4ZC-05

# ファイアウォールのデフォルトルール検出を防ぐ Delay Induced Response (DIR) 方式のための 優先ユーザ選択による通信遅延の改善

井田学† 木村成伴‡

†筑波大学情報学群情報メディア創成学類 ‡筑波大学システム情報系情報工学域

## 1. はじめに

ネットワークのセキュリティ機能の一つであるファイアウォールは，予め管理者が設定したルールセットに基づいて通過するパケットのフィルタリングを行うことで，外部ネットワークから企業等の内部ネットワークを保護する役割を持つ．ネットワークシステムのリソースに意図的に負荷をかけ，正当なユーザがサービスを利用できないようにする DoS 攻撃(Denial-of-Service attack)では，このファイアウォールを標的としたものが存在する．このとき攻撃者は様々なパケットを送り，それらに対するサーバからの返答時間からファイアウォールの処理に負荷のかかるパケットを特定する．そして，そのパケットを大量に送信することでファイアウォールのリソースを奪い，サービスを妨害する．

この攻撃に対する防御手法として，サーバからの返答時間にランダム時間の遅延を導入することで，攻撃者が処理負荷を特定できないようにする DIR (Delay induced Response)方式が提案されている[1]．しかし，DIR 方式では通信全体にランダム時間の遅延を導入するため，ネットワークの通信品質が低下してしまうという問題点があった．

そこで本論文では，通信を行うユーザを正規のユーザと推定される優先ユーザと，攻撃者の疑いのある非優先ユーザに分別し，非優先ユーザの通信に対してのみランダム時間の遅延を導入することでネットワークの通信品質の低下を抑える方法を提案する．但し，優先ユーザと非優先ユーザの判別方法は本論文の範囲外とする．そして，通信実験から，提案方式では優先ユーザの遅延が増えないことを確認する．

## 2. DIR (Delay Induced Response)方式

図 1 に示すように，ファイアウォールでは管理者が予め設定したルールに基づいて，通過するパケットの許可や拒否などのフィルタリングを行う．各ルール(図の R1～R4)は逐次的に並んでおり，最上位に位置するルール(図では R1)から通過するパケットに対応するルールとマッチするまで一つずつ順に照会していくため，より下位のルールにマッチするパケットほど処理に時間を要する．特に，最下位のルール(図では R4)はデフォルトルールと呼ばれ，このルールに至るパケットがファイアウォールに最も高い負荷をかけることになる．

DIR 方式では，サーバの応答時間から攻撃者がデフォルトルールに至るパケットを発見するのを防ぐために，ファイアウォールを通過する通信全体にランダム時間の遅延を導入する．この時，元の通信時間を考慮し，上位のルールには大きな遅延を，デフォルトルールを含む下位のルールには小さな遅延を加えることで，ルールの位置の解析をより困難にする．図 1 の例では，最上位のルール(R1)にマッチしたパケット A に 50 μs の遅延が，本来の応答時間 30 μs に追加されたのに対し，デフォルトルール(R4)にマッチするパケット B に対する本来の応答時間 50 μs に 10 μs の遅延が追加され，パケット A に対する応答時間よりも，パケット B への応答時間の方が短くなっている．

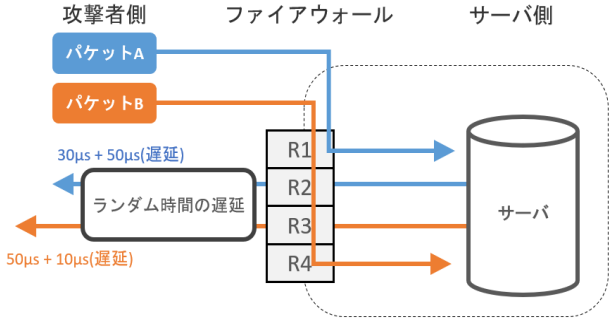


図 1:DIR 方式の動作例

## 3. 提案方式

前章における DIR 方式では，ファイアウォールを通過するすべてのパケットにランダム時間の遅延を導入していたために，正規ユーザの通信品質も低下してしまうという問題があった．そこで本章では，通信を行うユーザを正規ユーザ

Improvement of Communication Delay for Priority Users in Delay Induced Response (DIR) Method to Prevents from Detecting Default Rule in Firewall
Manabu IDA† and Shigetomo KIMURA‡
†Collage of Media Arts, Science and Technology of Informatics, University of Tsukuba

と推定される優先ユーザと攻撃者の疑いのある非優先ユーザに分別し，非優先ユーザの行う通信にのみランダム時間の遅延を導入することで，優先ユーザの通信品質の低下を抑える改善方法を提案する．

ユーザの分別は，様々な方法が考えられるので，本論文では規定しない．例えば，(1)送信元 IP アドレスより，特定のサブネットからの通信なら優先ユーザと見なすことが考えられる．また，(2)ある送信元アドレス(もしくは，サブネット)からの一定期間内の通信頻度が規定値以内であるか，(3)外部アプリケーションで認証されているか，などで選択する方法などが考えられる．

