動的観測点を利用したSYN Flood攻撃検出手法とその有効性評価について

成田 匡輝† 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@s.iwate-pu.ac.jp, {bbb, takata}@iwate-pu.ac.jp

あらまし サイバー攻撃による経済的損失や社会的信用の失墜を防ぐため，インターネット観測システムを利用した，攻撃の早期検出が行われている．しかし近年，インターネット上に配置した観測点への位置特定攻撃が問題になっている．観測点の配置位置の外部への露呈は，観測点の迂回等による観測性能の低下につながる．そこで我々は，攻撃者による観測点の迂回を困難にするため，多数の組織間で広域分散的に動的に観測点を確保することで攻撃を検出するという手法を提案してきた．本稿では，我々の動的観測手法を用いた，SYN Flood 攻撃の検出手法と実際のインターネット上で取得されたパケットを基にした，上記手法の攻撃検出性能を示す．

A Detecting Method of SYN Flood Attacks Using Dynamic Sensors and Availability Evaluation Results

Masaki Narita† Bhed Bahadur Bista† Toyoo Takata†

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

g231h201@s.iwate-pu.ac.jp, {bbb, takata}@iwate-pu.ac.jp

Abstract To detect cyber attacks which cause financial loses, the Internet threat monitoring system is developed. However, attackers have devised a technique which locates sensors' position recently. If the location of sensors is revealed by attackers, bypassing sensors becomes easier and the efficiency of the system is critically decreased. Thus, we have proposed a method for detecting SYN Flood attacks using dynamic sensors deployed by multiple organizations widely spread in the Internet. In this paper, we evaluate our method based on the actual network packets captured on the Internet and demonstrate the prospective detection performance.

1 はじめに

インターネットに接続するすべてのコンピュータは，常にサイバー攻撃の危険に晒されている．Symantec 社によれば，2009 年にサイバー攻撃を経験した米企業は，全体の 75%にも上る [1].

サイバー攻撃の一例として，DoS (Denial-of-Service) 攻撃がある．DoS 攻撃とは，インターネット上で稼働しているサーバが提供するサービスを妨害，あるいは停止させる攻撃である．

近年，DoS 攻撃は大規模化し，悪意あるユーザに操られたコンピュータ (ボット) で構成されるボットネットを用いた DDoS (Distributed Denial-of-Service) 攻撃が主流となっている [2].

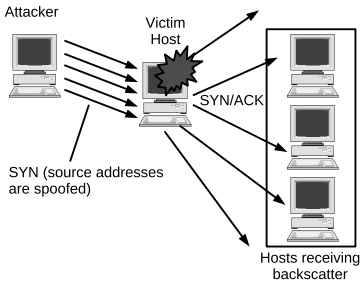

図 1: SYN Flood 攻撃の概要

この DDoS 攻撃の標的となった企業の経済的損失は，もはや無視できない金額となっている．

一方，管理しているネットワークに侵入を許すことにより，ボットを輩出し，意図せず DDoS 攻撃の加害者となる可能性もある．攻撃への加担は社会的信用の失墜につながるため，ネットワーク管理者には，自らの管理するネットワークからボットを輩出しないことも重要となる．

このことから，サイバー攻撃を早期検出することを目的とした，インターネット観測システムが研究されている．しかし，攻撃手法の進歩により，既存の固定観測式のシステムが攻撃者によって迂回される問題が指摘されている．そこで我々は，動的観測点による分散型インターネット観測システムを用いて DoS 攻撃の 1 種である，SYN Flood 攻撃を検出する手法を提案してきた [3].

