A solution for packet security 1 Gbps on layer 2 with technology FPGA

Ky Phan Van, Thang Tran Van, Phuc La Huu

***Abstract*— The Layer 2 network security has shown many advantages compared to Layer 3. However, the structure of Layer 2 does not indicate the size of data packet, it makes the difficult to capture the data packet, especially in the case the packet is captured by hardware. Also, there are limitation of using software to capture the packet. In addition, when the size of the packet is not defined, it will be difficult to handle the packet with inserting cryptographic parameters that exceed the permissible length. In this paper, a technical solution for capturing Ethernet packet directly from FPGA is presented, organising data to ensure transparent communication capability to implement Layer 2 packet security, to overcome the limitations when capturing packet by using software.**

***Tóm tắt*— Bảo mật mạng Layer 2 đã thể hiện được nhiều ưu điểm so với bảo mật Layer 3, tuy nhiên do cấu trúc của gói tin Layer 2 không cho biết kích thước gói tin nên gây khó khăn cho việc bắt gói tin, đặc biệt khi bắt trực tiếp bằng phần cứng, trong khi nếu sử dụng phần mềm thì có nhiều hạn chế. Hơn nữa, khi không biết kích thước sẽ gây khó khăn trong việc xử lý gói tin khi chèn các tham số mật mã vượt quá độ dài cho phép. Trong bài này trình bày một giải pháp kỹ thuật bắt gói tin Ethernet trực tiếp từ FPGA, tổ chức dữ liệu đảm bảo khả năng truyền tin trong suốt cho phép thực hiện bảo mật gói tin Layer 2, khắc phục được những hạn chế khi bắt gói tin bằng phần mềm.**

***Keywords*— FPGA; layer 2 security; network security.**

***Từ khóa*— FPGA; bảo mật Layer 2; bảo mật mạng.**

I. INTRODUCTION

Layer 2 security has been a growing trend of research and development to meet the increasing demand for bandwidth, data transmission over the network along with the emergence of cloud computing services, mobile devices, increasing of video traffic and development of technology IoT (Internet of Thing). Researches of Rohde & Schwarz [1] pointed out that security solution Layer 2 MACSec (Media Access Control Security) has higher performance than security solution Layer 3 IPSec because there is no need to transmit header IP (Internet Protocol) of data packet. Figure 1 compares the performance of MACSec and IPSec to the length of the encrypted frame. With average processing package size 250 byte per each encrypted packet, the performance of IPSec about 75% meanwhile the performance of MACSec about 90%. Moreover, one of the advantages of Layer 2 encryption is that the Layer 2 terminal is a simple device that don’t need to provide routing functions, no need to allocate additional network addresses for the network interfaces of security device.

Although Layer 2 MACSec security protocol [2] was standardized more than 10 years ago, but compared to Layer 3 IPSec security studies [3], study on the Layer 2 security with MACSec around the world is very modest.

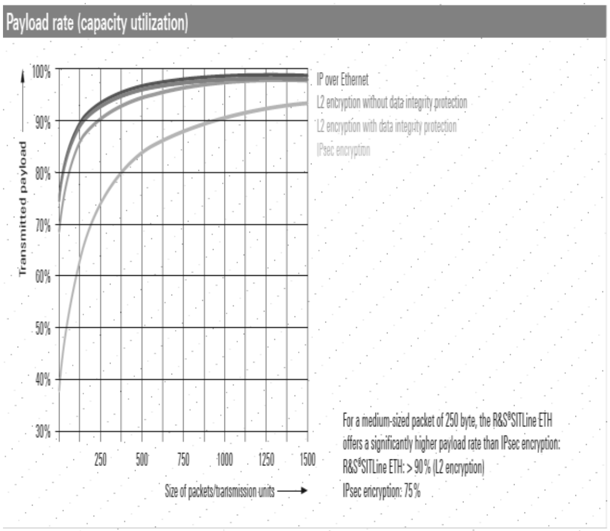

Fig 1. MACSec and IPsec performance [3]

This manuscript is received on December 1, 2018. It is commented on December 11, 2018 and is accepted on December 18, 2018 by the first reviewer. It is commented on December 16, 2018 and is accepted on December 22, 2018 by the second reviewer.

To capture network packets for processing, there are 2 common methods: 1) By software [4], using embedded operating system, capturing packets through software; 2) By hardware [5] [6], using FPGA to capture directly without the operating system.

