6E-2

FPGA による 10GbpsVPN の検討

竹内　清史†　　小林　智†　　小貫　淳史†　　後沢　忍†

三菱電機(株)情報技術総合研究所†

1. はじめに

近年のネットワークの高速化に伴い、VPN や IDS/IPS などネットワークセキュリティ装置の高速化が求められている。これらを高速化する手段として、従来はソフトウェアで実装していた処理を FPGA や ASIC 等のハードウェアで実装することも多く、最近は数ギガクラスの処理性能を持つネットワークセキュリティ装置が普及してきている。我々は今後更に高速化するネットワークの将来を見据え、10Gbps の性能を有する IPsec VPN 装置（以下、10G VPN 装置と記述する）の開発を目標としてその実現方式を検討した。本稿では FPGA 実装による 10G VPN 装置を実現する上での課題とその解決方法を提案する。

2. 10G VPN 装置を実現する上での課題

我々は以前 FPGA による 1Gbps の VPN 装置を開発しており[1]､今回はこれを基に 10G VPN 装置実現の検討を行った。IPsec の処理に必要な暗号処理部と認証処理部を FPGA で並列化する一般的な構成を図１に示す。

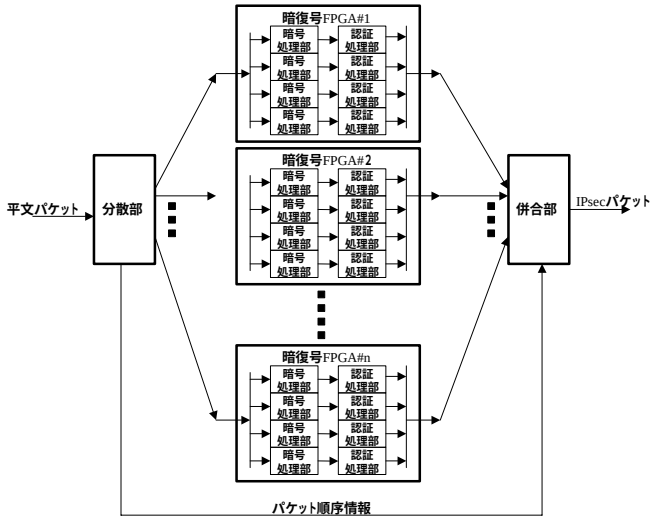

図１．FPGA による IPsec 処理の並列化

IPsec を用いた VPN 装置における暗号処理や認証処理の演算負荷は非常に高いため、図１では高速処理する目的で処理部をパイプライン化し、さらにこれを並列化することでスループットを向上させる方法をとっている。なお図１では FPGA 一石あたりに実装する暗号処理部と認証処理部の並列度は実装と照らし合わせて４並列としている。我々は、このような構成を基にしてスループットを 10Gbps に拡張する方法を検討した。

今回我々が 10G VPN 装置を実現する際に使用する暗号処理部と認証処理部の処理性能は 1 並列あたり 190Mbps で、この並列度を 53 並列とすることで理論的には 10Gbps の性能が実現可能となる。その結果、10Gbps の性能を達成するためには暗号パス、復号パスのそれぞれにつき 14 石の暗復号 FPGA が必要となる。

しかし、図１のように単純に 10Gbps のパケットフローを複数の暗復号 FPGA に分散させる方法は分散部～暗復号 FPGA～併合部の間の配線数が増大してしまう問題がある。実機への展開を考慮した場合、多数の暗復号 FPGA を 1 枚のボード上に配置するのは物理面積上困難である。これを複数のボードに分割して配置することを想定すると、図 1 の方法はボード間の信号線数が多くなり実装が非常に困難になる。また VPN 装置はパケット受信順に送信する必要があるため、併合部ではどの FPGA からパケットを受信して装置外部に送信するかの順序制御を行う必要がある。この順序制御を行うにあたっても暗復号 FPGA 数が多いほど順序制御処理の負荷が大きくなり、10Gbps を実現する上で性能上のボトルネックとなる可能性がある。

以上のように、10G VPN 装置を多数の暗復号 FPGA で負荷分散して実現するにあたり、10Gbps のパケットフローをどのように個々の暗復号 FPGA に負荷分散させるかが課題であった。

3. 10Gbps パケットフローの負荷分散

10G VPN 装置の実現を検討する上で採用した負荷分散方法について述べる。今回我々が採用したシリアル接続による負荷分散方法を図２に示す。

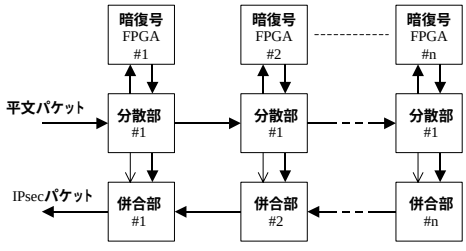

図２．シリアル接続によるパケットフローの負荷分散

A Study of the 10Gbps VPN by FPGA
Kiyofumi TAKEUCHI Satosi KOBAYASHI, Atsushi ONUKI, Shinobu USHIROZAWA,
Information Technoloty R & D Center, Mitsubishi Electric Corporation