本稿では，我々の動的観測手法を用いた，SYN Flood 攻撃の検出手法と実際のインターネット上で取得されたパケットを基にした，上記手法の攻撃検出性能を示す．

2 SYN Flood 攻撃

2.1 TCP コネクションの確立手順 我々が検出対象とする SYN Flood 攻撃について述べるため，まず TCP コネクションの確立手順を述べる．TCP コネクションの確立手順はスリーウェイハンドシェイクと呼ばれる．ここでは説明のため，ホスト A がホスト B に対し TCP による通信を開始する状況を想定する．始めに，ホスト A がコネクションの確立要求のため，ホスト B に SYN パケットを送信する．ホスト B は，コネクションの確立要求の承認とホスト A へのコネクションの確立要求のため，SYN/ACK パケットをホスト A に返信する．最後に，ホスト A はホスト B へコネクションの確立要求の承認のために ACK パケットを送信する．これにより，TCP コネクションは確立される．

2.2 SYN Flood 攻撃の概要と特徴 SYN Flood 攻撃は，上記 TCP コネクションの確立手順を悪用した攻撃である (図 1)．攻撃者は，送信元を詐称した大量の SYN パケットを犠牲 (攻撃対象) ホストに送信する．通常，犠牲ホストは，受信したパケットの送信元が正当なものであるかどうかは判断できず，送信元が詐称されていてもパケットを返信する．

犠牲ホストは，多数の無関係なホストとコネクションの確立を試み，詐称された大量の送信元からの返信を待つことで，リソースを浪費する．犠牲ホストのリソースの浪費は，応答速度の低下や OS の機能停止等を引き起こし，提供中のサービスの質は著しく低下する．

SYN Flood 攻撃においては，犠牲ホストが詐称された送信元にパケットを返信するため，犠牲ホストが返信したパケットが無関係なホストに到着する．この犠牲ホストによる返信パケットは backscatter と呼ばれており，このパケットを観測できれば SYN Flood 攻撃を検出できる．

3 関連研究

インターネット観測システムによる SYN Flood 攻撃検出に関する研究には，警察庁が運用する @Police [4]，NICT が運用する nicter [5]，IPA が運用する TALOT2 [6]，多国間で固定観測点の情報を共有する WOMBAT [7] 等がある．特に@Police は，57ヵ所の固定観測点を全国の警察関係施設に配置し，backscatter の観測に特化したシステムを運用している．

これらの問題点は，観測点の配置位置がほぼ固定されている点である．近年，インターネット上に配置された固定観測点が容易に検出可能であることが知られている [8, 9]．攻撃者が意図的に固定観測点を迂回して攻撃を行った場合，攻撃検出精度が低下する可能性がある．また，攻撃者が意図的に無意味なトラフィックを観測点

に対して送出することによる，観測の妨害も可能となる．

4 SYN Flood 攻撃の分散型検出手法

backscatter はインターネット上に配置されたどのホストにも到着しうる．本研究では，通常のスリーウェイハンドシェイク手順を経ることなく到着する，SYN パケット以外の TCP パケットを backscatter と定義する．本節では，分散された複数のホストから backscatter に関する情報を収集し，大規模な SYN Flood 攻撃を検出する手法を述べる．

4.1 我々の攻撃検出手法　本手法では，小規模なネットワーク管理者の有志によりインターネット上に配置された観測点を利用することで，分散された複数のホストによる backscatter の観測を行う．各観測点は，グローバル IP アドレス上で，他の観測点との通信にのみ応答する，受動的な観測点として動作する．本手法では，backscatter によるパケットの送信元 IP アドレス (犠牲ホスト) と送信元ポート番号 (犠牲サービス) の情報に backscatter の受信時刻を付加した情報を backscatter 情報とする．また，複数の観測点から backscatter 情報を収集する手段には，モバイルエージェントを用いる．モバイルエージェントに情報収集を依頼する形式をとることで，利用する観測点の IP アドレスを意識する必要がなくなり，観測点の所在を隠蔽しながらの情報収集が可能となる．我々の攻撃検出手法は，以下の 3 つの手順で構成される．

(1) 分散された複数の観測点において，攻撃検出に利用する backscatter 情報を抽出する．各観測点では，パケットモニタリングツールでパケットの記録を行っているものとする．

