International Journal of Cloud-Computing and Super-Computing
Vol. 6, No. 1 (2019), pp.9-14
http://dx.doi.org/10.21742/ijcs.2019.6.1.02

Virtual Secure Link over Software-Defined Bridged Networks

Ju-Ho Choi [1], Sung-Gi Min [2*], Pill-Won Park [3]

[1] Korea University,
[2,3] Dongguk University
[1]wizyoon@hycu.ac.kr ,[3] pillwon79@gmail.com, [2]sgmin@korea.ac.kr*

Abstract

Ethernet can transfer massive data stream flows as well as real-time flows supported by Time-Sensitive Network (TSN). The MAC layer security, MACsec, is defined at IEEE Std 802.1AE and IEEE Std 802.1X. However, a security association established by MACsec protects the communication among devices within single LAN at bridged networks. Therefore, a packet traversing several LANs must be decrypted and re-encrypted at each bridge. We propose a new virtual secure link over the Software-Defined Bridged Networks (SDBN). In SDBN, end-devices interact with the central MACsec module, running over the Software-Defined Network (SDN) controller, using the standard MACsec procedure. The central MACsec module recognizes a group of devices at the bridged networks regardless of their attached LANs. These devices are treated as they are attached to the same virtual link. The proposed scheme supports end-to-end unicast/multicast secure communication without any modification of the current MACsec standards as well as eliminating the security operation required at bridges in bridged networks.

Keywords: *MACsec; IEEE 802.1AE; IEEE 802.1X; Authentication and key management (AKM); Time-Sensitive Network (TSN); In-vehicle secure communication; Automotive Ethernet; Internet of Things (IoT)*

1. Introduction

Ethernet attracts attention as the next-generation network technology, as it can guarantee the high bandwidth and the transmission of time-sensitive data. Recently, automotive industry introduces automotive Ethernet [1]as their in-vehicle networking technology, and aerospace industry also uses Ethernet-based networking technology such as Avionics Full-Duplex Switched Ethernet (AFDX) to reduce networking cost within an airplane.

The original approach of Ethernet [2] has the advantages of simplicity and zero-configurability, but there are security vulnerabilities [3] such as intrusion and man-in-the-middle attacks. In order to solve these problem, IEEE Std 802.1AE [4] has been release for Local and Metropolitan Area Networks. Also, IEEE Std 802.1X introduces the authentication and key management (AKM) mechanism for IEEE Std 802.1AE. These MAC security standards are referred to as MACsec. It guarantees the confidentiality and integrity of all frames on an Ethernet link, but it has the limitation that its security scope is only valid on a single LAN.

In this paper, we propose a virtual secure link over Software-Defined Bridged Networks (SDBN) for end-to-end secure communication. The proposed scheme adopts the SDN concept

Article history:
Received (February 13, 2019), Review Result (April 7, 2019), Accepted (July 22, 2019)

Print ISSN: 2205-8567, eISSN: 2207-399X IJCS

so that the central MACsec module, running over the SDN controller, delegates the Authentication and Key Management (AKM) procedure of all bridges. In addition, the MACsec KaY module over the SDN controller installs a session key for the end devices. It also instructs the SDN controller to install forwarding rules at switches, which are used to connects end devices to establish connectivity. As a result, authenticated members of the group look like they are attached to a shared media LAN. We call the shared media LAN as the virtual secure link. By delegating some of the complex mutual authentication processes to the central SDN controller, it could expand the security scope of the Ethernet link. It enables more secure data transmission in IoT environments that transmit sensitive sensing data.

2. Related Work

IEEE Std 802.1AE [4], also referred to as Media Access Control Security (MACsec), is the IEEE MAC Security standard for secure communication between devices on Ethernet. The confidentiality and integrity of all traffic on the Ethernet link can be guaranteed by the MACsec. However, the MACsec cryptographically protects frames based on a hop-by-hop rather than an end-to-end basis. When a bridge receives an encrypted frame, it should decrypt the frame and re-encrypt the frame whenever it forwards this frame to another link

A Connectivity Association (CA) between MACsec devices within a LAN in bridged networks should be established to open bridge port at which it is connected. The CA is established via the mutual authentication protocol. IEEE Std 802.1X [5] defines the port-based authentication procedure for this purpose. IEEE Std 802.1X defines the MACsec Key Agreement (KaY) module, which establishes the Connectivity Association (CA) if the end-device is authentic. The KaY uses the MACsec Key Agreement (MKA) protocol [5] to communicate with each other.

3. Virtual Secure Link over Software Defined Bridged Network (SDBN)

A set of devices, which are attached at different LANs within bridged networks, are grouped in a virtual link in the proposed scheme.

