2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing

FPGA based Reconfigurable IPSec AH core suitable for IoT applications

Muzaffar Rao*, Thomas Newe, Ian Grout, Elfed Lewis, Avijit Mathur
University of Limerick, Ireland
*Muhammad.rao @ul.ie

***Abstract*— Real-world deployments of Internet of Things (IoTs) applications require secure communication. The IPSec (Internet Protocol Security) is an important and widely used security protocol (in the IP layer) to provide end to end secure communication. Implementation of the IPSec is a computing intensive work, which significantly limits the performance of the high speed networks. To overcome this issue, hardware implementation of IPSec is a best solution. IPSec includes two main protocols namely; Authentication Header (AH) and Encapsulating Security Payload (ESP) with two modes of operations, transport mode and tunnel mode. In this work we presented an FPGA implementation of IPSec AH protocol. This implementation supports both, tunnel and transport mode of operation. Cryptographic hash function called Secure Hash Algorithm – 3 (SHA-3) is used to calculate hash value for AH protocol. The proposed IPSec AH core can be used to provide data authentication security service to IoT applications.**

***Index Terms*—**FPGA, SHA-3, IPSec, AH

I. INTRODUCTION

The Internet of things (IoTs) [1] describe next generation of internet, where the physical things could be accessed and identified through the internet. So, we can say that is a world, where billions of objects can sense, share information and communicate over interconnected public or private Internet Protocol (IP) networks as shown in Fig. 1. As the adoption of IoT becomes pervasive, the quantity of data that is captured and stored becomes larger, that raised the data security concerns for deployment of IoT applications. The IoT will be faced with more severe challenges because it extends the 'internet' through the traditional internet, mobile network, sensor network and so on. Every 'thing' will be connected to this 'internet' and these 'things' will communicate with each other. Therefore, the new security and privacy problems will arise [2]. It demands that we should pay more attention to the research issues for confidentiality, authenticity, and integrity of data in the IoT.

The Internet Protocol (IP) [3][4][5] is the primary communication protocol for transferring data between parties across a network. It defines datagram structures that are encapsulating the data to be delivered. The IPSec protocol [6] developed by the IETF (Internet Engineering Task Force) in 1998, is one popular solution to protect the data transfer at the IP layer. The IPSec protocol can provide security services like access control, connectionless integrity, data origin authentication, protection against replays, confidentiality, and limited traffic flow confidentiality.

In IPSec, there are different protocols to provide above mentioned security services. For instance, the AH protocol [7] provides data authentication, the ESP protocol [8] defines mechanisms for confidentiality and data integrity (optional). Finally, the Internet Key Exchange (IKE) protocol is used for establishing secure connections. According to [6] manual configuration option can also be used instead of IKE to configure IPSec for desired security service and . These protocols use different cryptographic primitives such as encryption, hashing and modular arithmetic in order to provide security services.

The authors would like to thank the Erasmus Mundus STRoNGTiES program and IRC (Irish Research Council) for providing funding that has facilitated the completion of this work.

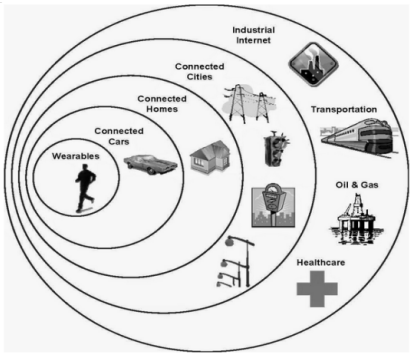

Fig. 1: IoT connecting 'Everything' [9]

IPSec AH and ESP protocols support two modes of operation, tunnel mode and transport mode. In transport mode, only the upper-layer protocol data segment of the IP packet is authenticated or encrypted and it is typically used for end-to-end protection of data packets between two hosts. In tunnel mode the entire IP packet is authenticated or encrypted within a new outer IP header. The tunnel mode can be used between security gateway (router or firewall) to create a VPN (virtual private network).

The IPSec protocol is almost embedded into TCP/IP protocol stack via software in OS (operating system), such as Linux and NetBSD. But the IPSec has proved to be computationally very intensive [10], which greatly affects the performance of the network. Data throughput in core routers has all ready achieved to terabits today, and the line card interface speed is already 10Gbps or above. But the high performance internet security device is far behind. The main reason is that, the data processing for security is complex and time consuming. So, it is difficult for the security devices to achieve the equal performance as the internet devices. Software solutions suffer from low performance (when compared to hardware) and some hardware implementations, such as ASIC (Application-Specific Integrated Circuit) implementations, lack the flexibility and programmability offered by the software.

