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

2007－DPS－130 (46)
2007－CSEC－ 36 (46)
2007／3／2

ダミーアドレスを用いた ワームの早期抑制手法の提案と評価

稲場 太郎† 川口 信隆‡ 田原 慎也‡
東 雄介‡ 重野 寛† 岡田 謙一†

これまで出現してきたネットワークワームのほとんどはスキャニングワームであった．しかし最近，より効率的な感染手法をとるワームが登場してきた．その中でも我々は内部アドレスリストを用いて感染活動を行うワームに注目する．本稿ではダミーアドレスを用いてこの種のワームを発見，抑制する手法を提案する．本手法では，各ホストのアドレスリストの中にダミーアドレスを混在させ，このアドレスに接続したホストが存在した場合，ワームを検知する．また，そのホストから接続履歴をトレースバックし，次々にネットワークから切断することでワームの拡散を抑制する．コンピュータシミュレーションによる評価実験を通じて，本手法により感染ホストは全ホストの1%以下に，ネットワークから切断されたホストは5%以下に抑えられることを確認した．

Containment of Worms with Dummy Addresses

Taro Inaba† , Nobutaka Kawaguchi‡ , Shinya Tahara‡ ,
Yusuke Azuma‡ , Hiroshi Shigeno† and Kenichi Okada†

Most of existing network worms used address scans to find vulnerable hosts. Recently, however, worms with more effective propagation strategies have emerged. Among the worms, we focus on the worms that use address lists at already infected hosts to find other vulnerable hosts effectively. In this paper, we propose a method to detect and contain such worms. In our method, a detection system inserts some dummy addresses into the address list of each host. The system detects the existence of worms when a host tries to open connection for a dummy address, and then traces back the connection logs to find potential infected hosts and removes them from the network. Computer Simualtion shows our method detects and contains worms with less than 1% infected hosts and less than 5% removed hosts.

1 はじめに

近年，CodeRedなど，様々なワームによる被害が報告されてきた [1]．これまでの主流はスキャニングワームであり，これは無作為に感染ターゲットとなるアドレスを作成し，感染コネクションを張るものであった．この種のワームに対する抑制手法は，各所で議論されてきた [2] [3]．しかし，スキャンを行うワームは非効率であり，近年では別の感染手法をとるネットワークワームが登場している．

その中でも我々は感染ホストの内部にあるアドレス情報を用いて感染活動を行うワームに注目した [4]．内部アドレス情報を用いた感染活動の場合，スキャンと異なり確実に存在するアドレスに対してコネクションを張ることができるため，確実に感染が広がる上，ネットワークの異常を発見してワームの存在を検知することが困難である．

そこで本稿では，ダミーアドレスを用いてワームを抑制する手法を提案する．本手法では，全ネットワークを監視する監視サーバを設け，このサーバによってワームを抑制する．監視サーバが各ホストのアドレスリストにダミーアドレスを持たせ，このアドレスへの接続が行われると監視サーバへ報告される．監視サーバは，このアドレスにコネクションを張ったホストはワームに感染していると判断し，このホストをネットワークから切断する．また，監視サーバは全ホスト間の接続履歴を保持している．これを利用して接続をトレースバックし，感染の疑いがあるホストを次々にネットワークから切断する．この作業を繰り返し，最終的にはアクティブな感染

† 慶應義塾大学大学院理工学部
Faculty of Science and Technology, Keio University
‡ 慶應義塾大学理工学研究科
Graduate School of Science and Technology, Keio University

ホストを根絶する．

コンピュータシミュレーションにより，本提案の有効性を確認した．

本稿では，まず，2章において提案の背景に触れる．3章でダミーアドレスを用いたワームの早期抑制手法を提案し，4章で提案手法のシミュレーション評価について述べる．そして5章は本論文のまとめとする．

2 背景

2.1 スキャニングワーム

近年登場した，CodeRedなどのワームはアドレススキャンにより感染活動を行ってきた [1]．従って，ワームが存在する場合ネットワークのトラフィックが異常に多くなり，それを利用して検知，抑制が可能である．