(2) (1) で抽出した backscatter 情報を複数の観測点から収集する．本手法では，SYN Flood 攻撃の発生調査を行う取得済みネットワークログの調査時間範囲を設定し，モバイルエージェントが複数の観測点を巡回することで情報を収集する．backscatter 情報の収集は，犠牲ホストに対応する backscatter によるパケット数を集計することで行う．表 1 は収集の一例である．

表 1: backscatter 情報の収集例

犠牲ホスト	犠牲サービス
backscatter	固有観測点数
Latest Timestamp	Oldest Timestamp
111.111.0.2	80
20 packets	20 sensors
30-Aug-2010 8:45	30-Aug-2010 6:30
111.111.0.3	28
20 packets	1 sensor
30-Aug-2010 6:35	30-Aug-2010 6:30

(3) 収集した情報を分析する．backscatter 情報の収集結果からは，指定した調査時間範囲に攻撃を受けた犠牲ホスト，攻撃を受けたサービス，推測攻撃継続時間等の情報が入手できる．

本手法では，同一の犠牲ホストからの backscatter 毎に backscatter を観測した観測点の IP アドレス数も集計している．本手法ではこれを，固有観測点数と定義する．固有観測点数を集計することで，当該 backscatter がどの程度インターネット上に送信されているかの推測が可能となる．すなわち本手法では，送信先 IP アドレス (観測点の IP アドレス) 自体は収集対象とせず，代わりに固有観測点数を集計する．本手法が，送信先 IP アドレスそのものを収集・公開しない理由は，攻撃者に観測点迂回のための手がかりを与えないためである．

また，固有観測点数の集計は，攻撃の誤検出への対策という側面も持つ．例えば，計 20 個の backscatter によるパケットを同一の送信元から観測したとする．この 20 個のパケットを観測した固有観測点数が，20 に近い値であるほど，SYN Flood 攻撃によるものである可能性が高いと判断できる．なぜなら，攻撃者が送信元を広範囲のアドレス帯に詐称していると推察できるためである．しかし，この 20 個のパケットがすべて一ヵ所で観測されたものであれば，観測点自体への攻撃等，別の原因と判断し，分析対象としての優先順位を下げることができる (表 1 の “111.111.0.3” の例)．

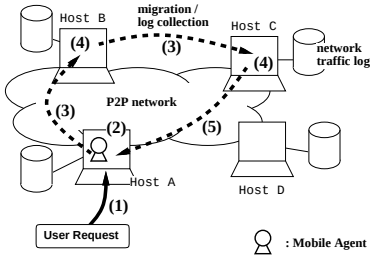

図 2: ABLA の概要

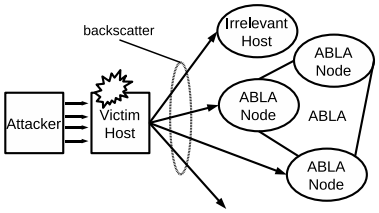

図 3: 本手法の概要

4.2 本手法の利点　我々の手法は，小規模なネットワーク管理者の有志により配置された観測点を利用するため，インターネット上のあらゆるホストが観測点となり得る．これにより原理上，様々な組織や国家間を横断した広域での観測が可能となる．また，動的に観測点を確保することで，観測点の特定は困難となり，攻撃者による観測点の迂回防止に期待できる．例えばネットワーク管理者は，本手法で SYN Flood 攻撃を検出し，管理下にあるネットワークから，仮に少量でも犠牲ホストへ疑わしいパケットが送出された場合，攻撃に加担しているボット等の存在を疑い，調査できる．

5　本手法の実装方法と有効性評価

5.1 本手法の実装　本手法は，分散型のインターネット観測システム ABLA (Agent Based Log Analyzing System) [10] を拡張することで実現した．このシステムを基に，分散された複数のホストから backscatter 情報を収集する．

ABLA は，インターネット上で ABLA をインストールしたホスト (ABLA ノード) 同士が接続し，P2P ネットワークを構築する．また，各ノードを IP アドレスではなく固有の識別子で管理し，匿名性を確保している．ABLA の概要を図 2 に示す．各ノードは ABLA ユーザに対して，観測したパケットに関する情報を提供

