M-011

ネットワークエッジにおける確率的キュー割り当てによる軽量な DDoS 緩和法

Light-Weight DDoS Mitigation by Probabilistic Queue Allocation at Network Edge

八重樫 遼 [1]　久野 大介 [2]　中山 悠 [1]
Ryo Yaegashi　Daisuke Hisano　Yu Nakayama

1. はじめに

近年急速な成長を遂げている Internet of Thing(IoT)分野は 5G の普及により，人々の生活にさらに不可欠なものになっていくと考えられる．一方，Mirai などの IoT デバイスを利用した Distributed Denial of Service(DDoS)攻撃が増加し[1]，その対策が重要な課題となっている．従来手法としては，Software Defined Networking を用いた検知方法[2][3]などが提案されてきた．しかし，ネットワークエッジで軽量かつ簡易な DDoS 緩和を行う手法はあまりなかった．そこで，本研究では未活用キューを利用した軽量な DDoS 緩和法を提案する．提案手法は，正規分布を利用した確率的キュー割り当てを行い，キュー長変位の観測結果から flooding 型の DDoS 攻撃を検知し，パケット廃棄を行う．さらに，提案手法の理論解析とシミュレーションによる性能評価について述べる．提案手法は安価な機器でも動作する簡易な緩和法であり，またネットワークエッジでの防御はネットワークに流入する攻撃トラヒックの抑制効果が大きいという利点がある．

2. 提案手法

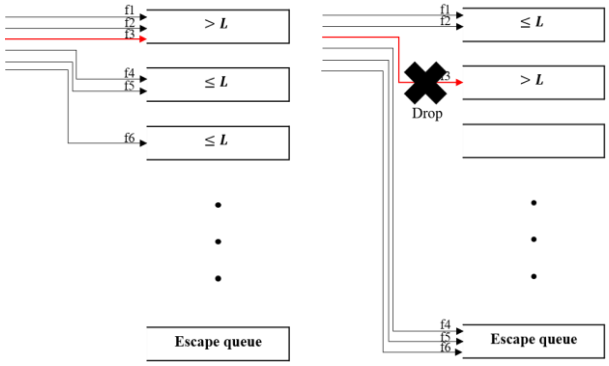
2.1 概要

提案手法は，レイヤ 2 スイッチや IoT ゲートウェイなど複数のキューを有する一般的なネットワークノードにおいて，確率的キュー割り当てにより DDoS 緩和を行う．

DDoS 緩和の流れを図 1 に示す．正当なフローを割り当てるキューとして，エスケープキューと呼称するキューを 1 つ用意する．まず，図 1(a)のように，流入するフローを利用可能なキューに割り当てる．あるキューのキュー長変位がある閾値(L)を超えると，そのキューに割り当てられたフロー(f1，f2，f3)が利用可能なキューにランダムに再割り当てされる．そうでない場合は，割り当てられたフロー(f4, f5，f6)が正当なフローとして検出され，エスケープキューに割り当てられる．以上の処理を続け，図 1(b)の f3 のようにキュー長変位が閾値より大きく，なおかつ割り当てられたフローの数が 1 つだけである場合のみ，悪意のあるフローと判定して廃棄することで，DDoS 攻撃を軽減することができる．

2.2 確率的キュー割り当て

フローを割り当てるキューの決定には平均μ，標準偏差σの正規分布に従って生成される乱数を用いる．まず，正規分布の-3σから3σまでの範囲を割り当てに用いるキューの数に応じて一様に分ける．すなわち，1 つのキューの割り当て範囲wはキューの数をN_qとすると，$w = 6\sigma/N_q$と計算



(a)フローの割り当て　(b)DDoS 緩和

図 1　提案 DDoS 緩和法の流れ

できる．次に，生成した乱数がどのキューの範囲に当てはまるのかによって，割り当てるキューを決定する．なお，標準正規分布の-3σから3σ以外の範囲については，-3σ 未満の範囲は 1 番目，3σ以上の範囲はN_q番目のキューに割り当てるとする．以上より，q番目のキューに割り当てられる確率a_qは次式のように計算できる．

$$a_q = \frac{1}{\sqrt{2\pi}\sigma}\int_{\alpha_q}^{\beta_q} e^{-\frac{(x-\mu)^2}{2\sigma^2}}dx \quad (1)$$