An Field Programmable Gate Arry (FPGA) is the best leading representative of reconfigurable hardware devices of modern era because of its architectural flexibility

978-1-5090-0154-5/15 $31.00 © 2015 IEEE
DOI 10.1109/CIT/IUCC/DASC/PICOM.2015.327

(parallelism, on-chip memory, etc.) and high performance features [11]. One of the possible implementation of FPGA based IPSec device implementation is given in Fig. 2. In Fig. 2 two networks communicate with each other using a secure internet connection. This security is achieved by using FPGA based IPSec device which takes IP datagram from gateway/router, apply IPSec protocol and forward the secure datagram to internet.

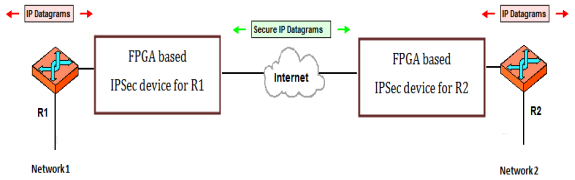

Fig. 2 FPGA based IPSec core implementation

In this work we have presented implementation of AH protocol of IPSec using tunnel and transport mode of operations. Manual configuration option is used for selection of operational modes and configuration of Key. To provide authentication, cryptographic hash function, SHA-3 [12] is implemented because this is the newly selected and most secure cryptographic hash function.

The remainder of this paper is organized as follows. A brief overview of the IPSec AH protocol is given in section II, while Section III discusses about FPGA. Section IV detailed about SHA-3 algorithm background and section V discussed about proposed IPSec AH implementation. Performance results are discussed in section VI, while Section VII concludes. Finally future work is discussed in section VIII.

II. IPSEC AH OVERVIEW

The IP version 4 (IPv4) has no inherent security and IP packets are completely modifiable in transit. When IPv4 was developed, the internet was relatively private. Nowadays it is truly public, which is causing more security problems. Several methods have been developed over years to cover security needs. The most effective solution was to allow security at the IP level so that all higher layer protocols in TCP/IP could use it. The security solution at the IP level beomes possible because of IPSec technology, that brings secure communications to the IP level [13].

The AH protocol of IPSec provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram. The parts of the datagram that are used for the calculation and the placement of the header, depend on the selected mode of operation and IP version. In AH protocol a cryptographic hashing algorithm is used together with a specific key known only to the source and the destination. On the source device, AH performs the computation using hash function and puts the result which is called the integrity check value (ICV) into an AH header with other fields for transmission. On the receiving side ICV value is recalculated and verified.

In transport mode, the AH header is added after the main IP header of the original datagram. In tunnel mode, it is added after the new IP header that encapsulates the original datagram that's being tunneled. The IPv4 datagram before

Fig. 3 IPv4 Datagram before applying IPSec AH protocol

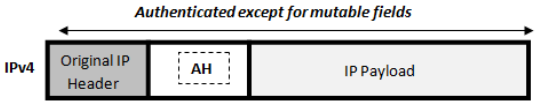

Fig. 4 AH insertion scheme for transport mode

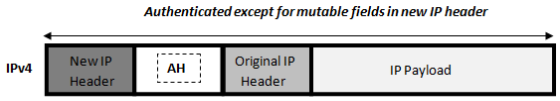

Fig. 5 AH insertion scheme for tunnel mode

applying IPSec AH protocol is shown in Fig. 3 while the AH header insertion scheme for tunnel and transport mode is given in Fig. 4 and Fig. 5 respectively.

The AH header consists of 06 fields as shown in Table I. The 'Next header' field is used to link the headers together and identifies the type of header immediately following AH header. The 'Payload length' field represents length of the AH in 32-bit words minus 2, while the 'Reserved' field is reserved for the future use. The 'SPI' (Security Parameter Index) field identifies a security association (SA) that specifies shared security attributes between entities. According to [7], SPI value of zero is reserved for local, implementation-specific (in absence of security association). The 'Sequence number' field represents a monotonically increasing counter value that is used to provide protection again replay attack. The last field of AH header i.e 'Authentication data' contains Integrity check value (ICV) for the datagram, calculated by using HMAC (Hash Message Authentication Code).

