Vol.2018-MBL-89 No.10
Vol.2018-ITS-75 No.10
2018/11/15

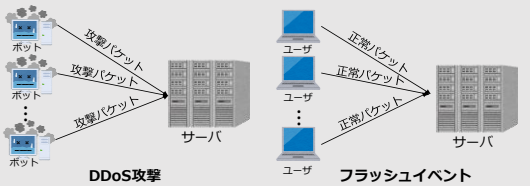
第75回高度交通システムとスマートコミュニティ

被疑クライアントのHTTPリクエスト送信挙動に基づいたボット判定手法

○藤 竜成，山場 久昭，油田 健太郎，岡崎 直宣
宮崎大学大学院　工学研究科

研究背景

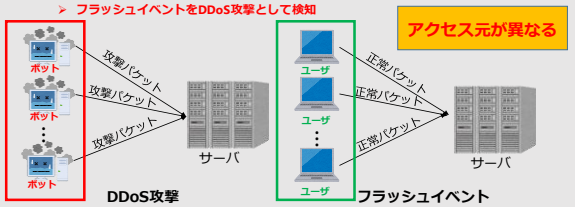
- DDoS攻撃はネットワークやサーバに対して深刻な悪影響を及ぼす
  - DDoS攻撃の検知は重要
  - DDoS攻撃の検知手法に関して多くの研究が行われている
- フラッシュイベントと呼ばれるDDoS攻撃に類似した現象の存在
  - DDoS攻撃の検知手法に関する多くの研究はフラッシュイベントの発生を想定していない
  - フラッシュイベントをDDoS攻撃として検知



研究背景

- DDoS攻撃はネットワークやサーバに対して深刻な悪影響を及ぼす
  - DDoS攻撃の検知は重要
  - DDoS攻撃の検知手法に関して多くの研究が行われている
- フラッシュイベントと呼ばれるDDoS攻撃に類似した現象の存在
  - DDoS攻撃の検知手法に関する多くの研究はフラッシュイベントの発生を想定していない
  - フラッシュイベントをDDoS攻撃として検知

アクセス元が異なる



DDoS攻撃とフラッシュイベント

	特　徴	アクセス元	対　応
DDoS攻撃	• 急激なトラフィック量の増加 • 大量のトラフィック • 大量のクライアント	ボット	ボットの検知・遮断
フラッシュイベント	• 急激なトラフィック量の増加 • 大量のトラフィック • 大量のクライアント	ユーザ	サーバ等の強化による サービス提供の継続

- フラッシュイベントをDDoS攻撃として誤って検知してしまうと
  - フラッシュイベントのトラフィックが遮断
  - 本来サービスを提供をすべきユーザにサービスを提供できない可能性
- フラッシュイベントとDDoS攻撃を識別せずに可用性を保とうとすると
  - 本来サービスを提供をすべきでないボットにサービスを提供
  - コストの増加

DDoS攻撃とフラッシュイベント

	特　徴	アクセス元	対　応
DDoS攻撃	• 急激なトラフィック量の増加 • 大量のトラフィック	ボット	ボットの検知・遮断

DDoS攻撃とフラッシュイベントの識別は重要

- 急激なトラフィック量の増加
- 大量のトラフィック
- 大量のクライアント

のアクセス元の特定が必要

- 本来サービスを提供をすべきユーザにサービスを提供できない可能性
- フラッシュイベントとDDoS攻撃を識別せずに可用性を保とうとすると
  - 本来サービスを提供をすべきでないボットにサービスを提供
  - コストの増加

[1] 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.52, No.2, 656-668(Feb. 2011)
[2] Sajal Bhatia, Ensemble-based model for DDoS attack detection and flash event separation, Future Technologies Conference (2016)

関連研究と提案

- **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[1]**
  - パケットのヘッダ情報(送信元IPアドレス、宛先ポート番号等)用いて**多様な異常を検知可能**

