**Cấu hình lại lõi IPSec AH thích hợp cho các ứng dụng IoT trên FPGA**

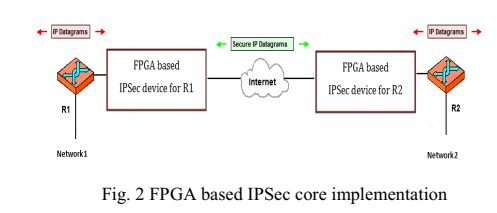
Tác giả: Muzaffar Rao\*, Thomas Newe, Ian Grout, Elfed Lewis, Avijit Mathur

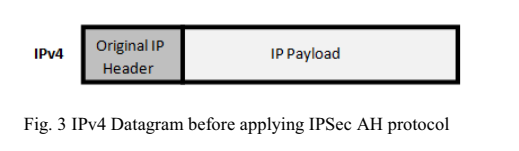
University of Limerick, Ireland

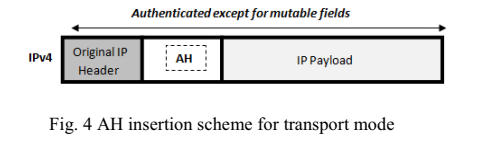
\*Muhammad.rao @ul.ie

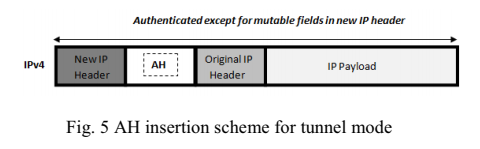
Tóm tắc

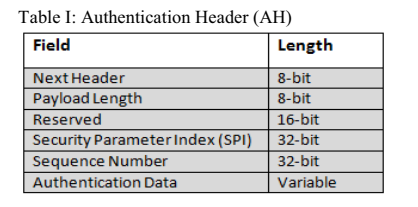
Triển khai Internet of Things của thế giới thực(IoT) ứng dụng yêu cầu giao tiếp an toàn. IPSec (Internet Protocol Security) là một quan trọng và được sử dụng rộng rãi giao thức bảo mật (trong lớp IP) để cung cấp bảo mật đầu cuối giao tiếp. Thực hiện IPSec là một máy tính công việc chuyên sâu, giới hạn đáng kể hiệu suất của các mạng tốc độ cao. Để khắc phục vấn đề này, phần cứng thực hiện IPSec là một giải pháp tốt nhất. IPSec bao gồm hai các giao thức chính là; Tiêu đề xác thực (AH) và Encapsulating Security Payload (ESP) với hai chế độ hoạt động, chế độ vận chuyển và chế độ đường hầm. Trong công việc này, chúng tôi trình bày một triển khai FPGA của giao thức IPSec AH. Việc triển khai này hỗ trợ cả chế độ đường hầm và phương tiện giao thông hoạt động. Hàm băm mật mã được gọi là Hash an toàn Thuật toán - 3 (SHA-3) được sử dụng để tính giá trị băm cho AH giao thức. Lõi IPSec AH được đề xuất có thể được sử dụng để cung cấp dịch vụ bảo mật xác thực dữ liệu cho các ứng dụng IoT.











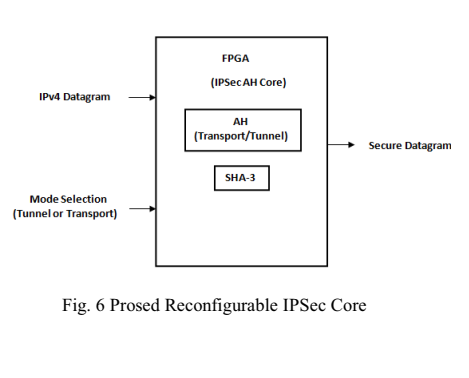
* SECURE HASH ALGORITHM -3 (SHA-3)

