間の長さ

この検知方式は一定時間間隔毎に通信情報を集め、これを基に検知作業を行う。検知時の判定には確率論を用いるため、この期間を長くする（サンプル数を多くする）ことによる誤差の減少を期待できる。また、各パケットは伝送に要する時間の分だけ r_{d} への到着が遅れ、その結果この期間の境界を跨ぐとパケット廃棄と判定されてしまうが、期間を長くすることでこの誤判定の機会を減らすことができる。そこで、この期間の長さに対する検知性能の変化を観察した。その結果、期間を倍にすると検知成功率が大幅に上がり、同時に誤判定の数も減った。

ただし、単純に期間が長いほうが性能が良いというわけではない点に注意が必要である。これは、通信情報の収集時間間隔を伸ばすと、それだけパケットロス攻撃が起きてから検知できるまでの時間（検知のす早さ）の期待値が長くなってしまうためである。

4.2 伝送時間

4.1 節で述べたように、この検知方式ではパケットの伝送時間が長くなると同期して行われる検知手順と実情が合わなくなり、誤検知を増やす。そこで帯域幅を変化させることで、パケットの伝送時間に対する検知性能の変化を観察した。その結果、帯域幅を 10 倍に（伝送時間を凡そ 10 分の一に）したが、検知性能（検知成功率、誤判定率）に大きな変化は無かった。これ

は通信の混雑を起こす設定で実験を行っているため、対象とするルータ r で待ち行列に入ってしまい、ルータ間での伝送時間を減らしても、転送先であるルータ r_{d} への到着時間に大きな違いがでなかったためと思われる。

4.3 正規のパケット廃棄

1 節で言及したように、パケットロス攻撃の検知を困難にしているのは、通信混雑による正規のパケット廃棄が多く行われていると、それより少数の攻撃によるパケット廃棄が隠れてしまうためである。そこで待ち行列 Q の容量を変えることで、通信混雑による正規のパケット廃棄の数に対する検知性能の変化を観察した。その結果、待ち行列の容量を半分に（正規のパケット廃棄数を凡そ 10 倍に）したが、検知性能（検知成功率、誤判定率）に大きな変化は無かった。これは、この検知方式が廃棄パケットの存在に強い方式である

5 まとめ

本稿では、Mizrak らが提案した待ち行列推定に基づくパケットロス攻撃検知方式について、三種類のパラメータに対する検知性能の変化を定性的に検討した。その結果、予想された通りの性能変化を示したものがある一方、そのパラメータに対する変化を見せないものもあった。ただし後者の場合でも、検知方式の詳細を考えると無理のない説明をすることができた。このことから、今回検討した範囲では、この検知方式は提案者らの考えている通りの性能を発揮していると言える。

今回は実験数の少なさから、定性的な結果しか述べることができなかった。また、時間の関係で未検討のパラメータがまだ多く残っている。今後はこれらの不足点を解消することで、この検知方式を実際に使用する際の適切な設定や、この検知方式の改良点の発見に寄与することができると考えている。

参考文献

[1] A. Mizrak, S. Savage, and K. Marzullo, “Detecting Malicious Packet Losses”, In IEEE Transactions on Parallel and Distributed Systems, Vol.20, No.2 (February 2009).

[2] A. Kuzmanovic and E.W. Knightly, “Low-rate TCP-targeted Denial of Service Attacks: the Shrew versus the Mice and Elephants”, Proceedings of ACM SIGCOMM’03, pp.75-86 (August 2003)