M_028

組込みシステム向けTCP/IPプロトコルスタックにおけるIPsecの実装と評価

Implementation and Evaluation of IPsec for Embedded TCP/IP Protocol Stack

堤 大祐† 堀 武司† 吉川 毅† 山本 寧†
Daisuke Tsutsumi Takeshi Hori Takeshi Kikkawa Yasushi Yamamoto

1．はじめに

家電製品や監視装置などの組込みシステムがインターネットに接続するようになってきた。このようなインターネットに接続する組込みシステムの開発において、TOPPERS プロジェクト[1]からリアルタイム OS として TOPPERS/JSP カーネル、組込みシステム用 TCP/IP プロトコルスタックとして TINET[4]がオープンソースとして公開されて無償で使用できる。TOPPERS/JSP カーネルはμITRON4.0 仕様[2]のスタンダードプロファイルの規定に沿って実装されたリアルタイム OS である。TINET は ITRON TCP/IP API 仕様[3]に準拠したプロトコルスタックで、FreeBSD のコードをベースに最小コピー回数、動的メモリ管理の排除など組込みシステム向けに改良されたコンパクトな設計となっている。

組込みシステムがインターネットに接続することに伴い、通信の安全性や IPv6 に関する要求が高まっている。セキュリティ・プロトコルには SSL(Secure Socket Layer)が WWW ベースの通信で広く用いられている。これは TCP による通信において機能するものである。一方、IPsec は IP を用いる通信のすべてが対象となり、かつ、IPv6 においては IPsec の実装が必須となっている。TINET は IPv4 と IPv6 の両方に対応したプロトコルスタックであるが、IPsec の実装は行われていない。そのため、筆者らは TINET に IPsec の実装を試みており、これまで、ICMP において ESP の処理をルネサステクノロジ社製 H8S2638、SH7615 で動作確認した[5]。今回、Xilinx 社製の FPGA 内に CPU(PowerPC 405 Processor)を内蔵した Virtex-II Pro と、ルネサステクノロジ社製 SH2(SH7615)上で、TCP の ECHO サービスを使用して暗号処理時間を含んだ通信時間の評価を行った。

2．IPsecの仕組みとESPプロトコルの実装

IPsec はネットワーク層で機能するため、IP を用いた通信を保護できる。IPsec は ESP(Encapsulating Security Payload：暗号ペイロード)と AH(Authentication Header：認証ヘッダ)の２つのプロトコルおよびトンネルモードとトランスポートモードの２つのカプセル化モードがある。トンネルモードは主にセキュリティゲートウェイ間で用いられ、トランスポートモードはホスト間で用いられる

IPsec はセキュリティ・ポリシー(Security Policy：SP)によって、IP パケットの処理方法を決定する。SP はネットワークアドレス、トランスポート層のプロトコルなどから構成され、「IPsec の適用」、「IPsec を適用せず通常の処理」、「パケットの破棄」といった処理方法を指定するルールを定義したものである。さらに、セキュリティ・アソシエーション(Security Association：SA)によって、使用する IPsec のプロトコル(ESP または AH)、暗号アルゴリズム、認証アルゴリズムなどを指定する。今回、実装した機能を表 1に示す。

表 1 実装した仕様

セキュリティ・プロトコル	ESP
カプセル化モード	トランスポートモード
Internet Protocol	IPv4
暗号鍵の交換	手動
暗号アルゴリズム	AES-CBC、鍵長 128bit

トランスポートモードにおける ESP は IP パケットの内容が暗号処理される（図 1参照）。また、IP ヘッダの次に新たに ESP ヘッダが挿入される。

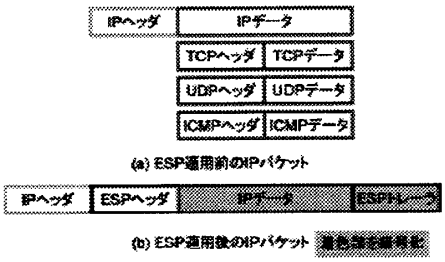

図 1 ESP 適用前後の IP パケット

IP パケットの処理フローを図 2に示す。IPsec を適用しない場合（図 2の点線）、IP 処理部と TCP/UDP/ICMP 処理部とでデータの受け渡しを行う。IPsec を適用した場合（図 2の実線）IP パケットは ESP 処理部で SP/SA と照合され、IPsec を適用するルールに従って、指定の暗号アルゴリズムで復号化または暗号化される。

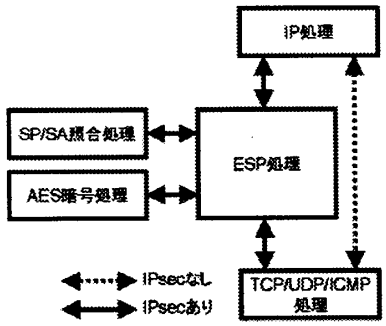

図 2 IP パケットの ESP 処理フロー

TINET では組込みシステム向けにネットワークバッファを固定長にし、上位層から下位層までのヘッダ領域を

† 北海道立工業試験場

あらかじめ確保し、動的メモリ管理を行わない設計になっている。IPsecの適用ルールを示すSP、SAにおいても、静的な構造体としてあらかじめ定義することによって、動的メモリ管理を行っていない。SP、SAの設定例を表2に示す。ESP処理とAES暗号処理とのインターフェースはFreeBSDのコードをそのまま利用できるようにした。このため、暗号処理の前後で異なるメモリ領域が必要となった。これにより、メモリを余分に消費することになったが、FreeBSDの暗号アルゴリズムをそのまま実装でき、他の暗号アルゴリズムの実装も容易になった。

