ICN におけるホワイトリストを用いた DDoS 攻撃の防御

Preventing DDoS Attack Using White List in ICN

内田 亘彦 [1]　上山 憲昭 [1]　山本 幹 [2]
Nobuhiko Uchida　Noriaki Kamiyama　Miki Yamamoto
[1] 福岡大学 工学部 電子情報工学科　[2] 関西大学 システム理工学部
Faculty of Engineering, Fukuoka University　Faculty of Engineering Science, Kansai University

1. はじめに

IoT ではキーワードなど曖昧な名前でデータが要求されるため，通信に先立つ名前解決が困難であり，名前を用いてパケットを転送する新しいネットワークとして情報指向ネットワーク (ICN: Information-centric Networking) が注目されている．ICN ではコンテンツ名を元に要求を行い，コンテンツの転送経路上のルータにてコンテンツをキャッシュし，要求パケット (Interest) の転送経路上のルータに要求コンテンツがキャッシュされている場合は，そのルータからコンテンツを配信する．また Interest の到着ポート番号をルータの PIT (Pending Interest Table) で記録し，PIT の記録に沿ってコンテンツを転送することによって，名前に基づくパケットの転送を可能としている．しかし，大量の悪意のある要求を転送することで，ルータの PIT に無効なエントリを注入し，PIT の機能低下を狙う DDoS 攻撃 (Distributed Denial of Service attack) が問題となる．そこで本稿では ICN の DDoS 攻撃を防ぐために，攻撃者のものと思われる要求をコンテンツ提供者が判断し，ネットワーク上のルータに正常なコンテンツ名をホワイトリスト (WL: White List) として配布し，ネットワークの入り口にて攻撃パケットを遮断する防御法を提案する．

2. 関連研究

ICN ルータの PIT では，受信 Interest の Prefix と到着ポート番号を記録し，コンテンツを返送する際に該当エントリを削除する．タイムアウト時間内にデータが返送されなかった場合も PIT のエントリを削除する．DDoS 攻撃では本機能を悪用し，実際には存在しないコンテンツの要求を大量に送ることで，PIT 内にタイムアウトになるまで大量のエントリが残留する結果，PIT の容量が不足し，正常なサービスが妨害される．

この問題に対して多くの研究がなされてきたが，ルータに到着する要求に対してコンテンツがユーザへ返送された比率 ISR (Interest Satisfaction Ratio) [1] や，各ルータの PIT の容量に対する PIT の使用率 PUR (PIT Utilization Ratio) [2] を測定し，設定した閾値を超えた場合に該当する Prefix に対する Interest を全て棄却するものが多い．しかし閾値を小さくしすぎると誤検出により正常ユーザの要求に対して規制が及ぶ可能性が発生するため，防御効果と正常ユーザの巻き添え率とのトレードオフを考慮する必要があり，閾値の適切な設定は難しい．そこで本稿では閾値を設定することなく，正常要求の巻き添えを回避しながら攻撃要求にのみ規制をかける方式を提案する．

3. 提案検知・防御方式

提案方式の手順を図 1 で示す．

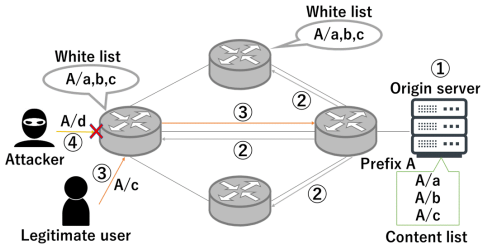

図 1: 提案方式の手順

1. 標的となるオリジンサーバ (Prefix A を管理，コンテンツ識別子 a，b，c を保有) が自身が保有していないコンテンツの要求を受信した時 DDoS 攻撃を検知
2. オリジンサーバは，Prefix A に含まれるコンテンツ識別子のリスト (WL) をネットワーク上の全ルータに送付
3. WL を受信したルータは，以後，Prefix A を含む要求を受信した場合，WL を照合し，WL 内に存在するコンテンツに対しては転送テーブルに従い次ホップのルータに転送
4. 実在しないコンテンツの要求であった場合，要求を破棄

