1L1-R-7-2

パケット監視エージェント間協調による不正アクセスの発信源特定手法の提案と評価

Suggestion and evaluation of the specific technique of the dispatch source of the unjust access by cooperation between packet monitoring agent.

郷原啓資[*1] 西山裕之
Gohara Keisuke Nishiyama Hiroyuki

[*1]東京理科大学理工学研究科経営工学専攻
Graduate School of Science and Technology, Tokyo University of Science

In recent years, damage by the unjust access is a tendency to increase. Therefore, in this study, I built the system which could be tied to the identification of the dispatch source of the attack by incorporating packet monitoring agent which write the information of user in packets to pass Edge Router (the router which is located between a network of the organizations such as a company or the university and the Internet) and hold digest of the packet in Edge Router and cooperating between agents.

1. はじめに

近年，インターネットの普及により，不正アクセスによる被害が増加している．特に大量のパケットを送りつけてサーバなどのシステムを停止させる DoS(Denial of Service) 攻撃や DDoS(Distributed DoS) 攻撃は最も脅威のある攻撃の 1 つである．これらの攻撃では，トラフィックを急激に上昇させることでネットワーク全体に大きな負荷をかけたり，IP アドレスの偽造や DDoS 攻撃のような複数の攻撃元が存在するといったことから攻撃者の特定が困難となっている．

そこで，本研究では，エッジルータ (企業や大学などの組織のネットワークとインターネットの境界に位置するルータ) を通過するパケットに対してユーザ情報の書き込み及びそのパケットのダイジェストの保持を行うパケット監視エージェントをそのエッジルータ内に組み込み，パケット監視エージェント間で協調し合うことで攻撃の発信源の特定に結びつくことができるシステムを構築した．

2. 設計方針

本節では，エッジルータ内に組み込むパケット監視エージェントの 2 つの機能 (パケット書き込み機能・ダイジェスト問い合せ機能) とそのシステムフローについて述べる．

2.1 パケット書き込み機能

パケット書き込み機能とは，パケット監視エージェントが自身が配置されているエッジルータを通過するパケットの IP ヘッダ中にユーザ情報 (エッジルータ自身の IP アドレス) を書き込み，そのパケットを受信したパケット監視エージェントで受信したパケットに書き込まれているユーザ情報を解析して発信元を特定する機能である．この機能は潘ら [1] の発信元特定に使われており，この機能を使うことで全てのルータにパケット監視エージェントを配置しなくても，エッジルータのみ配置させれば発信元の特定が可能である．

2.2 ダイジェスト問い合せ機能

パケット書き込み機能だけでは関係のないエッジルータを特定してしまう誤検知が多く発生するため，パケット監視エージェント間の通信に基づいたダイジェスト問い合せ機能をパケット監視エージェントに付け加えることで誤検知数を抑えていく．ダイジェスト問い合せ機能とは，パケット監視エージェントが通過するパケットのダイジェストを常に保持しておき，攻撃パケットを受信したパケット監視エージェントがその攻撃パケットのダイジェストを生成して外部のパケット監視エージェントにその攻撃パケットのダイジェストの有無を問い合せる機能である．この機能のみを用いて発信元の特定を行う研究 [2] は数多くあるが，通信路上の全てのルータにその機能が備わっていなければならないといった問題が生じる．

連絡先: 郷原啓資，東京理科大学，j7412610@ed.tus.ac.jp

2.3 システムフロー

本システムは攻撃者側（発信側）と被害者側（受信側）のパケット監視エージェントで構成されている．

2.3.1 攻撃者側のパケット監視エージェントのシステムフロー

攻撃者側のパケット監視エージェントがエッジルータを通過する 1 つのパケットを 4 つのパケットに複製し，その複製した 4 つのパケットの IP ヘッダ中に分割したユーザ情報をそれぞれ書き込んでいく．そして，書き込みを行ったパケットのダイジェストをその攻撃者側のパケット監視エージェントがそれぞれ保持する．

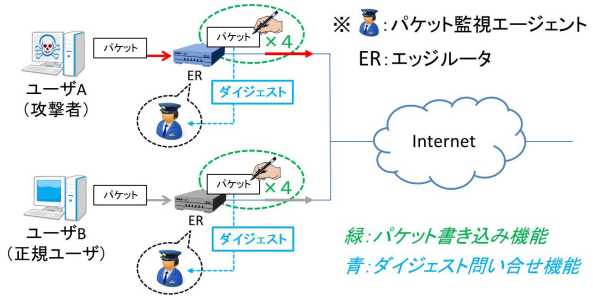

図 1: 攻撃者側のパケット監視エージェントのシステムフロー

2.3.2 被害者側のパケット監視エージェントのシステムフロー

常に被害者側のエッジルータを通過するパケットの IP ヘッダ部分だけをその被害者側のエッジルータのデータベースに保存していくことで，分割されたユーザ情報を被害者側のパケット監視エージェントに保持していく．被害者側のパケット監視エージェントが攻撃パケットを検知した場合，被害者側のパケット監視エージェントが保持している分割されたユーザ情報から検知した攻撃パケットに書き込まれている情報にもとに検索を行い，該当するものを統合していくことで攻撃者候補を導いていく．ここで，攻撃者候補を複数導いてしまった場合に

は，検知した攻撃パケットからダイジェストを生成し，攻撃者候補として挙げられた攻撃者側のパケット監視エージェントに保存してあるダイジェストと比較を行うことで発信元のエッジルータを特定していく．

