ギガビットイーサネットにおける IPSec 論理限界性能の実現

正員 小貫 淳史* 非会員 竹内 清史*
非会員 稲田 徹* 非会員 時庭 康久*
非会員 後沢 忍*

A Realization of Theoretical Maximum Performance in IPSec on Gigabit Ethernet

Atsushi Onuki*, Member, Kiyofumi Takeuchi*, Non-member, Toru Inada*, Non-member,
Yasuhisa Tokiniwa*, Non-member, Shinobu Ushirozawa*, Non-member

This paper describes “IPSec(IP Security) VPN system” and how it attains a theoretical maximum performance on Gigabit Ethernet. The Conventional System is implemented by software. However, the system has several bottlenecks which must be overcome to realize a theoretical maximum performance on Gigabit Ethernet. Thus, we newly propose IPSec VPN System with the FPGA(Field Programmable Gate Array) based hardware architecture, which transmits a packet by the pipe-lined flow processing and has 6 parallel structure of encryption and authentication engines. We show that our system attains the theoretical maximum performance in the short packet which is difficult to realize until now.

キーワード : IPSec, ギガビットイーサネット, VPN, FPGA

Keywords : IPSec, Gigabit Ethernet, VPN, FPGA

1. はじめに

インターネットはイントラネットやエクストラネット等の企業活動に必須なインフラストラクチャとして幅広く利用されている。しかしながらインターネットの通信プロトコルとして事実上標準の TCP/IP にはセキュリティ機能が備わっておらず、通信内容の傍受やデータ改ざんといった危険性が指摘されてきた。この問題を解決する方法の一つが IPSec(IP Security)で、TCP/IP のパケットを暗号化し認証子を付加して通信を行うことでネットワークのセキュリティ強化を図ることが可能である。

一方、動画等の大容量のデータ通信等においてインターネットの通信速度には更なる高速化が望まれており、物理層のイーサネットは従来の 100Mbps からギガビットイーサネットへの移行が進み、同様に転送速度の実効値を向上させるための取り組みも積極的に行われている。

このような市場動向からギガビットイーサネット上の IPSec に対応した VPN(Virtual Private Network)装置が散見されるようになってきた。ただし現状これらの製品では性能面においてパケット長が 1400Byte 程度と比較的長い場合は

スループットの論理限界まで性能が達するものの、パケット長が短くなると性能低下が著しく特に 64Byte のショートパケットでは多くの機種が論理限界の半分程度にまで性能が落ち込んでいる。昨今普及しつつある IP 電話のプロトコル(VoIP)等はこのようなショートパケットが多発するというトラフィック特性を持っており、今後は VPN 装置もこのようなアプリケーションに対応することが必須となっている。

以上を背景として我々は 64Byte のショートパケットを含む全てのパケット長で IPSec の論理限界を達成することを目標にギガビットイーサネット上の IPSec 通信に対応した VPN 装置の開発を行った。本論では、このような VPN 装置の実現手法を提案するとともに、これに基づいて開発した VPN 装置の有効性を性能評価によって示す。

2. ギガビットイーサネット上の IPSec 論理限界の定義

ギガビットイーサネット上で、IPSec で一般的に用いられる ESP(Encapsulated Security Payload)暗号・認証付きを実施した場合の論理限界を表 1 に示す。上段は VPN 装置に入力されるイーサネットのパケット長(Byte)。中段は単位時間あたりに VPN 装置から出力される IPSec パケット数(* 10^3 packet per second), 下段はイーサネットの論理限界に対する IPSec のパーセンテージである。なお入力パケット長 1464

* 三菱電機 (株) 情報技術総合研究所
〒247-8501 神奈川県鎌倉市大船 5-1-1
Information Technology R&D Center, Mitsubishi Electric Corporation
5-1-1, Ohfunai, Kamakura, Kanagawa, 247-8501

表 1 IPsec 論理限界

Table 1. IPsec theoretical maximum performance.