Hàm băm có thể được sử dụng để xác minh dữ liệu chính trực. Đây là quy trình xác định một chiều có đầu vào là một khối dữ liệu tùy ý và đầu ra của nó là chuỗi bit kích thước cố định, được gọi là giá trị băm. Các dữ liệu được mã hóa được gọi là thông báo và giá trị băm được gọi là thông báo thông báo. Tóm lại, thông báo tiêu hóa là dấu vân tay của dữ liệu và nếu dữ liệu thay đổi, nó thay đổi vân tay

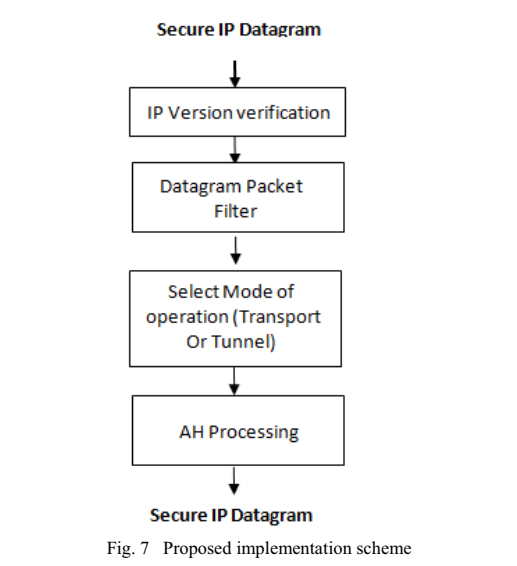
Hàm băm SHA-3 để cung cấp xác minh tính toàn vẹn dữ liệu

* Thực hiện AH ipsec được đề suất

Việc triển khai IPSec AH được trình bày bao gồm phương thức vận chuyển và đường hầm của các hoạt động và điều này lõi cấu hình lại có khả năng bảo mật gói dữ liệu IPv4 thể hiện trong hình 6.

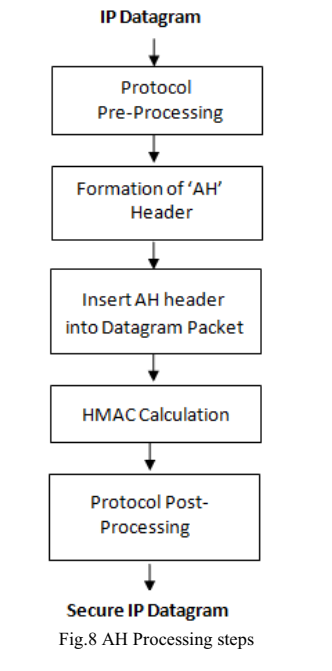


Xử lý giao thức AH chính được mô tả như sau



Việc xử lý AH được chia thành năm bước như được đưa ra trong

Hình 8.



* Hình thành tiêu đề AH:

Sự hình thành tiêu đề AH liên quan đến thế hệ 06 lĩnh vực. 06 trường này được trình bày chi tiết trong bảng 1. Trong giao thông vận tải chế độ trường tiêu đề AH tiếp theo được đặt thành trường 'Giao thức' của tiêu đề IPv4. Trong chế độ đường hầm, ‘Tiếp theo trường tiêu đề AH đại diện cho IP được đóng gói datagram, đó là lý do tại sao nó được đặt thành ‘4’ trong đó 4 là giao thức số lượng IPv4. Trường ‘AH len’ nghĩa là tổng chiều dài của AH header, phụ thuộc vào độ dài của giá trị HMAC. Các độ dài của giá trị HMAC dựa trên mật mã đã chọn hàm băm. Trong công việc này, để tính giá trị HMAC, chúng tôi đã chọn biến thể 256 bit của SHA-3. Ngoài ra, ‘AH len’ là được đề cập trong các từ 32 bit trừ đi 2. Điều này trừ hai là vì thực tế là AH về cơ bản là một tiêu đề mở rộng của IPv6, độ dài thường được đo bằng các từ 64 bit, không phải từ 32 bit. Vì vậy, ở đây cho IPv4, AH len = [3 (32-bit trường cố định của AH tiêu đề) + 8 (32-bit từ cho Giá trị HMAC)] - 2, tức là '9'. Trường tiếp theo của tiêu đề AH là ‘Reserved’ được đặt thành 0 không phân biệt chế độ được chọn. Trường 'SPI' cũng được đặt thành 0 cho biết không liên kết bảo mật tồn tại. Trường ‘số thứ tự’ là được tạo bằng cách sử dụng bộ đếm không dấu 32 bit, tăng bởi một khi nào tiêu đề AH được tạo ra. Trình tự số gói datagram an toàn đầu tiên là 1. Trường cuối cùng của Tiêu đề AH là trường ‘Dữ liệu xác thực’ được đặt thành Giá trị HMAC. Như đã đề cập trước đó, ở đây chiều dài của Giá trị HMAC là 256-bit và được đặt thành 0 cho HMAC phép tính.

