C-028

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

Development on robustness inclination of communication in embedded system

原田 長具† 松田 勝敬†
Nagatomo Harata Masahiro Matsuda

1. はじめに

ネットワークマイコンボードは，一般家庭のセキュリティ機器等の組込み機器に利用され，コンピュータネットワークを介して，遠隔操作・監視などを行うことができる．しかし，低コストの汎用ネットワークマイコンボードを搭載した組込み機器は，処理能力が比較的低いため，悪意のあるアクセスに対して脆弱である側面を持つ．一般的に，攻撃者側の機器がターゲットの機器よりも処理能力が優れている場合に有効な DoS 攻撃[1]には特に脆弱である．簡易なネットワーク装置では，端末単位での具体的な防御策といえるような対策は実装されていない場合が多く，ルータやファイアウォール等の上位のネットワーク機器のセキュリティ機能に頼っているのが現状である．そこで本研究では，DoS 攻撃のひとつである PingFlood による被攻撃時にも端末単体でロバストに動作するプロトコルスタックの開発を目指した．ping 機能を実装したネットワークマイコンボードに対して PingFlood 被攻撃時の正常な ping への応答性能を測定した．後に PingFlood 被攻撃時にもロバストに動作するように，改良したプロトコルを実装したネットワークマイコンボードに対して，同様の条件にて測定し，改良の効果を評価した．

2. 実験

本研究では，低コストのネットワークマイコンボードとして 10BASE-T のネットワークインターフェースカードを実装している北斗電子社製の H8/3067 スタータキット[2]をターゲットにした．また，プロトコルスタックには H8/3067 スタータキット向けに青木　直史氏が作成した IP 電話のプログラム[3]の ping リプライを行う部分のみを実装した。上記の環境にて， PingFlood 被攻撃時におけるパケットロスの測定実験を行った．次に，上記プロトコルスタックを PingFlood 被攻撃時にロバストに動作するように対策を施し，実装した環境ついて，測定を行った．

†東北工業大学，Tohoku Institute at Technology

2. 1 PingFlood 被攻撃時における応答性能の測定

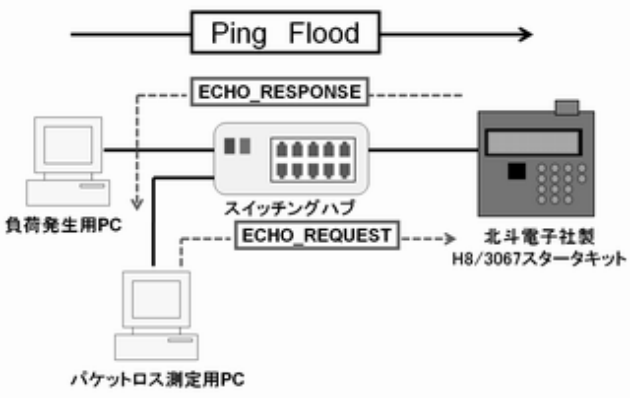

図 1 実験環境の接続概要図

実験機器の接続図を図 1 に示す．測定対象であるマイコンボードと PingFlood によってマイコンボードに対して攻撃を行う負荷発生用 PC をスイッチングハブで接続した．また，PingFlood 被攻撃時のマイコンボードの正常な ping に対する応答性能を測定するために，パケットロス測定用 PC を同様にスイッチングハブを介してマイコンボードに接続した．負荷発生用 PC にて PingFlood を行い，同時にパケットロス測定用 PC から正常な ICMP ECHO_REQUEST を 200 回送信し，端末からの応答として受信できなかった ICMP ECHO_RESPONS のパケットロス率を測定した．負荷発生用 PC から行う PingFlood は，バッファサイズを 32[byte]から，指数的に増加させていき，パケットロス測定用 PC で ICMP ECHO_RESPONS の到達率が 0%になった 4096[byte]まで測定を行った（図 2）．

