社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2004－DPS－120 (7)
2004／11／4

バックボーンネットワークにおけるトラフィック分析による ワーム自動検出に関する考察

塩出 一平[1], 横山 輝明[1], 山口 英[1]

衛星バックボーンネットワークであるAI3ネットワークでは, 高コストで狭帯域な衛星リンクを内部リンクとして利用しているため, ワームによる帯域浪費は帯域利用効率の低下や, 対向サイトとの通信途絶を招き, 脅威となる. そこでAI3ネットワークで, 素早いワーム検出・遮断機構が必要とされている. トラフィック分析手法の確立のために, ワームの感染モデルや通信機構に基づいた2つの仮説を立て, 実ネットワークの情報を使い2つのモデルについて検証実験をおこなった. 検証実験では不正ホストの検出に成功した. その検証実験の結果について述べる.

Report of experiments for making algorithm of worm traffic detection with traffic analysis

Ippei Shiode[2], Teruaki Yokoyama[2], Suguru Yamaguchi[2]

Recently there have been numerous reports of how network worms spread through the Internet and quickly eating up the network bandwidth by propagating themselves in an exponential speed. Network worms pose a serious threat to the Internet. AI3 (Asia Internet Infrastructure Initiative) is a satellite based testbed network which inter-connects a dozen universities and research facilities throughout the South East Asia and Japan. It is obvious that the precious and expensive narrow band satellite link-the backbone of AI3-would not stand long in front of network worm attacks. Therefore, it is rather essential to develop a mechanism that detects the worm traffic. Through investigating the mechanism of how network worm attacks and spreads, we come up with two characteristics which are unique to the traffics caused by worms. In this paper we discuss the two characteristics and implementation of the detection mechanism using these "signature", as well as the experimental results. At last we give a short brief on the problems that found in our detection mechanism.

1 はじめに

ワームは既存のシステムの脆弱性を利用し, 感染や攻撃を行う自己増殖型の不正プログラムである. ワームの攻撃によって, システムダウンの発生やリンク帯域の飽和などの被害が増加し, Slammer[1], Blaster[2], Nimda[3], CodeRed[4] による被害が, 代表的な事例として報告されている. ワームの不正トラフィックは, リンク帯域を圧迫し, 正常トラフィックの通信を阻害する. ワームの多様化や, 新型ワームの急速な発生が問題となっている. 近年では, ワームのより素早い拡散の可能性が指摘されている [5].

WIDE プロジェクト [6] 内の AI3 プロジェクト [7] によって運用されている, 衛星リンクを利用したアジア広域 Internet exchange(IX) である AI3 ネットワークにおいてもワームトラフィックによる帯域浪費は深刻な問題である. AI3 ネットワーク (図 1) は, 高コスト, 狭帯域な衛星リンクを内部リンクに利用しているため, ワームトラフィックによる帯域浪費は, 帯域利用効率の低下や, ネットワークの分断へとつながる. そこで,AI3 ネットワークでのワームトラフィックの素早い検出・遮断機構が求められている.

[1] 奈良先端科学技術大学院大学 インターネット工学講座
[2] Nara Institute of Science and Technology, Internet Engineering Laboratory

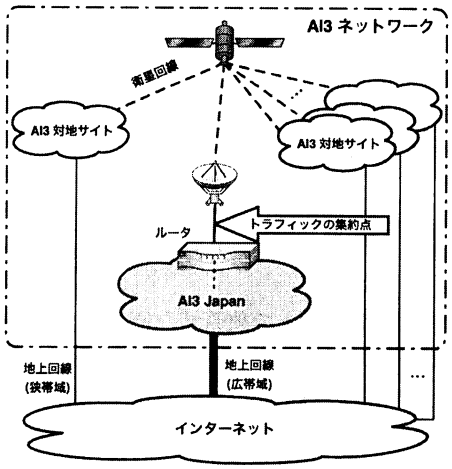

図 1: AI3 ネットワーク

ワーム不正トラフィック検出方法には, ルールベースによる検出方法とルールベースでない検出方法がある. ルールベースの検出方法では, シグネチャと呼ばれる検出ルールとのマッチングによって検出を行っているために, ルールに記述されている不正トラフィックの厳密な検出が可能であるが, ルールに記述されていないものについては検出することができない. 一方, ルールベースでない検出方法では, トラフィックの計測を行い, 分析を行うことで通常のトラフィックから逸脱したものを検出し, 未知の不正トラフィックであっても検出できる可能性がある. 新型ワームの発生間隔の短期化から, 今後はルールベースによる検出方法では, ルールの更新が追い付かず, 新型ワームの検出の遅れが懸念される.