✓ フラッシュイベントの発生を想定していない
↳ **フラッシュイベントを異常(攻撃)とみなしてしまう**

- **Ensemble-based model for DDoS attack detection and flash event separation[2]**
  - 単位時間当たりのパケット数、サーバのCPU使用率等を用いてDDoS攻撃・フラッシュイベントの検知

✓ クライアント単位での検知が出来ない
↳ **DDoS攻撃時においてユーザのアクセスまでも遮断**

提　案

クライアントのHTTPリクエスト送信動作に着目したボット検知手法の提案

[1] 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.52, No.2, 656-668(Feb. 2011)
[2] Sajal Bhatia, Ensemble-based model for DDoS attack detection and flash event separation, Future Technologies Conference (2016)

関連研究と提案

- **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[1]**
  - パケットのヘッダ情報(送信元IPアドレス、宛先ポート番号等)用いて**多様な異常を検知可能**

DDoS 攻撃時にはボットを検知し，
フラッシュイベント時にはユーザを発見することが可能

DDoS攻撃とフラッシュイベントの識別が可能

クライアント毎にボットまたはユーザの判定が可能

DDoS攻撃時においてもユーザの発見が可能

[2]

提　案

クライアントのHTTPリクエスト送信動作に着目したボット検知手法の提案

[3]Acarali, D., Rajarajan, M., Komninos, N. and Herwono, I.: Survey of approaches and features for the identification of HTTP-based botnet traffic, Journal of Network and Computer Applications 76 pp.1-15 (2016).

ボット検知に用いる特徴

1. **クライアント毎の単位時間当たりのリクエスト量**

クライアント	目的	リクエスト量
ユーザ	情報の収集など、ある特定の行動	少ない
ボット	サーバやネットワーク等のリソースの枯渇	多い

2. **Webページを要求するリクエスト送信間隔の類似性**
   - 一般にDDoS攻撃はボットネットを通じて実行される
   - ボットネット内においてはボット同士の挙動が類似する[3]

クライアント	リクエスト送信間隔の類似性
ユーザ	ユーザ同士では類似性なし
ボット	ボット同士では類似性あり

3. **大量のリクエスト送信の継続性**

提案手法のボット検知の流れ

単位時間(U_T)毎に実行

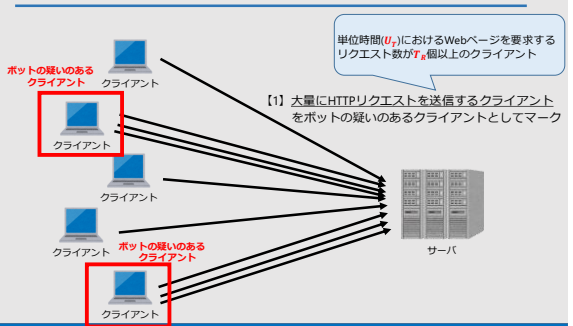
1. 大量にHTTPリクエストを送信するクライアントをボットの疑いのあるクライアントとしてマーク
2. ボットの疑いのあるクライアント間における、Webページを要求するHTTPリクエスト送信間隔の類似性によるボット検知
3. 大量のリクエスト送信の継続性によるボット検知
   長期間に渡って大量にリクエストを送信するクライアントはボットと判断

提案手法のボット検知の流れ

単位時間(U_T)毎に実行

1. 大量にHTTPリクエストを送信するクライアントをボットの疑いのあるクライアントとしてマーク
2. ボットの疑いのあるクライアント間における、Webページを要求するHTTPリクエスト送信間隔の類似性によるボット検知
3. 大量のリクエスト送信の継続性によるボット検知
   長期間に渡って大量にリクエストを送信するクライアントはボットと判断

