分散協調監視アーキテクチャにおける拠点間の攻撃情報通知フレームワークの開発と評価

今間　俊介† 福田　健介‡ 廣津　登志夫* 菅原　俊治†
†早稲田大学基幹理工学研究科 ‡国立情報学研究所/科学技術振興機構 *法政大学情報科学研究科

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攻撃やウィルス、ワームによる侵入などの妨害処理があり、社会的な問題になっている。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。この攻撃検知システムの中で、我々は特にDarknetによる攻撃パケットの検出に着目している。

[1]で提案されている分散協調監視アーキテクチャでは、複数拠点のDarknetに攻撃検知マシン(以下、監視エージェントと記述)を配置し、使用されているネットワークのエージェントに攻撃情報データを通知することで、攻撃を未然に防ぐことを目的としている。また、Darknetに到着したパケットを観測すると、アドレススキャン型攻撃が頻繁に発生していることがわかっている[2]。そこで本研究では、監視エージェントを複数拠点に設置し、条件に適合した攻撃検知時に、監視エージェント同士が自律的に情報を共有するフレームワークを開発し、その性能を評価する。

2 フレームワーク構成と実装

2.1 フレームワーク構成

フレームワークの機能を以下に示す。パケットキャプチャを行い、攻撃判定部で受信したパケットが攻撃かどうかを判定する。攻撃と判定された場合は、他の監視エージェントに攻撃情報パケットを通知する。攻撃情報パケットの内容は、送信元IPアドレス、最初に攻撃されたIPアドレス、プロトコル番号、攻撃パケットの宛先ポート番号、攻撃開始時間、攻撃速度、攻撃パケット数、オプションフィールドで構成される。フレームワーク構成図を図1に示す。図中で、太線はパケットの流れを、細線は攻撃情報の読み書きをそれぞれ示している。メインスレッド部では、攻撃判定部による攻撃/非攻撃の判定結果から、受信した外部パケットを攻撃パケットと非攻撃パケットに分離して保存する。

2.2 実装

監視エージェントを、Linux上に構築した。エージェントプログラムはCで実装、パケット収集モジュールにlibpcapを使用し、エージェント間通信用のトランスポート層プロトコルとしてTCPを使用した。プログラム内部は大きくメインスレッド部、攻撃判定部、攻撃情報受信部の3つに分かれている。メインスレッド部

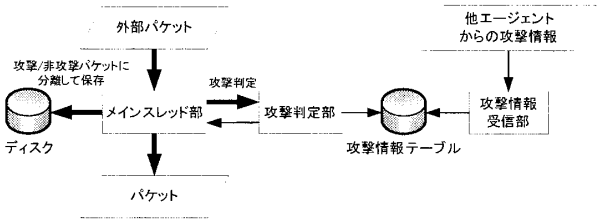

図1: フレームワーク構成図

では、他のエージェントとの接続ソケットの管理、攻撃判定部への攻撃パケットの判定依頼、攻撃情報パケットの送信、パケットの保存を行う。攻撃判定部では、メインスレッド部から受信したパケットの攻撃を判定する。攻撃判定部の実装の詳細については、第2.3節で述べる。攻撃情報受信部では、他のエージェントから受信した攻撃情報を、既に登録されている情報と比較して、受信した攻撃情報の方が新しい場合、自分の攻撃情報テーブルに登録する。なお、パケットを受信して攻撃検知をしながら、他のエージェントから通知される攻撃情報を登録・更新しなければならないため、処理をメインスレッド部と攻撃判定部のスレッド、攻撃情報受信部のスレッドに分離したマルチスレッドプログラムを実装した。

2.3 攻撃判定部実装

本研究の評価では、TCP-SYNパケットに着目し、Webサイト閲覧、メール送受信など通常のTCP接続ではあり得ない、短時間に複数のホストにTCP接続を開始しようとするパケットを攻撃と判定する実装を使用した。具体的には、パケットを受信する度に(送信元IPアドレス, 宛先ポート番号)のペア(キー)を攻撃情報テーブルに登録し、同じキーで登録された情報で宛先IPアドレスが変化していた場合、攻撃と判定した。この時の攻撃情報パケット内の攻撃速度フィールドには、以下式(1)で計算された値が代入される。

$$\text{攻撃速度} = \frac{IP_2 - IP_1}{t_2 - t_1} \quad (1)$$

ここで、t_1は登録されている攻撃情報の時間、IP_1は登録されている攻撃情報の宛先IPアドレス、t_2は受信パケットの日時、IP_2は受信パケットの宛先IPアドレスを示している。

3 実験と評価結果

3.1 実験環境

開発したフレームワークの性能評価を行った。本研究では、テスト機1(192.168.64.0/24を受信)、テスト機2(192.168.65.0/24を受信)に対して、ペネトレーションテストツールであるhping3[3]を使用し、ルータマシン

Development and evaluation of the attack information notification framework for distributed cooperative attack monitoring architecture
Syunsuke KOMMA†, Kensuke FUKUDA‡, Toshio HIROTSU*, Toshiharu SUGAWARA†
†Department of Computer Science and Engineering, Waseda University
‡National Institute of Informatics/Japan Science and Technology Agency
*Faculty of Computer and Information Sciences, Hosei University

