2012 International Conference on Software and Computer Applications (ICSCA 2012)
IPCSIT vol. 41 (2012) © (2012) IACSIT Press, Singapore

An Implementation of the IEEE 1588 MAC with a Packet Identification Encryption

Chi-Chun Chen [1 +], San-Fu Wang [2], Lung-Chih Kuo [1], Suan-Yuan Lai [1] Chang-Hsien Chen [1] and Hsiao-Hui Lee [1]

[1] Cloud Service Technology Center, Industrial Technology Research Institute, Taiwan
[2] Department of Electronic Engineering, Ming Chi University of Technology, Taiwan

Abstract. A packet encryption architecture embedded in MAC is proposed due to that the IEEE 1588 messages employed for synchronizing time with each other is of vital importance, especially the security-aspect applications. For instance, an industry demands a terminal host to provide a precise time to control these automatic machines to order the schedule of the mass production. The malicious attacks will break these systems down and cause many injurious results. The proposed MAC Core module is responsible for transmitting the IEEE 1588 packets from the upper layer software through the network driver and receiving the IEEE 1588 packets from Network via the media independent interface (MII). The IEEE 1588 Clock Servo module provides the hardware clock sources and adjusts the local time to synchronize with the master's time and manages the updated time from the software. Thus, the presented IEEE 1588 packet encryption method embedded in MAC layer can efficiently prevent the synchronization information from the hacker's attacks. The proposed scheme is better than the traditional encryption machine of the application layer, which passes through many protocol stacks caused path delay to increase the network jitters. The proposed scheme not only reduces efficiently the latency variables of the timestamp but also lowers the loading of the CPU processor resources.

Keywords: IEEE 1588, synchronization, encryption

1. Introduction

The IEEE 1588 standard is being a popular precision clock synchronization protocol for the many applications on the network [1]. The synchronized application is an important trend not only in the aspect of the test and measurement area but also in the telecommunication industry, where the standard networks like Ethernet are used to connect these measurement devices [2]. Especially, as the IEEE 1588 synchronization system is applied in the open environment, the malicious attacks will break these systems down and cause many injurious damage.

The common security properties of the master-slave based clock synchronization algorithm are investigated [3] [4], including an analysis of security vulnerabilities. In this paper, the overview of vulnerabilities of clock synchronization protocols is presented. It also shows that even if clock synchronization is used in private networks and not as a commercial middleware service, the dangers cannot be neglected. The attacked synchronization information of the clocks might break the synchronous system down to cause the scheduled activities of the system disorderly. For example, since the IEEE 1588 operates in a master-slave hierarchy, the master node of the industry schedules the functions of the equipments of the production line via the intranet network. As the hacker attacks into the intranet network of the industry, the hacker node might break the system down with one kind of the two main behaviors generally. One is to alter the timestamp information of the IEEE 1588 packets sent by the master node. The other is that the hacker

+ Corresponding author. Tel.: + 886-6-3847108; fax: + 886-6-3847182.
E-mail address: chichun@itri.org.tw.

node will acts as a master node and sends the IEEE 1588 messages to all the nodes in the synchronization system. It could produce a disorder production line to make the mass product failure or the damage of the database, etc. The issues of the security are more critical as the clock synchronization system employed IEEE 1588 standard protocol used in a public network environment. Even in a private network, such as companies or industries, the hacker's attacks will cause more property loss.

2. The Common Encryption Technology of the IEEE 1588-based Network

With the Internet and the Industry Network grows rapidly, the Network security becomes the vital issue and the relative solutions are very popular. Among these solutions, a common method is to add the additional encryption machine in the software of the application layer or the transmit layer or the IP layer [5], etc. To protect the transmitted messages, symmetric as well as asymmetric cryptographic algorithms can be used. The main difference for operation is the overhead introduced by the additional data and the progress for message protection [6]. Commonly, in order to reduce the time spent by the encryption, the symmetric cryptographic algorithm is employed, for example, DES or Triple-DES, etc. Figure 1 shows the common methodology of implementing the software program to prevent the communication data from the hacker's attacks. The precise time protocol (PTP) program in the application layer is responsible for encapsulating the IEEE 1588 packet and the synchronized progress, the packet format is also shown in the figure 1. The context of the SPTP-H field contains the information of the IEEE 1588 packet is encrypted or not, the length of the encrypted PTP message and the length of the filling sample, etc. The PTP-M field contains the encrypted synchronization data and the P field is the filling sample bits. The filling sample bits will fill the packet to be a suitable length. And among the three fields, the PTP-M field and the P field are encrypted. The header of the Secure PTP (SPTP-H) is inserted between the UDP header (UDP-H) and the encrypted PTP massage. This field is the header of the IEEE 1588 packet. The transmit layer can decide the corresponding special port to call the dedicated program to encrypt or decrypt the packet as the packet is achieved at the layer.