Table I: Authentication Header (AH)

Field	Length
Next Header	8-bit
Payload Length	8-bit
Reserved	16-bit
Security Parameter Index (SPI)	32-bit
Sequence Number	32-bit
Authentication Data	Variable

III. WHY FIELD PROGRAMMABLE GATE ARRAY (FPGA)?

The Field Programmable Gate Array (FPGA) is a family of reconfigurable hardware, where Field Programmable means the operation changing capability in the field, and Gate Array means the construction of basic internal architecture of the device. Digital computing tasks can be developed in software and compiled into a bitstream file. This bitstream file contains information about how the components should be wired together.

FPGAs combine the best parts of ASICs and processor-based systems, in fact FPGAs are parallel in nature. The

advantage of using a software programmed processor is that software is very flexible to change while a disadvantage is that performance can suffer if the clock is not fast. The advantage of an ASIC is that it can provide very high performance because of its dedicated type of operation and its disadvantages are: 1) high cost to volume ratio; 2) extended delay between design to end product; 3) incapability to include new changes after the system is fabricated and 4) difficulties in debugging errors.

FPGAs fill the gap between hardware and software and offer numerous advantages such as: 1) flexibility, 2) reliability, 3) low cost, 4) fast time-to-market and 5) long-term maintenance. Given this the authors consider that an FPGA is the best reconfigurable hardware platform for the implementation of cryptographic security mechanisms.

IV. Secure Hash Algorithm -3 (SHA-3)

Hash functions can be used for the verification of data integrity. This is a one-way deterministic procedure whose input is an arbitrary block of data and whose output is a fixed-size bit string, which is known as the hash value. The data to be encoded is called the message, and the hash value is called the message digest. In short, a message digest is a fingerprint of the data and if the data changes, it changes the fingerprint.

The hash of a piece of data is calculated and appended to the data. When the message arrives at its destination, the hash is recalculated from the data and compared it to the hash, that was appended to the original message. If the values do not match, then it means the data has been corrupted and will not be processed.

Previously used hash functions (SHA-0, SHA-1, SHA-2, RIPEMD and MD5) were found to have Vulnerabilities [14][15][16]. Although, no attack on SHA-2 has been reported yet, but the algorithmic similarity of SHA-2 with SHA-1, make this algorithm's security susceptible. That's why we implemented newly selected cryptographic hash function SHA-3, to provide data integrity verification. This new algorithm was announced by National Institute of Standards and Technology (NIST), USA in 2012 [17]. Our earlier presented SHA-3 implementation technique [18] is used for the IPSec AH protocol implementation.

V. Proposed IPSec AH implementation

The presented IPSec AH implementation involves transport and tunnel mode of operations and this reconfigurable core is capable to secure IPv4 datagram as shown in Fig. 6.

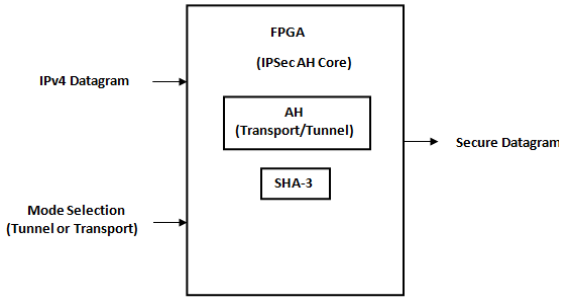

Fig. 6 Prosed Reconfigurable IPSec Core

This reconfigurable IPSec AH core can be configured manually for desired mode of operation. The implemented scheme steps are presented in Fig. 7. Initial 04 bits of datagram packet are used to check the IP version. This check is necessary to have the idea about the structure of datagram. So, that different datagram's fields can be accessed and updated during AH processing. The IP header bits are extracted from the IP datagram. Once the IP version is verified, the datagram packet is passed through the packet filter, that is used to decide either AH processing is required or not. This packet filtering worked as security policy for IPSec. Using this packet filtering, datagram packet is dropped, forwaeded without applying IPSec or forwarded with IPSec processing. In this implementation we checked 'protocol' field of IP datagram, if this field is equal to '51'(protocol number of AH protocol), it means received datagram is already secure. In this case datagram is forwarded without applying AH protocol. Similarly, by applying check on IP address of a particular network, IP datagram can be dropped and forwarded with and without applying AH protocol. Next block of Fig. 7 involves selection of mode of operatio that is configured through input. The last step is of main AH protocol processing, which is described below.

