IP トレースバックにおけるパケットマーキング方式に対する妨害攻撃とその対策に関する研究

池田　匡視 a)・川端　良樹 b)・岡崎　直宣 c)

An Examination of Attack against Packet Marking and Its Countermeasure

Yoshiki KAWABATA, Masami IKEDA, Naonobu OKAZAKI

Abstract

In recent years, the denial of service (DoS) attack and distributed DoS (DDoS) attack is a serious problem. Particularly, to identify the attacker for DDoS attack is difficult. Extended Fragment Marking Scheme (EFMS) is one of effective countermeasures against DDoS attack. However it is possible to interfere in EFMS easily by writing an invalid value to the packet. In this paper, firstly, we show two attacks of interference, and propose countermeasure for each attack. We evaluate the proposed method by simulation.

Keywords: DDoS attack, IP traceback, Packet Marking, EFMS

1. はじめに

近年、インターネットの急速な普及によりインターネットサービスは企業活動の重要なインフラとなっている。それに伴い、インターネット技術を用いたサービスの妨害攻撃(DoS 攻撃)、分散的に DoS 攻撃を行う DDoS 攻撃が問題視されている。DoS/DDoS 攻撃はサービスを妨害したい対象に向けて大量のパケットを送りつけることで、サーバの負荷を増大させたり、帯域を占有することでサービスの継続を困難にさせる攻撃である [1]。特に、DoS 攻撃を分散的に行う DDoS 攻撃は攻撃者一人あたりの攻撃レートを抑えることができるので、通常パケットと攻撃パケットの違いを判断することが困難になる。これらの攻撃は IP スプーフィングという技術を用いて送信元の IP アドレスを詐称しており、攻撃者の特定が難しい [2]。

DoS/DDoS 攻撃の有効な対策手法として IP トレースバックがある [3]。これは、攻撃者が攻撃パケットの送信元を詐称していても、パケットを中継したルータを辿り、攻撃パケットが通過した攻撃経路を再構築することができる技術である。これにより攻撃した端末を特定し、通信制御などの対策をとることができる。本論文では、IP トレースバックの中でもルータへの負荷が少ないなどの理由から、パケットマーキング方式 [4]に着目し、攻撃者による 2 つの妨害攻撃と、その妨害攻撃への対策をそれぞれ提案し、シミュレーションによりその有用性を示す。

a)　情報システム工学専攻大学院
b)　情報システム工学科
c)　情報システム工学科教授

2. パケットマーキング方式

ここでは、パケットマーキング方式の 1 つであり、他方式と比べ汎用性が高い Extended Fragment Marking Scheme(EFMS)[5]について紹介する。EFMS は、マーキングとトレースバックの 2 つの処理から構成されており、ルータはある確率(例:1/25)で通過パケットを取り出し、そのパケットにルータの識別情報を書き込む(マーキング)。マーキングは、すでに値が書き込まれている場合でも上書きして行う。被害者は攻撃パケットに書き込まれた情報から攻撃経路を再構築する(トレースバック)。

ルータが情報を書き込む領域には、現在ではほとんど使用されていない IPv4 ヘッダの Identification フィールドと ToS フィールドが用いられるが、Identification フィールドと ToS フィールドには合わせて 24bit までの情報しか書き込めないため、ルータ識別情報を幾つかに分割して、別々のパケットに書き込む必要がある。パケットに書き込まれるマーキング情報は、ルータ識別情報を幾つかに分割した“リンク情報”に加えて、リンク情報の位置を示す“オフセット”、被害者からルータまでのホップ数を示す“距離値”から構成される。以下でルータ識別情報とトレースバックの手順について説明する。

2.1 ルータ識別情報

ルータ識別情報は、32bit のルータ IP アドレスと 32bit の認証情報から構成される 64bit の情報である。認証情報とは、ルータ IP アドレスのハッシュ値であり、ルータ識別情報が正当なものであることを示すためのものである。

被害者は、攻撃パケットに書き込まれたリンク情報を組み合わせてルータ識別情報を構築し、その中のルータ IP アドレスにハッシュ関数を適用する。こうして得た値とルータ識別情報内の認証情報を比較し、一致していれば正当なルータ識別情報であると判断する。