* Chèn tiêu đề AH vào IP datagram

Trước khi tính giá trị HMAC, AH tạo ra tiêu đề được chèn vào giao thức IP được xử lý trước. Lược đồ chèn này phụ thuộc vào chế độ được chọn của hoạt động như trong hình 4 và hình 5. Bước này dẫn đến datagram cập nhật được sử dụng để tính toán HMAC.

* Tính toán HMAC

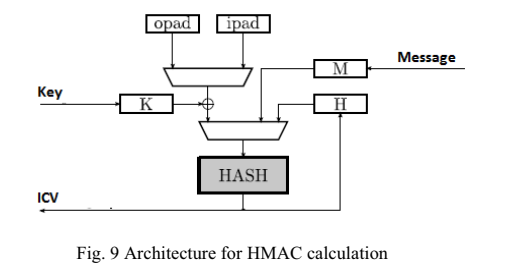
Để cung cấp tính toàn vẹn và tính xác thực của dữ liệu trong Giao thức AH, IPSec định nghĩa một HMAC đối xứng [19] được sử dụng để tạo ICV. Ưu điểm chính của một HMAC là tốc độ tương đối cao so với kỹ thuật số chữ ký. IPSec yêu cầu sử dụng HMAC xây dựng, cung cấp thẻ xác thực kích thước cố định cho các thông điệp tùy ý. Giá trị HMAC hoặc ICV của một thông điệp x được tính như

H(K XOR opad, H(K XOR ipad, x))

opad và ipad là hằng số đệm

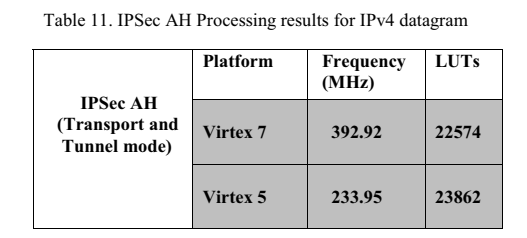
H là hàm băm mật mã

K là khóa bí mật



* Kết quả

Thực hiện trên Virtex-5 và Virtex-7 FPGA cho giao thức IPSec AH



* Kết luận

Trong công việc này, một IPSec AH có thể cấu hình lại dựa trên FPGA thực hiện cốt lõi được trình bày có thể được sử dụng để cung cấp dịch vụ bảo mật cho các ứng dụng IoT. Đề xuất thực hiện lấy gói dữ liệu IPv4 có độ dài mặc định tức là 576 byte và tiêu đề bổ sung (tiêu đề AH) được chèn trong datagram đầu vào. Việc triển khai này hỗ trợ cả hai, vận chuyển và chế độ đường hầm hoạt động và có thể được cấu hình bằng tay cho việc lựa chọn chế độ hoạt động cụ thể. Hàm băm mật mã, SHA-3 được triển khai tính giá trị ICV cho giao thức AH. Giao thức AH thực hiện chủ yếu liên quan đến việc xác minh phiên bản, bộ lọc gói, giao thức tiền xử lý (để chuẩn bị datagram để tính HMAC), hình thành tiêu đề AH, chèn của AH header vào IP datagram, tính toán HMAC và giao thức sau xử lý. Giao thức tiền xử lý liên quan đến cập nhật tiêu đề IP và tính toán kiểm tra đầu trang. Phần lõi IPSec được cấu hình lại có khả năng hỗ trợ bảo mật cho bất kỳ ứng dụng IoT nào yêu cầu xác thực ở tốc độ cao.