Matthew M. Williamsonは，この種のワームを抑制するウイルススロットルという手法を提案している [2]．この手法は，接続頻度がある値を超えるトラフィックに対して遅延を発生させ，ワームの感染活動を遅らせようというものである．通常の通信においてこの速度を超えてしまった場合も遅延が生じるが，通常の通信があまりに頻繁に行われることはほとんどないので，遅延の影響は最小限に抑えられる．それに対し，ワームのトラフィックの場合は常に高速で感染活動を行っているので遅延の影響が甚大となり，感染を遅らせることができる．

Stuart E. Schechterらは，スキャニングワームの早期検知抑制手法を提案している [3]．この手法では，スキャンパケットのほとんどが初めての接続先に対するものであることを利用し，ワームを検知する．また，ワーム検知システムが監視した結果の連続的な仮説検定と信頼性ベースの速度規制によってワームを抑制する．これにより，非常に低い誤検知率でワームの早期抑制が実現できる．

2.2 内部アドレスリストを利用したワーム

スキャニングワームは，ランダムに作成したアドレス宛てに感染活動を行おうとする．このため，実在しないアドレス宛てへの送信やコネクション確立要求が出されるため，非常に非効率的である．また，先述のような抑制手法も多数議論されている．このような現状に対し，より効率的な感染活動を行うネットワークワームが登場してきた [4] [5]．その中の一つが内部アドレスリストを利用したネットワークワームである．

この種のワームは，感染したホストが内部に保持するアドレスリストを用いてターゲットの発見を行う．従って確実に存在するアドレスに対して感染コネクションを張ることができ，効率的であると同時に低速で感染活動を行うことが可能となる．通常のコネクション速度とほぼ変わらない速度で感染活動が行われると，先述の抑制手法は全く効果がなくなる．そこで，これらのワームを抑制する手法の確立が必要である．

内部アドレスリストを用いて感染活動を行うワームの一種に，Eメールワームがある．Chin-Tser Huangらは，ユーザのEメールソフトのアドレス帳にそれぞれ一つダミーアドレスを加えることによって，Eメールワームを捕え，感染を抑える手法を提案している [6]．

この手法では，まずサーバ側が未使用のダミーアドレスを用意し，各ユーザのアドレス帳にこれを登録させる．ダミーアドレスにメールが送信された場合，そのユーザとシグニチャがブラックリストに加えられ，このリストによってEメールワームを抑制する．

この手法は，Eメールワームに特化しており，他の内部アドレスリストを用いたワームについては議論されていない．また，コネクションごとに攻撃コードのシグニチャを変更して感染活動を行うワーム（ポリモフィックワーム）の場合，シグニチャベースの抑制手法は効果を発揮しない．従って，より効率的な抑制手法が必要となる．

3 ダミーアドレスを用いたワームの早期抑制手法

3.1 検知対象ワーム

本提案手法での検知，抑制の対象となるのは，内部アドレスリストからランダムに感染対象ターゲットとなるホストを選択し，感染活動を行うワームである．ここで言う内部アドレスリストとは，Eメールソフトのアドレス帳，インスタントメッセンジャーの登録アドレス，ARPキャッシュ，他のホストへの接続履歴など，ホストマシンの内部に保存されているアドレスリストのことを指す．また，本手法では，シグニチャベースの抑制手法 [6] を回避できるポリモフィックワームも検知が可能となる．

3.2 ワームの抑制手法

本提案手法の概略を図1に示す．

本手法では，監視サーバが各ホストの持つアドレスリストにダミーアドレスをいくつか追加する．

このダミーアドレスに対して接続がなされると監視サーバが検知し，ワームがネットワーク中に存在すると判断する．この接続元のホストを感染ホストとみなし，ネットワークから切断する．また，監視サーバは各ホスト間の接続履歴情報を用いて感染ホストからトレー

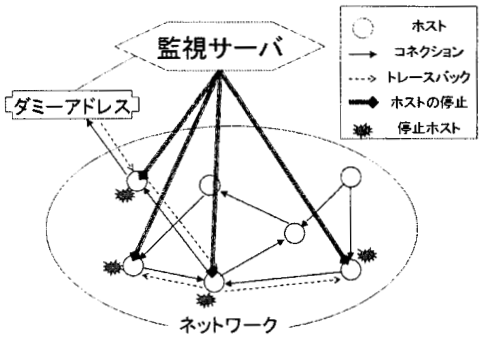


図 1: 提案概略

スバックすることで，感染の疑いがあるホストを次々にネットワークから切断し，ワームの根絶を行う．

3.2.1 監視サーバ

本提案手法において監視サーバは以下の役割と機能を持っている．

- あるネットワークの全ホストを監視し，各ホストのアドレスリストにダミーアドレスを挿入する．
- 全ホスト間の接続履歴を保持している．
- 任意のホストをネットワークから切断する．この際，一定の時間を要する．

