FPGA implementation of IPsec protocol suite  
for multigigabit networks

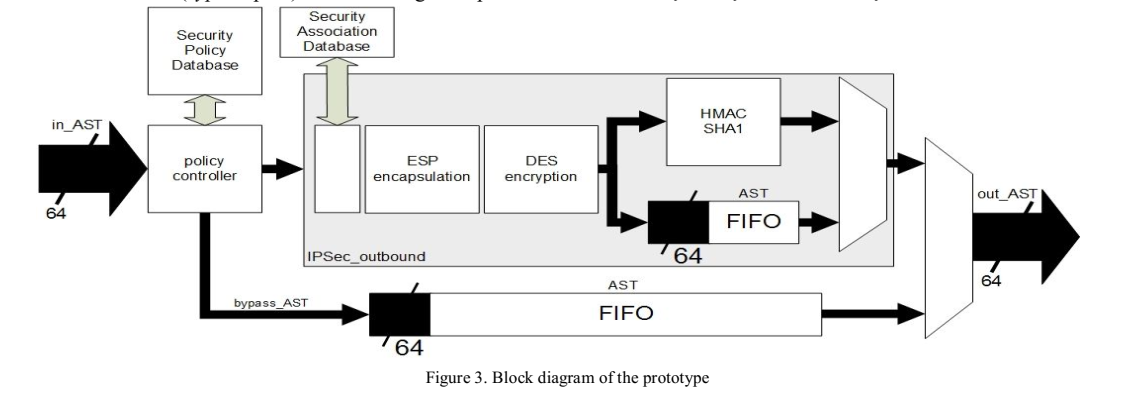
Mateusz Korona1, Krzysztof Skowron1, Mateusz Trzepiński1, Mariusz Rawski1  
1 Instytut Telekomunikacji, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska,  
Nowowiejska 15/19, 00-665, Warszawa, Poland

Bài báo trình bày việc triển khai phần cứng cổng IPsec trong FPGA. Hiệu quả của giải pháp được đề xuất cho phép sử dụng nó trong các mạng có tốc độ dữ liệu Gbit / s. Design does not support NAT-T (Traversal) feature and if it is located behind NAT, separate UDP encapsulation for ESP protocol must be performed.

**III/ PROTOTYPE DESIGN**

In section III. prototype of IPsec gateway is described and possible areas of its improvement are mentioned.( nguyên mẫu của cổng IPsec được mô tả và các khu vực có thể cải thiện của nó được đề cập.)

Trong thiết kế sẽ tối đa hóa lợi ích của xử lý gói phần cứng, bằng cách thực hiện tất cả các giai đoạn ở trong FPGA, , trái ngược với các giải pháp khác chỉ sử dụng phần cứng làm tăng tốc cho các chức năng quan trọng.

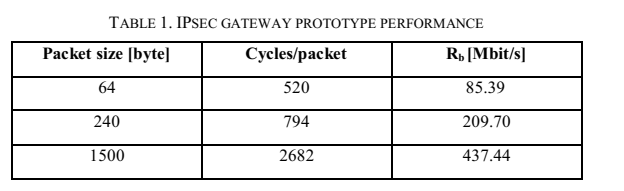


Hình 3 trình bày sơ đồ phần bảo mật gói của thiết kế (AST là viết tắt của giao diện AXI4-Stream).  
Sau khi tiếp nhận , IP packets are moved to simple security policy controller. Appropriate records are found in SPD database, basing on Pearson's hash calculated from IP header selectors. Mô-đun này xác định xem dữ liệu có cần được bảo mật hay không (đường dẫn bỏ qua/*bypass* path).

Quá trình bảo mật dữ liệu được thực hiện bởi mô-đun IPsec\_outbound. Các bước xử lý tiếp theo là: tra cứu cơ sở dữ liệu SAD, đóng gói ESP và mã hóa DES. Bước cuối cùng là tính toán băm(hash) HMAC-SHA1. Gói được lưu trữ trong FIFO, cho đến khi việc tính toán cuối cùng kết thúc.

Kết quả:

Thử nghiệm trên Terasic DE2-70 trang bị trên đó là Altera's Cyclone II FPGA. Clock tối đa của thiết kế là 86,72 MHz với 20% sử dụng logic FPGA.