1. ボットの疑いのあるクライアントのマーク



提案手法のボット検知の流れ

単位時間(U_T)毎に実行

1. 大量にHTTPリクエストを送信するクライアントをボットの疑いのあるクライアントとしてマーク
2. ボットの疑いのあるクライアント間における、Webページを要求するHTTPリクエスト送信間隔の類似性によるボット検知
3. 大量のリクエスト送信の継続性によるボット検知
   長期間に渡って大量にリクエストを送信するクライアントはボットと判断

2-1. Webページを要求するHTTPリクエスト送信間隔の類似度計算

【2】単位時間(U_T)内のそれぞれのボットの疑いのあるクライアントにおいて
Webページを要求するHTTPリクエストの送信間隔の集合を求める

【3】求めたWebページに対するHTTPリクエストの送信間隔の集合から送信間隔の確率分布を求める

例えば

ボットの疑いのあるクライアントA： [1,2,1,3,1]

$$p_A(x) = \begin{cases} 3/5 & (x=1) \\ 1/5 & (x=2) \\ 1/5 & (x=3) \end{cases}$$

[4]Saravanan, R., Shanmuganathan, Y., Planichamy, Y.: Behavior-based detection of application layer distributed denial of service attacks during flash events, Turkish Journal of Electrical Engineering & Computer Sciences 24 pp.510-523 (2016).

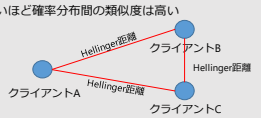
2-2. Webページを要求するHTTPリクエスト送信間隔の類似度計算

【4】求めたクライアント毎の確率分布間の類似度を<u>Hellinger距離</u>を用いて求める

<u>文献[4]において、高い検知精度</u>

$$D_H(p(x), q(x)) = \frac{\sqrt{\sum_x (\sqrt{p(x)} - \sqrt{q(x)})^2}}{\sqrt{2}}$$

- ✓ 0~1の範囲の値をとる
- ✓ 1に近いほど確率分布間の類似度は低い
- ✓ 0に近いほど確率分布間の類似度は高い

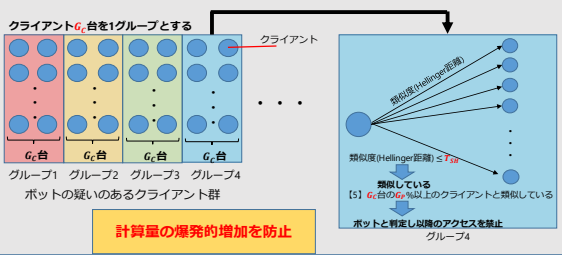


[4]Saravanan, R., Shanmuganathan, Y., Planichamy, Y.: Behavior-based detection of application layer distributed denial of service attacks during flash events, Turkish Journal of Electrical Engineering & Computer Sciences 24 pp.510-523 (2016).

2-3. Webページを要求するHTTPリクエスト送信間隔の類似度計算

文献[4]ではDDoS攻撃時に、ボットの疑いのある全てクライアント間で類似度の計算を行う

計算量の爆発的増加による<u>ボットのアクセス遮断の遅延</u>



計算量の爆発的増加を防止

提案手法のボット検知の流れ

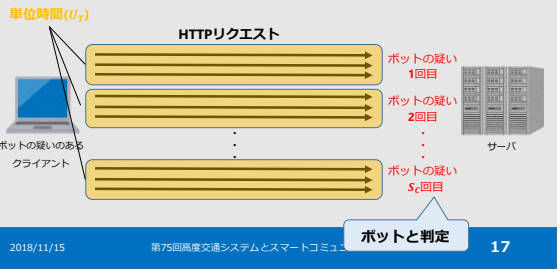
単位時間(U_T)毎に実行

1. 大量にHTTPリクエストを送信するクライアントをボットの疑いのあるクライアントとしてマーク
2. ボットの疑いのあるクライアント間における、Webページを要求するHTTPリクエスト送信間隔の類似性によるボット検知
3. 大量のリクエスト送信の継続性によるボット検知
   長期間に渡って大量にリクエストを送信するクライアントはボットと判断