In the Organization most products are focused on security processing with IP packets at the Layer 3. With the technical solutions products of the Organization mainly use embedded Linux operating system to separate the packets and combine with encryption/decryption part on FPGA as the solution in the document [4]. With this technical solution, there are many advantages in processing packets due to reading/writing packets managed by the operating system, but it also has many limitations:

- Reading and writing speed is not high due to read/write packet by software.
- It's impossible to avoid the security holes of the operating system needing the attention on the safety of the system.
- Encryption speed is not high due to dependence on communication between embedded computer and block FPGA implementing encryption.

In this article, presenting a technical solution to read and write directly the packet by FPGA hardware, forming of encrypted data frame can be implemented on Layer 2 security to avoid the above limitations. The content of the article includes part 1 introduction, part 2 presents the solution, part 3 is the implementation on Altera's KIT FPGA DE4, part 4 is the result of implementation and conclusion.

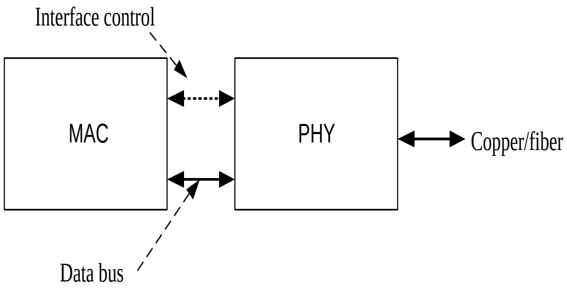

Fig 2. Interface between MAC and PHY

II. SECURITY SOLUTION

A. Read write the packet directly

According to IEEE 802.3 [7] the interface between the MAC block and PHY physical processing is shown in figure 2. In this figure the management interface is usually MDC/MIO and the data interface is MII/GMII/SGMII (Serial Gigabit Media Independent Interface).

To read and write the packet directly, it's necessary to set PHY component parameters via MDC/MIO communication and capture/transmit data packets via MII/GMII/SGMII communication with the purpose controlling the operation of MII/GMII/SGMII.

Depending on different tools and components, different transmission lines can control PHY's activities organized into libraries convenient for development.

B. Forming encrypted data frames

Formation of encrypted data frames on the transmission line ensures that the encrypted/ decrypted data stream is always concerned. The general rule for organizing data lines to allow security is to add signaling data that shows information about encrypted packets as well as information about the secret parameters that will be used at the beginning of the packet [2] [3]. To ensure compliance with IEEE 802.3, the security data frame is formed as Table 1.

With the selected encryption solution is stream cipher based on the block cipher (such as the gamma mode of GOST- or Counter of AES), the encrypted data stream on the transmission line is the result of XOR between the data stream and the generated key from the key generation block. The generated key is the output cipher text of the block cipher with the private key and the input is IV of each packet. The parameter of Table 1 is described: the first 3 fields are the header of Ethernet packet [7], shows the source MAC address; destination MAC address and type (type) of packet; 4 signaling bytes (32 bits) is organized with bits and their meaning is shown in Table 2; encrypted data has size from 0-1468 bytes to make sure not to exceed the frame size (1514) [7] and finally 4 bytes CRC.

C. Block diagram implementation

With purpose encrypting packet Layer 2, the proposed block diagram is described in Fig 3.

Function blocks are defined:

Block GetPkt-TransPkt: Capture and transmit Ethernet data packets from hardware directly, without using software, operating systems.

Block SelectIP: Distinguishing received packet is IP-data packet or signaling packet of network.

Block InsertIV: Insert the 16 bytes IV for cryptography algorithms.

Block LongPkt: processing packet block determines the packet need to split into two packets.

At the same time, this package has the task of adding 4 signaling bytes (32 bits) at the beginning of the packet.

TABLE 1. STRUCTURE OF DATA FRAME

MAC1	MAC 2	Type	Signaling	IV	Encrypted data	CRC
6 byte	6 byte	2 byte	4 byte	16 byte	0-1468	4 byte

TABLE 2. STRUCTURE OF SIGNALING DATA

Bit number	**Signaling**	**value**	**meaning**
0	Inform the separation of the large package	0/1	Non-separation package / Separation Package
1	Report the order in the separated large packet	0/1	First Package / 2nd Package
2-7	Signaling encryption parameters		Using in the cipher
8-18	Package size		
19-29	Package index		
30-31	Not used		

