JOURNAL OF SCIENCE
SAKARYA UNIVERSITY

Sakarya University Journal of Science

ISSN 1301-4048 | e-ISSN 2147-835X | Period Bimonthly | Founded: 1997 | Publisher Sakarya University | http://www.saujs.sakarya.edu.tr/

Title: Encrypted Data Transmission Model For Ethernet LANs

Authors: Cemal Koçak, Murat Durak
Recieved: 2019-01-02 00:00:00

Accepted: 2019-02-14 00:00:00

Article Type: Research Article
Volume: 23
Issue: 4
Month: August
Year: 2019
Pages: 641-649

How to cite
Cemal Koçak, Murat Durak; (2019), Encrypted Data Transmission Model For Ethernet LANs. Sakarya University Journal of Science, 23(4), 641-649, DOI: 10.16984/saufenbilder.506554
Access link
http://www.saujs.sakarya.edu.tr/issue/43328/506554

Sakarya University Journal of Science 23(4), 641-649, 2019

Encrypted Data Transmission Model For Ethernet LANs

Cemal KOÇAK*[1], Murat DURAK[2]

Abstract

Despite many research and development efforts in the field of data communication security, the security of the local area network (LAN's) is still not fully resolved. In this work, we proposed a model of encryption of the data field in the Ethernet frame to create secure Ethernet LANs. In this model, the data field in the Ethernet frame is encrypted and sent to the destination. The 1500-byte data field, defined as the standard for the Ethernet frame, is divided into 1497 bytes as the field used for the data. The remaining 2-bytes are defined as Message Body Length (MBL) and 1-byte as Message Number (MN). The message number is used to verify the encrypted data and the MBL is used for the length of the message. The proposed model provides secure data communication over Ethernet local area networks. Even if attackers obtain the packet at the time of communication, the encrypted message is difficult to decipher.

Keywords: ethernet networks, ethernet frame, encrypted data transmission, winpcap

1. INTRODUCTION

In recent decades, the progress of communication standards in physical environments (such as fiber optics) has made possible the demand for ever-increasing data traffic in broadband networks. In line with this situation, internet Protocol traffic is estimated to reach 15.3 Zettabytes per year by 2020 [1]. Ethernet offers infrastructure for the internet used around the world which is taken for granted by all users [2]. It is used from 1 Mb/s to 100 Gb/s for selected operating speeds with the common use of Ethernet local area network, media access control (MAC) and management information base (MIB) [3]. The IEEE 802 standards family is defined for the Local Area Networks (LANs) associated with the Physical and Data Link Layers specified by the ISO Open System Interconnection Reference Model (ISO / OSI) [4]. Different Physical Layer standards have been defined as 802.3, 802.4 and 802.5 [5-7] and Data Link Layer Standard 802.2 [8]. Although Ethernet was developed for shared connection communication, it is not to be enough the security feature. When Ethernet LANs are included in the Internet, they are open environments for attackers to eavesdrop and so the threat dimension is increasing [9]. To provide these kind of threats, Standardized Media Access Control security

* Corresponding Author: ccckocak@gazi.edu.tr
[1] Gazi University, Department of Computer Engineering, Ankara, Turkey. ORCID: 0000-0002-8902-0934
[2] Gazi University, Department of Computer Engineering, Ankara, Turkey. ORCID: 0000-0002-9611-9588

(MACsec.) provides segment-based security. The connection-restricted feature is basically built for scalability, key agreement simplicity and traffic analysis. However, unsupported multi-part reliability and integrity make MACsec. vulnerable [10].

In the study on the safety of Ethernet LANs [11], requirements were emphasized and to meet them, each node can only read packets addressed to it, verify the source of the data and accept the addressed package once. In another work [12], authors proposed a security hardware device model between the node and the network environment independent of the software to secure the Ethernet LANs. Thanks to this device model, the check of the delivery of the data to the destination node was provided. In another work [13], 1000Base-X Ethernet, physical layer encryption method was proposed and developed. The proposed encryption scheme uses a chaotic streaming cipher to encrypt the 8b10b symbol stream at the PCs (Physical Coding Sublayer) level. The study was implemented in an FPGA (Field Programmable Gate Array) and the experimental results suggested that the encryption of the Ethernet data traffic is possible and it can be hidden from the malicious observer.