3.1. End Device

End-devices refer to the devices which are able to be connected bridged networks. It includes a PAE module. The PAE consists of a supplant and a KaY. The supplicant performs IEEE 802.1X authentication for the device, and the KaY performs the MACsec key management (AKM) procedure. The PAE module uses the EAPOL messages during IEEE 802.1X AKM procedure. A MAC Security Entity (SecY) is installed at the MAC layer over Ethernet. The SecY performs the security operation defined at IEEE 802.1AE.

3.2. Openflow-enabled switches

The proposed scheme assumes that bridges used at bridged networks are Openflow-enabled switches. Openflow-enabled switches forwards EAPOL messages between the attaching end-device and the SDN controller, but blocks data packets from an end-device until the device is authenticated by the MACsec PAE over the SDN controller. Forwarding rules are installed by the SDN controller on behalf of the MACsec PAE when connectivity among members of a predefined device group is detected.

3.3. MACsec PAE over the SDN Controller

The SDN controller [6][7] is able to run several control applications, and it may supply the network-related information such as the topology information of bridged network to its control applications. The SDN controller interacts with Openflow-enabled switches using the Openflow protocol. It installs forwarding rules into Openflow-enabled switches on behalf of control applications. We assume that the SDN controller uses the Link Layer Discovery Protocol (LLDP) [8] to discover the network topology and connectivity information between devices. For the MACsec authentication, the SDN controller should run the MACsec PAE, which consists of the IEEE 802.1X authenticator and the KaY. A policy database on the SDN controller stores the configurable authentication information. It also stores the predefined device group information. The predefined device group information describes which of the end-devices should communicate directly via virtual secure links. The MACsec PAE may establish a virtual link dynamically. For example, the MSRP module may notify the KaY for a new point-to-multipoint real-time multimedia stream. Then the KaY establishes a SA on a virtual link, at which the KaY, the "Talker", and "Listeners" are attached to the virtual link. As the number of Listeners can be changed during the lifetime of the stream, the KaY changes the group key whenever a Listener joins at the stream or leaves the stream.

4. The Proposed Authentication Procedure

IEEE 802.1X authentication procedure is performed when an end-device is attached to an OpenFlow switch. IEEE 802.1X authenticator at the MACsec PAE over the SDN controller determines whether the attached end-device is allowed to connect to bridged networks. The KaY on the MACsec PAE over the SDN controller periodically broadcasts an EAPOL-Announcement message. The EAPOL-Announcement message includes information such as access information, MACsec cipher suites, and Network Identifier (NID) of the Authentication Server (AS).

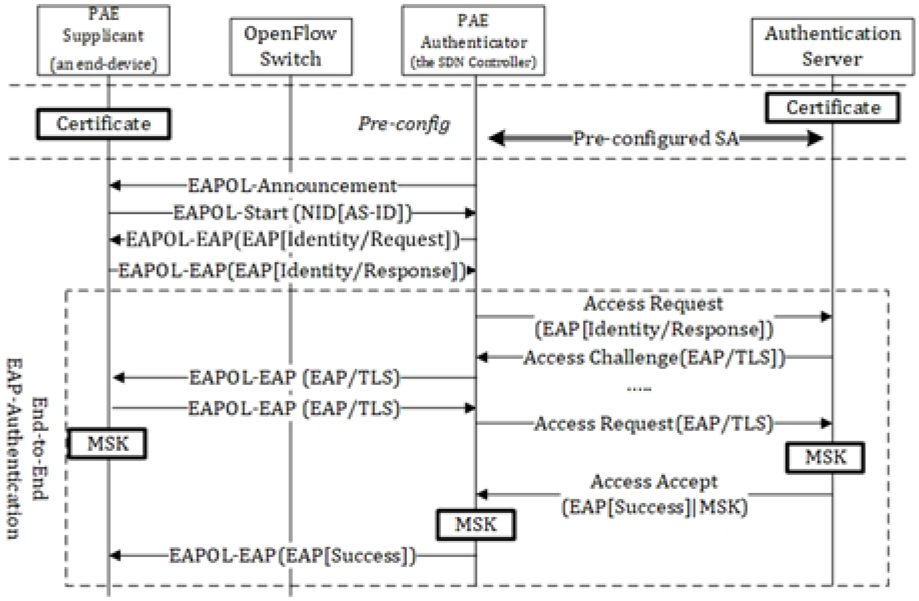
PAE Supplicant (an end-device)
OpenFlow Switch
PAE Authenticator (the SDN Controller)
Authentication Server
Certificate
Pre-config
Certificate
Pre-configured SA
EAPOL-Announcement
EAPOL-Start (NID[AS-ID])
EAPOL-EAP(EAP[Identity/Request])
EAPOL-EAP(EAP[Identity/Response])
Access Request (EAP[Identity/Response])
Access Challenge(EAP/TLS])
....
EAPOL-EAP (EAP/TLS)
EAPOL-EAP (EAP/TLS)
Access Request(EAP/TLS)
MSK
MSK
Access Accept (EAP[Success]|MSK)
MSK
EAPOL-EAP(EAP[Success])
End-to-End EAP-Authentication

Figure 1. The Proposed Authentication Procedure.

