Secure and Scalable IoT: An IoT Network Platform Based on Network Overlay and MAC Security

Junwon Lee, Heejo Lee

Secure and Scalable IoT: An IoT Network Platform Based on Network Overlay and MAC Security

Junwon Lee[0000−0003−2729−9113] and Heejo Lee

Korea University, Anam-dong, Seongbuk-gu, Seoul 136-713, South KOREA
{junimirang,heejo}@korea.ac.kr

Abstract. IoT, which is closely connected with our daily life, shows high growth in the automotive, healthcare, and retail fields. IoT security threats can cause severe problems in our lives. However, the security of the IoT network is insufficient to cope with security threats. Therefore, an attacker can use man-in-the-middle-attacks (MITM), DNS manipulation, and route tampering for eavesdropping, privacy breach, service outages and delay, power consumption, and system manipulation. Currently, VPN and data encryption is applied to protect the IoT network from these security threats. However, due to the limited resources of IoT device, the TCP/IP-based VPN and encryption are also limited. Although a lightweight IoT communication protocol such as LoWPAN is used, TCP/IP-based VPN such as IPsec, OpenVPN, and Wireguard require bandwidth, CPU/memory, and electric power at the level of general endpoint devices.
In this paper, we propose a secure and scalable IoT (SSI) network platform that can prevent security threats while minimizing use of computing resources of an IoT device. SSI, which has a lower load than TCP/IP-based VPN, is a layer 2 VPN and supply data link frame encryption. L2TP and VXLAN are provided for a scalable layer 2 VPN, and the MACsec algorithm encrypts layer 2 frames. SSI shows 30% network speed improvement and 31.6% CPU usage reduction compared to IoT network applied OpenVPN.

Keywords: IoT platform · Network overlay · Network separation · VXLAN · L2TP · MACsec.

1 Introduction

There are many types of IoT devices, including sensors, mobile devices, medical devices, wearable devices, home appliances, automotive and industrial devices. Gartner predicts that 1.9×10^9 IoT devices will be used for manufacturing and natural resources industries by 2028. Moreover, the IoT growth is very high in the automotive, healthcare, and retail fields [11]. IoT devices are required to connect to humans, other devices, and systems without environmental constraints through an IoT network. IoT architecture has evolved from a closed

and centralized network to a distributed cloud over the Internet. In the future, hyper-connectivity and Internet of Everything (IoE) [4], in which human, process, data, and things are interconnected, are expected to become the forms of IoT.

As IoT is widely expanded and closely connected to human life, IoT security threats will have an even more significant impact on privacy, health, reliability, and productivity. Considering these threats, we should approach IoT security with a different paradigm from endpoint security centered on end-user devices. OWASP has updated the IoT Top 10 threats for developers, manufactures, enterprises, and consumers. 5 IoT threats out of 10 threats (*"insecure network services", "insecure ecosystem interfaces", "insufficient privacy protection", "insecure data transfer and storage", and "lack of device management"*) are closely related to network security. In other words, we can effectively prevent many security threats by applying the secure IoT network platform [18].

In the former studies [8,13,20], we can find security threats related to the IoT network. Farris et al. describe the security threats (e.g., eavesdropping, denial of service, spoofing, MITM, routing attack, cloud service manipulation, privilege escalation, etc.) that can occur on IoT networks [8]. Minhaj et al. represent the end-to-end security and establishment/resumption of session in the network level security issues. In the IoT environment, which provides the same network to various devices, security threats can be propagated to other nearby devices due to the security hole of one device. Therefore, end-to-end protection for a device is essential [13]. Ryoo et al. reported that a security threat might arise when a home IoT device uses an insecure communication channel to interoperate with other devices. Also, it has shown that a user's conversation and video recordings may be revealed through weak communication channels, which may violate users' privacy [20]. In order to effectively respond to IoT security threats in various IoT devices, the IoT network platform that provides end-to-end encryption and network separation is required.

However, since the computing resources of the various devices are different, there are limitations in applying the same technology as the existing security architecture [12]. In the various studies, IoT network architectures have been proposed to minimize IoT security threats while minimizing the load of IoT devices for security functions. Farris et al. explained the necessity of traffic isolation and logical network separation in response to security threats [8]. Linda et al. described a network architecture using SD-VPN to improve the scalability and security of IoT [21]. Kumar et al. proposed an IoT model that securely exchanges messages between trusted publishers and subscribers using a many-to-many end-to-end encryption protocol [14]. McCormack et al. described an SDN-based IoT security gateway architecture using a micro-hypervisor that can easily provide new security functionality to respond to emerging threats [16]. Jason presented a WireGuard VPN that outperformed the throughput and response speed of IPsec and OpenVPN by applying a minimized key distribution process and stream cipher algorithm [7]. However, the former VPN models did not provide many-to-many and end-to-end encryption and a scalable network

separation simultaneously. Moreover, since IPsec, OpenVPN, and WireGuard are TCP/IP-based VPNs, they inherit the TCP/IP properties that require network buffers and sockets. Therefore, when a TCP/IP-based VPN is applied to IoT, the bandwidth, processing power, battery power, and memory of IoT device are additionally affected [3].