2.2 トレースバック手順

まず、被害者は攻撃パケットからマーキング情報を取り出す。次に、同一距離値を持つマーキング情報からリンク情報を取り出し、オフセットに従って組み合わせ、ルータ識別情報を構築する。ここで、得られたルータ識別情報の正当性を判断し、正当なルータ識別情報であった場合そのルータ識別情報を記録する。その後、リンク情報の組み合わせを変えて処理を繰り返す。すべての組み合わせを試したあと、距離値をインクリメントして処理を繰り返す。こうして得られた正当ルータ識別情報から攻撃経路を再構築することができる。

ここで問題となるのは、リンク情報が多くなるとトレースバックにおける組み合わせ数が増加することである。これに伴い、ルータ識別情報の数も指数関数的に増加し、正当性判断に時間がかかるため、EFMS は攻撃が大規模になってくると現実時間内にトレースバックすることができなくなるという問題を抱えている。

3. トレースバック妨害攻撃

本論文では、EFMS を運用する際に考慮しなければならないトレースバックの妨害攻撃について2つ提起する。

3.1 ランダムマーキング方式

EFMS では途中通過ルータ数の増加に伴い、指数関数的にルータ識別情報の数が増加する。さらに、攻撃者はパケットマーキング方式による検出を逃れるために、Identification フィールド、ToS フィールドの初期値をランダムな値(不正マーキング情報)に設定することが考えられる。これにより、ルータ識別情報の数はさらに増加する。本論文では、このような攻撃者によるトレースバック妨害攻撃のことを Traceback Jamming DDoS 攻撃 : “TJ-DDoS 攻撃”と呼ぶ。

被害者から d ホップ離れた位置にあるルータの数をr_dとする。ここで、被害ノードに届くパケットのうち、不正マーキング情報の値が、n 種類あると仮定する。この不正マーキング情報が、ある特定の距離値とオフセットを持つ確率は$1/(32 \times 4)$である。このような値を持つ不正マーキング情報のパケットの数の期待値は、$1/128$となる。ここで、距離値$\mathrm{d}-1$を持つパケットすべてを対象に考えた場合、ルータ識別情報の数$L_{max}(d)$は数式(1)のようになる。

$$L_{max}(d) = \left(r_d + \frac{n}{128}\right)^4 \qquad (1)$$

TJ-DDoS 攻撃により、不正マーキング情報を攻撃パケットに書き込んだとき、n は非常に大きな値となる。例えば$\mathrm{n} = 12800$であるとき、$L_{max}(d) > 10^8$となり、復元したルータ識別情報の正当性を判断するためには膨大な時間が必要となる。

3.2 限定マーキング方式

TJ-DDoS 攻撃では、不正マーキング情報としてランダムな値が設定されていたが、この攻撃方式では、不正マーキング情報として実際に存在するルータの正当なマーキング情報を用いる。これにより、トレースバックにおいて攻撃経路にないルータの識別情報まで正当なものであると判断してしまい、攻撃経路の再構築時に false positive が増加する。本論文では、このような不正マーキング情報を限定して書き込み、再構築された攻撃経路の false positive を増加させる攻撃を Restricted Marking TJ-DDoS 攻撃 : “RMTJ-DDoS 攻撃”と呼ぶ。

RMTJ-DDoS 攻撃による EFMS への影響の一例を図 1 に示す。この攻撃者は、RMTJ-DDoS 攻撃を行なっているものとする。このとき、トレースバックによって再構築される攻撃経路には、攻撃者からの攻撃トラフィックを中継した“正当な攻撃経路”のルータだけでなく、攻撃には関係のないルータまで含まれてしまい、攻撃経路の false positive が発生してしまう。

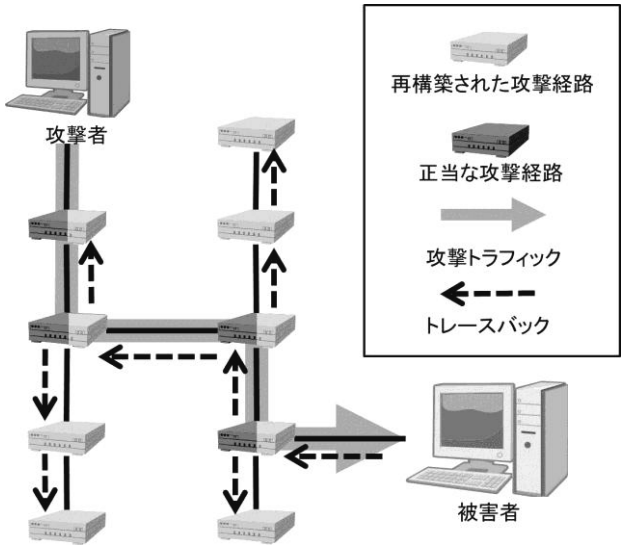

図 1. RMTJ-DDoS 攻撃.

