L-007

シミュレーション端末における通信のロバスト性に関する研究
Research on robustness of communication in simulation terminal

菊地　翔吾 †　　松田　勝敬 ‡
Shogo Kikuchi　Masahiro Matsuda

1. はじめに

昨今,防犯・防災意識の高まりと共にネットワークを用いたセキュリティ機器の開発や普及が進んでいる.これらセキュリティ機器はインターネット関係の技術を用いてネットワーク接続をする機器も多い.例えば,緊急地震速報[1]の様に,インターネットなどの技術を使った従来なかった,新しいセキュリティ機器も登場している.

これらの機器は家庭などの設置する端末機器,と情報を収集・配信するサーバから構成されることが多い.セキュリティ機器には,専用のハードウェアが用いられており,NIC(Network Interface Card)は,10BASE-T が用いられている事が一般的である.また,10BASE-T は flood 系のネットワーク攻撃に対して脆弱である事がわかっている[2].

今回は,NIC の規格を 10BASE-T,100BASE-TX,1000BASE-T に変えた環境において,DoS(Denial of Service)攻撃[3]の一つである,PingFlood 攻撃[4]時の対障害性について比較検討を行った.

2. システム

本研究では,ネットワークを利用するセキュリティ機器を想定した,ソフトウェアシミュレーションプログラムの開発を行った.シミュレーション端末は,ネットワークの信頼性を向上させる TCP(Transmission Control Protocol)[5]を使用している.機能としては,シミュレーション端末から情報配信収集サーバに対して端末確認データを送信する. 情報配信収集サーバが,端末確認データを解析し, 情報配信収集サーバからシミュレーション端末へ端末確認応答を送信する.この動作がある為, 情報配信収集サーバは端末の接続の有無, 複数の端末が接続されていた場合は,どの端末が接続されているか確認することができる.また,開発したシミュレーション端末から, 情報配信収集サーバへ端末確認データの送信時に障害などが発生し,データの送受信が行われなかった場合や,異なった端末のデータがシミュレーション端末に送信されてきた場合は,シミュレーション端末が端末確認応答のデータを比較し,異変を知らせてくれる機能となっている.

3. Ping Flood

Ping Flood 攻撃は,膨大な数の ICMPECHO_REQUEST パケットを相手の端末に対して送信する攻撃である.攻撃者はターゲットに対し,ICMP ECHO REQUEST パケットを送り続ける.通常 Ping では,送信先からの応答を確認するか,一定時間後に次の通信を行うが,Ping Flood 攻撃では,送信先からの応答や待機は行わず,パケット通信を行う.そのため,送信先は,受信した ICMP ECHO REQUEST に対する,ICMP ECHO_RESPONSE の応答を処理することになる.受信側の機器のデータ処理能を超えた場合,正常な通信が行われなくなる場合がある.本研究では,この Ping Flood 攻撃を用いて実験を行った.

†東北工業大学大学院工学研究科 Graduate school of Engineering Tohoku Institute of Technology

‡東北工業大学工学部 Faculty of Engineering, Tohoku Institute of Technology Institute of Technology

4. 実験環境

図 1 に実験環境の概要を示す.

シミュレーション端末の OS は Linux 開発言語は Java を用いた. 情報配信収集サーバも,OS は Linux を用いている. シミュレーション端末に Ping Flood 攻撃を行う攻撃用 PC①,PC②の OS は Windows XP を用いた.また,通信データをキャプチャーする為に,パケットアナライザーを用いてパケットキャプチャーを行った.スイッチングハブは,1000Mbps, 100Mbps,10Mbps 対応のスイッチングハブをそれぞれ用いた.