In this paper, we propose an IoT-specific network security platform to protect IoT devices against network threats while also reducing the load on such devices, which typically have limited bandwith and computing resources. First, we analyze IoT-related vulnerabilities and attacks with the STRIDE model and describe the requirements for the secure network platform. Second, we design a secure and scalable IoT network platform taking into account the characteristics of IoT devices such as location limitation, device growth, and the limited computing resource. SSI provides a scalable VPN and many-to-many and end-to-end encryption in the layer 2 network. Below, we describe a novel approach different from the previous IoT network platforms.

- **An IoT network platform using L2TP and Virtual Extensible LAN (VXLAN) provides 16 million separated networks without any distance limitation.**

- **Many-to-many and end-to-end encryption using the MACsec algorithm does not require a session-specific key exchange procedure. Thus it will reduce the IoT bandwidth, CPU/memory usage.**

- **An IoT network platform with encryption and network separation can replace the security function of IoT protocol and minimize the resource consumption of IoT devices.**

In the experiment environment of SSI platform using Raspberry Pi 3B+ and AWS EC2, SSI improved network performance by 30% and reduced CPU usage by 31.6% compared to the OpenVPN network in which IPsec was applied.

2 Related Work

2.1 L2TP (Layer 2 Tunneling Protocol)

L2TP is a tunneling protocol to support layer 2 virtual private network. However, since the L2TP protocol alone does not provide encryption, it is often implemented with IPsec to provide confidentiality, authentication, and integrity. The endpoints of an L2TP tunnel are the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server) [15]. When L2TP is applied to the IoT network, a number of unspecified IoT devices perform the LAC role, and the CN receiving a tunnel link performs the LNS. Since the network applying MACsec must support unicast, broadcast, and multicast, SSI uses the L2TPv3 protocol that supports these communications [1].

2.2 MACsec (802.1AE, MAC Security)

MACsec is the layer 2 security protocol that provides authenticity and integrity for data-link layer frames. MACsec increases transmission efficiency by minimizing the header size compared to IPsec. This is very useful in the layer 2 IoT network, which provides low bandwidth, such as Long Range (LoRa) Wide Area Network (WAN). MACsec is a very useful protocol for high-speed connectivity as it can implement physical port-based encryption and decryption [6]. Moreover, the MACsec security mechanism does not affect the upper layer, so there is no need to modify the user application. However, in order to apply MACsec, the layer 2 network capable of unicast, broadcast, and multicast must be provided.

2.3 VXLAN (Virtual Extensible LAN)

In order to accommodate various protocols and services and to guarantee user mobility, layer 2 network virtualization is appropriate, and technologies such as VXLAN, Stateless Transport Tunneling (STT), Network Virtualization Using Generic Routing Encapsulation (NVGRE), and Locator/Identifier Separation Protocol (LISP). Among them, VXLAN is supported by most vendors and is being used to provide an overlay network in the cloud-scale datacenter, and its application range is expanding to the software defined wan (SD-WAN). VXLAN provides layer 2 network services like VLAN, but it has higher network scalability and availability than VLANs. VXLAN provides the layer 2 overlay network service over the layer 3 transport network. VTEP (VXLAN Tunnel Endpoint) provides 16 million unique VNIs (VXLAN IDs). It enables users to acquire sufficient virtualized network resources on a single underlay network.

3 Problem Analysis

3.1 Security Threats on The IoT Network

Security threats are various depending on the kinds of IoT networks and devices. Examples of security threats include speed delays for high-speed wireless networks such as 5th generation mobile network, Denial-of-service-attack (DoS) attacks for application servers located in the cloud, power consumption for low-power IoT devices and small mobility, eavesdropping for home IoT, and replay attacks for IoT servers and devices.

The IoT network as shown in Figure 1, is exposed to various security threats [16]. According to the management entity of Internet, the Internet used in IoT networks can be classified into the public Internet and the trusted Internet. The public Internet is a network that allows anyone to access, and it contains risks that can include careless management and threats by attackers. On the contrary, the trusted Internet is relatively safe compared to the public Internet because it controls user access and allows access only to authorized users. However, it is expensive and inefficient to build a whole trusted network to prevent unauthorized

access. Therefore, we should review countermeasures to supplement the vulnerability of IoT devices on the public Internet. We can find that the configuration of the local gateway is sometimes poorly managed in the home IoT environment [22]. In that case, it can cause DNS manipulation, traffic detour, and DoS due to unauthorized access by an attacker. In addition, if the network between the IoT device and the IoT server is very far, some sections of the public internet can be delayed and threatened by an attacker's route tampering and sniffing. Moreover, if the IoT server does not strongly authenticate the IoT device, rogue devices can connect to the IoT service.

Although the IoT attacks on the public Internet are different, security threats can be minimized by preventing the exposure of the communication from the IoT device to the server and encrypting traffic.