It is very important to ensure the security of data since the data is carried in numerical form in the network environment. However, despite the conducted research and development work, a clear solution to ensure data security has not been found yet. Most of the current research have focused on developing cryptographic solutions to perceived problems [14-18]. Bayilmis and his friends in their work, using chaotic systems to meet the security needs of the WSN has performed a chaotic encryption system. The chaotic system developed in this study and the commonly used Skipjack encryption were used [19]. In another similar article, chaotic-based encryption was used in the IEEE 802.15.4 standard to secure communication [20].

In this work, it is aimed to transmit the data to the targeted MAC address securely using the Ethernet frame. An encryption model of the data field in an Ethernet frame was suggested to establish secure information communication on Ethernet LANs. In addition, the MBL and MN fields were created to validate the destination in the data section of the Ethernet frame.

2. ETHERNET TECHNOLOGY

Ethernet is a standard communication protocol used to connect devices such as switches, routers, and computers in wired or wireless networks. It was developed by PARC at the end of 1970 [21, 22]. From this date on, it has undergone constant development and change. Today, Ethernet performs data communication at approximately 3 Mbps to 100 Gbps, and Terabit Ethernet (TbE) is used for higher speeds. Due to Ethernet's cheap structure and simplicity, the token that is included in LANs has come to the forefront in terms of ring and high speed Fiber Distributed Data Interface (FDDI) technologies [5-8].

Preamble	SFD	Destination MAC Address	Source MAC Address	Type	Data	FCS
7	1	6	6	2	46-1500	4

Figure 1. Ethernet Frame Formats (field length are in bytes)

Ethernet frames are created with at least 60 bytes, and at most 1514 bytes. The reason for this is the data field included in the frame. An Ethernet frame specifies the first 6-byte destination MAC address (Destination MAC Address - DA), and the second 6 bytes specifies the source MAC address (SA). The next 2-byte portion is known as the protocol structure (Ethertype) of the frame. In the last part, there are data fields between 46 bytes and 1500 bytes in length [4]. The framing used for Ethernet was shown in Figure 1 [23].

2.1. Threats to Ethernet

There are weaknesses due to the Ethernet broadcast system. That is, every node that is included in the Ethernet receives messages sent by another node. This situation can lead to eavesdrop in the Ethernet environment easily. This network eavesdropping can be done either within or outside the network. Therefore, the communication information between the two end nodes can be obtained. A disadvantage of the

Ethernet is that it is vulnerable to attacks and viruses. With the Ethernet becoming a widely used technology, the efforts to prevent unauthorized access to the Ethernet environment have become an important issue. The most secure network environment is a network environment that is not connected to other networks. However, this does not give a good result, because it eliminates the advantage of the Ethernet usage, which is easy access to the internet. A safe environment can be created in terms of physical security as an effective security measure that is closed inside and outside unauthorized access. For example, switches and cable cabinets can be collected in a locked cabinet and protected against interference by unauthorized persons [24-26].

One of the security measures to be taken against the attacker's method in the Ethernet environment is based on routing and switching. This method can be applied by making the necessary configuration in switches and routers to route specific workstations to a destination. This application includes port security, password application and filtered access control list. One way to secure the Ethernet environment is to create Virtual LANs. With this method, access from the virtual network environment named 'A' to the virtual network environment named 'B' can be prevented [27, 28]. Firewalls too, are devices used on the network to provide security against unauthorized access. These devices control which units outside the network can or cannot be accessed. It works more detailed than according to the access control list [29, 30].

Another solution to security measures is encryption method that can be taken against attackers in the Ethernet environment. The encryption method meets the need for data integrity and privacy. The basic logic in cryptography is to convert a data block to a different data block. Encryption makes it difficult to read content against unauthorized eavesdrop. Encryption methods themselves are divided into 4 categories as Symmetric Encryption Algorithms, Data Encryption Standard, Advanced Encryption Standard and Asymmetric Encryption Algorithms and are usually based on the use of a key [31-34].

3. ETHERNET TECHNOLOGY

It is very important to ensure the security of the data section of the Ethernet frame. In this study, a 1500-byte data field of the Ethernet frame is divided into three section as shown in Figure 2 to provide secure data communication. These sections are Message Body Length (MBL), Message Number (MN) and Data. The MBL (2 bytes) contains the information how many bytes of data is stored in the frame in reality. In the MN (1 bytes) section; on the other hand, contains the message number information for the transmitted data content. Finally, the data to be transmitted in the Data section (43-1497 bytes) is sent by adding it to the Ethernet frame [35].