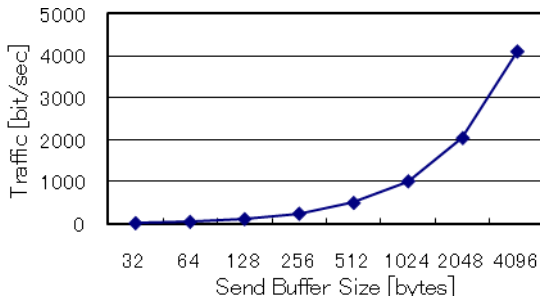

図 2 “PingFlood”における送信バッファサイズ［bytes］と通信量［bit/sec］

2.2 対策を施したプロトコルスタックのPingFlood被攻撃時における応答性能の測定

本研究における，プロトコルスタックの改良は，単位時間における同一IPアドレスへのICMP ECHO_RESPONSEの制限である．ICMP ECHO_RESPONSEの送信時に送信先のIPアドレスをメモリに記憶しておく．ICMP ECHO_REQUEST受信時に，ICMP ECHO_RESPONSE送信時に記憶しておいたIPアドレスと比較する．比較の結果，一致しなければICMP ECHO_RESPONSEを通常通り送信するが，一致した場合，前回のICMP ECHO_RESPONSE送信時からあらかじめ設定した単位時間を経過していなければ，ICMP ECHO_REQUESTを無視する．これにより，単位時間内に同一IPから大量のICMP ECHO_REQUESTが送信されても，マイコンがそのすべてを処理することがない．そのため処理能力に余裕ができ，ロバストに動作できると考えた．この時間は，プログラミングの段階で任意に設定できるが，単位時間が短すぎるとPingFlood被攻撃時に本改良の効果が表れにくく，長すぎると同一ノードからの連続した正常なpingに対して反応しなくなるので，適切な値を設定する必要がある．本研究では，1秒に設定した．

2．3 考察

測定結果のグラフを図3に示す。グラフの横軸はPingFlood時の送信バッファサイズを示しており，縦軸はICMP ECHO_RESPONSEのパケットロス率を表している．測定結果より，対策前のプロトコルスタックも改良後のプロトコルスタックも，送信バッファサイズが512byteまではICMP ECHO_RESPONSEのパケットロス率が0%である．しかし，対策前のプロトコルスタックでは，送信バッファサイズが1024byteではパケットロス率が70%，2048byteではパケットロス率が86%になり，PingFloodによる異常通信の影響をうけていることが解る．対して、改良後のプロトコルスタックを実装した環境では，送信バッファサイズ1024byteではパケットロス率は0%，送信バッファサイズ2048byteではパケットロス率が53%と，いずれも減少しており，本研究によるプロトコルスタックの対策の成果が表れていることがわかる．しかし，送信バッファサイズが4096byteの場合は，プロトコルスタックの改良の前後に関わらず，いずれもパケットロス率が100%であることから，今回の改善による効果が表れていないといえる．これは，送信バッファサイズ4096byteのpingは，本マイコンボードに対して，機器の処理を超えるバッファサイズのpingを受信して処理が停止していると考えられる．本対策を施す前のマイコンボード上のプログラムの総容量は4,145byteであり，本対策を施したプログラムの総容量は4,592 byteであった．

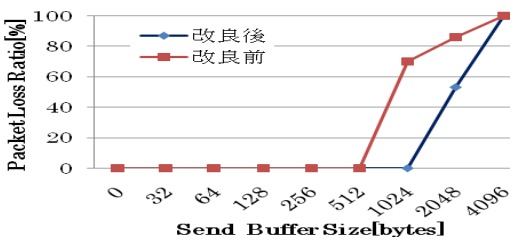

図3 PingFlood被攻撃時におけるパケットロス率

3．まとめ

低コストのネットワークマイコンボード向けに，PingFlood被攻撃時においてロバストに動作するプロトコルスタックの検討を行った．本研究では単位時間における，同一IPアドレスへのICMP ECHO_RESPONSEの制限に観点をおき対策を行った．結果，PingFloodの送信バッファサイズが1024byteと2048byteのときに，改良の効果が現れた．

今後は，この手法を応用し，単位時間当たりに同一のノードからの通信を制限する機能をL2レベルで実装し，他のプロトコルのFlood系攻撃に対しても有効な手法を検討する予定である．

謝辞

最後に，ping応答プログラムとH8/3067Fスタータキットの使用ついて，快く承諾していただいた青木直史氏と株式会社 北斗電子に感謝致します．

参考文献

[1]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:http://www.ipa.go.jp/security/fy12/contents/crack/soho/soho/chap1/dos.html

[2]株式会社 北斗電子 H8/3067 スタータキット:http://www.hokutodenshi.co.jp/

[3]青木 直史:H8マイコンによるネットワーク・プログラミング，pp. 159-174，技術評論社(2008)．