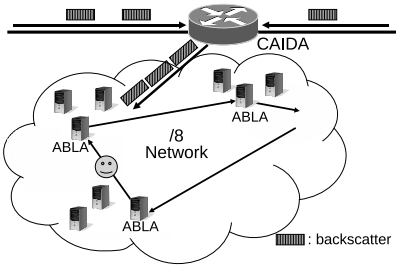

図 4: 想定する攻撃検出環境

する動的観測点となる．そして，各 ABLA ユーザは自身の ABLA ノードでモバイルエージェントを生成し，情報の収集を依頼する．依頼を受けたモバイルエージェントは，ABLA ノード間を自律的に移動して情報を収集する．本手法の概要を図 3 に示す．

5.2 有効性評価の内容　本手法の有効性は，誤検出を排除しつつ大規模な SYN Flood 攻撃を検出できているかで評価する．本研究では，初期設定の Linux OS 上で動作しているサービスの妨害が可能となる，1024 packets/min 以上のパケットレートで攻撃パケットが犠牲ホストに対して送出された場合を攻撃とみなす．そして，上記より低いパケットレートで送出された backscatter を観測し，攻撃と判定することを誤検出 (False Positive) とする．一方，大規模な攻撃の検出性能は，500 pps (packets per second)，5000 pps 以上のパケットレートの攻撃をどの程度検出できているかで評価する．

5.3 評価実験に用いるデータセット　評価実験には，/8 規模のインターネット観測を行う，カリフォルニア大学の研究機関, CAIDA (Cooperative Association for Internet Data Analysis) が提供する backscatter データセットを用いた．

CAIDA が提供するデータセットを実験に用いることで全インターネットの約 1/256 の状況を反映した，本手法の検出性能を評価できる．CAIDA が提供する最新の backscatter データセットは 2008 年のもの [11] [1]であり，我々はこの最新データセットにより評価実験を行った．