When an end-device receives the EAPOL-Announcement message, its PAE determines whether it can authenticate via the AS advertised in the EAPOL-Announcement message. If so, the supplicant of the PAE at the end-device initiates IEEE 802.1X AKM by sending the EAPOL-Start message to IEEE 802.1X authenticator at the MACsec PAE over the SDN controller. The supplicant, the authenticator, and the AS perform the authentication procedure described in IEEE 802.1X. If the authentication is successful, the supplicant and the authenticator have the Master Session Key (MSK). The supplicant and the authenticator notify their KaYs that the authentication is successful and supplies them the MSK. Figure 1 shows the proposed Authentication procedure.

5. The Proposed MACsec Key Management Procedure

After the end-device is successfully authenticated, they start MACsec key management procedure. The KaY at the MACsec PAE over the SDN controller interacts the KaY in the PAE at the end-devices. Each KaY derives the CAK from the MSK and then Integrity Check Value Key (ICK) and Key Encrypting Key (KEK) from the CAK. With the derived ICK and KEK, the Key server, the KaY over the SDN controller, establishes two unidirectional point-to-multipoint transmitting Secure Channels (SC). One for the attached device and the other for the Key server. The Key server derives the SAK for new SC and delivers it using EAPOL-MKA messages. The KaY over the SDN controller requests the information whether the newly authenticated device is belonging to any predefined device group and more than one device expects to attach to other authenticated devices. If so, the KaY establishes a SA for all authenticated devices of the group on the virtual link. It then installs the forwarding rules at switches required for connecting the member devices at bridged networks. The group SAK derivation follows the procedure described at IEEE Std 802.1X (section 6). Each KaY at an end-device receives the group SAK via an EAPOL-MKA message, then it installs the SAK in its SecY at the MAC layer on the interface. Figure 2 shows the MACsec key management procedure to establish a SA between two end-devices on a virtual link.

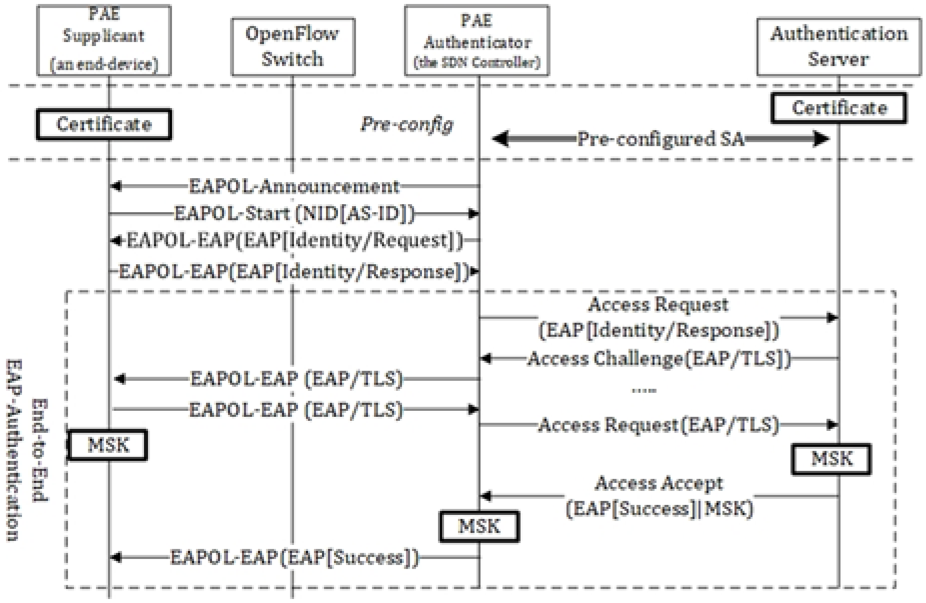

Figure 2. The Proposed MACsec Key Management Procedure.

6. Experiments

An experimental testbed is built to prove that the proposed scheme is applicable at the SDBN. The Open Network Operating System (ONOS) [9]is used as the SDN controller. Raspberry Pi 3 Model B boards are used as the Openflow-enabled switches. They run Open vSwitches (OVSs) implemented in Linux Operating system. The OVS interacts with the ONOS SDN controller with the OpenFlow protocol version 1.3.2 [10]. The ICMP ping packet is encrypted by the SAK at the end devices and the encrypted frame cannot be decrypted by any node except two end-devices. The receiving MACsec interface of end-device successfully decrypts the ping packet. Through the experimental results, we can confirm that the existing MACsec can be used for end-to-end secure communication.