AI3 ネットワークでは, 素早い検出が重要となるため, トラフィック分析に基づく検出方法が有効だと考える. トラフィック分析による検出では, 分析に利用する分析アルゴリズムに依存して検出精度が決まる. そこで, トラフィック分析アルゴリズムを確立するために, インターネット通信におけるＩＣＭＰパケットの振る舞いに注目した仮説と, ワームの感染モデルに基づく仮説を立てる. ＡＩ３ネットワークにおける実トラフィックを用いて, これらの仮説によるワームトラフィック検出の検証実験を行う.

本論文では, 2 節にて, 既存のワーム検出技術について説明し, トラフィック分析による検出手法の利点について述べる. 3 節ではトラフィック分析手法に利用する仮説を立てる. そして, それらの仮説を検証するために実験を行い, その結果を 4 節に記す. 5 節では, 検証実験の結果を元に, 今後の検出アルゴリズムの確立のために必要となる課題について述べる.

2 既存のワーム検出技術の特徴

現在のワーム検出技術はその検出手法によって"misuse detection(不正検出)"と"anomaly detection(異常検出)"の２つに大別できる. 以下にその詳細について述べ, ＡＩ３でのワーム検出にはトラフィック分析に基づくワーム検出が有効なことを論ずる.

2.1 misuse detection(不正検出)

シグネチャと呼ばれる検出ルールを定義し, 監視ネットワークに流れるパケットと検出ルールとのパターンマッチングを行うことによってワームトラフィックの判別を行う方法である. 検出ルールとパケットとのパターン比較を行うため, 厳密な検出が可能という利点があるが, 検出ルールに記述されていないワームは検出できない. そのため新型ワームは, 対応したルールが用意されるまで, 検出不可能である. 検出ルールの作成には, 高度な専門知識が必要とされ, ルールが用意されるまでは若干の時間が必要となり, 近年の新型ワームの急速な発生に対しては事後対策となっている.

2.2 anomaly detection(異常検出)

監視ネットワークのトラフィックを計測し, 統計処理, モデル化, データマイニング処理などの分析によって, 異常トラフィックの抽出を行い, 不正トラフィックの判別を行う方法である. 異常トラフィックの抽出は, 閾値や, トラフィックモデルによる判定が用いられる. こうした判定は, 分析手法に依存した特徴の抽出なので, 検出精度は"misuse detection"による検出手法に劣るが, 新型ワームに対しても検出が可能だと期待される.

AI3 ネットワークではコアネットワークに狭帯域な衛星リンクを利用しているため, 未知のワームトラフィックに対する素早い検出が必要となる. そこで, トラフィック分析による動的なワームトラフィックの検出が, 衛星リンク上でのワームの帯域浪費に対して有効な手段となる. AI3 ネットワークのようなＩＸにおいてトラフィック分析を行う場合, 広大なアドレス空間の通過トラフィックから大量の情報を収集することができる. それらの情報を利用して, 検出精度の向上が期待できる.

3 トラフィック分析に利用する仮説

トラフィック分析は統計処理やモデル化の利用, データマイニング処理の利用がある. データマイニング手法では現在は処理時間の問題があり, 実時間での検出はできない. そのため, 統計処理, モデル化によるトラフィック分析を行う. トラフィック分析での分析手法として利用するために, インターネット通信にお ICMP パケットの振る舞いに注目した仮説とワー

ムの感染モデルに基づく仮説を立てる.