5.4 実験の前提条件とパラメータ　本実験では，CAIDA が監視する /8 ネットワークに，複数の

[1]2011 年 8 月 17 日現在

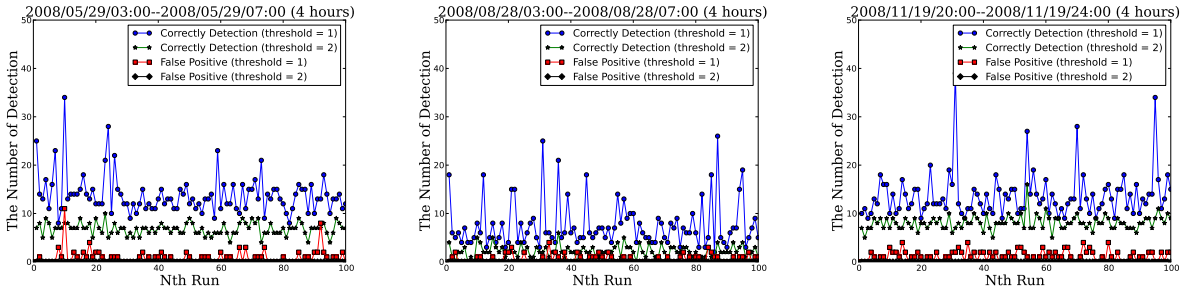

図 5: 2008 年 5 月 (左)，8 月 (中)，11 月 (右) の最新 4 時間分のデータセットによる攻撃検出結果

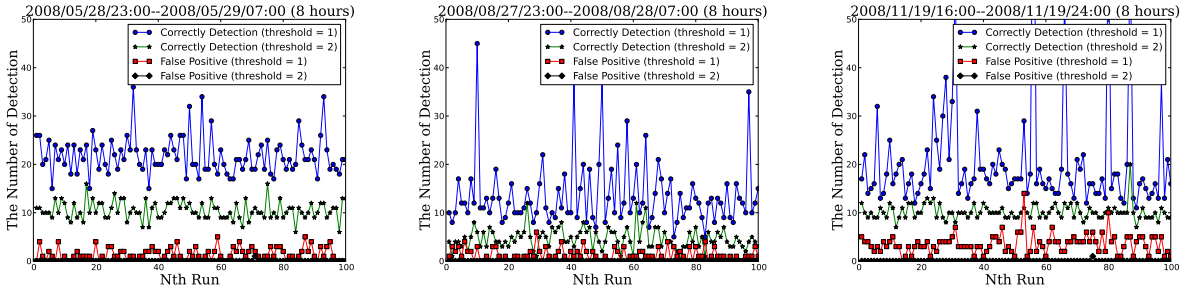

図 6: 2008 年 5 月 (左)，8 月 (中)，11 月 (右) の最新 8 時間分のデータセットによる攻撃検出結果

ABLA ノードが存在する状況を想定したシミュレーションを行う．想定環境を図 4 に示す．全 ABLA ノードは毎回ランダムに配置される．

ABLA ノードのユーザは，SYN Flood 攻撃を検出するため，モバイルエージェントを生成して backscatter 情報の収集を依頼する．依頼を受けたモバイルエージェントは，ABLA ノード間を移動し，各ノードで backscatter 情報を収集する．実験パラメータは以下の 2 つであり，シミュレーションは各 100 回行った．

1 つ目のパラメータは，情報収集のためにモバイルエージェントが訪れる ABLA ノード数である．@Police が配置している固定観測点の数に合わせ，今回は 57 ノードに設定した．

2 つ目のパラメータは，ネットワークログ (以下ログと略記) の調査時間範囲である．今回は，2008 年 5 月，8 月，11 月に取得された最新 1, 4, 8, 12 時間分を調査対象とした．本稿では，最新 4，8 時間分を調査した際の結果を示す．

5.5 実験結果と考察　図 5，図 6 はそれぞれ，2008 年 5，8，11 月の最新 4 時間分のデータセット，2008 年 5，8，11 月の最新 8 時間分のデータセットに本手法を適用した結果である．グラフの横軸は，シミュレーションの各試行に対応しており，1 回目から 100 回目までの結果を示している．また，グラフの縦軸は，検出件数を示している．凡例の Correctly Detection は，攻撃検出数，False Positive は，誤検出数を示している．括弧内の threshold は，攻撃判定に利用した固有観測点数の値である．

一般的に，より広くログの調査時間範囲を設定すれば検出可能な攻撃数は増加するが，同時に誤検出数も増加する．また，攻撃判定の閾値として利用する固有観測点数を高く設定すれば，攻撃検出数は減少するが，誤検出を排除できる可能性は高くなる．図 5，図 6 ともに，上記傾向通りの結果が得られている．今回の実験では，攻撃判定の閾値を 固有観測点数 $= 2$ とすることで，誤検出はほぼ 0 件となった．

ログの調査時間範囲別の結果であるが，最新 4 時間分のログを調査した場合 (図 5)，攻撃判定の閾値を 固有観測点数 $= 1$ のまま運用したとしても，誤検出の発生は低く抑えられている．

それに対し，最新 8 時間分のログを調査し (図 6)，攻撃判定の閾値を 固有観測点数 $= 1$ のまま運用した場合では，誤検出の割合が増加している．特に 11 月 19 日 (図 6 右) の場合，毎回多くの誤検出が発生している．

