モバイルエージェントを用いたSYN Flood攻撃に対する分散型検知手法

成田 匡輝† 加藤 貴司† ベッド バハドゥール ビスタ† 高田 豊雄†

†岩手県立大学 ソフトウェア情報学研究科
020-0193 岩手県岩手郡滝沢村滝沢字巣子 152 番地 52

g231h201@edu.soft.iwate-pu.ac.jp, {t-kato, bbb, takata}@iwate-pu.ac.jp

あらまし 近年のインターネットにおけるSYN Flood攻撃による被害は甚大であり, その影響は大規模な商用サイトから個人ユーザにまで及んでいる. ネットワーク管理者は自らの管理するネットワークを保護するため, また, 管理するネットワークから意図せず攻撃者を出さないようにするため, こうした攻撃の最新の攻撃動向を知ることが必要である. 本稿では, SYN Flood攻撃が行われた際に痕跡として残るbackscatterに着目し, SYN Flood攻撃の動向をモバイルエージェントシステムを用いて検知する分散型検知手法を提案する. また, 仮想ネットワークによる評価実験を通じて, 本手法の有効性を示す.

A Distributed Detecting Method for SYN Flood Attacks Using Mobile Agents

Masaki Narita† Takashi Katoh† Bhed Bahadur Bista† Toyoo Takata†

†Iwate Prefectural University, Graduate School of Software and Information Science
152-52 Sugo, Takizawa, Iwate 020-0193 Japan

g231h201@edu.soft.iwate-pu.ac.jp, {t-kato, bbb, takata}@iwate-pu.ac.jp

Abstract In recent years, the damage caused by SYN Flood attacks is real and has caused substantive problems. Such threat is widespread from major commercial sites to individual users. Therefore, it is important for network administrators to achieve a means to comprehend the latest trend of SYN Flood attacks for protecting their network and preventing from generating SYN Flood attackers unknowingly within their network. In this paper, we propose a distributed detecting method for SYN Flood attacks using mobile agents by focusing backscatter. Then, we show the effectiveness of our proposal by detecting SYN Flood attack in virtual network of simulation environment.

1 はじめに

近年のインターネットにおけるSYN Flood攻撃の被害は甚大であり, 無視できないものとなっている. Mooreらの研究によれば, 攻撃の標的は大規模な商用サイトから個人ユーザにまで及んでおり [1], インターネットユーザの誰もが攻撃被害に合う可能性がある. こうした状況から, ネットワーク管理者が最新のDoS攻撃の動向を把握できる手段を持つことは重要であると考えられる.

また最近では, たとえ攻撃する意思がなくとも, 攻撃に使われたコンピュータのユーザに対し, 厳しい目が向けられるようになってきている. 最新の攻撃動向を知ることは, 管理するネッ

トワークからの攻撃を早期検出するという目的からも有用である.

そこで本稿では, モバイルエージェントを用いた SYN Flood 攻撃に対する分散型検知手法を提案する. 本手法により, ネットワーク管理者は, 管理するネットワークを保護するための対策を立てることが可能となる.

2 SYN Flood 攻撃

SYN Flood 攻撃とは DoS (Denial-of-Service) 攻撃の一種であり, TCP コネクションの確立手順を悪用し, サーバリソースの枯渇を狙った攻撃である.

正常な TCP コネクションの確立手順では, 例としてホスト A とホスト B が通信を開始する場合, 図 1 のように, 1) ホスト A が SYN パケットを送信, 2) ホスト B が SYN/ACK パケットを返信し, 3) ホスト A が ACK パケットを送信する 3-way handshake が行われる.

SYN Flood 攻撃は, この 3-way handshake を悪用した攻撃であり, その概要を図 2 に示す. 攻撃者は送信元 IP アドレスを詐称した大量の SYN パケットを攻撃対象ホストへ送信する. 攻撃対象ホストは, 詐称された送信元 IP アドレスへ SYN/ACK パケットを返信してしまう. これにより, 攻撃対象ホストは多数の無関係なホストとハーフオープンな回線を維持することとなり, サーバリソースを大量に消費してしまう.

SYN Flood 攻撃において送信元 IP アドレスがランダムに詐称された時, backscatter と呼ばれる跳ね返りパケットが, 無関係なホストへ極めてスパースに到着することが知られている. このパケットの情報を取得することで, SYN Flood 攻撃が検知可能となる.