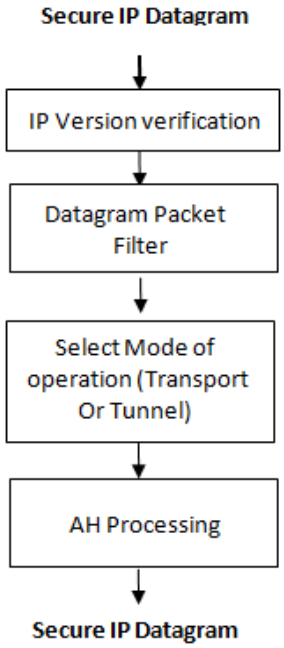

Fig. 7 Proposed implementation scheme

The AH processing is divided into five steps as given in Fig. 8.

a. Protocol Pre-Processing

The protocol pre-processing is used to prepare the IP header for the calculation of ICV and depends on selected mode of operation. In transport mode only IP header is updated, while in tunnel mode a new IP header is generated. In transport mode, the IP header is updated by replacing mutable fields (modified during transit) of IPv4 header by zero and also by updating some other fields; like 'Protocol'

field of IPv4 header by '51'(where '51' is the protocol number for AH). Also, the 'Total length' field of IPv4 header is updatted by adding the AH length in original length of datagram. In tunnel mode, fields of new IP header are set to the fields of original IP header and mutable fields are replaced by zero. The 'Protocol' field of new IPv4 header is replaced by 51, same like transport mode. But, the 'Total length' field of new IPv4 header is updatted by adding AH length and IP header length in original length of the datagram (because of IP header encapsulation in tunnel mode). The source and destination address of new IP header are the IP addresses of the devices between them tunnel is formed. The details about mutable and immutable fields of IPv4 header is given in [7]. This pre-processed IP header is used for the calculation of ICV value during formation of AH header.

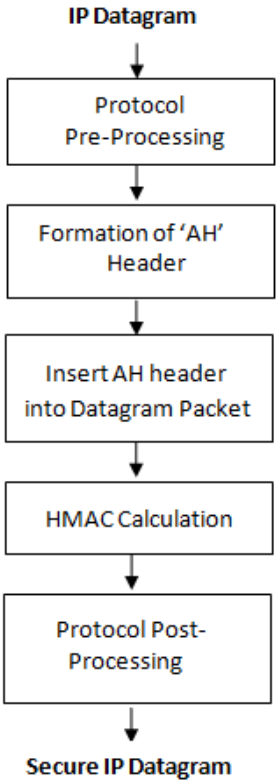

Fig.8 AH Processing steps

b. Formation of AH Header:

The AH header formation involves generation of 06 fields. These 06 fields are detailed in table 1. In transport mode the 'Next header' field of AH header is set to 'Protocol' field of IPv4 header. In tunnel mode the 'Next header' field of AH represents the encapsulated IP datagram, that's why it is set to '4' where 4 is the protocol number of IPv4. The 'AH len' field i.e the total length of AH header, depends upon the length of HMAC value. The length of HMAC value based on selected cryptographic hash function. In this work, to calculate HMAC value we selected 256-bit variant of SHA-3. Also, the 'AH len' is mentioned in 32-bit words minus 2. This minus two is because of the fact that AH is basically an extension header of IPv6, which length is usually measured in 64-bit words, not in 32-bit words. Therefore, here for IPv4 , AH len = [3(32-bit fixed fields of AH header) + 8(32-bit words for the HMAC value)] – 2, i.e '9'. The next field of AH header is 'reserved' that is set to zero irrespective of selected mode. The 'SPI' field is also set to zero that indicates that no security association exists. The 'sequence number' field is generated by using 32-bit unsigned counter, which increases by one whenever AH header is generated. The sequence number of first secure datagram packet is 1. The last field of AH header is 'Authentication Data' field, which is set to HMAC value. As mentioned earlier, here the length of HMAC value is 256-bit and is set to zero for HMAC calculation.