3.2.2 ワームの発見

本論文においては，ワームが存在しない状況ではダミーアドレスに対して接続が張られることはないと想定し，ダミーアドレスに対するコネクションが張られた時点でワームの存在を検知する．

3.2.3 ホスト停止によるワームの抑制

ダミーアドレスに対するコネクション（これ以降，ダミーコネクションという）が張られると，監視サーバはその送信元のホストをネットワークから切断する．このことを，ホストの停止と呼ぶ．ここで，ダミーコネクションを張ったホストのみの停止による，ワームの抑制性能について述べる．

今，あるネットワークにおいて内部アドレスリストを用いるワームに感染しているホストが 1 つあるとする．このワームに感染したホストは，Δt ごとに一つのアドレスに対して感染コネクションを張る．また，このネットワークにあるホストは全てアドレスリストに n 個の通常アドレスと d 個のダミーアドレスを持っている．

感染しているホストが初めてコネクションを張ったときにダミーアドレスに当たる確率 P_d は，

$$P_d = \frac{d}{d+n} \tag{1}$$

となる．この場合，他のホストにコネクションを張ることなくワームを根絶することができる．

ところが，

$$P_n = 1 - \frac{d}{d+n} \tag{2}$$

の確率でダミーアドレス以外のアドレスにコネクションを行い，ワームは根絶することなく増殖する．次の Δt 後には 2 つのホストから感染コネクションが張られる．これらが両方ダミーコネクションを放ってワームが完全に停止する確率 P_{d2} は，

$$P_{d2} = \frac{d^2}{(d+n)^2} \tag{3}$$

であり，この P_{d2} は P_d より小さい．以降ワームが増殖していく度にこの確率はさらに小さくなり，ワームの根絶が非常に困難となる．従って，この方法のみで早期にワームを根絶させるためには，d の値を大きくして P_d の値を大きくしなければならない．しかし，ダミーアドレス数が大きくなると各ホストや監視サーバにとって負担となる．そこで，ダミーアドレス数を抑えつつ，ワームの早期抑制を実現することが求められる．

3.2.4 トレースバックによるワーム抑制

前述のとおり，ダミーコネクションを張ったホストのみを停止していたのでは，ワームの根絶は困難である．

本研究ではこれを解決するために，各ホストの接続履歴を参照し，これに従って感染の疑いがあるホストを追跡し，次々と停止させていく．

ここで，感染の疑いがあるホストを以下の 3 種類に分類する．

- トリガーホスト
  ダミーコネクションを張ったホスト
- 感染源疑惑ホスト
  トリガーホストの感染源となり得るホスト
- 感染疑惑ホスト
  感染の疑いのあるホストからコネクションを受けたホスト

感染源疑惑ホストは，過去にトリガーホストへ対してコネクションを行ったホストのことを指す．また感染源疑惑ホストへ対して過去にコネクションを行ったホストもトリガーホストの元の感染源となり得るので，感染源

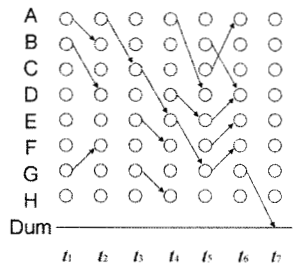


図 2: 接続履歴

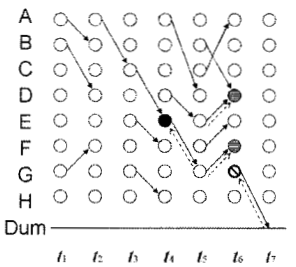


図 3: $N_t = 1$

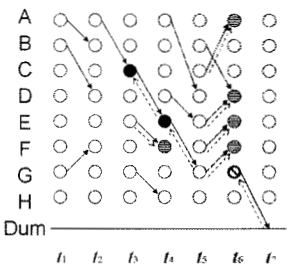
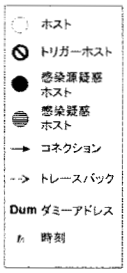