REFERENCES

[1] Shancang Li, Li Da Xu, shanshan Zhao, “ The Internet

of Things:Survey”, Information Systems Frontiers Journal,

April 2015,Volume 17, Issue 2, pp-243-259, DOI:

10.1007/s10796-014-9492-7.

[2] Hui Suoa , Jiafu Wan, Caifeng Zoua , Jianqi Liua,

“Security in the Internet of Things: A Review”, IEEE

International Conference on Computer Science and

Electronics Engineering, 2012, DOI: DOI

10.1109/ICCSEE.2012.373.

[3] “RFC-791,” http://www.ietf.org/rfc/rfc791.txt.

[4] “RFC-1349,” http://www.ietf.org/rfc/rfc1349.txt.

[5] “RFC-2474,” http://www.ietf.org/rfc/rfc2474.txt.

[6] S. Kent, and R. Atkinson, “Security architecture for the

internet protocol,” IETF network working group, RFC2401,

1998.

[7] “RFC-4302,” https://www.ietf.org/rfc/rfc4302.txt

[8] “RFC-4303,” https://www.ietf.org/rfc/rfc4303.txt

[9] The Internet of Things (IoT): 8 Myths and Facts, URL:

https://datafloq.com/read/internet-of-things-iot-myths-andfacts/1042.

[10] Alberto Ferrante, Vincenzo Piuri, and Jeff Owen,

“IPSec Hardware Resource Requirements Evaluation,” Next

Generation Internet Networks (NGI 2005), April 2005.

pp.240-246, “doi:10.1109/NGI.2005.1431672”.

[11] National Instruments. Introduction to FPGA

Technology: Top Five Benefits. http://zon

e.ni.com/devzone/cda/tut/p/id/6984, December 2010.

[12] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche,

“The KeccakSHA-3 Submission,” Submission to NIST

(Round 3), 2011. [Online].Available: http://keccak.

noekeon.org/Keccak-submission-3.pdf.

[13] Kozierok, C. M., The TCP/IP Guide, 2005.

[14] X. Wang, X.L. Feng, D. Yu, Collisions for hash

functions MD4, MD5, HAVAL-128 and RIPEMD.

Cryptology ePrint Archive, Report 2004/199, pp. 1–4

(2004), http://eprint.iacr.org/2004/199

[15] M. Szydlo, “SHA-1 collisions can be found in 263

operations” CryptoBytes Technical Newsletter (2005) [16]

M. Stevens, Fast collision attack on MD5. ePrint-2006-104,

pp. 1–13 (2006), http : //eprint.iacr.org/2006/104.pdf

[16] M. Stevens, Fast collision attack on MD5. ePrint-2006-

104, pp. 1–13 (2006), http : //eprint.iacr.org/2006/104.pdf

[17] National Institute of Standards and Technology (NIST):

SHA-3 Winner announcement. http :

//www.nist.gov/itl/csd/sha-100212.cfm

[18] M. Rao, T. Newe and I. Grout, “Efficient High Speed

Implementation of Secure Hash Algorithm-3 on Virtex-5

FPGA”. 17th Euromicro Conference on Digital System

Design (DSD 2014), Verona, Italy, August 27-29, 2014.

[19] “RFC2104,” https://tools.ietf.org/html/rfc2104