RMTJ-DDoS 攻撃を実現する際、必要な処理としてマーキング情報の収集があるが、EFMS では常にルータでマーキングを行なっているため、攻撃パケットではない通常パケットにも通過ルータによってマーキング情報が書き込まれる。そのため、攻撃者は受信パケットのマーキング情報を確認するだけで正当なマーキング情報を得ることができる。また、攻撃者はマーキング情報の収集に関して、パケット送信などの動作を行わないため、この処理が検知されることはない。

4. 提案手法

ここでは、2 つのトレースバック妨害攻撃への対策をそれぞれ提案する。

4.1 優先度トレースバック EFMS

本節では、TJ-DDoS 攻撃の対策について示す。EFMS において、被害者はすべてのマーキング情報に関してトレースバックを行なっていた。しかし、その手法では不正マーキング情報までトレースバックに組み込んでしまうため、トレースバックに膨大な時間がかかってしまう。

そこで、提案手法ではトレースバックの前に不正マーキング情報と正当マーキング情報を区別し、正当マーキング情報を抽出することで、効率的にトレースバックを行うことにする。ここで、マーキング情報は、リンク情報を組み合わせてルータ識別情報を構築するまで正当なものか不正なものかを判断することはできない。そこで、マーキング情報に優先度を付け、ある閾値以上の優先度を持つマーキング情報についてのみ処理を行うことで、提案手法を実現する。この提案手法を Priority Traceback EFMS：“PT-EFMS”と呼ぶ。

PT-EFMS は、マーキングとトレースバックに“抽出処理”を加えた 3 つの処理から構成される。PT-EFMS では、マーキングとトレースバックは EFMS と同様に行い、トレースバックの前に抽出処理を行うことで、正当マーキング情報を抽出し、効率的にトレースバックを行えるようにしている。

PT-EFMS の優先度の付け方は、マーキング情報ごとの到着パケットの数により決定する。攻撃パケットの不正マーキング情報は、通過ルータにより正当マーキング情報に上書きされて被害者に到着するため、正当マーキング情報の方が不正マーキング情報に比べて多くなる。このことから、到着パケット数が多いマーキング情報に高い優先度を付け、到着パケット数が少ないマーキング情報には低い優先度を付けることで不正マーキング情報と正当マーキング情報を区別する。

本提案手法では、優先度を値が低い順に確認していき、初めて優先度が急激に上昇したときの優先度の値を不正マーキング情報と正当マーキング情報を区別するための閾値として設定する。今回は、優先度の上昇値を 3 以上のとき閾値として設定することにした。

図 2 に PT-EFMS の抽出処理の一例を示す。各行は 1 つのマーキング情報を表しており、No.はマーキング情報を優先度順で並べたときの順番を示す。また、ToS、Identification はそれぞれのフィールドの値、Priority は優先度を示す。この例では、No.1002 と No.1003 において優先度が 2 から 19 まで上昇しており 3 以上の上昇値であるので、優先度 19 を不正マーキング情報と正当マーキング情報を区別するための閾値として設定する。これにより、No.1003 以上は正当マーキング情報、No.1002 以下は不正マーキング情報として区別することができる。

No.	ToS	Identification	Priority
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・
1000	53	347	2
1001	91	5876	2
1002	122	17235	2
1003	25	44072	19
1004	113	9940	20
1005	77	32930	20
1006	116	43400	20
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

図 2. 抽出処理.

4.2 宛先志向マーキング EFMS

本節では、RMTJ-DDoS 攻撃の対策について示す。EFMS において、パケットの通過したルータは宛先に関係なくマーキング情報を書き込む。そのため、RMTJ-DDoS 攻撃の被害者が得られるマーキング情報と、攻撃者が得られるマーキング情報の値が同じになり、攻撃者が有効なマーキング情報を収集することができてしまう。

そこで、提案手法では宛先ごとに書き込むマーキング情報を変更し、被害者と攻撃者の得られるマーキング情報を異なる値に設定することで、RMTJ-DDoS 攻撃を無効化する。このとき、書き込まれるマーキング情報を宛先ごとに変えるため認証情報に宛先 IP アドレスの情報を加える。