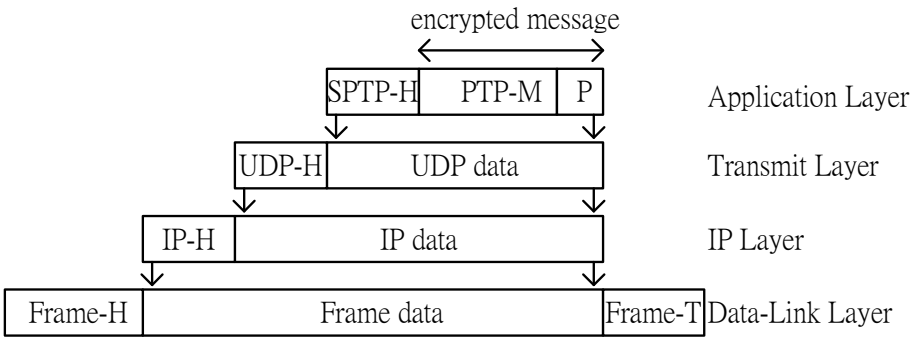

Fig. 1: The common technology of the software encryption

With the key generated by the Pseudo-Random Number, the program can encrypt the IEEE 1588 timestamp information and packet it out through the UDP/IP protocol. However, the encrypted IEEE 1588 packet should transmit through the long path formed by the protocol stacks. As these protocol stacks encapsulate the IEEE 1588 message simultaneously, these progress also increase the delay time and the various latency in the node before transmitting to the network. It is hard to estimate correctly the time that the progress spent so that the slave node can not synchronize its clock with the master accurately. Therefore, some studies suggested to use MACsec to secure the IEEE 1588 protocol [7] [8].

Besides, the software realizes the common data protection at any time as long as there is a packet would like to be transmitted out or a packet is received from the Network. The CPU must be interrupted to run the encryption or the decryption machines driven by the software program according to the interrupt priority. It would cost the extra CPU processing time to do these functions. The worst case is that some tasks own the higher priority and they will interrupt the CPU access to occupy the resources of the CPU for dealing with mass of data. These packets must wait to encrypt. In a PTP system, the internal latency of the inbound and outbound will increase seriously with an inestimable value. The internal latency of the packet also influences the degree of the accuracy of the clock synchronization [9].

3. The Proposed Packet Encryption Architecture Imbedded In MAC

The proposed packet encryption architecture embedded in MAC is shown in Figure 2. The 32-bit microprocessor via the internal bus controls the function of the MAC hardware. In the architecture, the MAC Core composed of the receiver module and the transmitter module is responsible for transmitting the IEEE 1588 packets from the software driver of the upper layer and receiving the IEEE 1588 packets from Network via the Media Independent Interface (MII/GMII). The IEEE 1588 Clock Servo module provides the clock sources of the MAC hardware and adjusts the local time of the node to synchronize with the master's time and sums the offset time calculated by the PTPd software into the timing counter of the Clock Servo. The Packet Detector module is responsible for detecting the IEEE 1588 messages and distinguishes them into event message and general message. As the event message is detected, the Packet Detector sends a pulse to the Time Stamp module and the Clock Servo module records the timestamp. By the comparison of the PPS, the relative jitters between the master clock and the slave clock can be measured. There is a 64-deep circular buffer in the Clock Servo module to store the packet key information including the subdomain, sourceUuid, sourcePortId, sequenceId, and timestamp information, etc. The IEEE 1588 Packet Encryption / Decryption module is to decrypt and encrypt the IEEE 1588 packets.

