断片ダークネット・アドレス宛てパケット収集ブリッジの開発と評価

今間　俊介† 福田　健介‡ 廣津　登志夫* 菅原　俊治†

† 早稲田大学理工学部　‡ 国立情報学研究所　* 豊橋技術科学大学

1 はじめに

インターネット上の様々なサービスに対し、DoS 攻撃、Virus や Worm による侵入などの妨害処理があり、社会的に問題になっている。これに対し、各種の侵入検知システム、攻撃検知システムが提案されている。

インターネットに対する攻撃の検知手法の種類は、アクティブ手法とパッシブ手法に分類される。アクティブ手法には、Honeypot/Honeynet[4] がある。特徴としては、攻撃を受けたソフトウェアの挙動を模倣し、攻撃の詳細な情報を得ることができる反面、ホストにかかる負荷により監視ネットワークが広げられない、backscatter による二次被害が起こりうるという欠点を持つ。パッシブ手法としては、Network telescope[1]、Blackhole/Darknet[5] が挙げられる。これら手法は、実際にはホストが存在しない IP アドレス宛ての（本来ありえない）パケットを収集、解析を行うことにより攻撃の情報を得るため、観測ホストに負荷がかからず、二次被害も起こらない。特に我々はこの中で Darknet による攻撃パケットの検出に着目している。[2]

しかし、これまでの Darknet 観測は、例えば、/12 などのように広大な不使用 IP アドレス空間を観測することが主であったが、このような広い空間を用意することは難しい。一方で、各組織に割り当てられた IP アドレス空間は、100% が使用されている訳ではなく、いわゆる虫食い状態で使われていると考えられる。そこで本研究では、ブリッジとしてルータの直後に設置し、ネットワーク内で稼働する IP アドレスを自動抽出しながら、未使用アドレス（ダークアドレス）宛へのパケットを収集する観測用ブリッジを開発した。本発表では、その概要と評価結果を述べる。

2 システム構成と実装

2.1 システム構成

システムの基本的な機能は、通常のブリッジ機能に加えて、受信したパケットをフィルタして、未使用アドレス宛パケットを DB に収集する。システム構成図を、図 1 に示す。図上では、太線はパケットの流れ、実線は未使用アドレスデータ読み書き、点線は未使用アドレス宛パケットデータをそれぞれ示している。フィルタする際に、宛先アドレスを見て、未使用アドレス検出 (Unused Address Detection、以下 UAD と記述) 機能を使用してホストの生存確認し、生存していない場合のみ DB にパケットデータを保存する。この UAD 機能は、ルータの内部において、ブリッジと同一サブネットに設置された未使用アドレスの検出を行う。

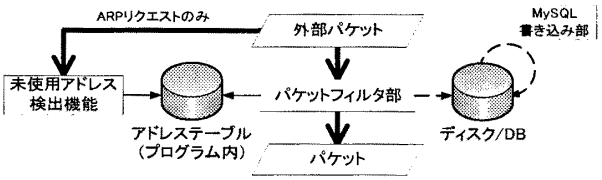

図 1　システム構成図

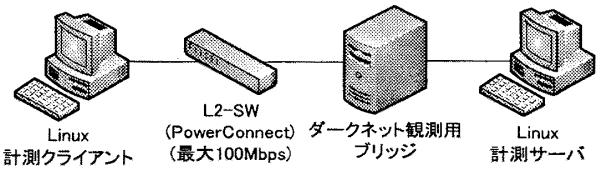

図 2　実験環境図

ハードウェア

CPU	Core 2 Duo E6300
メモリ	1GB

ソフトウェア

OS	CentOS Linux 5
libpcap	0.9.4-8
mysql	5.0.22-2
perl	5.8.8-10

表 1　ブリッジ用実験マシンの概要

2.2 実装

前述のブリッジを、Linux 上に構築した。パケットを収集するプログラムは、perl、libpcap ライブラリを使用し、パケットを収集し直接ディスクに保存するスレッド（パケットフィルタ部）、保存したパケットを読み込み MySQL DB に登録するスレッド（MySQL 書き込み部）、未使用アドレス検出スレッド（未使用アドレス検出機能）からなるマルチスレッドプログラムを実装した。

今回、UAD 機能には、ARP を用いた。上位ルータが、未使用アドレス向けの ARP リクエストを発行すると、観測機もそのホストの生存チェックを行い、返答がない場合、観測機自身の MAC アドレスを載せた ARP 返答をルータに返し、該当パケットを収集する。

3 実験と評価結果

3.1 実験環境

ダークアドレス宛てパケット検出・収集及び UAD 機能を実装したことによる効率の評価を行った。計測は、ネットワークスループット計測ソフトである iperf を使用し、帯域幅を自由に設定することができる UDP でパ

Development and evaluation of the bridge with packet capture for fragmented darknet addresses

Syunsuke KOMMA†, Kensuke FUKUDA‡, Toshio Hirotsu*, Toshiharu SUGAWARA†

†Waseda University, Faculty of Science and Engineering

‡National Institute of Informatics

*Toyohashi University of Technology

ケット収集状況を計測した。iperf がクライアント/サーバ型のソフトであるため、計測用マシンは 2 台用意し、クライアントからサーバにパケットを帯域幅 10~100Mbps の範囲で流し、ブリッジでのパケット収集状況を評価する。今回の計測では、計測クライアントを上位ルータに見立てて行う。使用した実験環境図は図 2 に、ブリッジの概要については表 1 に示す。なお、ブリッジのみの機能を当該マシンに実装したところ、最大で 95.7Mbps のスループットを得られた。