図 4: $N_t = 2$



疑惑ホストとなる．感染の疑いのあるホスト（トリガーホスト，感染源疑惑ホスト，感染疑惑ホスト）からのコネクションを受けたホストは，感染源ではないと推定されるが感染の疑いが強い．このホストを感染疑惑ホストと呼ぶ．

図 2 は監視サーバから見るホスト A〜H の接続履歴を示している．

各アルファベットはホストを表し，Dum はダミーアドレスを表す．また，t_n は時刻を表す．t_n と t_{n+1} の間の時間を 1ut とする．矢印は，始点の時刻においてあるホストから別のホストまたはダミーアドレスへの接続がなされたことを示す．図 1 ではホスト G が時刻 t_6 においてダミーコネクションを張っている．この場合，ダミーコネクションを張ったホスト G はトリガーホストとなり，監視サーバが直ちに停止させる．また，感染ホスト G から接続をトレースバックすることで感染源疑惑ホスト，感染疑惑ホストを発見し，停止させていく．

ここで，トレース数とトレース時間というパラメータを設け，それぞれ N_t と T_t で表す．N_t は，感染源疑惑ホストを何ホップ遡ってホストを停止させるか，ということを示す値であり，T_t は 1 ホップあたりどれくらいの時間（ut 単位）を遡るか，ということを表す．例えば $N_t = 1$，$T_t = 2ut$ とした場合のトレースバックの様子を図 3 に示す．まず，トリガーホスト G が t_4 以降にコネクションを張った先のホストは感染疑惑ホストとなり，停止される．図 3 ではホスト F がこれに当たる．また，トリガーホスト G に t_4 以降にコネクションを張った元のホストは感染源疑惑ホストとなり，停止される．図 3 ではホスト E がこれに当たる．さらに，これらの感染の疑いのあるホストが現在までにコネクションを張った先のホストは感染疑惑ホストとなり，停止される．図 3 では感染源疑惑ホスト E が時刻 t_5 にコネクションを張ったホスト D が感染疑惑ホストとなる．

$N_t = 2$ とした場合は，同様の作業をトリガーホストだけでなく $N_t = 1$ のときの感染源疑惑ホストに対しても行う．このときの様子は図 4 に示す．ここでは，$N_t = 1$ の場合に加え，さらに感染源疑惑ホスト C，感染疑惑ホスト A が停止される．

以降，N_t を増やした場合も同様で，感染源疑惑ホストをさらに遡って感染の疑いのあるホストを停止させていく．

本手法では感染コネクションと通常コネクションの区別がつかないため，監視サーバは実際には感染していないホストも停止させる可能性がある．従って誤検知があればその分停止台数は多くなる．そこで停止台数をできるだけ少なく抑えつつ，ワームを早期に抑制することが重要となる．

4 シミュレーション評価

本提案の有用性を示すために，C 言語でシミュレーションシステムを構築し，評価を行った．

4.1 シミュレーション条件

本シミュレーションでは 10000 台のホストが存在するネットワークを想定する．また監視サーバは全ホストのコネクションログをリアルタイムに取得できるものとする．本シミュレーションにおける時間の単位を ut とする．シミュレーション開始時は，全 10000 台のホストが通常の接続のみを行っている状態でシミュレーション時間を $100ut$ 経過させ，その時点で 5 台のホストをワームに感染させる．ダミーコネクションが張られるたびにトレースバックによって感染している疑いがあるホストを停止させていく．活動中の感染ホストが全てなくなった時点での，ワーム感染台数，停止台数を評価する．