3. 大量のリクエスト送信の継続性によるボット検知

長期間に渡って大量にリクエストを送信するクライアントはボットと判定

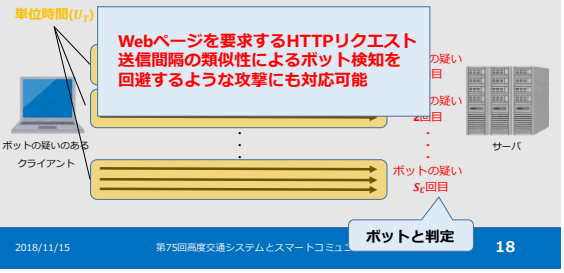
【6】S_C 回以上ボットの疑いのあるクライアントとして判定されればボットと判定し、
以降のアクセスを禁止する



3. 大量のリクエスト送信の継続性によるボット検知

長期間に渡って大量にリクエストを送信するクライアントはボットと判定

【6】S_C 回以上ボットの疑いのあるクライアントとして判定されればボットと判定し、
以降のアクセスを禁止する



[5]1998 World Cup Web Site Access Logs available at:http: //ita.ee.lbl.gov/html/contrib/WorldCup.htm (accessed 2018/10/23).
[6]GitHub - Markus-Go/bonesi: BoNeSi - the DDoS Botnet Simulator available at:https://github.com/Markus-Go/bonesi (accessed 2018/10/23).

評価・実験

目的

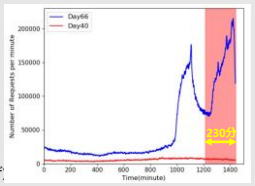
✓ 提案手法の検知精度の評価

方法

- 2つのデータセットに提案手法を適用

✓ **フラッシュイベント時のデータセット**
- 1998 FIFA World Cup[5]の66日目
- 約230分、63, 337 台のクライアント(ユーザ

✓ **DDoS攻撃時のデータセット**
- Bonesi[6]を利用してWebサーバに攻撃を実行した際に取得したトラフィック
- 60秒、30, 000台のボット



1998 FIFA World Cupの40日目と66日目におけるリクエスト数の推移

評価・実験

パラメータ

- $T_R = 4$ Webページに対するHTTPリクエスト数に関するしきい値
- $T_H = 0.3$ 類似度(Hellinger距離)に関するしきい値

1998 FIFA World Cupの40日目とBonesiを利用して取得したDDoS攻撃のトラフィックを用いてそれぞれ計算

- $U_T = 60$ 単位時間(秒)
- $S_C = 3$ 大量のリクエスト送信の継続性に関するしきい値
- $G_C = 10$ 類似度計算の際の1グループ当たりのクライアント数
- $G_P = 60$ 1グループ内のクライアント間の類似台数に関する割合(%)

適当な値に定めた

評価・実験

検知精度の評価指標

- Detection Rate(DR)とFalse Positive Rate(FPR)用いる
- DRの評価にはBonesiを利用して取得したDDoS攻撃のトラフィックを用いる
- FPRの評価には1998 FIFA World Cupの66日目の約230分を用いる

$$DR = \frac{TP}{TP + FN}$$

Detection Rate(DR)

ボットをボットとして正しく検知した割合

$$FPR = \frac{FP}{TN + FP}$$

False Positive Rate(FPR)

ユーザをボットとして誤検知した割合

記　号	定　義
True Positive(TP)	ボットをボットとして検知した数
True Negative(TN)	ユーザをユーザとして判定した数
False Positive(FP)	ユーザをボットとして検知した数
False Negative(FN)	ボットをユーザとして判定した数

評価・実験

実験結果

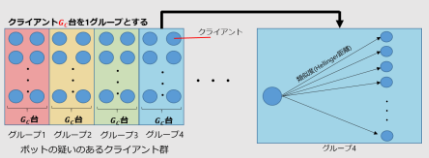
Detection Rate(DR)	False Positive Rate(FPR)
0.93	0.04