ここで，α_q及びβ_qはq番目のキューの範囲の下限と上限を表し，$q = 1$の場合，$\alpha_1 = -\infty$，$\beta_1 = -3\sigma + w$である．また，qが2から$N_q - 1$までの場合は$\alpha_q = -3\sigma + (q-1)w$，$\beta_q = -3\sigma + qw$，$q = N_q$の場合は$\alpha_{N_q} = 3\sigma - w$，$\beta_{N_q} = \infty$である．

2.3 理論解析

2.3.1 DDoS 検知の確率

DDoS 検知を行うのは，悪意のあるフローがキューに 1 つだけ割り当てられた場合である．よって，その確率は悪意のあるフローのみがキューに割り当てられる確率に等しい．ここで，2.1 節で述べたキュー長変位の観測から再割り当てまでの処理を 1 サイクルとし，そのサイクル識別子をcとする．また，c番目のサイクルでq番目のキューに 1 つのフローが割り当てられる確率を$p_{q,c}$と定義すると，次式で計算される．

$$p_{q,c} = a_q(1-a_q)^{N_{F,c}-1} \quad (2)$$

ここで，$N_{F,c}$はc番目のサイクルでエスケープ，または悪意のあるフローと判定されていないフローの数を表している．

ここで，利用可能なすべてのキューをQとすると，c番目のサイクルであるフローがいずれかのキューに割り当てられ，なおかつ他のフローが同じキューに割り当てられない確率p_cは以下のように表される．

$$p_c = \sum_{q\in Q} p_{q,c} \quad (3)$$

[1] 東京農工大学情報工学科
Department of Computer and Information Sciences,
Tokyo University of Agriculture and Technology
[2] 大阪大学 大学院 工学研究科,
Graduate School of Engineering, Osaka University