If the MBL values of the frame is different from the incoming data length frame, it will be possible to detect that the frame has been attacked or changed. Moreover, the MN is used to maintain communication between the destination and the source because a specific message number is answered in response to a message number specified in the incoming frame. Thus, a verification in the destination is provided against the attack and a change of the data frame is sent to the destination. The only disadvantage here is that the total length of the data that can be sent is between 43 -1497 bytes since a total of 3 bytes of data is reserved for verification and communication continuity.

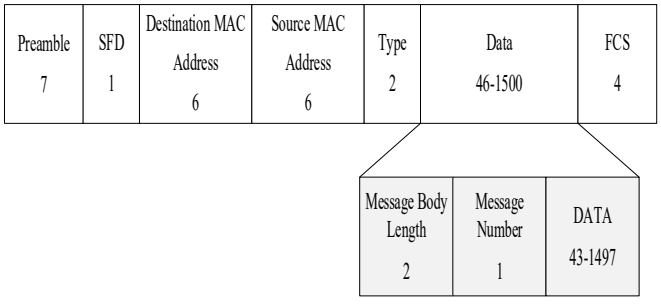

Figure 2. Changes in the data section of the Ethernet frame (field length are in bytes)

In addition, in this work, an encryption algorithm was applied independently for the security of the data to be sent. By considering the American Standard Code (ASCII) for the encryption algorithm, the conversion of each character (255

characters) to a different character was provided. This encryption algorithm has provided through a software. For example, the character corresponding to FF is encoded as 00 in the hexadecimal number system, the character corresponding to the FE is 01, and the character corresponding to FD is 02. In this way, each character was encrypted separately from FF to 00. That is, according to the ASCII table, the first character is encoded as the last character, and the last character is encoded as the first character. This encryption structure was shown in Table 1 [35].

Table 1. According to Hexadecimal Numbering System Encryption

ASCII Character	Converted Character
FF	00
FE	01
FD	02
..	..
..	..
..	..
01	FE
00	FF

The Message Body Length and Message Number fields are unencrypted. Because the attacker who gets the Ethernet frame is unaware of the 3-byte (MBL and MN) area there, the attacker will think that these fields are also data. The fields of MBL and MN are changed according to the messages. Thus, the understanding of the data by the attacker has been made much more difficult. Windows Packet Capture (Winpcap) Application Programming Interface (API) is used to provide communication between the Ethernet frame structure and the endpoints. The Winpcap API is used to obtain information about the network adapter, to view network stream and packet contents, to capture packets for desired protocols, and to create Ethernet frames. The purpose of using Winpcap in this article;

- Capture raw packets, both the ones destined to the machine where it's running and the ones exchanged by other hosts (on shared media). So in this study we are able to obtain all fields of the Ethernet framework (dest mac, src, ethernet type and data).
- Filter the packets according to user-specified rules before dispatching them to the application (For example, packets such as TCP-UDP are used in the network environment. However, in the study, only the Ethernet frames are detected according to the type of Ethernet we specify).
- Transmit raw packets to the network (We can pre-specify / create and send fields in the frame as desired.)

This work was done in the Windows operating system because the API can only be used by the Wireshark application in the Windows environment. The applications used in the data communication between the two end units was performed in an Ethernet network environment, including a switch. In addition, the interfaces that these units can use were developed with the Java programming language.

3.1. Source Node

For two-way data communication, the Source node was designed as a destination node. Thus, the response to the Ethernet frame sent by the source to the destination will also be visible on the source unit. The resource unit interface functions were provided with the help of the Winpcap API. This is done by running a Dynamic Link Library (DLL) in Visual Studio and the necessary functions were performed in the Eclipse environment with the Java Native Interface (JNI). The interface designed for the source unit was shown in Fig. 3. The desired adapter from the network adapters on the source node can be selected with the help of the Winpcap API, and the IP Helper API has been used to place the MAC address of this network adapter automatically in the Source MAC Address field of the interface [35].