Byte	64	128	256	512	1024	1464
Kpps	933	631	383	215	114	81
%	62.6	74.7	84.7	91.4	95.4	96.7

バイトは ESP 暗号認証でフラグメントが発生しないパケットの最大長である。IPsec は処理の前後で暗号・認証ヘッダが付加されるので、パケットの入力に対する出力の比率が低くなる。例えば 64Byte パケットの入力は 1488Kpps であるが、出力は 933Kpps となる。この IPsec 処理後の単位時間あたりの出力パケット数を IPsec の論理限界と定義する。

3. 実現上の課題

従来の 100Mbps イーサネット対応 IPsec VPN 装置の一般的なシステム構成を図 1 に示す。主要な制御は CPU によるソフトウェアで実現しているが、IPsec におけるパケットの暗号認証処理は演算負荷が非常に大きいため ASIC や FPGA 等の専用エンジンを搭載してソフトウェアとハードウェアで協調して処理を行う手法が用いられてきた。

図 1 に示す従来のシステム構成をもとにギガビットイーサネット上での IPsec 論理限界性能を満足する VPN 装置の実現方式を考えた場合、以下の問題がある。

〈3・1〉 リアルタイム性 図 1 中の CPU には通常時に実行するパケット転送の処理以外にも IKE(Internet Key Exchange)や ARP 解決等の IPsec に対応するための様々な処理が発生する。特に割り込み処理が発生した場合にパケット転送の処理に対する待ち時間を予測することが困難となる。

〈3・2〉 パケット格納用メモリのスループット 図 1 において装置外部から受信した平文パケットを暗号認証して再度外部に送信する場合(1)から(5)の順にパケットは転送される。このうちメモリバス上には(1)(3)(4)(5)の 4 種類のパケット転送が発生し、かつそれぞれの転送を同時に並行して行う必要がある。このためメモリバスには定常的に 4Gbps のスループットが要求される。さらに VoIP 等で全二重通信に対応することを考慮した場合、その 2 倍の 8Gbps のスループットが必要となる。これに対し現状の組込み機器のメモリとして一般に用いられている 133MHz SDRAM(64 ビット幅)のスループットはピーク値で 8.5Gbps である。実効値はパケット長が短いほど低下し、CL(CAS Latency)=2 のメモリでパケット長 64Byte(バースト長 8)でバースト転送した場合のスループットはピーク値の約 60%の 5.1Gbps まで低下する。

〈3・3〉 暗号認証処理のスループット 現状のハードウェア暗号認証エンジンのスループットは数百 Mbps にとどまり、特にパケット長が短い場合には鍵情報の設定やパケットに対するパディング処理によるオーバーヘッドの影響を受け更にスループットは低下する。1Gbps スループットを満足するためには並列処理等によるアーキテクチャを新

図 1 従来の IPsec VPN 装置の構成

Fig. 1. Conventional IPsec VPN system architecture.

たに確立する必要がある。

これらの問題を伴う既存のアーキテクチャをもとにしてギガビットイーサネット上での IPsec 論理限界性能を満足する VPN 装置を実現するのは不可能と判断し、我々はパケットの送受信から IPsec の暗号・認証といった一連の処理を全てハードウェアで実行する手法について検討した。

4. 提案システムの概要

今回我々が試作した VPN 装置の外観を図 2 に、装置の構成を図 3 に示す。装置は 1000Base-T インタフェースを持つメインボード、IPsec の暗号認証処理を行う 2 枚の暗号ボード、IPsec の IKE 処理および装置の全体管理を行う CPU ボードで構成される。以下に 3 章で述べた課題を解決する装置の特徴について説明する。

〈4・1〉 リアルタイム性の確保 IPsec の SA(Security Association)確立までは IPsec による通信を行う上での初期設定のフェーズに相当し、これらの処理は CPU ボードが実行する。一方 SA 確立後の処理は 1Gbps スループットでのパケット処理が必要となり、これをメインボードと暗号ボードが分担して実行する。メインボードと暗号ボードでのパケット処理は主に FPGA によるハードウェアで実現している。このようにパケットに対してリアルタイムで実行すべき処理に CPU によるソフトウェアの処理を一切介在させないことで、それぞれの処理時間を保証している。