提案方式では，オリジンホストで攻撃を検知するため，閾値を設定する必要がなく前述のトレードオフが発生しない．また攻撃の初期段階での検知が可能であり，WL 配布後はネットワークの入り口のエッジルータで攻撃 Interest を棄却するため，正常ユーザの巻き添えを回避しつつ攻撃を最大限，防御できるメリットがある．

4. 性能評価

ICN における DDoS 攻撃を ISP ネットワークトポロジ Allegiance Telecom(ノード数 53，リンク数 88) を用いた計算機シミュレーションにより行い，提案方式の有効性を評価する．攻撃対象とする Prefix を Allegiance Telecom のシアトルに位置するノードとし，シミュレーションにおけるコンテンツ数を 10,000 個，キャッシュ容量を 50，PIT 容量を 100，コンテンツの要求をパラメタ $\theta = 0.8$ の Zipf 分布に従う確率でランダムに選択したコンテンツに対し行う．またシミュレーション時間を 10 秒，測定開始時間を 1 秒，攻撃発生時間を 3 秒から 6 秒，PIT のタイムアウト時間を 4 秒とし，要求の発生間隔は正常ユーザと攻撃者のどちらも，平均が 1ms の指数分布に従う．コンテンツのキャッシュ方式は，配信経路上の全ルータでキャッシュを行う AllCache を用いる．

提案方式の性能評価のため，(1)DDoS 攻撃が発生しない状況，(2)DDoS 攻撃が発生した状況，(3)DDoS 攻撃が発生して提案方式を適用した状況，の 3 パターンを比較する．

図 2(a) に，各ルータの PIT 使用率 (PIT 容量に対するエントリ数の比率) の平均値を，時間に対してプロットする．DDoS 攻撃が発生した場合，DDoS が開始された 3 秒目からルータ全体の平均 PIT 使用率は増加し，タイムアウトを迎える 7 秒目から減少している．しかし提案方式を用いることで，平均 PIT 使用率は通常時とほぼ変わらない値となり，PIT 使用率の増加を抑制できる．

図 2(b) に，DDoS 攻撃発生期間における各ルータの平均 PIT 使用率の累積分布をプロットする．DDoS 攻撃発生時は約 30% のノードでルータの平均 PIT 使用率は 0.6 を超えるが，提案方式を用いることで，正常時の累積分布に近づき，ルータの PIT 使用率の増加が抑えられることが確認できる．

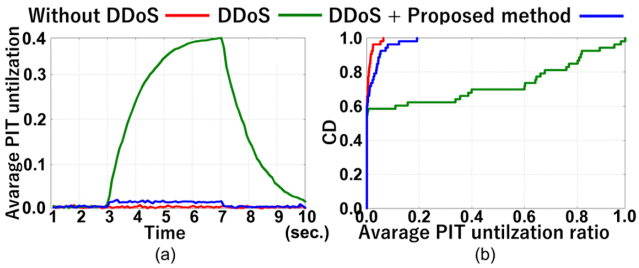

図 2: 平均 PIT 使用率の (a) 時系列と (b) 累積分布

5. まとめ

本稿では ICN における DDoS 攻撃に対し，正常ユーザの巻き添えを回避しつつ効果的に攻撃を防御する方式として，コンテンツ提供者の検知に基づく WL 配布による防御方式を提案し，ISP ネットワークトポロジを用いた計算機シミュレーションによって性能評価を行った．その結果，提案方式は DDoS 攻撃の影響を大きく軽減することを確認した．今後は，WL の実装方法について研究を行いたい．

謝辞　本研究成果は，JSPS 科研費 18K11283 の助成を受けたものである．ここに記して謝意を表す．

参考文献

[1] Alberto Compagno, Mauro Conti, Paolo Gasti, Gene Tsudik, “Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking”, August, 2013
[2] Hani Salah, Julian Wulfheide, Thorsten Strufe, “Coordination Supports Security: A New Defence Mechanism Against Interest Flooding in NDN”, October, 2015