c. Insertion of AH header into IP datagram

Before computation of HMAC value, the generated AH header is inserted into protocol pre-processed IP datagram. This insertion scheme depends on the selected mode of operation as shown in Fig. 4 and Fig. 5. This step resulted in updatted datagram that is used for HMAC calculation.

d. HMAC calculation

In order to provide data integrity and authenticity in AH protocol, the IPSec defines a symmetric HMAC [19] that is used to generate the ICV. The main advantage of a HMAC is its relatively high speed as compared to digital signatures. IPSec requires the usage of the HMAC construction, which provides a fixed size authentication tag for arbitrary messages. The HMAC or ICV value of a message *x* is computed as

$$\mathbf{H}(\mathrm{K} \mathit{XOR} \mathit{opad}, \mathbf{H}(\mathrm{K} \mathit{XOR} \mathit{ipad}, x))$$

Where, *opad* and *ipad* are padding constant

H is the cryptographic hash function
K is the secret key

To make the construction secure, it is required that the key length used is equal or greater than the output length of the employed hash function H. The The implementation of an HMAC wrapper, given a hash function H, is shown in Fig. 9. Here, the 'message' is updated datagram after the insertion of AH header.

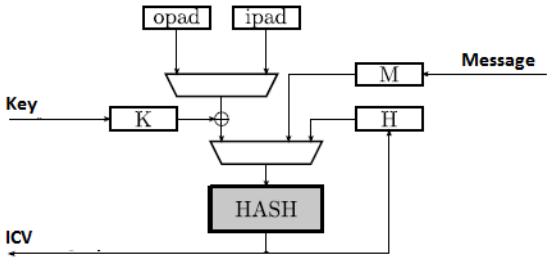

Fig. 9 Architecture for HMAC calculation

e. Protocol Post-Processing

The protocol post-processing implementation involves three steps, (1) The 'Authentication data' field of AH header

is set to the calculatted ICV value (2) The mutable fields, which were replaced by zero for ICV calculation are set back to their original values (3) An additional step is implemented i.e to re-calculate the header checksum and update the 'header checksum' field of IPv4. Now, the secure datagram is ready to forward.

To calculate the header checksum, 160 bits of updated IP header are divided into 16-bit words. These 16- bit words are added together and the resulted 16-bit ourput is inverted. This inverted output is the required header checksum.

VI. PRERFORMANCE RESULTS

In this work a Virtex-5 and a Virtex-7 FPGA is used for the implementation of IPSec AH protocol. Selection of these Xilinx FPGAs was made because of their high performance feature. The design was implemented and synthesized using ISE Xilinx 14.2 tool and the HDL language Verilog is used. The target device xc5vtx240t-2ff1759 was used for Virtex-5 and xc7vx690t-2ffg1157 for Virtex-7.

The implemented IPSec AH core supports input datagram of 576 bytes. This length of datagram is selected because the default maximum size of IPv4 datagram is 576 bytes [3].

Table 11. IPSec AH Processing results for IPv4 datagram

	Platform	Frequency (MHz)	LUTs
IPSec AH (Transport and Tunnel mode)	**Virtex 7**	**392.92**	**22574**
	Virtex 5	**233.95**	**23862**

VII. CONCLUSION

In this work an FPGA based reconfigurable IPSec AH core implementation is presented that can be used to provide security services to IoT applications. The proposed implementation takes IPv4 datagram of default length i.e 576 bytes and an additional header (AH header) is inserted in input datagram. This implementation support both, transport and tunnel mode operation and can be configure manually for the selection of specific mode of operation. The cryptographic hash function, SHA-3 is implemented to calculate ICV value for AH protocol. The AH protocol implementation mainly involves verification of version, packet filter, protocol pre-processing (to prepare datagram for HMAC calculation), formation of AH header, insertion of AH header into IP datagram, HMAC calculation and protocol post-processing. Protocol pre-processing involves update of IP header and calculation of header checksum. The presented reconfigurable IPSec core is capable of supporting security for any IoT application that requires authentication at a high speed.

VIII. FUTURE WORK

IPSec AH protocol supports the data authentication service, not the data confidentiality service. To provide data confidentiality service IPSec ESP protocol is used. Therefore, future work includes implementation of IPSec ESP protocol.

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-and-facts/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://zone.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