DM-EFMS における、宛先ごとに異なった認証情報を求める方法を示す。EFMS において認証情報はルータ IP アドレスのハッシュ値であったが、DM-EFMS では以下の【DM-認証情報の計算】により得られる値とする。ここで得られる値を“DM-認証情報”と呼ぶ。

1. ルータ IP アドレスの 32bit ハッシュ値を求める。
2. 1. 値と宛先 IP アドレスの排他的論理和を求める。
3. 2. れた値の 32bit ハッシュ値を求め、この値を DM-認証情報とする。

図 3 に DM-EFMS の様子を示す。ルータが宛先ごとに DM-認証情報を計算し、別々のマーキング情報を書き込んでいる。これにより、攻撃者が被害者に有効なマーキング情報を収集することができなくなり、RMTJ-DDoS 攻撃を無効化することができる。

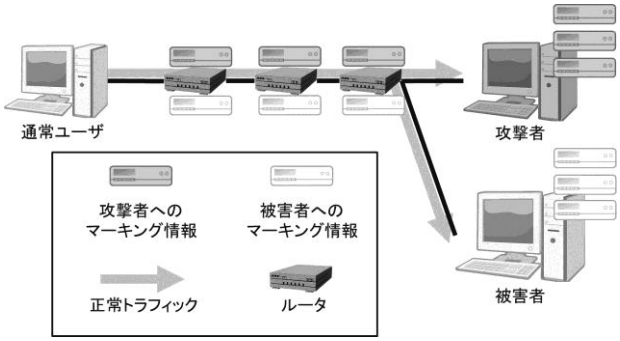

図 3. DM-EFMS.

5. 評価

本章では、PT-EFMS のスケーラビリティについてシミュレーションを用いて評価する。シミュレーションでは、PT-DDoS 攻撃とルータによるマーキングを QualNet 上に実装した。また、EFMS、PT-EFMS のアルゴリズムを C++ 言語を用いて実装しトレースバックと抽出処理を行った。評価項目としてルータ識別情報の正当性を判断した回数(計算量)と、マーキング情報を収集し攻撃経路を再構築するまでの時間（攻撃経路再構築時間）を用いて、EFMS と PT-EFMS を比較することで処理コストを評価する。

ネットワークトポロジは、実際にインターネット上で構築されているトポロジを参考に構築した [5]。本ネットワークは、複数のリングネットワークが連結した状態を想定し、298 個のルータから構成されている。そして、攻撃経路はダイクストラ法によって導出した最短経路を用いて生成した。

攻撃モデルは、現在最も頻繁に行われ、今なお頻度の増加が確認されている SYNflood 攻撃 [6] を、TJ-DDoS 攻撃に拡張した TJ-SYNflood 攻撃を想定する。攻撃レートは全攻撃者で等しく 10packets/second(pps) で連続的に行われるものとする。攻撃者は 10 人から 30 人を想定し、TJ-DDoS 攻撃全体の攻撃レートは 100pps から 300pps で行われる。

実験結果を図 4、図 5 に示す。 今回のシミュレーションでは、EFMS は攻撃者数が 10、15、20 の場合、PT-EFMS は攻撃者数が 10、15、20、25、30 の場合について実験を行った。また、トレースバックに必要な数のマーキング情報を得るための時間(マーキング情報収集時間)を、EFMS では 120sec、PT-EFMS では 600sec にそれぞれ設定した。

図 4 から、計算量は攻撃者が何人の場合でも PT-EFMS の方が EFMS よりも非常に低い値を示しており、PT-EFMS を用いることによる改善が見られることが分かる。これは、EFMS と比べ PT-EFMS のマーキング情報の種類が大幅に省かれ、ルータ認証情報の数が少なくなったためである。また、図 5 から、攻撃経路再構築時間においても PT-EFMS の方が EFMS よりも低い値を示しており、PT-EFMS の有効性が示されている。図 5 において PT-EFMS の値がほぼ同一であるのは、マーキング情報収集時間が一定である一方、トレースバック時間がグラフに顕れないほど小さな値であるためである。

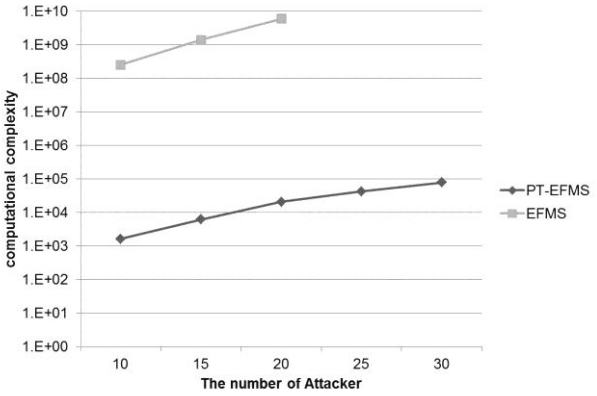

図 4. 計算量.