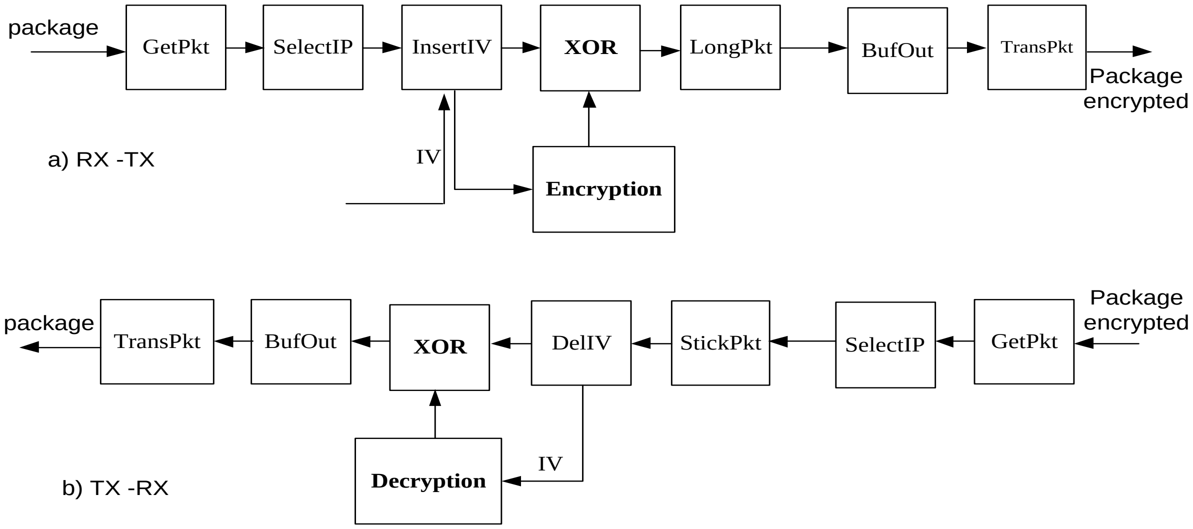

Fig 3. Block diagram implementing the proposed solution

Keystream generation block: Perform encryption IV with the key with the specified block cipher algorithm to generate the keystream for packet encryption.

Encryption block: perform XOR data with the key generated from the keystream generation block.

Block DelIV: In contrast to the block InsertIV, separate IV from the packet and feed to the keystream generation block.

Block StickPkt: In contrast to the block LongPkt, perform joining packet if necessary.

Block BufOut: Select IP packet and ARP synthetic to communicate with block TransPkt.

With the function of the blocks defined above, the operation of model is: When the packet arrives, it'll be read and written to the FPGA directly, with the aim of only encrypting data packets (IP packets) without encrypting signaling packets (ARP packets), the device will check whether the packet is an IP packet - that needs to be encrypted or not, if not it’ll be directly taken to the BufOut block to transmit. If it’s an IP packet, perform steps to insert IV simultaneously with this process is the process of generating keystream with packet IV; encryption (XOR) with the generated keystream; after that it’ll then handle large packets in order to meet the maximum size requirement of the packet, feed to the block BufOut to transmit on the transmission line. In the receiving, when there’s an encrypted packet, the process is reversed.

III. IMPLEMENTING ON THE FPGA WITH KIT DE4

With Altera's FPGA, directly reading and writing the packet from hardware (section 2.1) is integrated into the TSE (Triple-Speed Ethernet) core [8]. Thus, blocks GetPkt-TransPkt are used by 02 core TSE.

Implementing the proposed solution in the part 2 on KIT DE4 [9] according to the diagram of Fig 4.

In this model:

- 2 computers/end to end: perform data transfer function with 1Gbps (RJ-45) copper cable interface.
- 2 KIT DE4 of Altera: perform all functions shown in Figure 4 to secure packets on Layer 2.
- Block USER LOGIC: including blocks SelectIP, InsertIV / DelIV, LongPkt / StickPkt, generation keystream, Encryption/Decryption and BufOut in Fig 3.

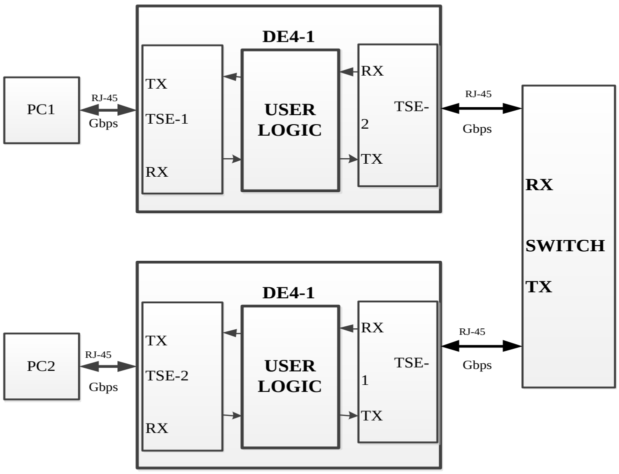

Fig 4. Model implemented on KIT DE4

With block diagram as shown in Figure 3 and deployment model in Altera's FPGA on DE4 KIT as shown in Figure 4, when not interested in the algorithm of generating keystream and encryption, implementation structure USER LOGIC on DE4 is shown in Fig 5.