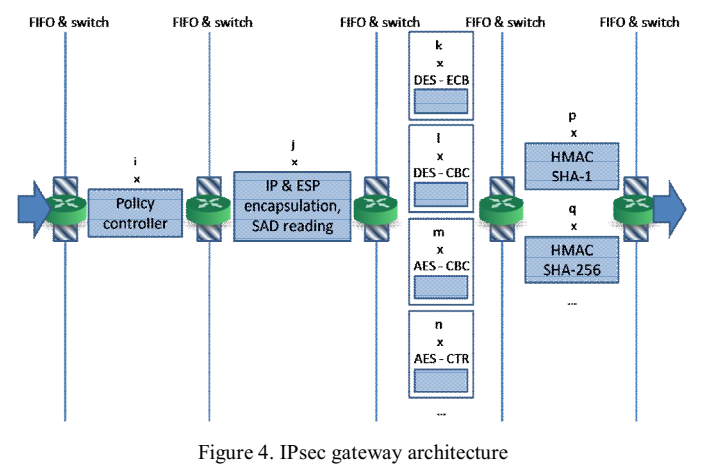
Vấn đề xem xét:

* The main “bottleneck” of the prototype là mô-đun chịu trách nhiệm tính toán băm HMAC. Thuật toán HMAC yêu cầu xử lý SHA-1 hai lần - đối với gói IP 240 byte, cần 86% thời gian xử lý của nó (685 chu kỳ của tổng số 794).
* Một vấn đề khác là thiết kế bộ xử lý bảo mật - chức năng IPsec được chia giữa bộ điều khiển chính sách bảo mật và mô-đun phức tạp thực hiện tất cả các hoạt động khác. Trong giai đoạn tính toán băm(hash) HMAC, đây là giai đoạn dài nhất trong toàn bộ quá trình, các tài nguyên chịu trách nhiệm đóng gói IP và ESP hoặc mã hóa dữ liệu vẫn chưa được sử dụng.

IV/ IPSEC GATEWAY

Thảo luận về kiến trúc của cổng IPsec đầy đủ chức năng và hiệu suất của nó được phân tích trong phần V.

Các phương pháp tối ưu hóa phần cứng tiên tiến đã được áp dụng để thực hiện, dẫn đến tăng tốc độ xử lý và sử dụng logic tốt hơn (Hình 4).



Ý tưởng :

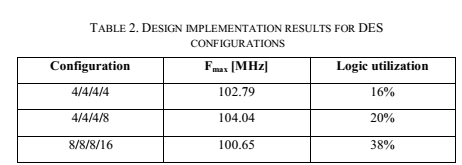
Các chức năng IPsec được chia thành nhiều phần của thiết kế. Mỗi phần có thể chứa nhiều mô-đun thực hiện một giai đoạn xử lý cụ thể, làm việc song song. Các phần được phân tách bằng hàng đợi FIFO và các công tắc vòng tròn, phân phối các gói giữa các mô-đun trong phần cụ thể. Kết quả là, nhiều gói có thể được xử lý cùng một lúc. Việc sử dụng các công tắc cho phép kiểm soát tải trọng của các phần tử xử lý trong phần đã cho.

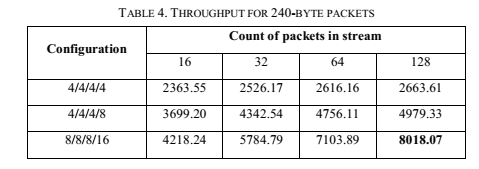
Việc tăng số lượng mô-đun tính toán HMAC thời gian nhất dẫn đến tăng thông lượng.

Ưu điểm của kiến trúc được trình bày cũng là ứng dụng đơn giản hóa của nhiều thuật toán mã hóa khác nhau.

Hiệu suất:

Thử nghiệm trên Kit Terasic DE5-Net với Altera's Stratix V FPGA.



Các thử nghiệm tương tự đã được tiến hành cho cổng IPsec sử dụng mật mã khối AES trong chế độ CBC, cao hơn DES.

Các thử nghiệm tương tự đã được tiến hành cho cổng IPsec sử dụng mật mã khối AES trong chế độ CBC, cao hơn DES.