〈4・2〉 フロー転送方式 装置内の FPGA および FIFO 等のデバイス間にはそれぞれ個別の片方向伝送路を設け、これによってパケットの転送を行う。各伝送路は動作周波数 40MHz, 32 ビット幅で構成され 1.28Gbps のスループットを有している。パケットはこれらの伝送路に沿ってデバイス間をフロー方式で転送される。このようにパケットに対する処理を複数の FPGA に分散し、各 FPGA 間を専用の伝送路で接続しているため、従来のパケット格納メモリによるバッファリング方式のように特定の伝送路にパケットが集中して数 Gbps といった高いスループットが必要となるこ

図2 ギガビットイーサネット IPSec VPN 装置

Fig. 2. Gigabit ethernet IPSec VPN system.

図3 ギガビットイーサネット IPSec VPN 装置の構成

Fig. 3. Gigabit ethernet IPSec VPN system architecture.

とはない。これによってデバイスの選定や部品配置，配線等のハードウェアの設計を容易にした上で 1Gbps のパケット転送を可能にしている。

〈4・3〉 暗号認証の並列処理 暗号ボードの構成を図4に示す。暗号認証処理は暗号ボード上の2石のFPGAが行う。それぞれのFPGAを暗号処理用と復号処理用に割り当てることで全二重通信に対応している。暗号FPGAは3並列3ステージ，復号FPGAは3並列4ステージのパイプラインで構成しており，各ステージにはIPコアによる暗号エンジンおよび認証エンジンを実装している。VPN装置1式につき暗号ボード2式を組み込むことで暗号側復号側それぞれ6並列とし42個のパケットの並列処理が可能である。

パイプラインの構成を決定する上では特に以下の点を考慮した。最終的にはFPGA内部論理をVerilog HDL(Hardware Description Language)により記述し，論理シミュレーションを実施した上で決定した。

(1) 各ステージのスループットと並列度の検討

パイプライン構成の検討に際しては，本実装において選定対象となった暗号処理用もしくは認証処理用のIPコア単体のスループットをもとに，各ステージのスループットは200Mbps(IPコアに対する初期設定等のオーバーヘ

図4 暗号ボードの構成

Fig. 4. Encryption board architecture.

ッドに対するマージンを含む)，また並列度は6(1Gbps/200Mbps=5にマージン1を加算)をそれぞれ目標とした。なお各ステージのスループットとして200Mbpsを実現するにあたり特に以下の2点を考慮した。

・認証処理の2ステージ化

IPSecのパケット認証方式として規定されているHMAC(Keyed-Hashing for Message Authentication)は特定のパケットに対してハッシュ演算を2回実行するため，同様の演算処理を1回しか実行しない暗号処理および復号処理に比べスループットが約半分にまで低下する。このため認証処理は2ステージに分離する方式を採用した。

・復号側のパケット検証

復号側では復号結果のIPパケットとしてのフォーマット検証，認証結果判定，SPD(Security Policy Database)に登録された発信元/宛先アドレスやプロトコルの比較判定等の処理が必要となる。このためパケット検証用のステージを別途実装した。

(2) パイプラインにおけるSAの転送

SAと呼ばれる暗号認証処理に必要な鍵等の情報は暗号ボード上の外部SRAMに格納する方式を採用した。FPGA内部にはSA専用の伝送路を新たに設け，読み出したSAはパイプラインのステージ間をこの伝送路によってパケットに同期して転送される。このように伝送路を別途設けることで本来のパケット転送のスループットが低下す

るのを防いでいる。

(3) 複数回の暗号認証処理への対応

IPSec の運用では特定パケットにつき暗号処理および認証処理を高々1回ずつ実行するのが一般的である。一方で IPSec はセキュリティ強度を高めるために特定パケットにつき複数回の暗号処理あるいは認証処理を実行することを認めている。本実装ではパイプラインの外側にパケットをループさせる経路を設けることでこのような仕様にも対応している。