## 4. 実験

提案方式の有効性を確認するため，図 2 に示すトポロジで，前章で述べた(1)の選択方法により通信実験を行った．図のユーザ PC は，非優先ユーザと優先ユーザの IP アドレスを切り替えて，実験をそれぞれ行った．サーバ兼ファイアウォールにおいて，ファイアウォールには iptables を用い，特定のポートへのアクセスを拒否(REJECT)するルールを 50 個(R1～R50)設定した．さらに，tc (traffic control)コマンドの netem (Network Emulation)を用いて，非優先ユーザの IP アドレスからの通信に対してのみ，ランダム時間の遅延を R1～R9 は 60～120 μs，R10～R29 は 40～100 μs，R30～R39 は 20～90 μs，R40～R49 は 20～80 μs，R50 は 10～50 μs の範囲の一様乱数で導入した．すなわち，全てのルールで応答時間がほぼ同じになるように，最初の方にマッチするルールには長い遅延を，最後の方にマッチするそれには短い遅延を追加している．伝搬遅延は，ファイアウォールや tc コマンドをオフにして，ping コマンドで 10 回測定したときの平均値である．この条件下で優先ユーザと非優先ユーザは，telnet コマンドを用いてファイアウォールで拒否するポートにアクセスを行い，TCP の SYN パケットを送信した時刻とそれに対する ICMP port unreachable メッセージが届いた時刻を tcpdump で観測し，その差から応答時間を求める．

最上位の R1 から R10，R20，R30，R40，R50(デフォルトルール)に対応するポートへのアクセスを，優先ユーザ，非優先ユーザともに 10 回ずつ行った時の応答時間を図 3，図 4 にそれぞれ示す．図 3 より，優先ユーザの通信では，応答時間が概ねルールの並び順に並んでおり，不必要な遅延が入っていないことが分かる．これに対して，図 4 では，R1 よりも R50 にマッチした通信への応答時間の方が短い場合がある等，どのルールに対しても応答時間が不規則であり，デフォルトルールの発見が困難になっている．

## 5. まとめ

本論文では，DIR 方式を改良するため，優先ユーザと非優先ユーザに分類し，非優先ユーザに対してのみ遅延を導入する方法を提案し，実験を通してその有効性を示した．今後は他のユーザ分別方法の更なる検討と実験を行う．

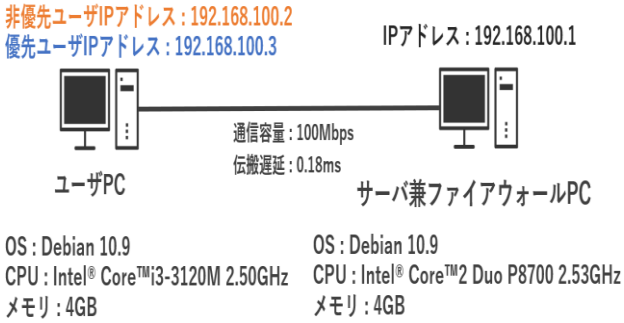


図 2:実験トポロジ

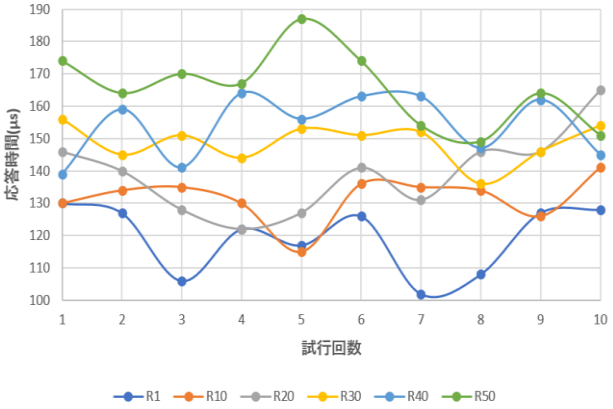


図 3:優先ユーザへの応答時間

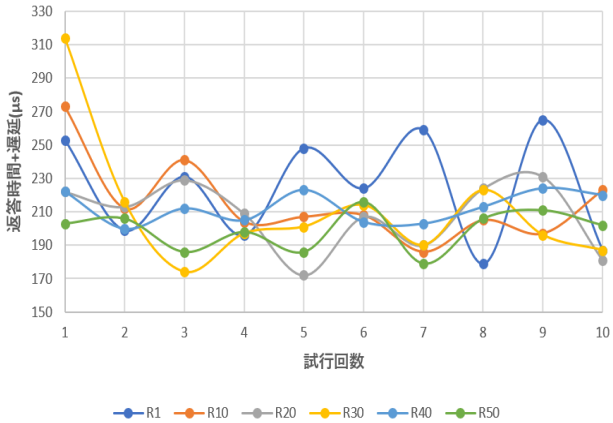


図 4:非優先ユーザへの応答時間

## 参考文献

[1] K. Sattar, K. Salah, M. Sqalli, R. Rafiq, and M. Rizwan, A Delay-Based Counter-measure Against the Discovery of Default Rules in Firewalls, Arabian Journal for Science and Engineering, Vol. 42, pp. 833-844, Springer (2017).