3.1 ICMPの役割に注目する仮説

一般的なワームは感染を行う際には無作為に選んだアドレスに対してICMP Echo Requst Message(Echo Request) を利用したホストスキャンを行う. Echo Requestは送信先ホストが存在していれば, その応答としてICMP Echo Reply Message(Echo Reply) を送信先ホストに返信する. 送信先ホストが存在していなければ, 送信先ホストの直上ルータがICMP Unreachable Message(Unreachable) を返信する. ワーム感染ホストは, より多くのホストに対して感染を試みるために多くのアドレスに対してスキャンを行う. そこで, ワーム感染ホストが送信するEcho Requestの量と, 受信するICMP Echo Reply,Unreachableの量は大量になると考えられる. また, ワーム感染ホストは,Echo Requestの送信先ホストの数も多くなり,Echo Reply, Unreachableも多くのホストから送信されると考えられる. それゆえに,Echo Request, Echo Reply, Unreachableのパケット数と通信先のホスト数には特徴があると考えられる.

ここでワームが行う通信はホストスキャンであるため, このときのEcho Requestにおける送信元アドレス, 受信元アドレスの詐称の可能性は低い. Echo Reply,Unreachableは正常な通信を行っているホストまたは, ルータによって応答されるので, 同様に送信元アドレス, 受信元アドレスは詐称されない. よって,ICMPの情報はワームトラフィックの検出において有効な情報であると考えられる.

3.2 感染パケットの均一性に注目する仮説

ワームが感染活動を行う時には機械的な増殖を行う. そのときのワームの通信は, 以下の3つのプロセスにモデル化できる [5].

ホストスキャン

ワームはまず, ホストスキャンによってワームが持つランダムなアドレスリストからそのアドレスを持つホストが存在するか調べる. 一般的にはICMP Requestを用いることによってホストスキャンを行う. スキャンのために送信するパケットは同一のパケットであるので均一性が存在すると予想される.

脆弱性検査

ホストスキャンの後, ワームはホストスキャンに反応のあったホストに対して, そのホストでのワームが利用できる脆弱性の有無の調査やワームが感染可能な脆弱性の作成を行う. このときに送信されるデータも同一のものを大量のホストへ送信すると予想されるために, 通信パケットには均一性が見られると考えられる.

感染

脆弱性を発見すると, ワームは感染のために自身の複製を対象ホストに対して送信する. この時の送信データは自身のコピーであるため, 均質性は非常に高いと考えられる. また, ワーム感染ホストは多くの感染を試みるために, 正常なホストと比べて, 非常に多くのホストに対して通信を行っていると考えられる.

そこで, ワームの均質性を, 各ホストの送信データ量の類似に注目して分析を行う. ここでは, 各ホストの送信パケット数の分散値δと, 各ホスト毎のアクセスホスト数nを指標として用いる.

あるホストnの各ホストへの送信パケット数をT_nとすると, そのときのある一つのワーム感染ホストが各ホストに通信している平均パケット数$\overline{T}$は式1で, 分散値δは式2で表すことができる.

$$\overline{T} = \frac{\sum T_n}{n} \tag{1}$$

$$\delta^2 = \frac{1}{n}\sum (T_n - \overline{T})^2 \tag{2}$$

ワーム感染ホストである場合, 上記のモデルの内, 感染プロセスの時の分散値δは0に近づき, アクセス先ホスト数nは大きくなると考えられる.

4 実験

実ネットワークにおいて, 前節で述べたワームが感染を行う際の通信の特徴についての検証を行った.

4.1 実験環境

検証ネットワークとしてAI3ネットワークを利用した. 衛星リンクに流入するすべてのトラフィックを計測するために, 図1のトラフィックの集約地点である衛星リンクの直下のルータで計測を行った. tcpdumpを使用して,2004年9月10日午前0時から24時間計測を行った. 1日の平均流量は3.4Mbpsで, データの総サイズは約38GBになっている. 今回の分析では, 分析周期を24時間とみなして, この蓄積データを用いて, 仮説の検証を行う.