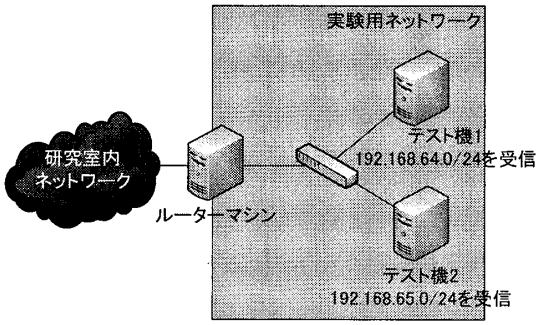

図 2: 実験環境図

表 1: テスト機の概要 (ハードウェア)

	ルータマシン	テスト機 1	テスト機 2
CPU	Xeon X3353	Core 2 Duo E6300	Xeon 3050
メモリ	4GB	1GB	4GB
NIC	BCM5722	Broadcom BCM5754	

表 2: テスト機 (共通) の概要 (ソフトウェア)

OS	CentOS Linux 5.4
kernel	2.6.18-164
libpcap	0.9.4-14

から 192.168.64.0/23 に向けて、1000 アドレス/秒の速度でアドレススキャン型攻撃パケットを送信した。今回使用する実験環境図は図 2 に、実験で使用したマシンの概要については表 1、表 2 に示す。

評価は、テスト機 1 が Darknet 担当エージェント、テスト機 2 は使用されているネットワークを担当するエージェントという想定で行った。テスト機 2 で動作するエージェントの攻撃判定部を無効にし、テスト機 2 ではテスト機 1 から通知される攻撃情報だけを基に攻撃パケットを防御する。

3.2 攻撃情報通知パケットへの遅延付加による攻撃情報通知への影響の評価

本実験では、ネットワークエミュレーションソフト netem[4] を使用して、テスト機 2 において、テスト機 1 から受信する攻撃情報パケットに 10~100ms の 10ms 刻み、100~1000ms の 100ms 刻みで遅延を追加し、それぞれ 10 回の実験を行い、攻撃情報パケットの伝送遅延が攻撃防御に与える影響の評価した。

テスト機 2 における防御率 (=防御パケット数/受信パケット数) のグラフを図 3 に示す。図 3 から、伝送遅延が 200ms までは伝送遅延による攻撃パケットの防御に影響が出ないことが確認できる。300ms から、テスト機 2 がテスト機 1 から攻撃情報パケットを受信して攻撃情報テーブルに登録する前に、攻撃パケットを受信してしまう量が徐々に増加し、1000ms 遅延が起こると、80%まで防御率が下がる。これは、1000 アドレス/秒のアドレススキャン型攻撃で、テスト機 1 の/24 ネットワーク (=256 アドレス) を網羅するまで 256ms かかる。したがって、その時間内にテスト機 2 に攻撃情報が通知できればテスト機 2 で攻撃パケットが防げることから、整合性のある結果であると言える。遅延が増加すれば、テスト機 2 は攻撃情報を受信するまでは防御できないので、防御率は低下する。

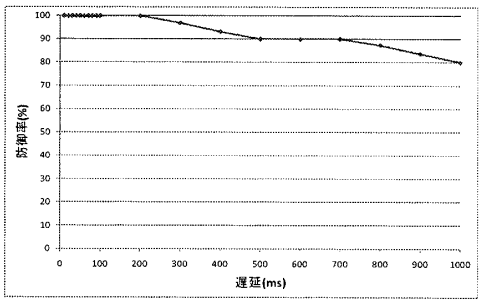

図 3: テスト機 2 での攻撃パケット防御率 (遅延付加実験)

3.3 攻撃情報パケットのサイズによる攻撃情報通知への影響の評価

この実験では、攻撃情報パケットに 0~16,000 バイトのダミーデータを追加し、それぞれ 100 回の実験を行い、テスト機 1 からテスト機 2 へ通知される攻撃情報パケットのパケットサイズが攻撃防御に与える影響の評価をした。その結果、全てのサイズにおいて、防御率が 100%であることを確認した。

4 おわりに

本研究では、攻撃パケット受信時に自律的に攻撃情報を共有する攻撃情報通知フレームワークについて、監視エージェントのプログラムを動作させ、エージェント間の攻撃情報パケット通知への影響の評価を行った。その結果、遅延が攻撃速度よりも短ければ、攻撃情報の通知により、未然に防ぐことができた。今後の課題としては、未使用アドレス検出機能 (UAD)[5] による、実際に使用されているアドレス空間での攻撃検知への対応、別の条件を利用した攻撃判定部での性能計測が挙げられる。

参考文献

[1] 廣津登志夫, 福田健介, 栗原聡, 明石修, 菅原俊治. 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. 情報処理学会 OS 研究会研究報告 (83), pp. 39–45, 2007.

[2] 杉本周, 福田健介, 廣津登志夫, 明石修, 菅原俊治. 特定のアドレス空間を基準とした遅延相関解析によるインターネット上の攻撃予測の可能性. インターネットテクノロジーワークショップ (WIT), 2009.

[3] Hping - Active Network Security Tool. http://www.hping.org/.

[4] netem. http://www.linuxfoundation.org/collaborate/workgroups/networking/netem.

[5] 今間俊介, 福田健介, 廣津登志夫, 菅原俊治. 断片ダークネットのためのパケット観測用ブリッジの提案. インターネットテクノロジーワークショップ (WIT), 2008.