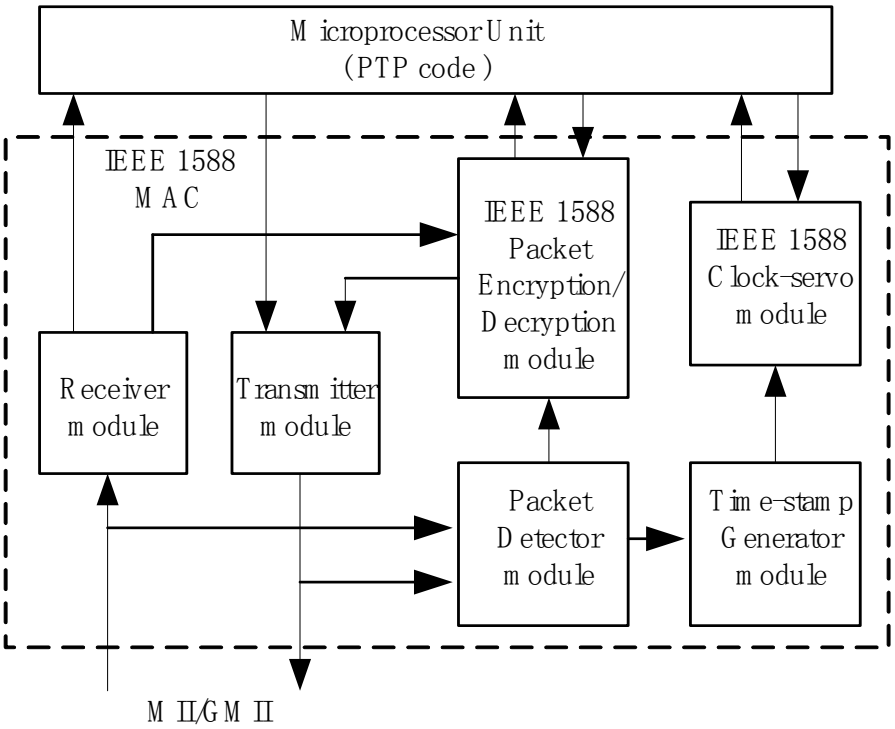

Fig. 2: The presented packet encryption architecture imbedded in MAC

The presented Packet Encryption / Decryption module initially keeps in the idle state until the IEEE 1588 message is detected. To encrypt the IEEE 1588 messages and shorten the operation time, a symmetric cryptographic algorithm is used with an authenticated key. There are two main pathway operations; one is the MAC hardware checks out the received the IEEE 1588 messages, the packet will be sent to decrypt. The decrypted message with its timestamp in the Clock Servo module will be read by the CPU to do the calculation of the time synchronization. The other pathway is the upper layer software assigns the MAC hardware to send the IEEE 1588 messages. The encryption function will be executed to encrypt the packet. The timestamp information is read out from the Clock Servo for the sent messages will be encrypted, too. The precise timestamp in cipher will be sent out by the Follow-Up message after the Sync message as the node is the master node.

4. Conclusion

The proposed IEEE 1588 packet encryption scheme can eliminate the latencies induced by internet protocol stacks. It lowers the loading of the micro-processor unit and also speeds up the encryption and decryption operations simultaneously. The proposed IEEE 1588 packet encryption scheme presents the IEEE

1588 packet encryption of each node supporting the IEEE 1588 standard. The hardware implementation of packet encryption embedded in a node also reduces the delay and latency induced by internet protocol stacks. Implementing the encryption and decryption of the IEEE 1588 packets in the MAC layer can lower the loading of the CPU and speed up the access time. The proposed scheme can also be rapidly synchronize the clock of the new slave node to the master clock and decides the new master node when the original master node is removed from the current synchronized system.

5. References

[1] J. C. Edison. *Measurement, Control, and Communication Using IEEE 1588.* Springer-Verlag, 2006.

[2] J. C. Edison. The Application of IEEE 1588 to Test and Measurement Systems. *Whitepaper 1, Agilent Technologies.* 2005, pp. 9–13.

[3] G. Gaderer, A. Treytl and T. Sauter. Security Aspects for IEEE 1588 based Clock Synchronization Protocols. *IEEE-1588 Conference.* 2006, pp. 247-250.

[4] A. Treytl and B. Hirschler. Security Flaws and Workarounds for IEEE 1588 (Transparent) Clocks. *in Proceedings of 2007 International Symposium for Precision Clock Synchronization for Measurement, Control and Communication (ISPCS).* 2009, pp. 1-6.

[5] S. Kent and K. Seo. Security Architecture for the Internet Protocol. *IETF, RFC 4301.* 2005.

[6] A. Treytl and T. Sauter. Security Concept for a Wide-Area Low-Bandwidth Power-Line Communication System. *in 2005 International Symposium on Power Line Communications and Its Applications*. 2005, pp. 66–70.

[7] A. Treytl, G. Gaderer, B. Hirschler and R. Cohen. Traps and Pitfalls in Secure Clock Synchronization. *in Proceedings of 2007 International Symposium for Precision Clock Synchronization for Measurement, Control and Communication (ISPCS).* 2007, pp. 18-24.

[8] IEEE 802.1X-2010. *IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control.*2010.

[9] IEEE Std 1588-2008. *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.* 2008..