Vol.2018-MBL-89 No.7
Vol.2018-ITS-75 No.7
2018/11/15

スライドウィンドウを利用したエントロピー手法による軽量なDDoS攻撃検知手法の検討

宮崎大学工学研究科　○臼崎 翔太郎
宮崎大学工学部　山場 久昭
油田 健太郎
岡崎 直宣

研究背景 2

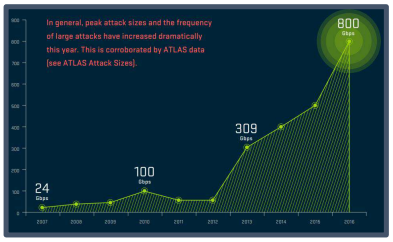
◆DDoS攻撃の規模は2012年を境に年々増加している[1]

◆**IoTボットネット**や**リフレクション攻撃**の流行

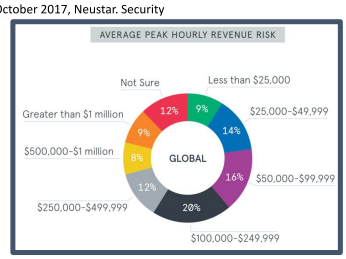
◆被害額も甚大になっており[2] 素早い検知が求められる

➢ リアルタイム性を考慮した統計的検知手法が利用される

[1] Arbor 12th Annual World Infrastructure Security Report, 2017



[2] Global DDoS Attacks & Cyber Security Insights Report, October 2017, Neustar. Security



エントロピー手法 3

◆DDoS攻撃検出手法としても最もよく利用される手法

◆パケットのヘッダ情報を情報源としてエントロピー値を算出する

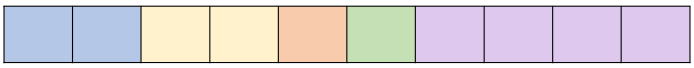
◆分散度を測るエントロピー値がDDoS攻撃の特徴をよく反映

◆対象はインバウンドパケット

DDoS攻撃時の特徴

送信元IPアドレスが分散 → エントロピー値**増加**

宛先IPアドレスが集中 → エントロピー値**減少**



$$H = -\frac{2}{10}\log\frac{2}{10} - \frac{2}{10}\log\frac{2}{10} - \frac{1}{10}\log\frac{1}{10} - \frac{1}{10}\log\frac{1}{10} - \frac{4}{10}\log\frac{4}{10}$$

エントロピー手法の利点 4

◆DDoS攻撃検知の精度が高い（文献[3]では最も高いと報告）

◆高速計算性が高い＝リアルタイム性が高い

◆閾値ギリギリの攻撃を行うことが難しい（組織内に到着するすべてのパケットを監視する必要）

[3] İlker Özçelik, Richard R. Brooks, "Deceiving entropy based DoS detection," Computers & Security, vol. 48, 2015, pp. 234-245,

エントロピー手法の欠点 5

◆ウィンドウサイズを大きくするとオーバヘッドが発生する[4]

➢ ノイズの影響などを考えると数万が推奨される[5]

◆ウィンドウサイズを大きくすると通常パケットも含まれる可能性が高い

◆閾値が固定値であることが多くトラフィックへの追従性が少ない[6]

➢ 過去の特徴量を利用してリアルタイムに閾値を変えるアプローチが存在

[4] Hoque, N. ;Kashyap, H. ;Bhattacharyya, D. K.: "Real-time DDoS attack detection using FPGA," Computer Communications, Vol. 110, pp. 48-58,2017

[5] L. Feinstein ;D. Schnackenberg ;R. Balupari ;D. Kindred, "Statistical approaches to DDoS attack detection and response," Proceedings DARPA Information Survivability Conference and Exposition, Vol.1, pp. 303-314, 2003

[6] 小島 俊輔、中嶋 卓雄、末吉 敏則、『エントロピーベースのマハラノビス距離による高速な異常検知手法』、情報処理学会論文誌, Vol. 53, No. 2, pp. 656-668, 2011

