**Cấu hình lại IPSec ESP Core thích hợp cho các ứng dụng IoT trên FPGA**

Tác giả:

Muzaffar Rao, Thomas Newe

Optical Fibre Sensors Research Centre,

Mobile & Marine Robotics Research Centre,

Department of Electronic and Computer Engineering

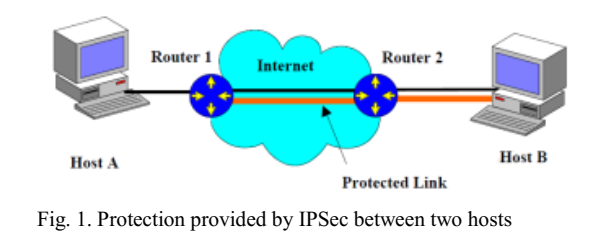
University of Limerick

Limerick, Ireland

* Tóm tác

Công việc này được thực hiện trên FPGA dựa trên cấu trúc lõi IPSec ESP. Giao thức IPSec được phát triển bởi IETF vào những năm 1998, là một giải pháp phổ biến để tao diều kiện bảo mật dữ liệu được truyền ta lớp IP. IPSec ESP là một trong 2 giao thức chính (AH: Authentication Header và ESP:Encapsulation Security Payload). IPSec ESP được sử dụng để cung cấp dịch vụ bảo mật dữ liệu bảo mật với tính xác thực (tùy chọn). Thực hiện IPSec là một công việc chuyên sâu về máy tính,đó là lý do tại sao việc triển khai phần cứng của IPSec là một giải pháp tốt nhất.

Ở đây, để thiết kế IPSec ESP lõi một thuật toán mã hóa AES là đã sử dụng. Thiết kế đề xuất cũng hỗ trợ chế độ ESP-tunnel và ESPtransport. Cốt lõi này được kiểm tra bằng cách áp dụng độ dài mặc định là 576 byte cho gói dữ liệu IPv4 và kết quả là báo cáo về Virtex-5 và Virtex-6 FPGAs. IPSec được đề xuất ESP lõi có thể được sử dụng để cung cấp bảo mật dữ liệu bí mật để Ứng dụng IoT



* Tổng quan về IPSec ESP

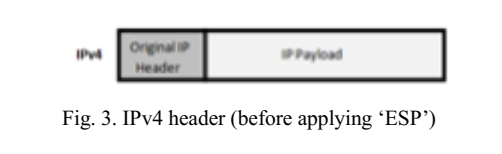
Giao thức ESP cung cấp cả mã hóa và xác thực

(không bắt buộc). Hai giao thức này hỗ trợ hai chế độ hoạt động sau

 Chế độ vận chuyển

 Chế độ đường hầm

Chế độ vận chuyển được sử dụng cho giao tiếp kết thúc đến cuối giữa hai máy chủ, trong khi chế độ đường hầm cung cấp đường hầm ảo giữa hai cổng. Tiêu đề IPv4 trước khi áp dụng ‘ESP’ được đưa ra trong hình 3.