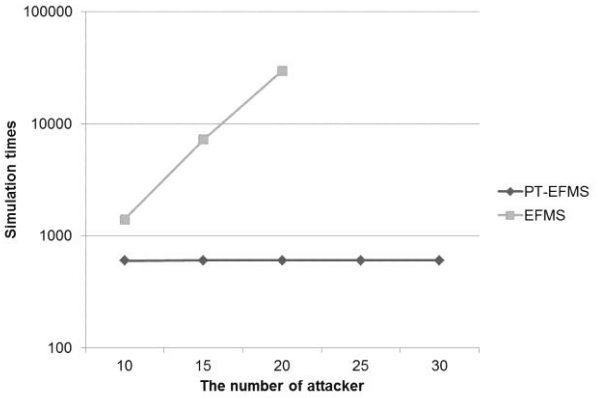

図 5. 攻撃経路再構築時間.

6. 提案手法の併用

本論文では、2 つのトレースバック妨害攻撃について紹介し、それぞれの対策を述べた。ここでは、PT-EFMS の RMTJ-DDoS 攻撃耐性と DM-EFMS の TJ-DDoS 攻撃耐性について考察し、2 つの提案手法の併用について述べる。

PT-EFMS は、TJ-DDoS 攻撃に対して有効な対策であると考えられるが、攻撃者により不正マーキング情報を少なく設定された場合、不正マーキング情報と正当マーキング情報の区別ができなくなり、その効果を発揮することができなくなるという欠点を持つ。RMTJ-DDoS 攻撃の場合、TJ-DDoS 攻撃と違い、攻撃の効果を残しつつ不正マーキング情報を少なくすることができるため、PT-EFMS では RMTJ-DDoS 攻撃を防ぐことが難しいと思われる。

DM-EFMS は、RMTJ-DDoS 攻撃に対して有効な対策であると考えられるが、計算量を減らすことはできないので、TJ-DDoS 攻撃のような計算量を増加させることが目的の攻撃を防ぐことはできない。

両提案手法は以上のような欠点を持つが、それをお互いに補い合うことができる。そこで、DM-EFMS をベースに抽出処理を追加することで、両提案手法を併用し、TJ-DDoS 攻撃と RMTJ-DDoS 攻撃両方に耐性のあるマーキング方式を実現することができる。

7. まとめ

本論文では、既存の DDoS 攻撃対策手法である EFMS において、攻撃者が容易に実行可能な妨害攻撃について 2 つ示し、それぞれの対策について提案した。また、両提案手法の欠点と、それをお互いが補い合えることを示し、併用方式について述べた。

今後は、実験出来なかった RMTJ-DDoS 攻撃、DM-EFMS、併用方式について検証したい。

参考文献

1) D. Moore, C. Shannon, S. Savage, D. J. Brown, G. M. Voelker : Inferring Internet Denial-of-Service Activity, ACM Transactions on Computer Systems, Vol.24, No.2, pp.115-139, 2006.
2) R. T. Morris : A Weakness in the 4.2BSD UNIX TCP/IP Software, Bell Labs Computing Science Technical Reports, No.117, 1985.
3) 門林　雄基, 大江　将史：IP トレースバック技術, IPSJ Magazine, Vol.42, No.12, pp.1175-1180, 2001.
4) S. Savage, D. Wetherall, A. Karlin,T. Anderson : Practical Network Support for IP Traceback, Computer Communication Review, Vol.30, No.4, pp.295-306, 2000.
5) 古賀　勝寛, 岡崎　直宣, 渡邊　晃, 朴　美娘：動的マーキングを用いた効率的なネットワーク攻撃追跡手法に関する研究, 電気学会論文誌 C, Vol.129, No.3, pp.532-544, 2009.
6) TCP SYN Flooding and IP Spoofing Attacks, CERT Advisory, Vol.CA-1996, No.21, 1996.