Detection Rate(DR)とFalse Positive Rate(FPR)の結果

DRが0.93、FPRが0.04
↓
提案手法は**十分な検知精度**を持つ
↓
DDoS攻撃とフラッシュイベントの識別が可能

クラスタリングを利用したボット検知の検討

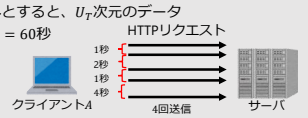
- 検知精度向上のためには、全てのボットの疑いのあるクライアント間で類似度計算が必要
  - 計算量の爆発的増加による**ボットのアクセス遮断の遅延**



クラスタリングを利用したボット検知の検討
- 計算量を抑えつつ、検知精度が向上するのではないか？

クラスタリングの対象となるデータの表現

✓ 現在の提案手法はWebページに対するHTTPリクエストの送信間隔の類似性
✓ クラスタリングの対象もWebページに対するHTTPリクエストの送信間隔
✓ クラスタリングには**k-means++法**を利用
✓ 単位時間U_Tとすると、U_T次元のデータ



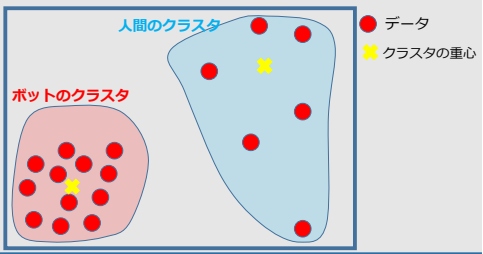
送信間隔1秒が観測された回数
送信間隔0秒が観測された回数

$$[0,2,1,0,1,0,0 \ldots, 0]$$

60次元

ボットのクラスタの判定方法

- ✓ 各クラスタ内において、データとクラスタの重心との距離の分散を利用する
  - ➢ 分散が小さいならば、ボットのクラスタ
  - ➢ 分散が大きいならば、人間のクラスタ



k-means++法を利用したクラスタリング結果

DDoS攻撃のデータセットに適用

- ✓ Bonesiを利用して作成
- ✓ 60秒間
- ✓ 30,000台のボット
- ✓ 29,888台のボットの疑いのあるクライアント
- ✓ $k = 3$

フラッシュイベントのデータセットに適用

- ✓ 1998 FIFA World Cupの66日目
- ✓ 60秒間
- ✓ 5,928台のクライアント
- ✓ 508台のボットの疑いのあるクライアント
- ✓ $k = 3$

k-means++法を利用したクラスタリング結果

DDoS攻撃のデータセット

アルゴリズム収束まで：22回

クラスタ名	クライアント数	重心からの距離の分散
Cluster 0	13,467	118.27
Cluster 1	8,594	165.40
Cluster 2	7,827	87.18

フラッシュイベントのデータセット

アルゴリズム収束まで：14回

クラスタ名	クライアント数	重心からの距離の分散
Cluster 0	86	282.76
Cluster 1	418	12.35
Cluster 2	4	1112.04

まとめ・今後の課題

まとめ

- ✓ **クライアントのHTTPリクエスト送信動作に着目したボット検知手法の提案**
  1. クライアント毎の単位時間当たりのリクエスト量
  2. Webページを要求するリクエスト送信間隔の類似性
  3. 大量のリクエスト送信の継続性
- ✓ **提案手法の検知精度の調査**
  - ➢ Detection Rate(DR)が0.93、False Positive Rate(FPR)が0.04
- ✓ **クラスタリングを利用したボット検知の検討**

今後の課題

- ✓ **パラメータを適切に設定する仕組み**
  - ➢ U_T, S_C , G_C, G_pは経験的に定めた
- ✓ **実際に観測されたDDoS攻撃のトラフィックを用いての評価実験**
  - ➢ 今回の評価実験にはBonesiを用いた
- ✓ **クラスタリングの対象となるデータの表現方法の更なる検討**