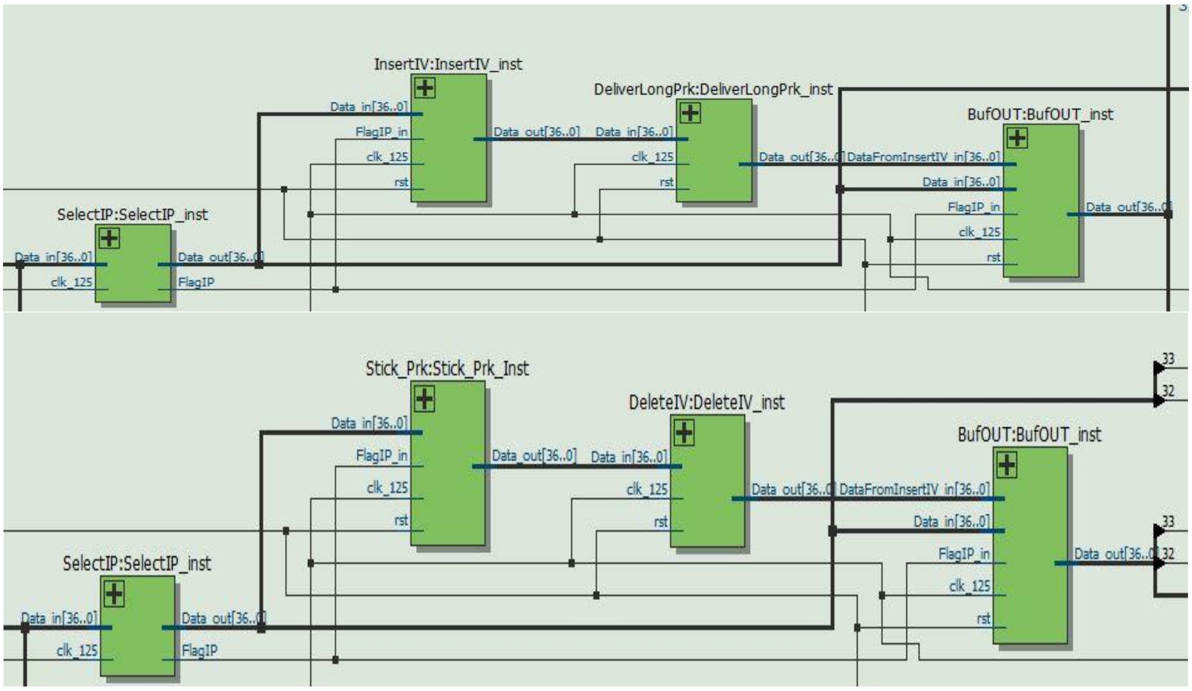

Fig 5. Deploy USER LOGIC on DE4 KIT

Block SelectIP performs the function of distinguishing IP packets and other signaling packets, input data is Data_in 37 bit (32 bits low are packet data, 5 bits high are ST_AVALON signals of TSE block), output is Data_out 37 bit and FlagIP. If the packet is an IP packet, the FlagIP signal will receive the output value of this block transferring to the block InsertIV, and vice versa receive the output value is 0 transferring to the block BufOUT.

Block InsertIV performs adding 16 bytes IV into the IP packet. This block will be designed a RAM memory to store IP packets (FlagIP = 1) and 1 FIFO to write the size of the packet. After being processed in this block the packet will be transferred to the block LongPkt, at that time the packet size will be changed after adding data IV. There is a case that the size excess the allowable packet size of 1518 Bytes on Layer 2.

Block LongPkt performs packet splitting if it exceeds the maximum size, in this block also have a RAM memory and a FIFO as block InsertIV, this block add 4 Bytes signal after Type and before data IV is added from block InsertIV. The packet after passing this block will be transferred to the block BufOUT.

Block BufOUT will perform packet selection from block SelectIP and block LongPkt. The packet from block BufOUT will be sent by the core TSE and transmitted to the Switch to send to the second DE4.

In the opposite direction, block SelectIP and block BufOUT are designed and have same function as the direction RX to TX. The only difference is blocks Stick_Prk and Delete_IV. Block Stick_Prk performs joining of packets that have been split at the 1st DE4. Block structure is also designed similarly to the packet splitting block. Block Delete_IV will receive data from block Stick_Prk, which will perform splitting data IV that was added to perform decrypting. The packet after passing this block will return as the packet before going into the block InsertIV.