シミュレーションパラメータは表 1 のように設定した．なお，ここで示す値はデフォルト値であり，特に断りのない限りはこの値でシミュレーションを行う．

ホスト同士のリンクは，実世界に近いものとなるよう，スケールフリーネットワーク [7] とした．スケールフリーネットワークを構築するため，BA モデル [8] に

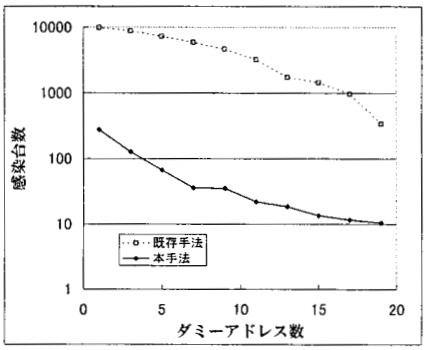


図 5: 既存手法と提案手法における感染台数

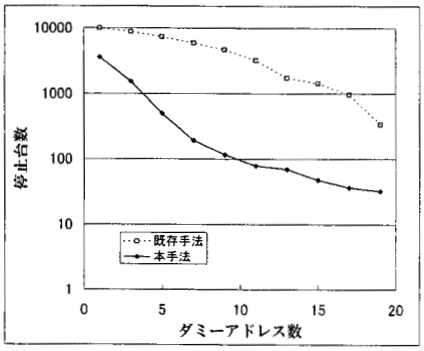


図 6: 既存手法と提案手法における停止台数

表 1: シミュレーションパラメータ

シミュレーション回数： R	30 回
全ホスト数： N	10000 台
初期感染台数： I_0	5 台
BA モデルにおける初期ホスト数： M_0	6
BA モデルにおける初期リンク数： M	5
平均アドレス数： A	15
ダミーアドレス数： d	5
トレース数： N_t	2
トレース時間： T_t	$8ut$
平均通常コネクション間隔： B_n	$5ut$
平均感染コネクション間隔： B_i	$1ut$
平均ホスト停止遅延時間： Q	$2ut$

従ってホストの生成を行った．なお，BA モデルに従ってホストを生成した結果の平均アドレス数が 15 個となる．

1 台のホストがアドレスリスト中のあるホストに通常のコネクションを張る間隔，1 台の感染ホストが感染コネクションを張る間隔に対して平均値を設け，それぞれ $N(5ut, 2ut^2)$，$N(1ut, 2ut^2)$ の正規分布に従って変動する．

ホストを停止するのにかかる時間は，$N(2ut, 1ut^2)$ に従う．

4.2 評価方法

既存手法との比較

トレースバックを行う場合（本提案手法）と行わない場合（既存手法）での比較を行った．両者においてダミーアドレス数 d を変動させ，その際の感染ホスト台数，停止ホスト台数を比較することによって評価を行った．なお，本提案手法におけるトレース時間 T_t は d によって最適値が異なるため，各 d における最適な T_t を用いて評価を行った．

各感染速度における効果

感染コネクションインターバル B_i を変化させ，様々な速度のワームにおいて感染ホスト台数，停止ホスト台数がどれだけ抑えられるか評価を行った．

4.3 シミュレーション結果

既存手法との比較

シミュレーション結果を図 5，図 6 に示す．

図 5 は，感染台数についての結果である．本手法を用いることによって感染台数が大幅に減少することがわかる．ダミーアドレス数 5 のときで比較すると，既存手法では 7000 台 (70%) あまりが感染した段階でワームが根絶するが，本手法では 100 台 (1%) 以下に抑えることが可能となっている．既存手法でもダミーアドレス数が 20 個近く挿入されれば感染台数を 1000 台以下に抑えることができているが，ホストの持つ平均アドレス数が 15 個であることを考えるとこのダミーアドレス数は多すぎる．少ないダミーアドレス数でも感染台数を抑えることができるという点で，本提案手法は既存手法よりも優れている．

また図 6 は停止台数についての結果である．既存手法はダミーコネクションを張ったホストのみを停止させるので，感染台数と停止台数は等しくなる．それに対し本手法はトレースバックを行うため，実際は感染していないホストも停止させる．従って感染台数よりも停止台数は多くなる．しかしそれでも本手法は既存手法よりも優れた結果となっており，ダミーアドレス数 5 の場合感染台数を 500 台 (5%) 程度に抑えることが可能となっている．たとえば，既存手法が停止台数を全体の 10% に抑えるダミーアドレス数においては，本手法では 1% 以下に抑えることが可能となっている．停止台数を抑えるという観点からも本手法は提案手法よりも効率的であると言える．