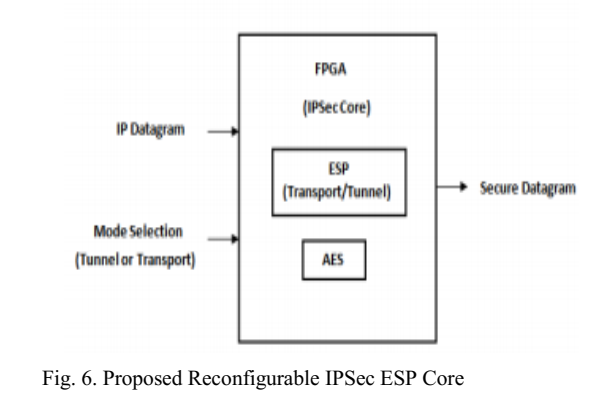


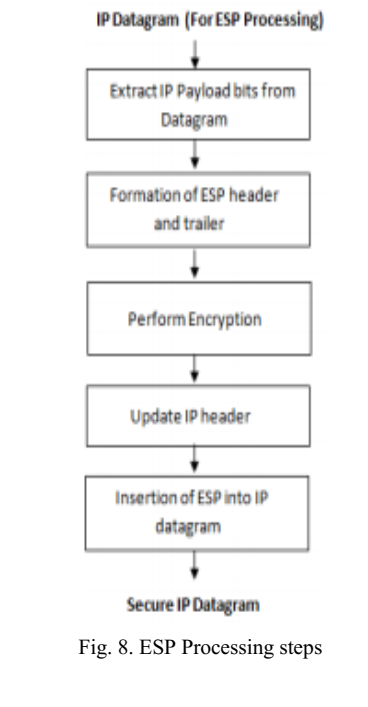
* TIÊU CHUẨN ENCRYPTION NÂNG CAO (AES)

AES là một thuật toán mật mã khối đối xứng dữ liệu cố định của khối 128 bit. Mật mã khối có nghĩa là số byte mà nó mã hóa được cố định nghĩa là 16 byte. Nó hỗ trợ kích thước khóa 128, 192 và 256 bit với vòng lặp lặp lại là 10, Lần lượt là 12 và 14. Số lượng các vòng được chọn tùy thuộc vào kích thước khóa. Một đơn vị mở rộng khóa riêng biệt là được sử dụng để tạo khóa cho mỗi vòng thuật toán AES. Bit chuỗi liên quan đến đầu vào, đầu ra và khóa mã hóa là được xử lý như mảng byte; được gọi là Tiểu bang. Mảng nhà nước bao gồm bốn hàng byte và mỗi hàng bao gồm 4 hàng byte. Trong mỗi vòng AES, một khối dữ liệu 128 bit là chuyển đổi bằng một chuỗi các hoạt động như được đưa ra trong [12]. Của chúng tôi trước đây trình bày kỹ thuật thực hiện AES [13], sử dụng tài nguyên BRAM và LUTs của FPGA, được sử dụng trong AES Chế độ truy cập ở đây để cung cấp mã hóa cần thiết cho IPSec Lõi ESP

Thực hiện IPSec ESP đề xuất

Việc triển khai IPSec ESP được trình bày bao gồm phương thức vận chuyển và đường hầm của các hoạt động như trong Hình 6. Lõi tái định cấu hình này có khả năng bảo mật gói dữ liệu IPv4.





* Thực hiện mã hóa

Việc thực hiện đề xuất AES được đề cập trong phần 3 được sử dụng để áp dụng dịch vụ mã hóa. Phạm vi mã hóa phụ thuộc vào phương thức hoạt động được chọn. Đối với chế độ vận chuyển IP tải trọng và đoạn giới thiệu ESP được mã hóa và cho chế độ đường hầm hoàn thành IP datagram và ESP trailer được mã hóa. AES lõi được sử dụng trong chế độ truy cập, sao cho một số 128 bit khối mã hóa có thể được thực hiện trong paralle.

* Trích xuất các bit Bit Payload từ datagram

Các bit payload IP được trích xuất từ datagram, bởi vì các bit được sử dụng trong tiêu đề ESP và cũng cần được mã hóa. Trong IPv4, độ dài của các trường được trích xuất này bằng ‘Tổng chiều dài - Độ dài tiêu đề ’.