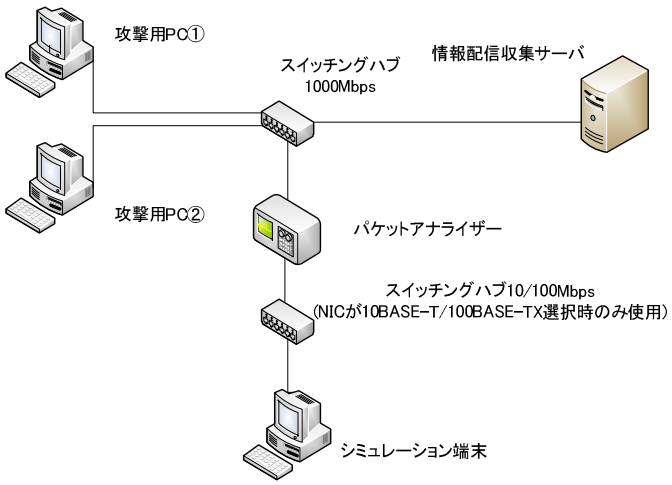

図 1　実験環境

5. 実験方法

シミュレーション端末 PC の NIC を 10BASE-T,100BASE-TX,1000BASE-T の規格を有する物にそれぞれ変更する.しかし,本研究では 10BASE-T と 100BASE-TX の両方の規格を有している NIC を用いた為,10BASE-T,100BASE-TX のそれぞれ通信を行う場合は,シミュレーション端末とアナライザーの間に,スイッチングハブを接続し,10Mbps,100Mbps それぞれの通信を選択し,10BASE-T,100BASE-TX の実験を行った.

攻撃用 PC①,PC②で,ICMP ECHO REQUEST パケットを生成し,シミュレーション端末 PC に対して Ping Flood 攻撃を行った.10BASE-T,100BASE-TX,1000BASE-T それぞれの環境において,Ping の送信バッファサイズを,32[bytes]から 65500[bytes]まで,変化させ比較検討を行った.

それぞれの通信環境,送信バッファサイズ時に再配信サーバからシミュレーション端末 PC へ Ping を 100 回送信

し,Ping Flood 攻撃時の情報配信収集サーバからシミュレーション端末の RTT(Round Trip Time)の計測を行った.

また,PC 上でシミュレーション端末を起動し,端末確認データを情報配信収集サーバへ送信,それに対して情報配信収集サーバがシミュレーション端末に対して端末確認応答のデータの送受信をそれぞれの環境,バッファサイズにおいて 100 回行い,比較検討を行った.

6. 実験結果

RTT は,攻撃用 PC から Ping flood 攻撃を行っている時のバッファサイズを,32[bytes]から 65500[bytes]までの変化時に, 情報配信収集サーバからシミュレーション端末 PC に Ping を 100 回送った時の平均値となっている(図 2).

1000BASE-T の場合は,バッファサイズを上げたが,変化が見られず安定した通信が行われていることが分かる.

100BASE-TX の場合は,バッファサイズが 2048[bytes]以降から,多少の RTT の変化は見られるが,通信に影響がある程の物ではない事が分かる.

10BASE-T の場合は,512[bytes]以降から徐々に RTT に変化が見られた.4096[bytes]から 8192[bytes]の間では,急激な RTT の変化が見られ,データの通信速度に影響が出て,RTT が遅延している事が分かる.また,16384[bytes]にした所, 処理が追いつかなくなり,通信ができない状態となった.