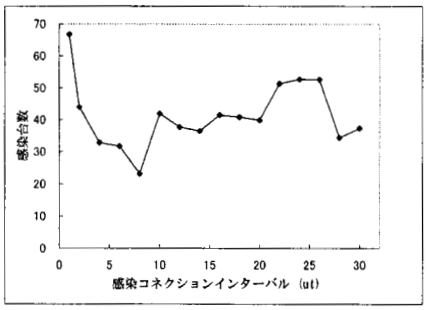


図 7: 各感染インターバルにおける感染台数

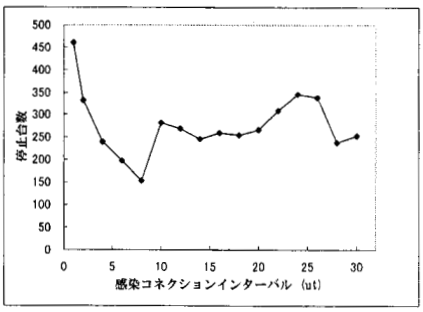


図 8: 各感染インターバルにおける停止台数

各感染速度における効果

シミュレーション結果を図 7，図 8 に示す．

これらの図は，感染コネクションインターバル B_i を 1ut から 30ut まで動かしたときの感染台数，停止台数を表している．これは通常コネクションと比較すると 1/6 倍から 5 倍の速度である．結果は，どの感染速度においても感染台数は 50 台程度となっており，これは全台数の 0.5% に当たる．また，感染台数と誤検知台数を合わせた停止台数はどの速度においても 300 台程度となっており，これは 3% に相当する．このように，通常コネクションの 1/6 倍から 5 倍の速度のワームは本提案手法を用いることによってワーム感染台数が 1% 以下となっており，その際に誤検知されたホストを加えた停止台数台数は 5% 以下となっている．

5 まとめと今後の課題

最近，アドレススキャン以外の方法で感染活動を行うワームが登場し，その対策が必要となっている．そこで我々は内部アドレスリストを用いて感染活動を行うワームに注目し，その抑制手段としてダミーアドレスを挿入する手法を提案した．ダミーアドレスに対して接続を張ったホストをネットワークから切断し，さらにトレースバックして感染の疑いがあるホストを発見，停止する．この手法により，感染台数 1% 以下，停止台数 5% 以下の状態でワームの感染活動を止めることが可能となった．

今後の課題としては，本提案手法の実用化や運用上の問題の解決が挙げられる．まず本提案では監視サーバが各ホストの接続履歴を全て持っていることが前提であったが，これを実現しなければならない．小規模な組織ネットワークから可能性を探っていきたいと考えている．また，より早期のワーム抑止のためには，様々な感染速度のワームに対して最適なパラメータを見つけなければならない．ダミーアドレス数やトレース数，トレース時間等を動的に変化させることを含め，最低限のダミーアドレスで被害を最小限に抑えることができるよう，提案アルゴリズムを改良していく必要がある．

謝辞

本研究は文部科学省科学研究費補助金 (C) 課題番号 1850063(2006 年) の支援を受けて行われた．ここに記して謝意を表す．

参考文献

[1] Cliff Changchun Zou, Weibo Gong and Don Towsley. Code Red Worm Propagation Modeling and Analysis. Proceedings of the 9th ACM conference on Computer and communications security, 2002.

[2] Matthew M. Williamson. Throttling Viruses: Restricting propagation to defeat malicious mobile code. Proceedings of Computer Security Applications Conference, 2002.

[3] Stuart E.Schechter, Jaeyeon Jung, and Arthur W. Berger. Fast Detection of Scanning Worm Infections. Recent Advances in Intrusion Detection, 2004

[4] Nicholas Weaver, Vern Paxson, Stuart Staniford, Robert Cunningham. A Taxonomy of Computer Worms. Proceedings of the 2003 ACM workshop on Rapid malcode, 2003.

[5] http://www.symantec.com/avcenter/venc/data/w32.bropia.html/ (2007/01/25 確認)

[6] Chin-Tser Huang, Nathan L. Jhonson, Jeff Janies, Alex X. Liu. On Capturing and Containing E-mail Worms. Proceedings of IEEE IPCCC 2006, 2006.

[7] Cliff C. Zou, DonTowsley, Weibo Gong. Email Worm Modeling and Defense. 13th International Conference on Computer Communications and Networks, 2004.

[8] 石田晋哉，荒川伸一，村田正幸．べき乗則に従う WDM ネットワークにおける論理トポロジー設計．電子情報通信学会技術研究報告 (PN2003-27), December 2003.