このことから，本手法を利用して任意の 4 時

表 2: 調査するログの時間範囲と特定の攻撃規模を検出対象とした際の攻撃検出結果

	Over 500 pps threshold = 1	Over 500 pps threshold = 2	Over 5000 pps threshold = 1	Over 5000 pps threshold = 2
05/29/03:00–05/29/07:00 (4h)	20.6 % (57)	11.8 % (57)	65.7 % (11)	54.8 % (11)
08/28/03:00–08/28/07:00 (4h)	17.1 % (40)	5.4 % (40)	24.7 % (9)	14.2 % (9)
11/19/20:00–11/19/24:00 (4h)	29.1 % (41)	19.7 % (41)	84.5 % (10)	76.4 % (10)
05/28/23:00–05/29/07:00 (8h)	30.5 % (57)	18.0 % (57)	67.1 % (14)	57.8 % (14)
08/27/23:00–08/28/07:00 (8h)	26.7 % (42)	11.0 % (42)	43.2 % (10)	26.3 % (10)
11/19/16:00–11/19/24:00 (8h)	27.2 % (54)	18.6 % (54)	78.5 % (13)	71.9 % (13)

間程度のログを調査する場合は，攻撃判定の閾値を 固有観測点数 = 1 のまま運用しても，誤検出を抑えたまま運用可能と予想される．しかし，任意の 8 時間程度のログを調査する場合は，攻撃判定の閾値を 固有観測点数 = 2 と設定するのが運用上望ましいと考えられる．

次に，大規模な攻撃の検出性能について述べる．表 2 は，異なる 2 つのパケットレート (500 pps, 5000 pps) 以上の攻撃を検出対象と想定した際の本手法による平均攻撃検出率である．検出率横の括弧内の値は，その調査時間範囲に発生していた実際の攻撃数である．

8 月の最新データセットを調査した場合の一部に検出性能の低下が見られたものの，500 pps 以上の攻撃を検出対象とした場合，約 2 割程度 (攻撃発生時の約 5 回に 1 回) を検出可能であった．また，5000 pps 以上の攻撃を検出対象とした場合は，約 6 割程度を検出可能であった．これらの攻撃検出率は，インターネット上のわずか 57 個のグローバル IP アドレスで得られた結果と考えれば，妥当な検出性能であると言える．

8 月の最新データセットを調査した場合の一部に検出性能の低下が見られた原因は，攻撃者により非常に偏った送信元詐称が行われたためと推測される．この場合，情報収集規模を拡大することで検出が可能になると考えられる．

6 おわりに

本稿では，攻撃者による観測点の迂回を困難にするための，動的観測点を利用した SYN Flood 攻撃の検出手法を示し，誤検出の影響を抑えながら大規模な攻撃を検出できることを示した．今後は，既存の固定観測式のシステムと比較した，動的観測手法の性能を定量的に示す予定である．

参考文献

[1] Symantec Corporation, “State of Enterprise Security 2010”. http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf

[2] C. Li, W. Jiang, and X. Zou, “Botnet: survey and case study,” Proc. 4th International Conf. on Innovative Computing, Information Control (ICICIC), pp.1184–1187, Dec. 2009.

[3] M. Narita, T. Katoh, B.B. Bista, and T. Takata, “A distributed detecting method for SYN Flood attacks and its implementation using mobile agents,” Proc. 7th German Conf. on Multi-Agent System Technologies (MATES), pp.91–102, Springer LNAI 5774, Sept. 2009.

[4] @Police. http://www.cyberpolice.go.jp

[5] nicter. http://www.nict.go.jp

[6] TALOT2. http://www.ipa.go.jp

[7] WOMBAT. http://www.wombat-project.eu

[8] Y. Shinoda, K. Ikai, and M. Itoh, “Vulnerabilities of passive internet threat monitors,” Proc. 14th USENIX Security Symposium (SEC), pp.209–224, July 2005.

[9] W. Yu, N. Zhang, X. Fu, R. Bettati, and W. Zhao, “Localization attacks to internet threat monitors: Modeling and countermeasures,” IEEE Trans. Computers, vol.59, no.12, pp.1655–1668, Dec. 2010.

[10] Agent Based Log Analyzing System (ABLA). http://sourceforge.jp/projects/abla/

[11] C. Shannon, D. Moore, E. Aben, and K. Claffy, “The CAIDA Backscatter 2008 Dataset”. http://www.caida.org/data/passive/backscatter_2008_dataset.xml