On the "Outgoing Ethernet Type" combobox, the Ethernet type of the Ethernet frame to be sent must be selected. In the "Destination MAC

Address" combobox, the MAC address of the target node needs to be entered. In the "Message Numbers" combobox, the selection of the MN of the frame should be done (there are 12 MNs in this study). According to the selected MN, the data and MBL fields were filled automatically by the software. In the "Incoming Ethernet Type" combobox, eavesdropping the network by selecting the Ethernet type was provided to receive answers from the destination. The Ethernet frame created with the selected information will be sent to the MAC address specified with the "Send" button. In the "Sent and Received Messages" window, incoming and outgoing frame contents were displayed.

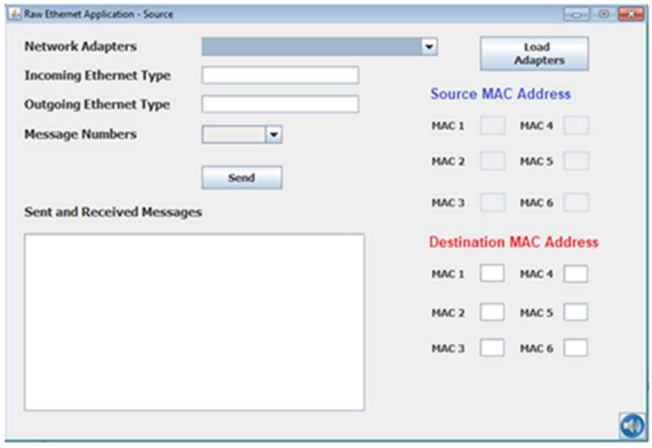

Figure 3. Interface created for the source node

If the "Outgoing Ethernet Type" information in the source node interface differs from the "Incoming Ethernet Type" information in the destination node interface, the destination node will not be able to show this frame information. The same is the case for the source node. In addition, the source node gives an audible warning for the incoming reply and the date and time information of the incoming frame are shown.

3.2. Destination Node

The interface designed for the destination unit was shown in Fig. 4. In this interface, the Destination MAC address is not entered by the user. If the Ethernet type in the incoming Ethernet frame is equal to the incoming Ethernet type specified by the user, the frame will be received. The MAC address from which the frame is sent will be displayed in the Destination MAC Address field in this interface [35].

The MN and Send combobox and button in the source node interface are not available in the destination node interface. Because in the developed application destination, the MN on the Ethernet frame can be seen, and known which MN is used to send an answer. The other difference is that you can always listen to the network environment with the Listen Network button.

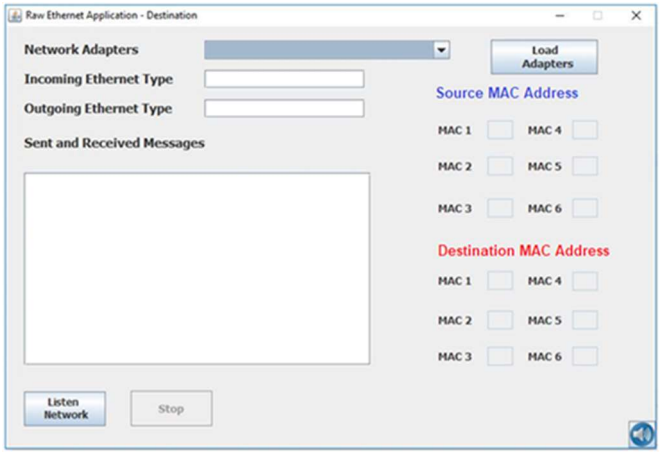

Figure 4. Interface created for the destination node

4. ANALYSIS OF THE DEVELOPED APPLICATION WITH WIRESHARK

A sample application for the source node was shown in Figure 5. Initially, the adapter is selected in the Network Adapters section, so the source MAC address is filled in automatically. Incoming Ethernet Type and Outgoing Ethernet Type entries are made by the sender. Then the MN is selected and the MAC address to which this message will be sent is entered in the Destination MAC address section. The created Ethernet frame is sent to the destination MAC address with Send in this way. Since a real-time communication is established here, the contents sent from the source

node and the destination node were shown in the Sent and Received Massages box section. The frame content sent from the destination node was shown in Fig. 6.

