リアルタイムバースト検出手法を利用したパケット到着間隔による DDoS 攻撃検知手法の検討

臼崎翔太郎 * 橘弘智 * 有川佑樹 * 高塚佳代子 * 山場久昭 * 久保田真一郎 * 岡崎直宣 *
* 宮崎大学工学部

1 はじめに

DDoS(Distributed Denial-of Service) 攻撃による被害は年々増加傾向にあり，社会にとって大きな脅威となっている．IoT 機器からの DDoS 攻撃も確認されており被害がますます大きくなっていくことが予想されているが，効果的な攻撃検出手法がまだ存在しない．我々はデータストリームのバーストを検出する手法を DDoS 攻撃検知に利用することを考えた．本稿では，リアルタイムな解析を可能とし，大量のイベント発生に強いリアルタイムなバースト検出手法 [1] を利用し，DDoS 攻撃を検知する手法について検討した．本手法の有効性を確認するために評価実験を行い，検知精度について議論する．

2 リアルタイムバースト検出手法

リアルタイムなバースト検出手法 [1] はイベントの発生ごとにバーストを解析する手法である．バーストとは，直前の期間よりもイベント発生間隔が急激に狭くなっている状態を指す．この手法の利点はイベントの発生ごとに処理を行うことによりリアルタイムな解析を可能にしている点と，ある期間 W_{min} の間に集中したイベントデータを圧縮することにより大量のデータにも対応できる点である．我々は，これら 2 つの利点に着目し，この手法を利用した DDoS 攻撃検知手法を検討する．

2.1 Aggregation Pyramid

[1] で重要な Aggregation Pyramid と呼ばれるデータ構造を説明する．このデータ構造は N の階層を持っている．レベル h の階層には $N-h$ 個のセルが存在しており，新たにセルが生成されるたびに各階層の右側に追加されていく．ここでセルの終了時刻を t とすると，レベル h のセルは $c(h,t)$ と表現され，イベントの合計到着間隔 $gaps$，到着時刻 $arrt$，間隔個数 $gapn$ を保持する．イベントが発生するたびに，生のイベント情報を保持するレベル 0 のセル $c(0,t)$ を生成し，続いてレベル h のセル $c(h,t)$ を，$c(h-1,t-1)$ と $c(0,t)$ のセルデータを集約することで生成する．

2.2 バースト判定処理

バースト判定処理では，セル $c(h,t)$ が生成されるたびに，期間の重複していない直前のセル $c(N-1,t-1-h)$ とイベント平均到着間隔を比較する．以降このセルのことを $tgcell$ と呼ぶ．各セルを同じ状況で比較するためにイベント平均到着間隔関数 $avg(c(h,t)) = c(h,t).gaps/c(h,t).gapn$ を定義し，$avg(c(h,t))/avg(tgcell) \leq \beta$ の式を満たし，かつ，$c(h,t).gapn$ が過剰なバースト検出を抑制するパラメータ A_{min} 以上の場合にバーストが発生したと判断する．

本手法ではパケットの到着をイベントとしてその到着間隔を監視し，バーストを検出したら DDoS 攻撃であると判定する．

3 実験

3.1 提案手法の検知精度

本手法の攻撃検知精度を評価する．実験データとして，MIT Lincoln Laboratory が人為的に作成した DDoS 攻撃のデータセットである DARPA2000[2] を用いた．

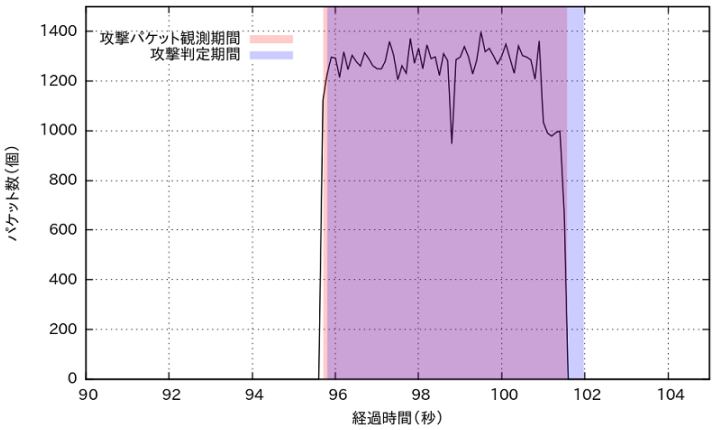

図 1: DARPA2000 の Phase 5 における攻撃パケット観測期間と提案手法による攻撃判定期間

DARPA2000 のシナリオは，ある組織のホストを踏み台にし，攻撃ツールを用いて，別の組織に DDoS 攻撃を仕掛けるまでの 5 段階のフェイズを想定している．我々は DDoS 攻撃パケットが含まれているフェイズ 5 のキャプチャデータのうち，組織のファイアウォールの内部で観測された inside データと外部で観測された dmz データの両方で評価を行った．提案手法のパラメータを $N = 50, \beta = 0.1, W_{min} = 0.1, A_{min} = 100$ に設定して評価実験を行った結果を図 1 に示す．紙面の都合上 inside データの結果のみを示している．横軸の経過時間とはキャプチャデータのうち最初に観測されたパケットの到着時刻からの経過秒数である．図 1 を見ると，攻撃パケットを最初に観測した時刻と提案手法で判定された攻撃開始時刻が非常に近いことから，攻撃開始のタイミングは高い精度で判定できていることが分かる．一方，攻撃終了のタイミングはやや遅れている．これは，$tgcell$ に攻撃開始前の期間も含まれたために，$avg(tgcell)$ が実際の攻撃期間の平均到着間隔より大きくなり，攻撃終了直後のそれとの差が大きくなったためと思われた．

4 まとめ

本稿ではリアルタイムなバースト検出手法を利用した DDoS 攻撃の検知手法を検討した．評価実験の結果，有効なパラメータ値を設定すれば正しく DDoS 攻撃検知ができることが分かった．しかし，パケット到着間隔は攻撃の規模や各組織のパケット流入量によって異なることから，有効なパラメータ値は異なることが予想される．そのため，将来的には適切なパラメータ値を自動的に獲得する仕組みが望まれる．

参考文献

[1] 蛯名 亮平，中村 健二，小柳 滋．”リアルタイムバースト検出手法の提案”，日本データベース学会論文誌，Vol.9，No.2，2010 年
[2] MIT : DARPA Intrusion Detection Evaluation Data Set．https://www.ll.mit.edu/ideval/index.html