Hình thành tiêu đề ESP / Đoạn giới thiệu

các trường giao thức ESP được trình bày chi tiết trong Bảng 1. 'SPI' trường được đặt thành 0, cho biết không có liên kết bảo mật nào tồn tại. Trường ‘số thứ tự’ được tạo bằng cách sử dụng 32- bit unsigned counter, tăng lên bất cứ khi nào ESP tiêu đề được tạo. Số thứ tự của an toàn đầu tiên gói datagram là 1. Trường 'Đệm' của đoạn giới thiệu ESP được sử dụng ở đây để đảm bảo độ dài của văn bản thuần túy được yêu cầu bởi lõi AES để mã hóa. Đoạn giới thiệu 'Độ dài đệm' của đoạn giới thiệu ESP được đặt số byte được chèn vào trường đệm. Đang vận chuyển chế độ trường tiêu đề ESP 'Tiêu đề tiếp theo' được đặt thành 'Giao thức' trường của tiêu đề IPv4. Ở chế độ đường hầm, trường ‘Tiêu đề tiếp theo’ của ESP đại diện cho gói dữ liệu IP gói gọn, đó là lý do tại sao đặt thành ‘4’ trong đó 4 là số giao thức của IPv4. Tải trọng IP được chèn vào giữa tiêu đề ESP và đoạn giới thiệu ESP trongphương thức vận tải, trong khi ở chế độ đường hầm hoàn thành gói dữ liệu IP là được thêm vào giữa tiêu đề ESP và đoạn giới thiệu.

* Cập nhật tiêu đề IP

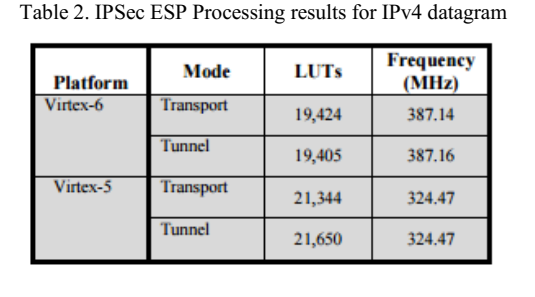
Trong IPv4, hai trường tiêu đề được cập nhật (1) Giao thức (2) Kiểm tra tiêu đề. Trường ‘Giao thức’ được đặt thành ‘Giao thức’ số ESP là 50 cho cả phương tiện vận chuyển và đường hầm. Vì sự thay đổi này, một kiểm tra đầu trang mới được tính toán và được đặt vào trường 'Tiêu đề kiểm tra' của tiêu đề IPv4

* Chèn ESP vào IP datagram

Bước cuối cùng trong quá trình xử lý ESP là chèn ESP vào IPdatagram, và nó phụ thuộc vào chế độ hoạt động và IP được chọn phiên bản. Đề án này được thực hiện như đã đề cập trong hình 4 và Hình 5. Bây giờ, datagram IP an toàn đã sẵn sàng để chuyển tiếp.

* Kết quả thực hiện được sử dụng cho giao thức IPSec ESP.

Project thực hiện trên một Virtex-5 và một Virtex-6 FPGA



* Kết luận

Trong công việc này một FPGA dựa trên cấu hình lại IPSec ESP lõi thực hiện được trình bày có thể được sử dụng để cung cấp dịch vụ bảo mật cho các ứng dụng IoT bằng BITW Ipsec dung dịch. Việc triển khai BITW này sẽ giúp giới thiệu Các tính năng bảo mật IPSec trong mạng IPv4 hiện có. Đề xuất thực hiện lấy gói dữ liệu IPv4 và một tiêu đề bổ sung (ESP header) được chèn vào trong datagram. Triển khai này hỗ trợ cả phương thức vận chuyển và đường hầm của hoạt động và chế độ có thể được cấu hình bằng tay cho việc lựa chọn cụ thể phương thức hoạt động. Chức năng mã hóa, AES là được triển khai để cung cấp các dịch vụ mã hóa cho giao thức ESP. Việc thực hiện giao thức ESP chủ yếu liên quan đến xác minh của phiên bản, bộ lọc gói, trích xuất các bit tải trọng IP từ datagram, sự hình thành của ESP header / Trailer, Mã hóa của các trường dữ liệu IP đã chọn, hình thành tiêu đề IP được cập nhật và chèn đầu vào ESP vào gói IP