3 関連研究

backscatter の観測による SYN Flood 攻撃検知の研究はすでに行われており, その手法は二つに分類される. 一つはインターネット上のルータを監視することで backscatter を観測するルータ型検知手法であり, もう一つはインターネット上に複数のセンサを配置し, backscatter を観測する分散型検知手法である.

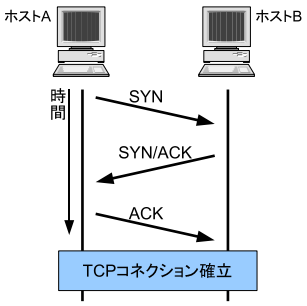

図 1: 3-way handshake

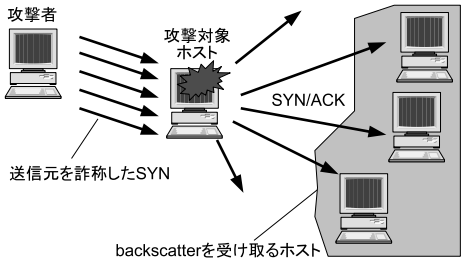

図 2: SYN Flood 攻撃の概要

3.1 ルータ型検知手法

インターネット上のルータを監視することで, SYN Flood 攻撃を検知する研究としては, Kompella らによる手法 [2] や Wang らによる手法 [3] が挙げられる.

しかし, これらの手法には, 以下 3 つの問題が挙げられる. 1) 監視しているルータを経由しない backscatter は観測することができない. 2) 一般に管理者権限がなくてはルータにアクセスできないため, 一般的なユーザが攻撃の情報を集めるのは困難である. 3) SYN Flood 攻撃において送信元 IP アドレスが一様ランダムに詐称された時, ルータを通過する backscatter の総量は, そのネットワークの大きさに比例する. ルータ内のネットワークが小規模の場合, 検出できる backscatter の量が制限されてしまう.

3.2 分散型検知手法

SYN Flood 攻撃の分散型検知手法の一例としては, 警察庁の定点観測システム@Police [4] が挙げられる. このシステムでは, backscatter をインターネット上の複数のセンサで観測する. 観測結果は Web 上で一般に公開されるが, このような組織が提供する情報は攻撃の概要であったり, 断片的な情報に留まることが一般的である. また, それらの情報は最新のものでないことも多いため, 最新の攻撃動向の情報をネットワーク管理に活かすことは難しい.

4 SYN Flood 攻撃に対する分散型検知手法の提案

本稿では backscatter を, ACK が返されない SYN/ACK パケットと定義する.

インターネットに直接接続されていれば, どのホストにも backscatter が到着する可能性はある. しかし, 単一のホストに backscatter が到着したことを検知できた場合でも, 同様の backscatter が他のネットワークでも観測されているかを確認することは極めて困難である. また, 攻撃者が一様ランダムに送信元 IP アドレスを詐称した場合, backscatter は攻撃発生時において, インターネット上に極めてスパースに広がることが多い. すなわち, 単一のホストだけで得られる情報では, 情報が少なくなるため, 攻撃の動向を検知するのは非常に困難である.

そこで, 複数のホスト間で backscatter 情報を収集することができれば, SYN Flood 攻撃の動向を検知できると考えられる. 本稿では, backscatter 情報を分散された複数のホストから収集し, SYN Flood 攻撃の動向を検知する分散型検知手法を提案する. 我々の手法は, 以下の 3 つのステップで構成される.

1. まず, 各ホストで tcpdump 等のネットワークモニタリングソフトウェアで取得したパケットログから backscatter 情報 (表 1) を抽出する. backscatter 情報は, 1) backscatter を受信した時間, 2) 攻撃対象ホストと攻撃対象サービスを意味する送信元 IP アドレスと送信元ポート番号, 3) 送信先 IP アドレスや送信先ポート番号といった情報で構成される.

2. 次に, このように抽出された backscatter 情報を分散された複数のホストから収集する. 情報の収集は, 特定の時間間隔毎に送信元ホスト, つまり攻撃対象となったホストから到着する backscatter をカウントする. 表 2 は我々の提案に基き, backscatter 情報を収集した一例である. この例では, 5 分間隔毎に backscatter の集計を行っている. backscatter 情報のカウントの際, 同様の backscatter が他の観測点でも観測されているかを確認するため, 同様の backscatter が観測された観測点数も同時にカウントする. これをユニーク観測点数と呼称する. この情報を用いることで, ある送信元からの backscatter の合計がユニーク観測点数に近ければ, 送信元 IP アドレスをランダムに詐称した SYN Flood 攻撃が行われていると推測できる.