3.2 UAD 機能なしの場合

この実験では、観測機を間に挟み UAD を未使用で、(1) 収集対象パケットしか流さない場合、(2) 収集対象外パケットを 10Mbps 流す、(3) 収集対象外パケットを 50Mbps 流す（実際には、対象パケット、対象外パケットのスループットの合計は、スイッチの上限値である 100Mbps になる）、という 3 パターンについて観測を行った。なお、対象外パケットとは、使用アドレス宛てのパケットを意味し、UAD 未使用状態は、ダークアドレスが予め与えられた場合、もしくは既に UAD による未使用アドレス検出が完了している状態に相当する。

ブリッジにおけるパケットドロップ数の結果を、図 3 に示す。どの場合も、受信側スループットが 40Mbps を超えたあたりからドロップが発生しているのだが、特に、(3) の場合は顕著に見られる。これは、パケットを収集して単純にディスクに書き込むスレッドで、対象外パケットの処理の影響でディスク I/O が流れるパケットの速度に追いついていないから、と予想される。ただ、ディスクでドロップは発生しても、受信側で観測される対象外パケット数は送信側が流した対象外パケット数と一致し、libpcap のバッファリング機能により、観測機のパケット収集動作が観測対象外のパケットをドロップさせることは観測されなかった。

3.3 UAD 機能ありの場合

観測機の UAD 機能設定では、上位ルータが出した ARP リクエストの宛先に対して、観測機自身からも ARP リクエストを出し、1 秒間待って返答がない場合自身の MAC アドレスを載せて返答を返す。宛先ホストの MAC アドレスが ARP キャッシュに入っていない場合、観測機からの ARP 返答が来るまでのパケットは収集できないので、ブリッジでは最初の 1 秒分を除いたパケットが収集される。UAD 機能なしの場合と同様、どの程度パケットがドロップされるかを調べるため、/24 の darknet を対象として収集パケットのドロップ数を調査した。グラフは、図 4 に示す。UAD 機能なしの場合とほぼ同じく、50Mbps からドロップが発生している。なお、上記はすべてのパケットが収集対象であり、前節での (1) に相当する。しかし、実際のネットワークでは未使用アドレス宛のパケットの割合は小さく、本実験の結果は実用的には問題のないと言える。

4 おわりに

本研究では、未使用アドレス宛てパケット収集を行う観測ブリッジについて、収集スクリプトを用い、収集スループット、送受信マシンでの通信への影響の評価を行った。今後の課題としては、プログラムの C 言語への移植による速度向上、Gigabit Ethernet 上でのスループット評価がある。また、ルータの上流側に本ブリッジを配置することを想定した実装も挙げられる。

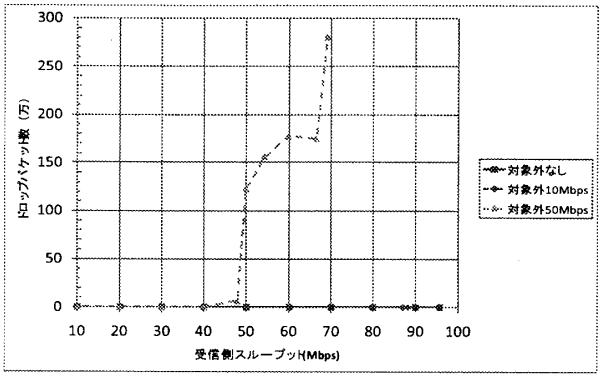

図 3　ドロップパケット数比較

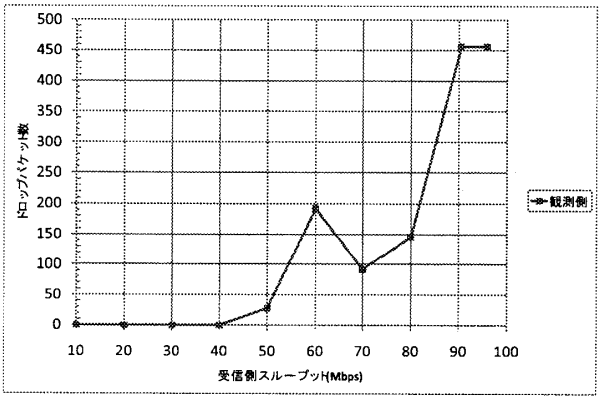

図 4　UAD 使用時のドロップパケット数

謝辞

本研究は科学研究費補助金特定領域「情報爆発時代に向けた新しい IT 基盤技術の研究」の支援を受けている。

参考文献

[1] D. Moore, C. Shannon, G. Voelker, and S. Savage. "Network telescopes: Technical Report," CS2004-0795, UC San Diego, July 2004.

[2] 廣津, 福田, 栗原, 明石, 菅原, "断片アドレス を用いた分散協調インターネット監視に関する一考察," SWoPP 2007, 情報処理学会 OS 研究会, Vol. 2007, No. 83, pp.39–45, 2007.

[3] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson. "The Internet Motion Sensor: A distributed blackhole monitoring system," NDSS'05, 2005.

[4] The Honeynet Project & Research Alliance: Know your Enemy: Honeynets, 2003. http://www.honeynet.org/papers/honeynet/.

[5] E. Cooke, M. Bailey, F. Jahanian, and R. Mortier, "The Dark Oracle: Perspective- Aware Unused and Unreachable Address Discovery," NSDI'06, pp.101–114, 2006.