IXP425 における暗号処理のオフローディングについて

大釜 正裕† 杉浦 寛† 黒羽 秀一†† 齋藤 孝道†
† 明治大学

1 はじめに

IP パケットの高速処理が求められるルータやレイヤ 3 スイッチなどのネットワーク機器の実現において, ASIC(Application Specific Integrated Circuit) と比較して柔軟で高機能なデバイスであるネットワークプロセッサ (以下, NP と呼ぶ) が注目されている. 高速化の手段として, NP では, 専用モジュールを用いて, パケット処理や暗号処理を行っている.

暗号モジュールを持つ NP を用いて, IPSec-VPN における暗号処理をオフロードし評価したものとして [1] があるが, SSL(Secure Socket Layer)[2] や TLS(Transport Layer Security)[3] を用いた VPN の実装例は少ない. そこで, 本論文では, Intel 社の NP である IXP425 [4] を搭載する評価ボード (以下, 評価ボードと呼ぶ) 上に SSL-VPN を実装し, パフォーマンス計測と考察を行う.

2 ネットワークプロセッサ

2.1 概要

NP は, 一般に, 汎用プロセッサ, パケット処理専用モジュール (以下, NPE[1] と呼ぶ), メモリ, 外部接続のためのインタフェースから構成されている. NP 用の基本ソフトウェアは, NPE 上で動作するパケット処理用のプログラムと汎用プロセッサ上で動作する制御プログラムの 2 種類のプログラムから構成されている.

2.2 IXP425 アーキテクチャ

本論文で用いる IXP425 は, 主に, XScale アーキテクチャを基にした汎用プロセッサ (以下, XScale コアと呼ぶ) と 2 つの NPE から構成されている.

XScale コアは, NPE と周辺装置などの一般的な処理を行い, NPE は主に IP パケットの処理を行う.

片方の NPE は暗号モジュールを内蔵している. この暗号モジュールは, 共通鍵暗号化方式の DES, 3DES と AES[2] に対応しており, その利用モードとして, CBC(Cipher Block Chaining) と ECB(Electronic Code Book) が利用可能である. また, ハッシュアルゴリズムとして SHA-1 と MD5 に対応している.

3 開発環境

3.1 IXP425 搭載評価ボード

評価ボードは, 主に, IXP425, プログラムメモリである Flash ROM, メインメモリである SDRAM と 2 つの NIC から構成されている. また, 今回, OS は μClinux を利用する.

3.2 暗号モジュールの利用法

IXP425 の NPE が提供する暗号処理機能を利用するための一手法として, IXP4*xx* シリーズ向けのデバイスドライバ開発用の API である AccessLibrary がある. アプリケーションから暗号処理機能を利用するためには, まず, 専用のデバイスドライバを実装し, そのデバイスドライバにアクセスする仕組みが必要となる. しかしながら, この手法は開発コストが高くつき, さらに, 低レベルの暗号処理を独自に実装することは非常にリスクが高いため, 本論文では, OpenSSL と OCF(OpenBSD Cryptographic Framework)[5] を組み合わせた開発基盤を構築し, 暗号モジュールを抽象化する OCF 経由でユーザ空間から AccessLibrary を介して暗号モジュールにアクセスする (図 1).

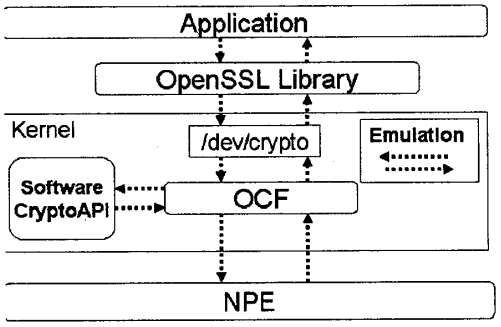

図 1: 利用の概要

4 SSL-VPN の実装

実装した SSL-VPN の概要について, ホスト 1 が異なるネットワーク上のホスト 2 にパケットを送信する場合を例にして, 図 2 を用いて説明する :