端末確認応答の送受信確率は, 攻撃用 PC から Ping flood 攻撃を行っている時のバッファサイズを,32[bytes]から

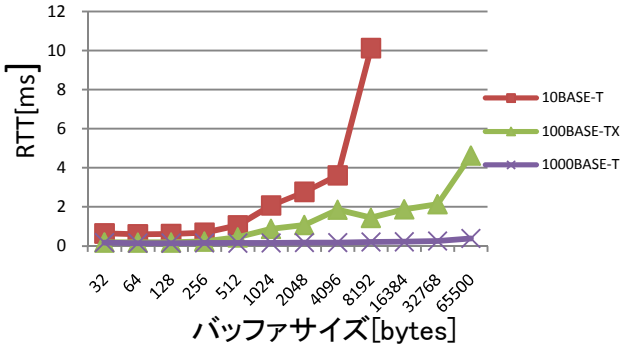

図２　攻撃用 PC からシミュレーション端末 PC への ICMP ECHO REQUEST パケットバッファサイズに対しての RTT

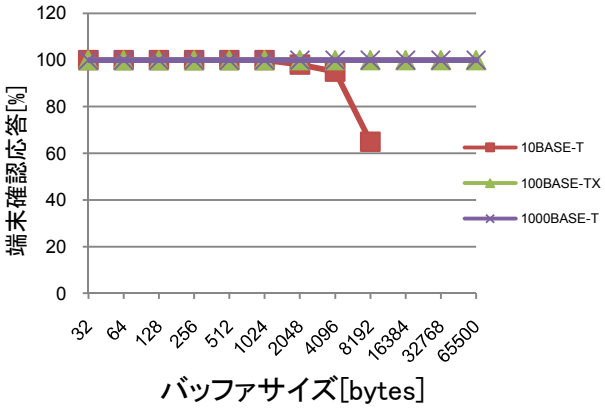

図３　攻撃用 PC からシミュレーション端末 PC への ICMP ECHO REQUEST パケットバッファサイズに対しての端末確認応答の送受信確率

65500[bytes]まで変化時にシミュレーション端末 PC 上でシミュレーション端末を起動させた.シミュレーション端末が情報配信収集サーバに対して端末確認データを送信し,再配信サーバが端末確認データに対して,端末確認応答を返す.その時のバッファサイズ変化時に対して正常な端末確認応答が行われる確率である(図 3).

1000BASE-T,100BASE-TX 共に,バッファサイズを 32[bytes]から 65500[bytes]まで変化させた場合,バッファサイズの変化に関係なく,シミュレーション端末から情報配信収集サーバ間の端末確認データ,端末確認応答の送受信が 100%で行われているのが分かる.

10BASE-T の場合は,2084[bytes]からシミュレーション端末; 情報配信収集サーバ間のデータの送受信の確率に変化があるのが分かる.バッファサイズを 8192[bytes]にした所, 送受信確率は 65%まで低下した.また,8192[bytes]以降もバッファサイズを変化させた所,16384[bytes]以降はデータの送受信が行われなく,機器のデータ処理能力を超えたと思われる.

7. 考察とまとめ

通信量が少ない場合は,10BASE-T で十分通信が行う事が出来るが,ネットワーク攻撃や通信量が多いデータが送信されてきた場合は,本来の動作を行う事ができない事が本研究で確認できた.また,100BASE-TX,1000BASE-T の場合,RTT が通信に影響が出る程長くならず,端末確認応答も 100%であった.その為,1000BASE-T より安価で通信に影響が少ない,100BASE-TX の規格を有する物を使用した場合の方が, セキュリティ上 10BASE-T を使用した場合より信頼性が向上するのではないのかと考えられる.

以上より,通信量が少ないネットワークを用いているセキュリティ機器でも,100BASE-TX や 1000BASE-T の NIC を実装した方が,Flood 系の攻撃に強い事が分かった.また,コストの面から 100BASE-TX の NIC を実装した方が良いと考えられる.

参考文献

[1]気象庁:緊急地震速報,気象庁（オンライン）,入手先 <http://www.seisvol.kishou.go.jp/eq/EEW/kaisetsu/Whats_EEW.html>.

[2]原田長具,松田勝敬:組込みシステムにおける通信のロバスト性向上に関する研究,FIT2009 第 8 回情報科学技術フォーラム講演論文集,第 1 分冊,pp501-502(2009).

[3]独立行政法人　情報処理推進機構:DoS 小規模サイト管理者向けセキュリティ対策マニュアル,独立行政法人　情報処理推進機構（オンライン）,入手先 <http:www.ipa.go.jp/security/fy12/contents/crack/soho/soho/chap1/dos.html>.

[4]独立行政法人　情報処理推進機構:TCP/IP に関する既知の脆弱性に関する調査報告書,独立法人　情報処理推進機構, pp.112-113.

[5] IETF:RFC793 TCP,IETF（オンライン）,入手先 < http://www.ietf.org/rfc/rfc793.txt>.