4.2 実験1:ICMPの役割に着目した検証実験

概要

ICMP によるスキャンではスキャンホストが Echo Request をスキャン対象ホストに送信し，スキャン対象ホストの内，存在するホストからの Echo Reply や，スキャン対象ホストの直上ルータによる Unreachable が返信される．その結果スキャンホストは大量の Echo Request を送信し，また大量の Echo Reply と Unreachable を受信すると予想される．

検証実験では計測データから各ICMP を取り出し，各ホストが送信した Echo Request，受信した Echo Reply,Unreachable をカウントした．また，各ホストが送信した Echo Request の送信先のホストの数と受信した Echo Reply,Unreachable の送信元アドレスの数もカウントした．次に各 ICMP のパケット数が多いホスト上位 10 個を取り出し，通信内容を確認することで不正ホストの判別を行った．

結果

表 1: ICMP Echo Request の送信パケット数が多いホスト上位 10

ホスト	パケット数 X	アクセス数 Y	X/Y	判定
req-A	71948	11413	6.304	△
req-B	56951	56951	1	○
req-C	38312	38312	1	×
req-D	10218	5167	1.978	×
req-E	8587	4381	1.96	×
req-F	8062	8062	1	×
req-G	6105	7	872.142	△
req-H	1885	1388	1.358	×
req-I	1508	1487	1.014	×
req-J	1449	1	1449	○

表 2: ICMP Echo Reply の受信パケット数が多いホスト上位 10

ホスト	パケット数 X	アクセス数 Y	X/Y	判定
rep-A	11413	11176	1.021	△
rep-B	3967	1	3967	○
rep-C	3806	3	1269	△
rep-D	1799	1	1799	△
rep-E	959	1	959	○
rep-F	955	1	955	○
rep-G	954	1	954	○
rep-H	954	1	954	○
rep-I	953	1	953	○
rep-J	953	1	953	○

表 3: ICMP Unreachable の受信パケット数が多いホスト上位 10

ホスト	パケット数 X	アクセス数 Y	X/Y	判定
unr-A	283675	1	283675	○
unr-B	11492	231	49.749	○
unr-C	10088	37	272.649	○
unr-D	8323	3344	2.489	△
unr-E	7454	714	10.44	○
unr-F	7327	770	9.516	○
unr-G	5286	560	9.439	○
unr-H	4642	1329	3.492	○
unr-I	2391	1	2391	○
unr-J	2264	6	377.333	○

表 1，表 2，表 3 は Echo Request,Echo Reply,Unreachable の合計パケット数が多いホストの上位 10 ホストを表している．それぞれの表の項目において左からパケット数は Echo Request ではホストが送信したパケット総数を示し，アクセス数は送信先のホストの数を示している.Echo Reply, Unreachable ではパケット数は受信した Echo Reply, Unreachable の総数を示し，アクセス数は送信元のホストの数を示している．パケット数をアクセス数で割ったものはパケットの送信先のちらばりを意味している．判定の項目は○は正常通信ホスト，×は攻撃スキャンホスト，△は正常ホストと攻撃スキャンホストの判定ができなかったホストを示している．また,req-A は rep-A,unr-D と同一のホストであり,req-G は rep-C と同一のホストであった．

表 1 において req-A～req-F はパケット送信量とアクセス先ホストの数が req-G～req-J に比べ極めて多く，スキャンホストである可能性が高いと考えられる．req-A～F の通信内容を確認したところ,req-B～req-F は連続したアドレスに対するスキャンを行っていたため，スキャンホストだと判定した．また,req-A は,ICMP のスキャンを行ってはいるものの，通常トラフィックも観測された．そのために，正常な通信を行っているホストとスキャンホストの判別がついていない．表 2 では AI3 ネットワーク内にある衛星リンク直下のルータへの通信を検出した．アクセス先のホスト数も少ないことから，実際の通信を確認することによって，正常通信を行っているホストであると判断した．表 3 での検出結果は，そのほとんどが Domain Name Server(DNS サーバ) であった．DNS サーバによるクエリは UDP の 1023 番ポート以上のポートを利用して行うが，このポートは Slammer の利用するポートと重複するため，そのポートは閉じられていることが多い．そのため,DNS サーバがクエリの応答を