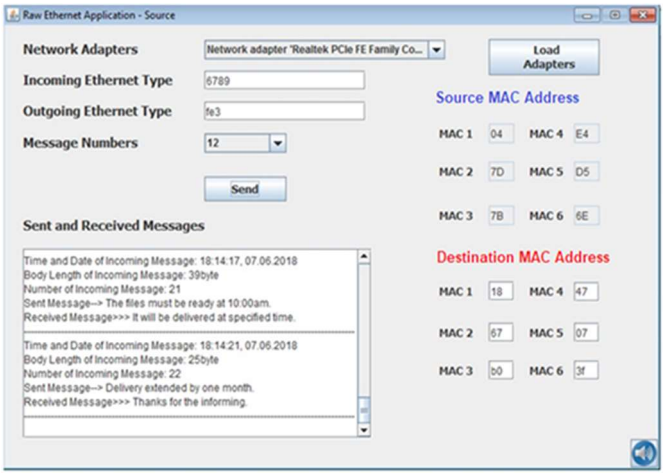

Fig. 5. Source node runtime

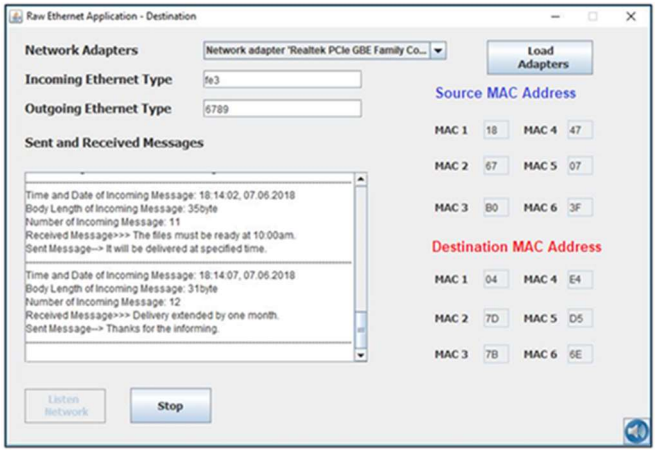

Fig. 6. Destination node runtime

In the Wireshark application, the Ethernet frame information sent from the source node to the destination node was shown in Fig. 7. The Frame 242 is the Ethernet frame to the incoming destination node (sent from the source node). Here, the protocol number "fe3" indicates the value selected as Incoming Ethernet Type by the destination node.

It is seen that the total number of incoming frames is 60 bytes and the data part is 46 bytes. However, Wireshark gives false information because of the design made at this point. Because of the arrangement in the data section of the Ethernet frame, the data portion is actually sent as 31 bytes (as shown in Fig. 5). The reason why it looks like 46 bytes in Wireshark is that the end of the frame is filled with 12 zeros and the 3-byte portion defined for the verification and communication continuity in this study is evaluated as data. In total, if these 15 bytes are appended to 31 bytes, the 46 bytes will be the result of the data portion.

