

IPsec のハードウェア実装方式の提案

永井 靖¹ 鈴木 誠人¹ 海老名 明弘¹

¹日立製作所 システム開発研究所 第六部

1 はじめに

ADSL(12Mbps), FTTH(100Mbps)の進展によりブロードバンド化が家庭に普及し、PC のみではなく様々なデジタル機器 (AV 機器, センサ, 白物家電など) の IP ネットワークとの接続が進みつつある。プライバシー保護及び機器制御の安全性の観点から、これらの機器を通信データの傍受, 制御データの改竄の危険から守る必要があり, その共通基盤として IP レイヤでセキュリティを実現できる IPsec 技術が着目されている。しかし処理能力の低い組込み系 CPU 搭載機器では, IPsec 通信による認証・暗号処理は, 負荷が重く十分な処理が行えないことが予想されている。そこで, 本稿では, 組込み系 CPU による IPsec 通信時のパケット処理特性の分析結果をもとにハードウェアによる認証・暗号/復号処理の高速化を進めた内容について述べる。

2 ネットワーク処理性能の現状分析

2.1 ソフトウェア処理性能

組込み系 CPU (133MHz) 搭載ハードウェア上に Usagi-Linux⁽¹⁾を実装し, ソフトウェア処理による送受信処理時間の測定を実施した。この結果, サイズ 1024byte のパケットで IPsec 処理を行うと IPsec 処理を行わない場合に比べその処理性能が 1/6 以下に低下し十分な性能を発揮できないという結果を得た (図 1)。さらにその処理内容と処理時間を詳細に解析したところデータの認証・暗号/復号処理時間が全体の 80%以上を占めておりこれらの処理負荷の低減による高速化が効果的であることが分かった。

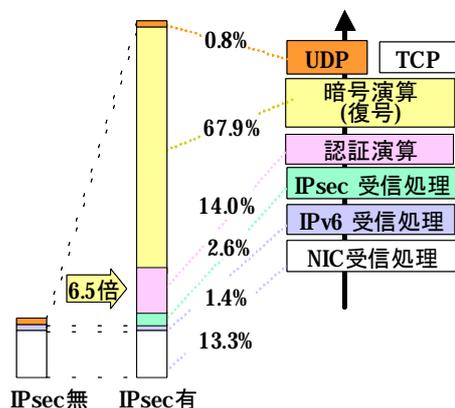


図 1 IPv6 IPsec 受信処理時間

2.2 認証・暗号演算のハードウェア化における課題

認証・暗号/復号処理にかかる CPU 処理負荷の低減及び高速化の手法としてハードウェアによるアシストの効果が大きい。しかし, 認証・暗号/復号処理部分をハードウェア化した場合, 図 2に示すよう(1) 受信データのバッファへの格納, (2) IPv6, IPsec 受信ヘッダの処理, (3) 受信データの認証・暗号ハードウェアへの転送, (4) 認証・暗号/復号演算処理, (5) 演算結果格納バッファの確保とそのキャッシュのページ, (6) 演算結果のバッファへの格納処理を順に行う必要がある。これら(1)から(6)の処理のうち(1), (3), (5), (6)ではSDRAMに対するパケットサイズのデータ転送が発生する。これらの処理は2.1の結果からパケットのサイズに比例しスループットの低下をまねくことが分かっている。また, 組込み機器のアーキテクチャにおいては(4)の暗号/復号演算処理中にCPUバスを使用する必要が無い為, CPU 等その他のバスマスタがバスを使用する処理と並列化することによりオーバヘッド低減が可能となると考えた。

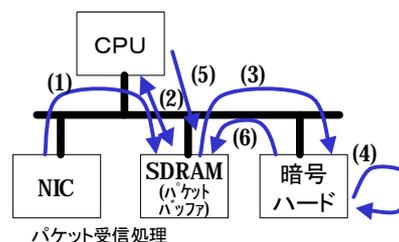


図 2 認証・暗号ハードウェアとデータ転送

3 認証・暗号ハードウェア

上記課題を解決する為必要となるハードウェア機能について説明する。

3.1 CPU バス性能の有効利用

(a) Single Address Mode DMA の利用

前記(1), (3), (6) の処理を CPU により実行する場合 CPU バスの使用回数は Read と Write で合計 6 回必要となる。この処理を単純なコピー処理として扱い DMA (Direct Memory Access) 転送を利用する事を考え, 各モジュールと SDRAM 間でデータを直接転送する DMAC (DMA Controller) の Single Address Mode 転送を活用した。これにより (1), (3), (6) にかかる CPU バス利用回数は 半分の 3 回に抑えられ CPU バスの有効利用が可能となる。

Implementation of IPsec Hardware

Yasushi Nagai¹, Masato Suzuki¹, Akihiro Ebina¹

¹6th Research Dept., Systems Development Laboratory, Hitachi,Ltd.

292, Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagaya-ken, 244-0817 Japan

E-mail: nagai@sdl.hitachi.co.jp

(b) SDRAM の有効利用

組込み機器で汎用的に利用される SDRAM の特徴を引き出すことを考えた。SDRAM に対するアクセスを行うためには Read/Write Command のみではなく Bank Active, Precharge Command 等、様々な Command の組み合わせでシステム性能を向上することを行わなければならない。そこで、認証・暗号演算処理の入出力データ幅 32bit、動作周波数 66MHz で最適な高速メモリアクセス性能の実現を考えた。CL2 の SDRAM アクセス性能はシングルアクセスに対し 4 バースト長のアクセスで 2.8 倍、8 バースト長で約 4.3 倍と大きく性能を向上させることが可能となる。

3.2 暗号演算時間の隠蔽

CPU バスを使用するパケット処理と認証(SHA1/MD5)・暗号(DES/3DES)演算処理の並列化のため、CPUバス I/F を 2 面の SRAM バッファ、各、認証・暗号演算器と DMA 機能付き Switch を介して接続する(図 3)。この様な構成をとることにより演算の為のデータ格納と取得の処理を並列処理できる。

Packet 0, 1, 2 の処理を例に示すと Packet 1 の認証・暗号演算中に 1 つ前の Packet 0 の演算結果の SDRAM への格納と次の Packet 2 データの SRAM への格納が可能となる。この様に DMA 機能付き Switch で複数データパスの確立を実現する事により認証・暗号演算と SDRAM と認証・暗号ハードウェア間のデータ転送の並列化が可能となり、CPUバス、演算器双方の利用効率向上が図れる。

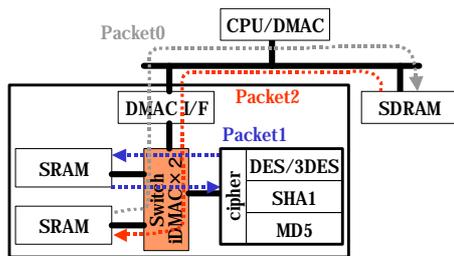


図 3 認証・暗号ハードウェア構成とパケットの流れ

暗号演算処理は図 4 の様に(1)演算器の Register 設定、(2)バッファのキャッシュパーズ、(3) バッファから認証・暗号ハードウェアへのデータ転送、(4) 演算結果格納バッファのキャッシュパーズ、(5) 演算結果のバッファ転送処理の Register 設定、(6) 暗号演算、(7) 演算結果のバッファ格納を行っている。今回は(4),(5) の処理と(6) 暗号演算処理の並列化を実施しその効果を確認した。さらに、次パケットの(1),(2),(3)の CPU バスを使用する処理及び前パケットの(7)の処理を(6)の暗号演算と並列化可能であることから、さらに 60.2%まで処理時間を短縮できる見通しを得ている。

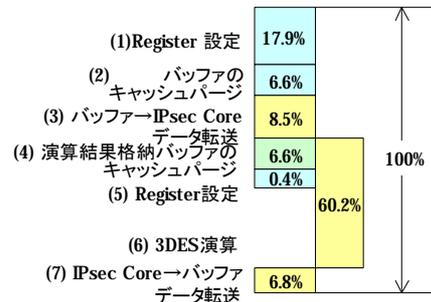


図 4 1024byte 暗号処理並列化状態

4 性能評価

4 バーストの SDRAM アクセスを実現する DMAC I/F 及び DMA 機能付き Switch を FPGA で実現し、組込み系 CPU (133MHz) に適用、Usagi-Linux⁽¹⁾ を用いて UDP/IP 通信時の測定を実施した。その結果を図 5 に示す。1024byte のパケット送受信処理においてソフトウェア処理に対し、暗号演算処理時間を 1/16、認証演算処理時間を 2/7 と短縮し、全体の処理時間を約 1/4 までの低減を実現した。

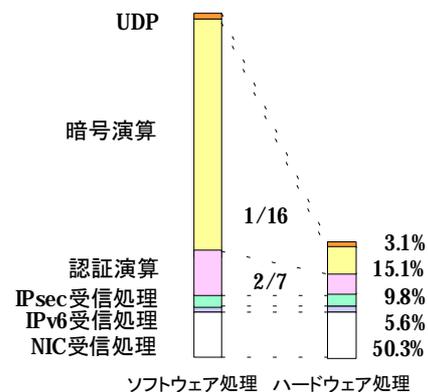


図 5 性能評価

5 おわりに

提案認証・暗号ハードウェアを FPGA 上に実装し組込み系 CPU による性能評価を行い並列化処理による高速化とその有効性を確認した。

6 参考文献

- 1) 日立製作所 半導体事業部 半導体グループカスタマサービス本部:SH7709A ハードウェアマニュアル 第 5 版, 2001, 9
- 2) 馬場達也:マスタリング IPsec, オライリー・ジャパン, 2001.

(1)Linux は, Linus Torvalds の米国及びその他の国における登録商標あるいは商標である