受け取る際の，内部フィルタ設定ミスと考えられる．

4.3 実験2：感染パケットの均一性に着目した検証実験

概要

ワームは感染対象ホストに対して，自分自身のコピーを送信する．このときの各感染対象ホストに対して送信するデータは同一のデータであると考えられるのでワーム感染ホストが通信している各ホスト毎のパケット数はほぼ同一になる．そこで，パケット数の同一性を検証するためにあるホストが通信している通信先の数とその通信のパケット数の分散値を調べ，3節の感染モデルの感染プロセスにおける感染パケットの均質性についての検証を行った．行った検証方法は各ホストが送信しているTCP,UDPの通信から，それぞれのホストが通信しているホストの数，そのときのパケット数を計測し，それぞれのホストが通信しているパケット数の分散値を求めた．次に閾値を1として，分散値が閾値1未満のホストについて，実際の通信を観測して，ワーム感染ホストの判別を行った．

結果

図2と図3はTCP,UDPの通信に関して分散値が1未満であるホストについて，アクセスホスト数，各アクセスホスト数に対するパケット数の分散値をプロットしたものである．アクセスホスト数は通信先ホストの数を示し，分散値は各ホストの通信毎での均質性を意味している．通常通信を行っているホストは多様な通信を含むため，分散値が大きくなる．ワームに感染したホストでは，パケット量は均一になると考えられるので分散値は，0の付近に分布する．本検証では分散値の閾値を1に規定し，閾値未満のホストを均質性が高いと判断し，感染ホストの判定を行った．

分散値が閾値未満のホストを感染ホストとみなし，それらのホストに注目した．それらのホストの内，TCPの通信ではあるホスト(分散値:0.7)においてTCPポート2745への通信を試みているのを発見した．TCPポート2745へ通信はBeagle[8]によって作られるバックドアポートであり，一定数のパケットを2205個のホストに対して送信しているのを確認した．同じく閾値未満のホストの中でUDPの通信ではあるホスト(分散値:0)において47314個の連続したアドレスに対してUDPポート137へのスキャンを試みているのを発見した．また，別のホスト(分散値:0.8)においてはFTPによる正常通信もこれらのホストに含まれていた．しかし，このホストはアクセス数が53と小さいためにUDPのポートスキャンを行っているホストと区別できる．パケットの均一性に着目した検出ではワーム感染ホストの検出が可能であるが，同時に通常通信のホストを検出してしまう可能性がある．そこで，アクセス数についても閾値の規定が必要である．

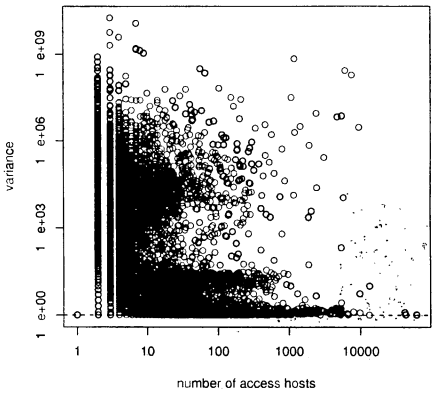

図2: アクセス先ホスト数と分散値(TCP)

4.4 考察

実験1では，各ICMPのタイプ別の総量に着目した検証実験を行った．Echo Reply,Unreachableのパケット総数に着目して，その上位10個のホストについて分析を行った．Echo Reply，Unreachableにおいて今回の検証ではパケット総数のみに着目した分析しか行っていないために，正常通信のホストしか見当たらなかった．パケット総数以外のアクセス数などにも着目して分析を行う必要がある．一方，Echo Requestのパケット総数に着目した分析ではスキャンホストの検出ができた．検出されたスキャンホストはパケットの送信先のちらばりが1に近づくホストはスキャンホストであると考えられる．これはスキャンホストは多くのホストに対してEcho Request,Echo Reply,Unreachableを送信・受信している．これはスキャンホストは大量のEcho Request，Echo Reply,Unreachableを送信・受信しているという仮説と一致している．