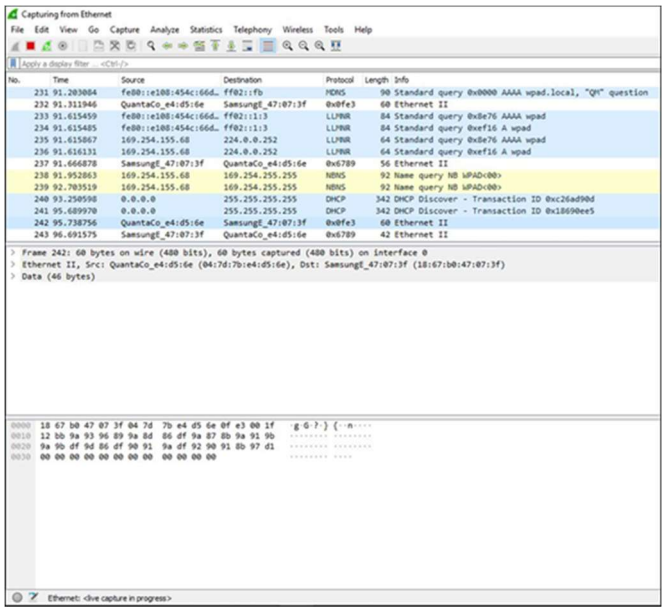

Fig. 7. The Ethernet frame content incoming to the destination node

In the of frame contents; the first 6 bytes (18, 67, b0, 47, 07, 3f) Destination MAC address, second 6 bytes (04, 7d, 7b, e4, d5, 6e) Source MAC address, then in turn; 2 bytes (0f, e3) Outgoing Ethernet type given by source node, and the last 2 bytes (00, 1f) is the Body Length of Incoming Message value. The hexadecimal "1f" value corresponds to "31" in decimal and it will give the value of 31 bytes (as shown in Fig. 6). The first byte in the next line of information indicates the value of MN is 12 selected. The next values represent the encrypted portion of the message "**Delivery extended by one month**"

corresponding to the message number 12. The number 44 is the hexadecimal response of the ASCII table of the first character "D" in the message. However, it was sent by encryption as "D" character "bb". Because the whole message is encrypted, the attacker will have no information about the content of the message. It will not be a problem in received and sent messages because decryption is performed on both nodes.

5. CONCLUSION

With Encryption of the data field in the Ethernet frame, secure information communication was provided on Ethernet LANs. For this, the 1500-byte data part in the Ethernet frame was divided into three different parts. With MBL and MN, validation and communication continuity at the destination node was provided and those sections were unencrypted. Only the data to be sent was encrypted and sent to the destination. Even if attackers who do not know the changes in the data field damage the data field, this will be understood in the target unit, and communication will preferably be terminated accordingly. There are 12 messages defined in this study. Since a section of 1 byte is reserved for the MN, up to 255 messages can be created in this work so that the defined fixed messages in the software can be sent and received.

For future work, the number of messages can be increased by increasing the MN size defined in the frame, and messages can be entered manually with a software to be developed. With the changes to be made, different verification and control areas can be added to the frame structure. For data fields, different encryption methods and algorithms can be developed.

6. REFERENCES

[1] A. Pérez-Resa, et al., “Using a Chaotic Cipher to Encrypt Ethernet Traffic,” In Circuits and Systems (ISCAS), 2018 IEEE International Symposium on, pp. 1-5, 2018.

[2] T. Kiravuo, et al., “A Survey of Ethernet LAN Security,” In IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1477-1491, 2013.

[3] IEEE Standard for Ethernet, IEEE Std., Rev. IEEE Std. 802.3-2015 (Revision of IEEE Std. 802.3-2012), Mar. 2016.

[4] J. Postel, J. Reynolds, “A Standard for the Transmission of IP Datagrams over IEEE 802 Networks,” RFC 1042, 1988.

[5] IEEE, "IEEE Standards for Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications," IEEE, New York, 1985.

[6] IEEE, "IEEE Standards for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification," IEEE, New York, 1985.

[7] IEEE, "IEEE Standards for Local Area Networks: Token Ring Access Method and Physical Layer Specifications," IEEE, New York, 1985.

[8] IEEE, "IEEE Standards for Local Area Networks: Logical Link Control", IEEE, New York, 1985.

[9] Cisco Systems, "Cisco Global Cloud Index: Forecast and Methodology 2015-2020," 2016.

[10] K. F. Wahid, “Rethinking the link security approach to manage large-scale Ethernet network,” In Local and Metropolitan Area Networks (LANMAN), 17th IEEE Workshop on, pp. 1-6, 2010.

[11] R. Khoussainov, A. Patel,” LAN security: problems and solutions for Ethernet networks,” Computer Standards & Interfaces, Vol. 22, no. 3, pp. 191-202, 2000.

[12] N. Hadjina, P. Thompson,” Data security on Ethernet LANs,” 10th Mediterranean Electrotechnical Conference. Information

Technology and Electrotechnology for the Mediterranean Countries Proceedings. MeleCon 2000 (Cat. No.00CH37099), Lemesos, vol.1, pp. 23-26, 2000.

[13] A. Pérez-Resa, et al., "Using a Chaotic Cipher to Encrypt Ethernet Traffic," In Circuits and Systems (ISCAS), 2018 IEEE International Symposium on, pp. 1-5, 2018.

[14] G. King, "A survey of commercially available secure LAN products," In Computer Security Applications Conference, Fifth Annual, pp. 239–247, 1989.