3. 最後に, 収集結果を解析することで SYN Flood 攻撃の動向を検知する.

前節で述べた既存のルータ型検知手法では, 広域のネットワークから backscatter 情報を収集することは困難であるのに加え, 個人ユーザが backscatter 情報を入手することが難しいという問題もある.

また, @Police のような既存の分散型検知手法は, 固定観測点を使用しており, 常に同じ場所を観測することとなる. これにより, backscatter を観測できるアドレス範囲は制限されてしまう.

我々の提案する手法では, インターネット上のどのホストも観測点となりうるため, 理論上インターネットのいたるところで backscatter の観測が可能である. ゆえに, 個人ユーザまでもが広域の最新の攻撃動向を知ることができる.

5 実装と提案の有効性評価

本手法の有効性を示すため, 仮想ネットワーク上で発生させた SYN Flood 攻撃を検知する評価

表 1: backscatter 情報

タイムスタンプ	backscatter の受信時刻
送信元 IP アドレス	攻撃対象ホスト
送信元ポート番号	攻撃対象サービス
送信先 IP アドレス	詐称 IP アドレス
送信先ポート番号	攻撃者のポート番号

表 2: backscatter 情報の収集の一例

計測時間	攻撃対象:サービス	パケット数
08/1/30 8:30	111.11.0.2:135	5
	123.123.0.3:80	50
08/1/30 8:35	111.11.0.2:135	10
08/1/30 8:40	111.11.0.2:135	15
08/1/30 8:45	···	···
···	···	···
ユニーク観測点数		
111.11.0.2		30
123.123.0.3		1

実験を行なった. backscatter 情報の共有手段には, 分散型インターネット観測システム ABLA (Agent-Based Log Analyzing System) [5] を想定した. この節では, まず ABLA の概要と実験環境について述べる. その後, 評価実験の結果について考察する.

5.1 ABLA

ABLA は我々が研究・開発を行なっている個人参加型のインターネット観測システムである (図 3). 本提案手法の実装に ABLA を採用した理由は, ABLA が既存のルータ型検知手法では困難な, 広域に分散されたホストから情報を収集する手段として最適であると考えられるためである.

ABLA では, インターネット上に P2P ネットワークを構築し, 各ノードがネットワークパケットのログを提供する. そしてモバイルエージェントが各観測点を移動し, 観測点上のログ情報を解析・収集する. ABLA ネットワークへは任意の参加・離脱が可能であり, 動的かつ多数の観測点を確保できる.

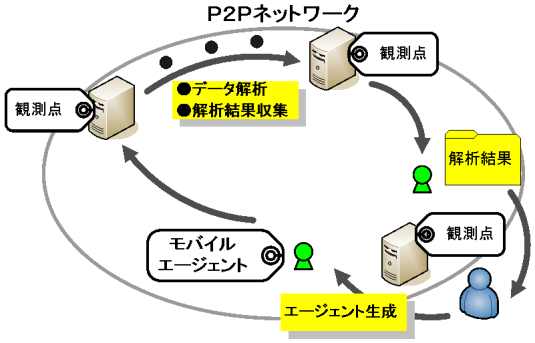

図 3: ABLA 概要

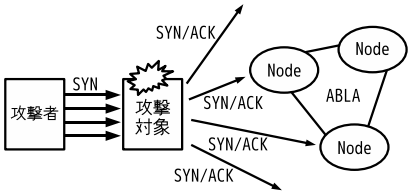

図 4: 提案手法の概要

5.2 提案の実装

実装は, ABLA に新しく追加モジュールを加えることで行なった. この実装により, ABLA ユーザはモバイルエージェントに SYN Flood 攻撃の動向を検知するため, backscatter 情報を収集・解析するように要求を出すことが可能となる. ABLA を用いた本提案手法の概要を図 4 に示す.

5.3 実験内容とその手順

本実験では, 特定の攻撃規模や攻撃トラフィックパターンの SYN Flood 攻撃を発生させ, ABLA ノードの巡回数を変化させることで, SYN Flood 攻撃の時間推移が把握可能かを検証した.