表2　SPとSAの例

SP		SA	
終点アドレス	10.1.1.0/24	終点アドレス	10.1.1.1
プロトコル	tcp	IPsecプロトコル	ESP
ポート	any	SPI	0x2000
適用する処理	ESP	暗号アルゴリズム	AES-CBC

SPI：Security Parameter Index

3. ECHOサービスにおける通信時間の評価

IPsecによる通信試験とESP暗号処理に要する時間を評価試験を、PCとマイコンボードの間でECHOサービスを用いて行った。コネクションの確立からECHOメッセージの交換およびコネクションの解放までに要した時間を測定した。コネクションの確立におけるTCPのやりとりもESPのパケットとして通信しているので、これらの暗号処理時間も含まれる。

ECHOのメッセージの大きさを64バイト、128バイト、256バイト、512バイト、1024バイトとし、IPsecを適用した場合と適用しない場合で各々約1000回繰り返し、要した時間の平均値を求めた。時間の測定はPC上でプロトコルアナライザを起動し、そのタイムスタンプを用いて行った。

マイコンボードはCPUにPowerPC405を内蔵したXilinx社製Virtex-II Proを搭載したアットマークテクノ社製SUZAKU-V（図3参照）とルネサステクノロジ社製SH7615を搭載した北斗電子社製HSB7615ITを使用した。PowerPC405は動作周波数約64MHz、キャッシュ無効で、SH7615は動作周波数約15MHz、キャッシュ無効でそれぞれ動作させた。

ESPプロトコルに使用する暗号アルゴリズムはAES-CBC、鍵長128ビット、鍵交換は手動で行った。

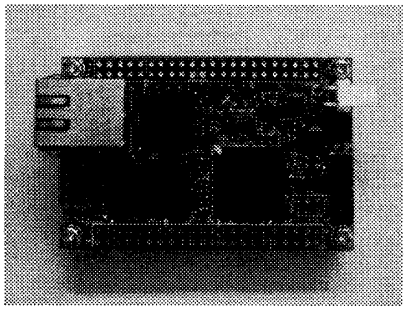

図3　Virtex-II Proを搭載したマイコンボード

PowerPC405とSH7615における通信時間の測定結果を図4に示す。IPsecを適用した場合、適用しない場合と比較して送信メッセージが大きいほどESP処理による通信時間は増大した。送受信メッセージが少ない場合、通信のオーバーヘッドのため、増大の程度は小さくなった。この結果より、通信データ量が少ないシステムや通信頻度が少ないシステムにおいて適用が可能である。

TCPパケットの暗号化および復号化は正しく処理されており、IPsec適用時のPCとマイコンボード間のECHOメッセージの交換は正常に行われた。

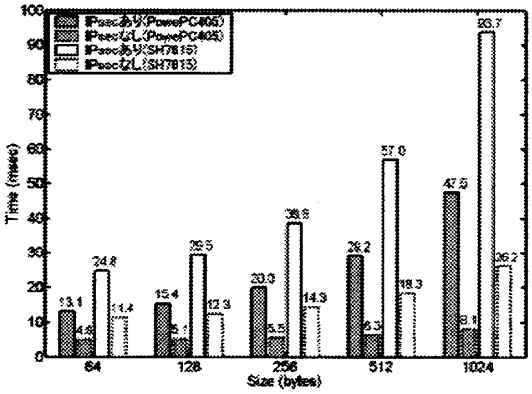

図4　ECHOサービスの通信時間

4. まとめ

μITRON仕様に準拠した組込みシステムに適用するために、TOPPERS/JSPカーネルとTINET上で、IPsecを最小構成で実装した。今回、Virtex-II PROに内蔵しているCPU (PowerPC405)を用いてIPsecの動作確認できた。これにより、H8S2638、SH7615、PowerPC405の異なるCPUにおいてIPsecの動作確認ができた。

今回行ったソフトウェアによるIPsecの実装は扱うデータ量が小さい用途または通信の頻度が少ない用途に適用が可能である。

今後は実装していない仕様のうち、AH、ESPのオプション、鍵交換の対応は必須と考え、その他の暗号アルゴリズム、認証アルゴリズムの実装を通して、組込みシステム向けIPsecとして完成度を高めていきたい。また、実装したIPsecはオープンソースとして公開する予定である。

参考文献

[1] TOPPERSプロジェクト、http://www.toppers.jp/index.html

[2] 坂村健(監修)、高田広章(編)：μITRON4.0仕様4.02.00、トロン協会(2004)

[3] 高田広章(編)：ITRON TCP/IP API仕様1.00.01、トロン協会(1998)

[4] 阿部司、吉村斎、久保洋：組込みシステム用TCP/IPプロトコルスタックの実装と評価、情報処理学会論文誌、Vol.44, pp.1583-1592(2003)

[5] 堤大祐、堀武司、長内研、吉川毅、山本寧：組込システム向けTCP/IPプロトコルスタックにおけるIPsecの実装、情報処理学会全国大会、Vol.1、pp61-62、2006