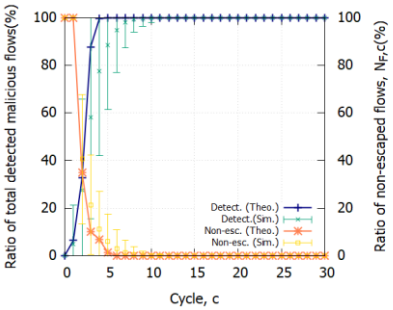


図2　フローの数が16の場合

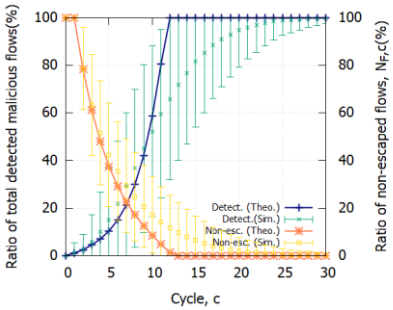


図3　フローの数が64の場合

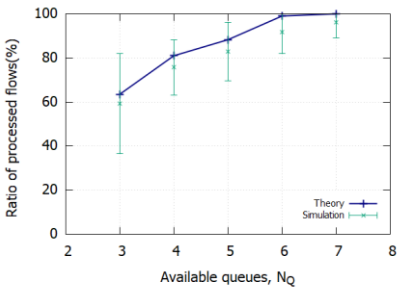


図4　処理済みフローの数

c番目のサイクルにおける未検出の悪意のあるフローの期待値をU_c，検出された悪意のあるフローの期待値をE_cとすると，これらの変数の関係は

$$U_{c+1} = Max(0, U_c - E_c) \tag{4}$$

で表される．また，E_cは式(5)で求まる．

$$E_c = p_c U_c \tag{5}$$

ここで，$U_0 = \rho N_{F,0}$であり，ρはすべての流入フローに対する悪意のあるフローの割合を表している．

2.3.2 残存フローの予想個数

c番目のサイクルでq番目のキューに割り当てられたフローの数の期待値$n_{q,c}$は次のように計算される．

$$n_{q,c} = a_q N_{F,c} \tag{6}$$

割り当てられたフローの中に悪意のあるフローが含まれない確率$\gamma_{q,c}$は

$$\gamma_{q,c} = \left(1 - \frac{U_c}{N_{F,c}}\right)^{n_{q,c}} \tag{7}$$

で表される．以上より，c番目のサイクルでエスケープするフローの期待値は次式で求まる．

$$V_c = \sum_{q \in Q} \gamma_{q,c} n_{q,c} \tag{8}$$

以上より，非エスケープフローの数$N_{F,c}$から，検出された悪意のあるフローの数E_cとエスケープするフローの数V_cが次のサイクルで減少するため，$N_{F,c+1}$は式(9)のように記述できる．

$$N_{F,c+1} = Max\left(0, N_{F,c} - E_c - V_c\right) \tag{9}$$

3. シミュレーション評価

3.1 条件

初めに，式(5)，式(9)で定式化した理論との整合性を確認した．利用可能なキューの数を 6，流入するフロー数を 16，64 に設定し，異なる条件での検出精度を評価した．

次に，限界性能を明らかにするために，流入フロー数とキュー数の関係性について評価した．流入するフローを 128 に設定し，利用可能なキューの数を 3 から 7 へと変化させ，30 サイクルで処理を終えたフローの数を測定した．処理を終えたフローとは，検出できた悪意のあるフローとエスケープキューに割り当てられたフローのことである．

以上のシミュレーションで一般的に用いたその他のシミュレーション条件は以下の通りである．キューサイズの閾値を 62.5 MB，リンク帯域幅 50 Mbps，悪意のあるフローは flooding 型の攻撃を想定して 100 Mbps，悪意のあるフローである確率を 0.1 とした．また，正常なフローのデータサイズは平均 2.0 Mbps，標準偏差 0.5 Mbps の正規分布に従う．また，割り当て先のキューの決定の乱数生成には標準正規分布を用いた．1 サイクルにかかる時間を 10 秒，合計シミュレーション時間を 300 秒とし，シミュレーションは各条件で 1000 回繰り返し行った．

3.2 評価結果

流入するフローの数を 16 にした場合の結果を図 2，64 にした場合の結果を図 3 に示す．これらは流入してきた悪意のあるフローに対して検知できた悪意のあるフローの割合と，流入フロー数に対する非エスケープフローの数$N_{F,c}$の割合の理論値とシミュレーション結果を表している．図 2，3 より，理論値とシミュレーション結果がよく合致していることが分かる．また，フロー数が少ないと 30 サイクル以内には緩和処理を完了させることが可能であることが分かる．以上の結果から，提案方式が DDoS 攻撃の検知，軽減に正しく機能することが確認できる．

図 4 は，キューの数が 3〜7 の場合の流入フロー数に対する 30 サイクル後の処理フローの割合の理論値とシミュレーション値を示している．図 4 から，キュー数が多くなると処理率が高くなり，利用可能なキューの数が 4 であっても，流入フローの約 8 割を処理できることが分かる．

4. まとめ

本論文では，ネットワークエッジで軽量かつ簡易な DDoS 緩和を行う手法を提案した．さらに，理論解析及びシミュレーションによって，提案手法の有効性を確認した．しかし，さらなる効率的な確率的割り当てを行うことで改善の余地があると考えられる．よって，今後はより良い確率的な割り当てを議論していきたい．

謝辞

本研究の一部は，JST ACT-I（JPMJPR18UL）の支援を受けて行われた．

参考文献

[1] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,”Computer, vol. 50, no. 7, pp. 80–84, 2017.

[2] G. Liu, W. Quan, N. Cheng, H. Zhang, and S. Yu, “Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things,”Journal of Network and Computer Applications, vol.130, pp. 1–13, 2019.

[3] S. Lim, J. Ha, H. Kim, Y. Kim and S. Yang, "A SDN-oriented DDoS blocking scheme for botnet-based attacks," 2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN), Shanghai, 2014, pp. 63-68.