まず最初に, ネットワークシミュレータを用いて実験で使用するログを取得した. ネットワークシミュレータには 'Yet Another Network Simulator [6]' を用いた. シミュレータ上には実験用ネットワーク (図 5) を構築する. このネットワークには, 60,000 台のホストを設置した観測対象ネットワーク, 攻撃者, 攻撃対象がそれぞれ所属するネットワークを設定した. 観測対象

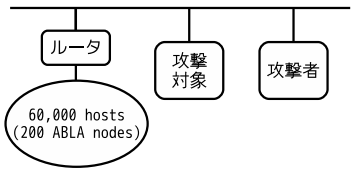

図 5: 実験用ネットワーク

ネットワークには, ABLA ノードを 200 台設置し, 到着するパケットのログを取得した.

次に, 上記手順で取得したログを用いて, SYN Flood 攻撃の検知シミュレーションを行なった.

5.4 実験時のパラメータ設定

Moore [1] らによれば, DoS 攻撃の全体の 60%が 10 分以内に終了し, 全体の 85%が 1 時間以内に終了しているとされている. そこで本実験では, 攻撃継続時間を 30 分と設定した.

攻撃トラフィックパターンは, 2 種類を想定した. 攻撃トラフィックパターン 1 は, 時間経過とともに攻撃パケット数が増加していく攻撃であり, 攻撃トラフィックパターン 2 は, 30 分の間に 2 度攻撃パケット数が急増する攻撃である.

攻撃検知のための ABLA ノードの巡回数は 25, 50, 75, 100 ノードと変化させた.

攻撃規模は 1 秒間に 120 万, 100 万, 60 万パケットの 3 種類を想定した. それぞれの攻撃規模に対応する, backscatter 到着率は, 0.50, 0.40, 0.25 である. backscatter 到着率とは, backscatter が攻撃継続期間を通して 1 つのホストに 1 つ以上到達する確率である.

5.5 実験結果と考察

評価実験は, 情報収集を行うノードをランダムに変化させ, それぞれ 10 回行なった. 実験結果は 5 分毎の平均値である.

到着率 0.50 での検知結果 (図 6 右, 図 9 右) backscatter 情報を, 100, 75, 50 ノードから収集した場合, いずれの攻撃トラフィックパターンにおいてもルータのトラフィックに近似した理想的な検知結果が得られた. 25 ノードから情報を収集した場合は, 攻撃のピーク検出がやや曖昧になっているものの, いずれの攻撃トラフィックパターンの場合も攻撃の時間推移を把握できている.

到着率 0.40 での検知結果 (図 7 右, 図 10 右) backscatter 情報を, 100, 75, 50 ノードから収集した場合, いずれの攻撃トラフィックパターンにおいても理想的な検知結果が得られている. 25 ノードから情報を収集した場合でも, トラフィックパターン 1 においては, 問題なく攻撃の時間推移を検知できている. しかし, トラフィックパターン 2 において情報収集を行うノード数を 25 ノードとした時, 攻撃の 2 度目のピーク時を検知できていない.

到着率 0.25 での検知結果 (図 8 右, 図 11 右) backscatter 情報を, 100, 75 ノードから収集した場合, 取得できたパケット数は少ないがいずれの攻撃トラフィックパターンにおいても攻撃の時間推移を検知できている. トラフィックパターン 1 において, 50, 25 ノードから情報を収集した場合, どちらも攻撃のピーク時を検知できていない. トラフィックパターン 2 で 50 ノードから情報を収集した場合は, 攻撃の最初のピーク時を検出できていない. また, トラフィックパターン 2 で 25 ノードから情報を収集した場合, グラフが横ばいとなり, 攻撃の時間推移の検知が困難であった.

結論として, 攻撃規模 60 万 packets/sec, すなわち, 到着率 0.25 における一部の検知結果を除き, 想定した攻撃トラフィックパターンに類似した攻撃検知結果を得ることができた. これらのことから, 提案手法による攻撃検知は有効であるといえる.

6 まとめと今後の課題

本稿では, モバイルエージェントを用いた SYN Flood 攻撃に対する分散型検知手法を提案した. また, 仮想ネットワーク上で SYN Flood 攻撃の検知実験を行い, その有効性を示した. これに

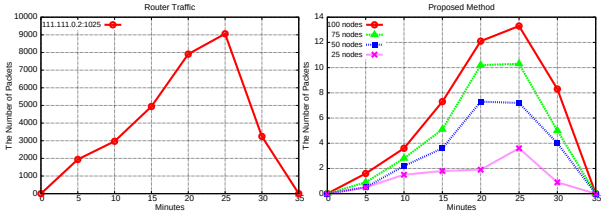

図 6: 到着率 0.50 の攻撃検知結果 (トラフィックパターン 1)