7. Conclusions

The proposed virtual secure link over the Software-define bridged networks expands the security scope of the 802.1AE from hop-by-hop secure channel to end-to-end secure channel without any modification of the current standards (IEEE 802.1AE and IEEE 802.1X). We exploit the SDN concept which separates the user and control planes and provides the central control module on the SDN controller. As a result, the overall transmission delay of the frame could be decreased, and it could ensure more stringent end-to-end latency. The experimental results show that the proposed scheme is practical for end-to-end secure communication in bridged networks.

Acknowledgements

This research was supported by the Korean MSIT (Ministry of Science and ICT), under the National Program for Excellence in SW (2015-0-00936), supervised by the IITP (Institute of Information & communications Technology Planning & Evaluation)

References

[1] T. Steinbach, K. Muller, F. Korf, and R. Rollig. Demo: Real-time Ethernet in-car backbones: First insights into an automotive prototype. Vehicular Networking Conference (VNC), pp. 133-134 **(2014)** DOI: 10.1109/VNC.2014.7013331

[2] IEEE, IEEE Standard for Ethernet, in IEEE Std 802.3-2012 (Revision of IEEE Std 802.3-2008), IEEE: New York, 2012, NY, USA, pp. 1-634 **(2012)**

[3] T. Kiravuo, M. Sarela, and J. Manner. A Survey of Ethernet LAN Security. IEEE Communications Surveys and Tutorials 15, pp. 1477-1491 **(2013)**

[4] IEEE, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security. IEEE Std 802.1AE-2006, IEEE: New York, NY, USA, pp. 1−142 **(2006)**

[5] IEEE, IEEE Standard for Local and Metropolitan Area Networks: Port-based Network Access Control. IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004), IEEE: New York, NY, USA, pp. 1-222 **(2010)**

[6] P. Berde, M. Gerola, J. Hart, and Y. Higuchi. ONOS: Towards an open, distributed SDN OS. Proc. 3rd Workshop Hot Topics Software Defined Networking **(2014)** DOI: 10.1145/2620728.2620744

[7] J. Medved, R. Varga, and A. Tkacik. Opendaylight: Towards a Model-Driven SDN Controller Architecture. Proc. 15th IEEE WoWMoW, pp. 1–6 **(2014)** DOI: 10.1109/WoWMoM.2014.6918985

[8] IEEE, IEEE Standard for Local and metropolitan area networks - Station and Media Access Control Connectivity Discovery. 802.1AB-2016. IEEE: New York, NY, USA, pp. 1-146 **(2016)**

[9] D. Kreutz, Fernando M. V. Ramos, Paulo Esteves Veríssimo, Christian Esteve Rothenberg and Siamak Azodolmolky. Software-defined networking: A comprehensive survey. Proc. IEEE, vol. 103, no. 1, pp. 14–76 **(2015)**

[10] Open Networking Foundation. OpenFlow Switch. Specification 1.3.2 **(2013)**

Authors

Ju-Ho Choi

He received B.S. degrees in Computer Science from Korea University, Korea in 2014. He is currently working toward Ph.D. degree in Computer Science and Engineering at Korea University, Seoul, Korea. His interests in research include Future Internet, Vehicle Ad Hoc Network, mobility protocol design, and performance analysis.

Sung-Gi Min

He received his B.S. degree in Computer Science from Korea University, Seoul, Korea, in 1988. He received his M.S. and Ph.D. degrees in Computer Science from University of London in 1989 and 1993, respectively. From 1 January 1994 to 28 February 2000, he worked in LG Information and Communication Research Center, and from 2 March 2000 to 28 February 2001, he was a Professor in the Department of Computer Engineering at Dongeui University, Busan, Korea. Since 2 March 2001, he has been a Professor in the Department of Computer Science and Engineering at Korea University, Seoul, Korea. His research is focused to wired/wireless communication networks, especially heterogeneous network environment, and he is interested in mobility protocols such as MIP, SIP, and SCTP, network architectures, QoS, and mobility management in future network.

Pill-Won Park

He received his B.S. degree in Computer Science from Chungnam National University, Daejeon, Korea, in 2008. He received his M.S. and Ph.D. degrees in Computer Science from Korea University, Seoul, Korea in 2010 and 2017, respectively. His research is focused to wired/wireless communication networks, and he is interested in mobility protocols such as MIP, network architectures, QoS, and mobility management in future network.