IV. RESULT IMPLEMENTATION

With the implementation and test model as shown in Figure 4, the proposed Layer 2 packet security solution allows integration of encryption into the system with following test results.:

With network analyzer Berkut:

- When the physical transmission rate is less than 95%: the packet transmission rate is high speed (approximately 900 Mbps) and there is no loss of packet, working smoothly.

- When the physical transmission rate is greater than or equal to 95%: With large packets, errors occurring at TSE-2 continuously: receiving full packets but not fully transmit.

The terminal is 02 computers with 1Gbps network connection:

- Use multiple ping commands: Get full, accurate even with maximum packets (1514 bytes).

- Copying files between two machines: The speed gradually increases when reaching 80 Mbyte (650 Mbps), then the packet retransmission starts. Average speed of 30 Mbyte.

Comment:

The above result is consistent with practice and theory because with the above solution, each packet has been added 20 bytes. With packets of 512 bytes size, the real data is 512 + 20 = 532 bytes. Thus, the working efficiency of the channel is 532/512 = 104%, exceeding the permissible capacity of 1 Gbps channel and exceeding the TSE core capability integrated in DE4. When the input bandwidth is 900 Mbps, the system will work properly due to TSE requirements.

V. CONCLUSIONS

The proposed solution allows implementing of direct packet capturing, processing and forming of encrypted data frames to secure Ethernet Layer 2 packets, avoiding the risk of operating system security holes when using the Software solutions also it has a high performance bandwidth, 95% 1Gbps bandwidth (900 Mbps).

In order to integrate with encryption to make the most of the bandwidth available, it’s a matter of concern. Altera FPGA's data bus structure is 32 bits, the clock rate (clk) uses 125

MHz (0.008 µs) in theory to ensure that the data stream is directly encrypted per clock (0.008 µs) it's necessary to generate 32 bit keystream. With block cipher 64/128 bit, it takes 2/4 clk to perform encrypting 1 block or encrypting speed of 4 Gbps. This is a speed almost impossible to achieve with a block cipher. Therefore, the problem of organising encryption to exploit the most bandwidth is the next research direction and the problem will be studied in the near future.

REFERENCES

[1]. Rohde & Schwarz (2009), "R&S SIT ETH Ethernet Encrypto", data manual.

[2]. IEEE 802.1ae, IEEE Standard for Local and metropolitan area networks, "Media Access Control Security", 2006.

[3]. S. Kent, "IP Encapsulating Security Payload (ESP"), RFC 4303, 2005.

[4]. Đề tài "Nghiên cứu thiết kế chế tạo thiết bị bảo mật gói IP tốc độ cao (IP14) trên công nghệ FPGA và ARM". Ban Cơ yếu Chính phủ, Dương Huy Bình và cộng sự, 2014.

[5]. Glen Gibb, John W. Lockwood, Jad Naous, Paul Hartke, and Nick McKeown "NetFPGA – An Open Platform for Teaching How to Build Gigabit-rate Network Switches and Routers", IEEE Transactions on Education, 2008.

[6]. John W. Lockwood, Nick McKeown, "NetFPGA - An Open Platform for Gigabit-rate Network Switching and Routing" IEEE Internationnal Conference on Microelectronic System Education", June 3-4, San Diego,CA, 2007.

[7]. IEEE 802.3 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks; "Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 1: Media Access Control (MAC) Parameters, Physical Layers, and Management Parameters for 1 Gb/s Operation", 2002.

[8]. Altera Corp, "Triple-Speed Ethernet MegaCore Function User Guide – Altera" https://www.altera.com/literature/ug/ug_ethernet.pdf, 2016.

[9]. Altera Corp, "DE4 User manual". ftp://ftp.altera.com/up/pub/Altera_Material/Boards/DE4/DE4_User_Manual.pdf unpublished, 2016.

ABOUT THE AUTHOR

Ms. Ky Phan Van

Workplace: Institute of Cryptography Science and Technology.

Email: pvk.hvktqs@gmail.com

The education process: has received master's degree in 2017.

Research today: integrated circuit technology, FPGA.

Ms. Thang Tran Van

Workplace: Institute of Cryptography Science and Technology

Email: vanthang.qsbk@gmail.com

The education process: has received master's degree in 2018.

Research today: integrated circuit technology, FPGA.

PhD. Phuc La Huu

Workplace: Institute of Cryptography Science and Technology

Email: phucpvkt@hotmail.com

The education process: has received master's degree in 2012 and PhD in 2015.

Specialization: Electronic engineering

Research today: Designing and producing security device, specialized cipher machine.