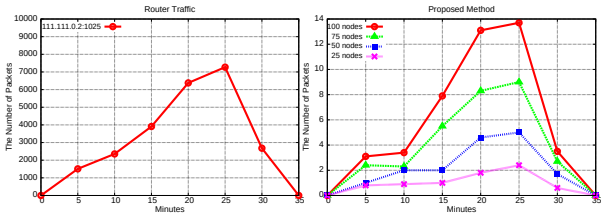

図 7: 到着率 0.40 の攻撃検知結果 (トラフィックパターン 1)

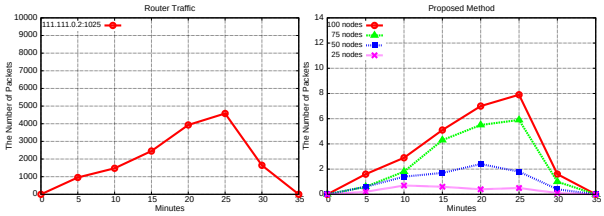

図 8: 到着率 0.25 の攻撃検知結果 (トラフィックパターン 1)

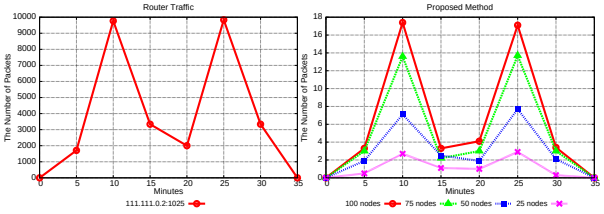

図 9: 到着率 0.50 の攻撃検知結果 (トラフィックパターン 2)

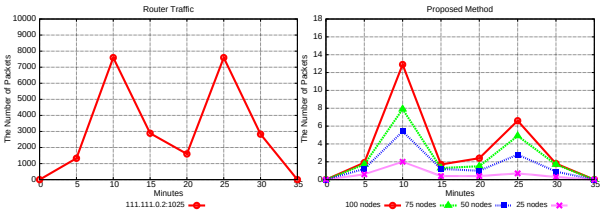

図 10: 到着率 0.40 の攻撃検知結果 (トラフィックパターン 2)

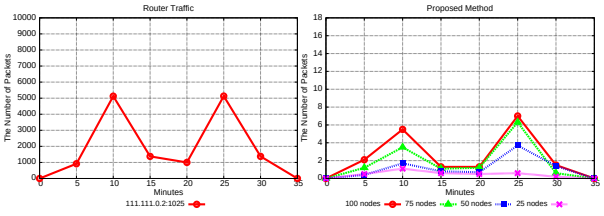

図 11: 到着率 0.25 の攻撃検知結果 (トラフィックパターン 2)

より, 小規模なネットワーク管理者が最新の攻撃動向の情報を, 管理するネットワークを保護するための対策に役立てることが期待できる.

今後の課題としては, 本手法のインターネット上での運用実験が挙げられる. また他の課題として, backscatter の収集結果に対する解析の自動化手法の検討が考えられる. 具体的には, 攻撃発生時のアラートの自動発生等が挙げられる.

本研究は一部科研費 (基盤研究 (C)20500072) 及び 若手 (B) 21700084) の助成を受けたものである.

参考文献

[1] Moore, D., Shannon, C., Brown, D.J., Voelker, G.M., Savage, S.: Inferring Internet Denial-of-service Activity, *ACM Transactions on Computer Systems (TOCS)*, Vol. 24, Issue. 2, pp. 115–139 (2006).

[2] Kompella, R.R., Singh, S., Varghese, G.: On Scalable Attack Detection in the Network, *IEEE/ACM Transactions on Networkin*, Vol. 15, Issue. 1, pp. 14–25 (2007).

[3] Wang, H., Zhang, D., Shin, K.G.: Change-point Monitoring for the Detection of DoS Attacks, *IEEE Transactions on Dependable and Secure Computing*, Vol. 1, Issue. 4, pp. 193–208 (2004).

[4] @Police, SYN flood 攻撃被害観測システム. `http://www.cyberpolice.go.jp/server/rd_env/pdf/synflood_detect.pdf`.

[5] 葛野弘樹 他：モバイルエージェントを用いた分散型インターネット観測システムの提案, 情報処理学会論文誌, Vol. 47, No. 5, pp. 1393–1405 (2006).

[6] Yet Another Network Simulator. `http://yans.inria.fr/`