この方式は10Gbpsパケット伝送路上に複数の分散部と併合部をシリアル接続する方式である。個々の分散部は隣接する暗復号 FPGA と後段の分散部にパケットを分散し、また各分散部は暗復号 FPGA と後段の分散部に振り分けた順序情報を併合部に渡す。併合部では分散部から受信するパケットと後段の併合部から受信するパケットの送信順序を制御する。この方式により、従来方式では課題となった分散部～暗復号 FPGA～併合部の間の信号線数を減少させることができる。また、パケットの分技先ポート数と集合元ポート数を少なくすることで順序制御すべきポート数が少なくなるため順序制御処理が高速化できる。更に本方式は、分散部/併合部/処理部を一組としてシリアルに接続することで容易に拡張することが可能である。

10G VPN 装置ではこの負荷分散方法を用いることにより、ボード間の信号線数の減少を実現する。また順序制御ポート数の減少による処理の高速化を実現する。

4. 10G VPN 装置のシステム構成

今回我々が検討した 10G VPN 装置のシステム構成を紹介する。10G VPN 装置のボード接続構成を図３に示す。

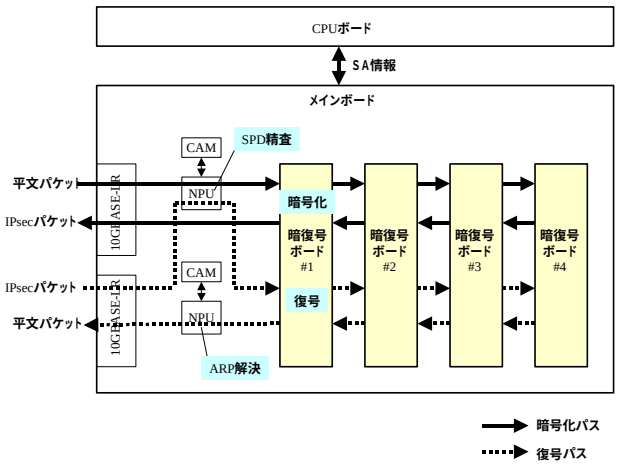

図３．10G VPN 装置ボード接続構成図

10G VPN 装置は 10GBASE-LR インターフェースを２個持ち、SA を指定するための CAM 検索を行う NPU とデカプセル後の MAC アドレスを取得するための CAM 検索を行う NPU を持つメインボード、４枚の暗復号ボード、IKE 処理等を行う CPU ボードから構成される。メインボード～暗復号ボード#4 に前項で述べたシリアル負荷分散方式を採用することで、ボード間の信号線数を減少させることが可能である。暗復号ボード内部の FPGA の接続構成を図４に示す。

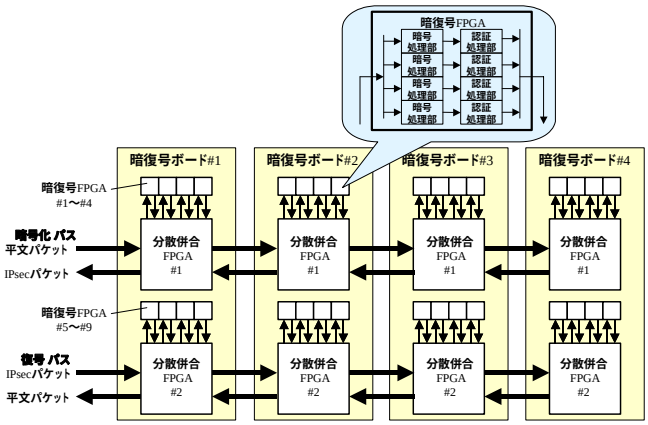

図４．暗復号ボード内部の FPGA 接続構成

分散併合 FPGA は図２の分散部と併合部の両方の機能を持つ。1 枚の暗復号ボード上には分散併合 FPGA を２石（暗号化パス/復号パスそれぞれで１石ずつ）、暗復号 FPGA８石が配置されている。暗復号 FPGA はいずれも４並列の暗号・認証処理部を持ち、暗号化/復号パスそれぞれで 16 石の FPGA にて、計 64 並列で IPsec パケット処理を行うことで 10Gbps の性能を達成する目処が立った。また、メインボードと暗復号ボードおよび暗復号ボード間は SPI4.2（System Packet Interface Level 4 Phase 2）を用いることにより 10Gbps でパケットを転送する方式を採用した。最後に今回の 10G VPN 装置にて使用予定の FPGA の型名を以下に示す。

暗復号 FPGA ：XC4VLX100（ザイリンクス社）
分散併合 FPGA：XC4VLX40（ザイリンクス社）

5.おわりに

10G VPN 装置を FPGA で実現する上で課題となる 10Gbps パケットフローを複数の FPGA に分散する新しい負荷分散方式を紹介した。また、この負荷分散方式を採用した 10G VPN 装置のシステム構成例を紹介した。今後は本システムのシミュレーションを実施し、実機動作させる予定である。

6.参考文献

[1] 小貫 淳史　他, “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”, 電気学会論文誌 C 電子・情報・システム部門誌 2004 年 8 月号 P.1533-1537,2004

[2] 稲田 徹　他, “VPN 構築技術の検討・リピータアーキテクチャ”, 情報処理学会第 61 回全国大会,2000

[3] 海老名 明弘　他 : “組み込み機器における最適な IPsec 実装方式の検討”, 情報処理学会第 65 回全国大会, 2003.

[4] **澤川 渡, 網島 明浩** : “TCP/IP **解析とソケットプログラミング**”,**オーム社**,Feb.2000.