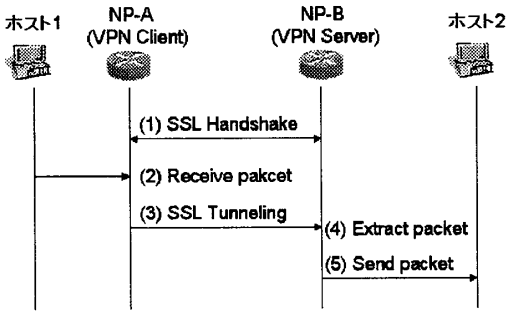

図 2: VPN の概要

まず, VPN クライアントとして動作する NP-A と VPN サーバとして動作する NP-B 間で SSL ハンドシェイクによって VPN 接続 (SSL セッション) を確立する (図 2 (1)). 次に, NP-A が libpcap でホスト 1 からのイーサネットフレームを受信し (図 2 (2)), 宛先 IP アドレスの確認し, 接続先のネットワーク宛ての場合 OpenSSL の SSL_write を用いて IP パケットをカプセル化し, NP-B へ送信する (図 2 (3)). NP-B が OpenSSL の SSL_read を用いてそのパケットを受信し, 元のパケットを抽出し (図 2 (4)), sendto を用いてホスト 2 へ送信する (図 2 (5)). SSL-VPN システムには OpenSSL-0.9.7c と libpcap-0.4 を使用する.

5 評価

5.1 計測項目

IXP425 を用いた際の暗号処理のオフローディングにおけるボトルネック特定のため, 図 2 の環境でホスト 1 からホスト 2 へ Ping を送信し, NP 上での各処理の時間計測をおこなった. 計測をおこなった箇所は,

† Ohgama Masahiro, Sugiura Kan, Saito Takamichi
†† Kuroba Shuichi
{ohgama, kan_s, kuroba, saito}@cs.meiji.ac.jp
Meiji University(†), Graduate School of Meiji University(††)
1-1-1 Higashimita, Tama-ku, Kawasaki-shi, Kanagawa, 214-8571, Japan(†)(††)

[1] NPE は Network Processor Engine の略称である.

[2] 鍵長は 128bit のみに対応している.

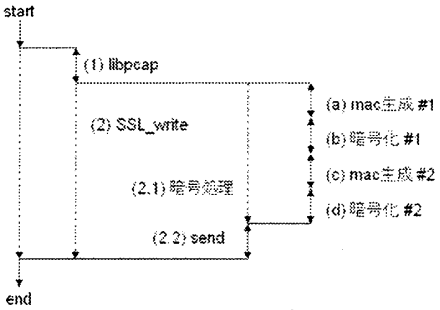

図 3: ssl_write の処理

表 1: SSL_write における計測結果

計測項目	計測結果 (μs)
(1) libpcap	12
(2) SSL_write	794
(2.1) 暗号処理	676
(a) MAC 生成 #1	193
(b) 暗号化 #1	160
(c) MAC 生成 #2	170
(d) 暗号化 #2	120
(2.2) send	102
(1) と (2) の合計	806

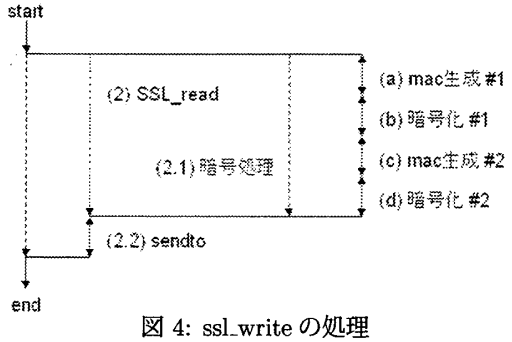

図 4: ssl_write の処理

表 2: SSL_read における計測結果

計測項目	計測結果 (μs)
(1) SSL_read	759
(a) MAC 生成 #1	163
(b) 暗号化 #1	212
(c) MAC 生成 #2	133
(d) 暗号化 #2	133
(2) sendto	75
(1) と (2) の合計	834