5. 性能評価

性能評価時のシステム構成を図5に示す。試験用パケットの生成と測定には Smartbits を使用した。Smartbits により特定長の IP パケットを 1Gbps 論理限界のレートで連続して生成する。それを VPN 装置#1 に入力し暗号認証を実行して出力し対向の VPN 装置#2 で復号認証を実行する。このとき図5中(1),(2)におけるパケット数を Smartbits で測定した。

性能評価の測定結果を図6に示す。ここでは IPSec プロトコルとして ESP 暗号認証を使用し、暗号および認証のアルゴリズムには IPSec の評価指標として一般的である 3DES と

HMAC-SHA1-96 を用いている。図6において論理限界と(1)暗号認証後のパケット数が一致し VPN 装置が論理限界性能を実現していること、同じく(1)と(2)復号認証後のパケット数が一致し VPN 装置がパケットを取りこぼすことなく復号認証していることがわかる。

なお今回の評価では上述の結果に加えて以下の IPSec プロトコルと暗号・認証アルゴリズムの全ての組合せにおいて論理限界性能の達成を確認している。

- IPSec プロトコル： ESP 暗号+AH 認証, ESP 暗号認証, ESP 暗号, ESP 認証, AH 認証
- 暗号アルゴリズム： DES,3DES,MISTY,AES,Camellia
- 認証アルゴリズム： HMAC-SHA1-96,HMAC-SHA2-128

6. まとめ

本論では、ハードウェアによる暗号認証制御方式を採用した VPN 装置によりギガビットイーサネットにおける IPSec 論理限界が実現できることを明らかにした。なお今回の開発では入力パケット長としてフラグメントが発生しない範囲を想定したが、今後はフラグメントが発生する範囲においても論理限界性能の達成に向けて検討を進めていく所存である。

(平成 15 年 11 月 25 日受付)

文 献

- (1) ナガナンド・ドラスワミ, ダン・ハーキンス: IPSec テクニカルガイド, ピアソン・エデュケーション (2000)
- (2) Stephen Saunders 著, 井早優子訳: ギガビットイーサネット徹底解説, 日経 BP 社 (1999)
- (3) John L. Hennessy and David A. Patterson 著・富田眞治・村上和彰・新實治男訳: コンピュータ・アーキテクチャ 設計・実現・評価の定量的アプローチ, 日経 BP 社 (1992)
- (4) Barry Wilkinson 著・渡邊 尚・小林真也・長谷川 誠訳: 計算機設計技法 第2版 マルチプロセッサシステム論, トッパン (1998)
- (5) 森岡澄夫: HDL による高性能デジタル回路設計, CQ 出版社 (2002)

図5 性能評価のシステム構成

Fig. 5. System configuration at performance evaluation.

図6 性能評価結果

Fig. 6. Result of performance evaluation.

小 貫 淳 史

(正員) 1967年9月27日生。1993年3月東京工業大学大学院総合理工学研究科システム科学専攻修了。同年4月三菱電機(株)入社。以来計算機および通信機器のハードウェア開発設計に従事。

竹 内 清 史

(非会員) 1977年2月22日生。2001年3月中央大学大学院理工学研究科情報工学専攻修了。同年4月三菱電機(株)入社。以来通信機器のハードウェア開発設計に従事。

稲 田 徹

(非会員) 1965 年 5 月 16 日生。1989 年 3 月早稲田大学理工学部香華用経営学科卒。同年 4 月三菱電機(株)入社。以来、通信機器のファームウェア開発・研究に従事。

後 沢 忍

(非会員) 1961 年 3 月 7 日生。1983 年 3 月岩手大学工学部電気工学科卒業。同年 4 月三菱電機(株)入社。パケット多重化装置、マルチプロトコルルータ、ネットワーク暗号装置等の研究開発を経て、現在は暗号による VPN や IDS を中心とするネットワークセキュリティの研究に従事。NPO 日本ネットワークセキュリティ協会理事。

時 庭 康 久

(非会員) 1963 年 1 月 10 日生。1986 年 3 月中央大学理工学部数学科卒業。同年 4 月三菱電機(株)入社。以来 WAN/LAN 関連通信機器のソフトウェア開発設計に従事。