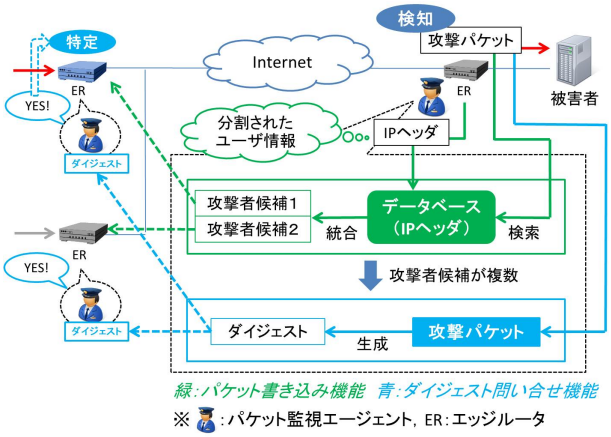

図 2: 被害者側のパケット監視エージェントのシステムフロー

3. 実装

本システムにおけるエッジルータは通常の PC を使用し，OS は CentOS，開発言語は C 言語を用いた．また，パケットなどを保存するデータベースには PostgreSQL8.1 を使用した．

本研究では，以下の図 3 のような本システムに適応していないルータを含んだ小規模ネットワークを実際に構築し，2.3.2. で登場した攻撃者候補が複数になるように攻撃者と正規ユーザのエッジルータの IP アドレスをそれぞれ設定して，構築した小規模ネットワーク上で被害者端末から本システムを用いた発信元の特定を行った．

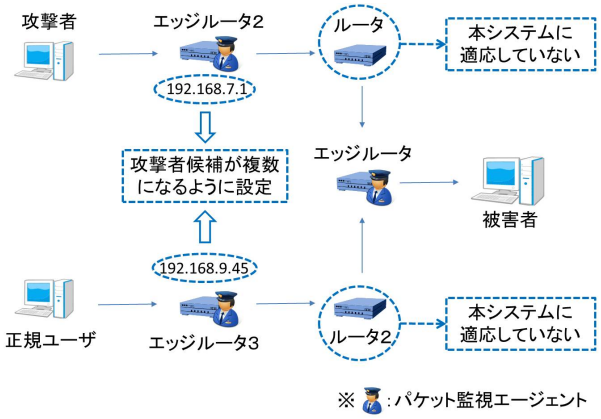

図 3: 構築したネットワーク

その結果，正規ユーザ側のエッジルータを誤検知せず，攻撃者側のエッジルータのみ検出することに成功した．しかし，本システムを適応したネットワークからのインターネットの利用が困難であることもこの実験を通して判明した．

4. 評価

大規模なネットワークにおける本システムの誤検知台数の測定をシミュレーションを使って評価した．

4.1 シミュレーション評価の概要

本シミュレータでは，エッジルータの IP アドレスを数万単位で生成し，その中で攻撃者側のエッジルータの IP アドレスを指定していく．そして，パケット監視エージェントが備える機能がパケット書き込み機能のみである既存モデルと備える機能がパケット書き込み機能とダイジェスト問い合せ機能の両方である本提案モデルのそれぞれを用いた攻撃者側のエッジルータの特定を行う．ここで，攻撃者とは関係のないエッジルータを特定した数を誤検知台数とする．

4.2 シミュレーション評価の結果と考察

本シミュレータを攻撃台数 50 台から 50 とびで 400 台までの 8 つの場合に分けて，既存モデルと本提案モデルの誤検知台数を測定し，この測定を 1000 回繰り返してそれぞれの誤検知台数の平均を算出した結果，表 1 のような結果が得られた．この結果から，本提案モデルでは攻撃台数が増加しても既存モデルのような誤検知台数の急激な増加がみられないことがわかる．これにより，本提案モデルでは，DDoS 攻撃に対しても有効であることが考えられる．

表 1: シミュレーションにおける誤検知台数の平均の測定結果

攻撃台数	既存モデル	本提案モデル
50	344.86	0.16
100	1571.93	0.76
150	4978.33	1.54
200	12135.16	2.89
250	25412.26	4.35
300	47533.13	6.46
350	80991.28	8.57
400	130520.21	10.83

5. おわりに

DoS（Denial of Service）攻撃や DDoS（Distributed DoS）攻撃に対する対策の 1 つとして，本研究では，パケット書き込み機能とダイジェスト問い合せ機能を備えたパケット監視エージェントをエッジルータ内に組み込み，パケット監視エージェント間で協調し合うことで発信元の特定を可能にする本システムを構築した．そして，実際に構築した小規模ネットワーク上で本システムを用いた実験を行ったことでエッジルータのみパケット監視エージェントを配置すれば発信元特定が可能であることを確認し，シミュレーションによる評価を行ったことで本システムが DDoS 攻撃に対しても有効であることが示された．しかし，攻撃者側のパケット監視エージェントが通過する 1 つのパケットから攻撃者側のエッジルータの IP アドレスを分割した分だけパケットを作り変えることから回線帯域を多く使うため，通常のインターネットの利用が困難であったことが実験を通して判明した．今後，回線帯域の問題を解決するためのパケット生成率を考慮しつつ，踏み台 PC を用いた DDoS 攻撃の発信元特定にも対応したシステムの構築を行なっていく．

参考文献

[1] 潘 博文, 佐々木 良一. IP トレースバックのための出国印方式の試作と評価. 情報処理学会論文誌, Vol.51, No.9, pp.1610-1621, 2007

[2] 甲斐 俊文, 橋口 輝, 中谷 浩茂. Hash ベース IP トレースバックシステムの改良方式の提案と評価. 情報処理学会論文誌, Vol.51, No.3, pp.673-681,2010