ホスト 1 からホスト 2 への Ping の RTT と，NP-A と NP-B における処理，すなわち図 3, 図 4 に示すとおりである．

SSL_write における計測項目 (図 3 参照)

(1) libpcap のコールバック関数が呼ばれてから SSL_write 関数を呼ぶ直前までの処理時間．
(2) SSL_write 関数の呼び出しから終了までの時間．
(2.1) SSL_write 関数の呼び出しから，SSL_write 内部でパケットを送信する関数を呼び出す前までの時間
(2.2) パケットを送信する関数を呼び出す前から SSL_write の終了までの時間
(a)(c) SSL_write の MAC 作成時間
(b)(d) SSL_write の暗号化処理時間

SSL_read における計測項目 (図 4 参照)

(1) パケットを受け取ってから SSL_read の終わりまでの処理時間
(a)(c) は SSL_read の復号処理時間
(b)(d) は SSL_read の MAC 作成時間
(2) は sendto 全体の処理時間

5.2 計測方法

計測は各処理の開始箇所と終了箇所の時間を取得し，その差を処理時間とした．Ping パケットが一往復する間に，NP-A，NP-B では SSL_write，SSL_read の処理をそれぞれ 1 度ずつ行っている．その際，暗号化，復号されるデータサイズは Ping のデータサイズである 64bytes と IP ヘッダのデータサイズである 20bytes の合計で 84bytes である．表 1 は NP-A 上での SSL_write，表 2 は NP-B 上での SSL_read の計測結果 (片道) である．Ping を 5 回実行し，その平均値を結果とした．

5.3 計測環境

ホスト 1 とホスト 2 は Celeron(1.86GHZ) と 1024Mbyte の RAM メモリを搭載し，NP-A と NP-B は IXP425(533MHz) と 64Mbyte の RAM メモリを搭載する評価ボードで動作する．NIC はすべて 100BASE-TX である．暗号スイートは DES-CBC-SHA を用いた．

5.4 計測結果

SSL_write における計測

表 1 とおりの結果となった．SSL_write の暗号処理で大半の時間を占めている．暗号化処理では NPE を使用しているが，MAC 生成処理では，使用していない．1 回の暗号化処理で，NPE へのメモリコピーは OpenSSL から OCF，OCF から NPE，この逆の処理も含め，Ping の一往復で合計 4 回おこなっている．4 回の合計時間は，平均で，18 μ sec であった．これは暗号化処理の 1 割程度であった．

SSL_read における計測

表 2 のとおりの結果となった．SSL_read も SSL_write と同じく，暗号処理が処理時間の大半を占めており，NPE へのメモリコピーの時間も同じく，平均 18 μ sec であった．

一往復の Ping の RTT は約 5.8msec であった．その内，NP-A と NP-B での SSL_write と SSL_read の処理の合計 (往復) は平均約 3.10msec であり，Ping の RTT の約 53%である．残りの部分として考えられるものは，libpcap によるイーサネットフレームのコピー時のオーバヘッドやパケットがケーブルを通過している時間が考えられる．

6 まとめと今後の課題

実装した SSL-VPN のパフォーマンス上のボトルネックになりうる箇所の計測をおこなった．今後の課題として，SSL の暗号化処理や MAC 処理の細部の解析，パケット長の長い通信の計測が挙げられる．

参考文献

[1] Yi-Neng Lin, Chiuan-Hung Lin, Ying-Dar Lin, and Yuan-Chen Lai, "VPN Gateways over Network Processors: Implementation and Evaluation", RTAS2005.
[2] Alan O. Freier, Philip Kocher, and Paul C. Kaltorn, "The SSL Protocol Version 3.0 draft", March 1996
[3] Tim Dierks and Christopher Allen, "RFC2246: The TLS Protocol Version 1.0", Jan 1999.
[4] http://www.intel.com/design/network/products/npfamily/index.htm
[5] A. D. Keromytis, J. L. Wright, and T. de Raadt, "The Design of the OpenBSD Cryptographic Framework", In Proceedings of the USENIX Annual Technical Conference, June 2003.