[15] R. Housley, "Encapsulation security protocol design for local area networks," In Local Area Network Security. Lecture Notes in Computer Science, T. Berson and T. Beth, Eds. Springer Berlin Heidelberg, vol. 396, ch. 10, pp. 103–109, 1989.

[16] F. Poon, M. Iqbal, "Design of a physical layer security mechanism for CSMA/CD networks," Communications, Speech and Vision, IEE Proceedings I, vol. 139, no. 1, pp. 103–112, 1992.

[17] M. Soriano, et al., "A particular solution to provide secure communications in an Ethernet environment," In CCS'93: Proc. 1st ACM conference on Computer and communications security, NY, USA: ACM Press, pp. 17–25, 1993.

[18] M. El-Hadidi, et al., "Implementation of a hybrid encryption scheme for Ethernet," In Computers and Communications, Proceedings. IEEE Symposium on. IEEE Comput. Soc. Press, pp. 150–156, 1995.

[19] C. Bayilmis, et al., "Enhanced secure data transfer for WSN using chaotic-based encryption," Tehnicki Vjesnik-Technical Gazette vol.24, no.4, pp. 1065-1070, 2017.

[20] C. Bayilmis, et al., "Employing Chaotic Encryption for IEEE 802.15. 4-based LR-WPANs." International Conference on Computer Science and Information Systems (ICSIS'2014), pp. 89-92, 2014.

[21] G. E. Pake, "Research at Xerox PARC: A Founder's Assessment," IEEE Spectrum, vol. 22, no. 10, pp. 54-61, 1985.

[22] R. M. Metcalfe, "Computer/network interface design: Lessons from Arpanet and Ethernet," IEEE Journal on Selected Areas in Communications, vol.11, no. 2, pp. 173-180, 1993.

[23] "802.3-2012 – IEEE Standard for Ethernet" (PDF). ieee.org. IEEE Standards Association. 2012-12-28.

[24] M. Khan, M. Ayyoob, "Computer Security in the Human Life," International Journal of Computer Science and Engineering (IJCSE), vol. 6, no. 1, pp. 35-42, 2017.

[25] A. Zúquete, et al., "Packet tagging system for enhanced traffic profiling," In Internet Multimedia Systems Architecture and Application (IMSAA), 2011 IEEE 5th International Conference on, pp. 1-6, 2011.

[26] L. Heberlein, et al., "A network security monitor," In Research in Security and Privacy, Proceedings, IEEE Computer Society Symposium on. IEEE, pp. 296-304, 1990.

[27] J. Akram et al., "Future and Techniques of Implementing Security in VLAN," Journal of Network Communications and Emerging Technologies (JNCET), vol. 7, no. 5, pp. 14-17, 2017.

[28] A. Mehdizadeha, et al., "Virtual Local Area Network (VLAN): Segmentation and Security," In The Third International Conference on Computing Technology and Information Management (ICCTIM2017), pp. 78-89, 2017.

[29] S. Lin, et al., "A design of the ethernet firewall based on FPGA," In Image and Signal Processing, Biomedical Engineering and Informatics (CISP-BMEI), 10th

International Congress on IEEE, pp. 1-5, 2017.

[30] S. Yonghong, et al., “Design of Security Gateway Based On Dual-Homed Architecture,” International Conference on Robots & Intelligent System, pp. 159-163, 2016.

[31] A. Pérez-Resa, et al., “Using a Chaotic Cipher to Encrypt Ethernet Traffic,” In Circuits and Systems (ISCAS), International Symposium on IEEE, pp. 1-5, 2018.

[32] A. Yin, S. Wang, “A novel encryption scheme based on timestamp in gigabit Ethernet passive optical network using AES-128,” Optik-International Journal for Light and Electron Optics, vol. 125, no. 3, pp. 1361-1365, 2014.

[33] D. Pawar, “Survey on network based cryptographic techniques for key generation and data Encryption/Decryption,” International Research Journal of Engineering and Technology (IRJET), vol. 4, no. 5, pp. 1361-1363, 2017.

[34] R. Karmakar, et al., “Enhancing security of logic encryption using embedded key generation unit,” In Test Conference in Asia (ITC-Asia), International IEEE, pp. 131-136, 2017.

[35] M. Durak, "Ethernet ağlarda güvenli veri iletişimi," Gazi University Faculty of Technology Computer Engineering graduation thesis, 2018.