研究目的

ウィンドウサイズが小さく、追従性の高い
エントロピーベースのDDoS攻撃検知手法の提案

提案手法 6

◆現在のスライドウィンドウから抜けた分が過去のものに集約

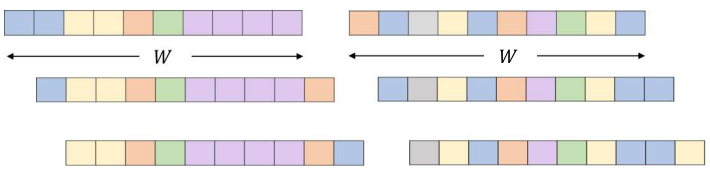
◆効率の良い更新処理・集約処理

[7]Eran Assaf, Ran Ben Basat, Gil Einziger, Roy Friedman: "Pay for a Sliding Bloom Filter and Get Counting, Distinct Elements, and Entropy for Free", arXiv:1712.01779 [cs.DS]

◆短いウィンドウサイズでもノイズの影響を軽減＋リアルタイム性の向上

◆スライドウィンドウは文献[7]を利用 → 複数の特徴量も計算可能

過去のウィンドウ（H_p）　現在のウィンドウ（H_c）

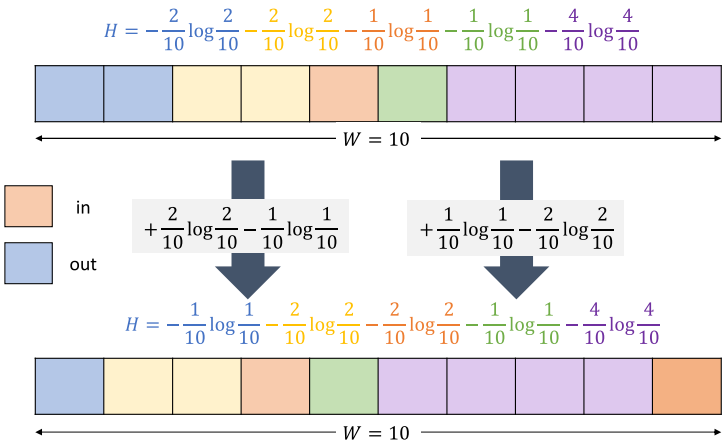


$$H_p^k = S_{i-w-1}^{in} - S_{i-2w}^{out} + H_p^{k-1} \qquad H_c^k = S_i^{in} - S_{i-w}^{out} + H_c^{k-1}$$

※$S_i = -p(i)\log p(i)$

スライドウィンドウ方式のエントロピー手法[7]

7



提案手法

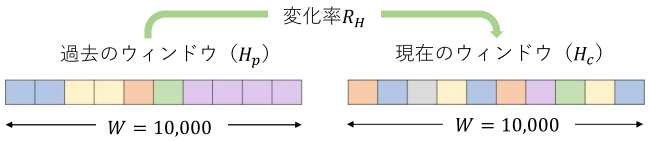
8

◆攻撃検知

- **攻撃開始判定状態**から**攻撃終了判定状態**までのIPアドレスを被疑クライアントとする
  → 1パケットずつリアルタイムに開始・終了を判定し**被疑クライアントを最小限**に
- 過去のエントロピー値と現在のエントロピー値の変化率で監視

攻撃開始判定

$$R_H = \frac{H_c}{H_p} \geq \beta$$



提案手法

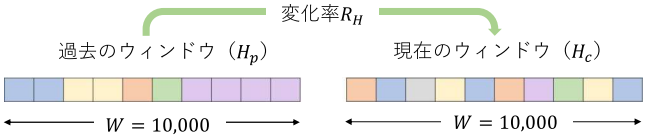
9

◆攻撃検知

- **攻撃開始判定状態**から**攻撃終了判定状態**までのIPアドレスを被疑クライアントとする
  → 1パケットずつリアルタイムに開始・終了を判定し**被疑クライアントを最小限**に
- 過去のエントロピー値と現在のエントロピー値の変化率で監視