実験2では，ワームによる感染ホストの送信パケットの均一性に着目した検証を行った．分散値が閾値未満で通信先ホスト数が多いホストの中でワームによる感染や特定ポートを狙ったスキャンを検出した．また，アクセスホスト数に対する閾値を規定していないために，FTPの通信のような正常通信のホストも検出した．ワーム感染ホストは通信を行うパケット数が均一になり，アクセスホスト数の数も大きくなるという仮説に一致している．

ワーム感染ホストは今回考えた2つの仮説と一致

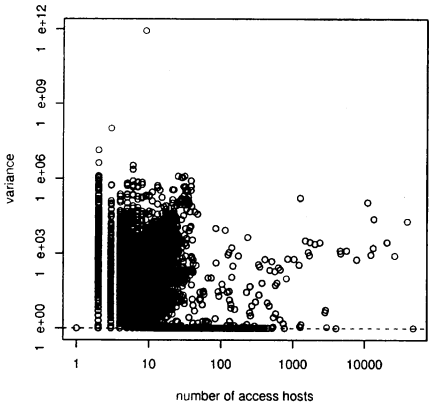

図 3: アクセス先ホスト数と分散値 (UDP)

している. しかし, いくつかの正常通信のホストも実ネットワークでは仮説に一致する. 今回の検証で規定した閾値のパラメータ以外にも閾値を規定することによって検出精度は向上すると考えられる. それゆえに, 今回の仮説は検出において有効である.

5 おわりに

本稿では, 新型ワームの発生間隔の短縮によって現在主流のルールベースの検出では検出の限界があることを指摘した. また, 衛星リンクをコアネットワークにもつ AI3 ネットワークにおいて, 実時間で検出の必要性について述べた. そこで, 実時間で検出を行うためのトラフィック分析による検出手法を確立するために, とワームの感染の際の送信パケットの均一性に着目しの検証を行った. その結果, いくつかの通常通.

今後, 実時間での検出アルゴリズムの提案をするために, 課題として以下が考えられる.

- 今回の検証で立てた 2 つの仮説の中でそれぞれワームの特徴を挙げた. 今回挙げたワームの特徴以外にもさまざまな特徴が考えられる. ワームは感染を行う際には特定ポートを使用する. 通常通信を行っているホストは使用ポート数は多数になる. 各ホストが使用するポートの均質性がワーム感染ホストでは見られると予測している. 検知精度の向上のためにも他の仮説についても検証していく必要がある.

- 今回の実験では正常なホストについても仮説に一致するホストが検出された. 適切な閾値の決定をしていないことが原因であると考えられる. 適切な閾値の決定を行うための方法が必要であると考えられる.

- 実験 1, 実験 2 の特徴を抽出する際は 24 時間を分析周期にして行った. また, 実験 2 に関しては, 分散値を求める際の計算コストも大きい. そのために, 今回の実験の特徴をそのまま実時間での検出アルゴリズムに適用することは難しい. 今後, 今回の特徴抽出方法を実時間でのアルゴリズムに置き換える必要がある.

上記の課題を含め, 実時間での検出アルゴリズムについて検討する.

参考文献

[1] The Spread of the Sapphire/Slammer Worm. http://www.cs.berkeley.edu/ nweaver/sapphire/.

[2] SecurityFocus HOME News: The Bright Side of Blaster. http://www.securityfocus.com/news/6728.

[3] Dynamic Graphs of the Nimda Worm - CAIDA:DYNAMIC: analysis: security: nimda. http://www.caida.org/dynamic/analysis-/security/nimda/.

[4] Cooperative Association for Internet Data Analysis. Caida analysis of code red. http://www.caida.org/analysis/security/code-red/.

[5] Nicholas Weaver,Potential Strategies for High Speed Active Worms: A Worst Case Analysis. whitepaper, U.C. Berkeley,- http://www.cs.berkeley.edu/ nweaver/worms.pdf.

[6] WIDE Project. http://www.wide.ad.jp/index-j.html.

[7] Asian Internet Interconnection Initiatives Project. http://www.ai3.net/.

[8] The Beagle Worm History Through April 24, 2004. http://www.securityfocus.com/data/library-/Beagle_Lessons.pdf.