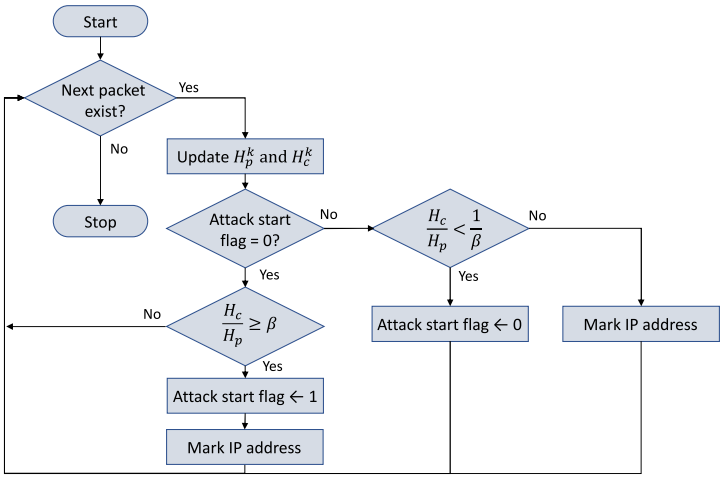
攻撃終了判定

$$R_H = \frac{H_c}{H_p} < \frac{1}{\beta}$$



フローチャート

10



評価実験

11

◆DDoS攻撃のデータセットを用いて検知精度を評価

- 閾値を変化させたときのPrecision, Recall, F-valueを計測

$$P = \frac{TP}{TP + FP} \quad \text{Precision} \qquad R = \frac{TP}{TP + FN} \quad \text{Recall} \qquad F = \frac{2PR}{P + R} \quad \text{F-value}$$

◆検知処理にかかる時間を測定

- 1パケット到着時の検知処理時間の平均値を算出

	異常	正常
異常と判定	True Positive	False Positive
正常と判定	False Negative	True Negative

◆パラメータセット

閾値β	1〜2.7 （2.8以上は検知できず）
ウィンドウサイズW	10,000 （文献[5]を参考に）

実験結果

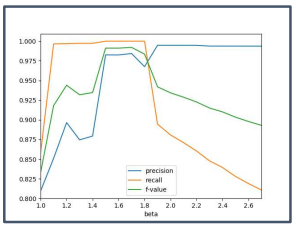
12

◆F値が最大0.992（閾値が1.7の時） → 既存手法と同程度の精度

- 文献[6]ではF尺度は0.993、文献[4]では0.999

◆平均検知処理時間は2.62μs → 既存手法に比べて約113倍の性能

- 文献[4]ではソフトウェア実装の場合296μs



閾値βを変化させたときの各検知精度の結果

平均 [μs]	標準偏差 [μs]
2.62	2.28

検知処理時間の結果

まとめ

13

◆リアルタイム性と追従性を向上したエントロピーベースのDDOS攻撃検知手法を検討

- スライドウィンドウ方式＋集約処理により、小さいウィンドウサイズに伴うノイズの影響を軽減し、直近の過去との変化率を比較することで追従性を向上
- 1パケットごとの処理＋攻撃開始・終了検知の導入により、被疑クライアントを最小限に

◆検知精度と処理性能を調査

- DARPA2000データセットを対象に調査
- 最大でF値が0.992となり、既存手法と同程度の性能を持つ
- 更新・検知処理は平均2.26μs → 十分な高速計算性でありリアルタイムな対応が可能

今後の課題

14

◆エントロピー値の倍率だけでは変化率が顕著に見えない

- スライドウィンドウ方式による計算手法が原因
- DARPA2000の場合、$W = 1{,}000$では2.8倍以上となるケースが存在しない
- パケットレートを導入するなどしてエントロピー値増幅方法を検討している

◆閾値の決定方法が困難

- 通常状態でも変化率が高くなる恐れがある
- さらなる追従性の向上のために自動学習の必要性

◆複数のデータセットで評価する必要がある

- CICIDS2017[8][9]などの新しいデータセット
- フラッシュイベントの含まれるデータセット
- 攻撃の含まれないデータセット

[8]Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Purtogal, January 2018

[9] Intrusion Detection Evaluation Dataset (CICIDS2017), Canadian Institute for Cybersecurity, http://www.unb.ca/cic/datasets/ids-2017.html (accessed 2018/10/22)