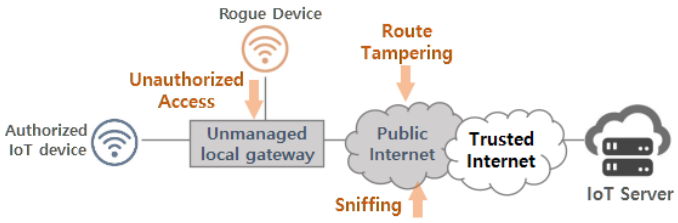

Fig. 1: IoT security threats in the network structure: Attackers can threaten IoT services at any location of a gateway, routing path, in addition to IoT devices.

3.2 Limitations of IoT Application Protocol

There are two popular IoT protocols: MQTT and CoAP are lightweight application protocols that can be used in IoT devices with limited resources. First, MQTT provides a machine-to-machine (M2M) network connection based on a TCP/IP network. MQTT consists of a broker that relays messages from a machine and a publisher that creates messages. MQTT shows a network diagram of the hub and spoke. It is used in low-bandwidth or low-reliability networks to ensure the reliability and data delivery with the minimum resource of device. Second, CoAP supports M2M applications using unicast and multicast without a broker based in the UDP network. CoAP with a point-to-point network architecture provides an asymmetric message exchange method [10].

Because MQTT and CoAP are application protocols for message delivery, they do not provide encryption by themselves. Therefore, MQTT and CoAP run on SSL/TLS and DTLS for encrypted data transmission. However, since the SSL/TLS and DTLS method requires key exchange for each session, an IoT device that attempts many-to-many encryption requires many key exchange procedures to attempt communication with all devices. Given the end-to-end encryption that requires no additional key exchange and an IoT network platform that only authorized devices can access, IoT applications such as MQTT and CoAP do not need to enforce SSL/TLS for secure data transmission.

Table 1: IoT Security Threat Analysis Using STRIDE Model

※ C&C*: Command and control server is controlled by an attacker

STRIDE	Vulnerabilities	Security Threats	Countermeasures
S (Spoofing)	Opened network Untrusted network Insecure Transfer	Unauthorized Access	Authentication Data Encryption
T (Tampering)	Opened network Untrusted network	Route Detour/Tampering Broadcast false information Replay attack	DATA Encryption Network Separation Route Management
R (Repudiation)	Opened network Insecure Transfer	Misuse, Malfunction	Authentication Data Encryption
I (Information Disclosure)	Opened network Insecure Transfer Insecure Application	Unauthorized Access Eavesdropping Privacy breach	Authentication Data Encryption Network Separation
D (Denial of Service)	Opened network Low Power supply	Service Outages/Delay Power Consumption	Network Separation Route Management
E (Elevation of Privilege)	Opened network Insecure ACL Insecure Software Hardcoded Password	Misuse, Malfunction System Manipulation C&C* Connection	Authentication Network Separation

3.3 Security Threat Modeling using STRIDE

STRIDE modeling helps to find all possible IoT security threats by analyzing the environment as a category of STRIDE security threats. Table 1 shows IoT vulnerabilities, security threats, and countermeasures by STRIDE classification [19]. Most vulnerabilities are caused by the IoT network exposed to the Internet. In order to provide the countermeasures, Authentication, Data Encryption, and Network Separation can be applied. In the countermeasures, the IoT network must provide authentication so that the only approved IoT devices can access the network. Second, Data encryption should work even on low-spec IoT devices using small computing resources. Third, route management should provide the trusted network in a wide area to block unauthorized users from intervening in the transmission route. Finally, in the network separation, the network access between each other services must be completely blocked even in the same transport route in order to guarantee various services. In addition, data encryption and network separation should be reviewed as a network platform to support various network protocols to ensure various communication.

4 Secure and Scalable IoT (SSI) Model

4.1 Overview

VPN and encrypted communication are required to prevent security threats in the IoT environment, but TCP/IP-based VPN and encryption is not suitable due to the limited resources of IoT device [3]. We designed SSI that overcomes

the limitations of TCP/IP-based VPN and encryption using layer 2 overlay network and MAC security. SSI provides authentication, data encryption, route management, and network separation.

SSI provides configuration information to access Communication Node (CN) during the first authentication, and it provides the network separation information and encryption key information during the second authentication. MACsec, the end-to-end encryption algorithm that uses low CPU resources and supports various network protocols, has been applied for the data encryption. Route management is accomplished by connecting the IoT device to the nearest trusted Internet CN. Finally, the layer 2 overlay network based on L2TP and VXLAN is provided for the network separation. In the SSI diagram of Figure 2, the IoT device is connected to the IoT server through CN. A single overlay network is provided between the IoT device and CN, and multi overlay networks are provided between CNs. Both single overlay networks and multi overlay networks provide the layer 2 network.

In the following subsections, we describe the MACsec and L2TP, and VXLAN as overlay network protocols. Next, we will look at the detailed elements of the SSI platform and the entire operation process, including authentication.

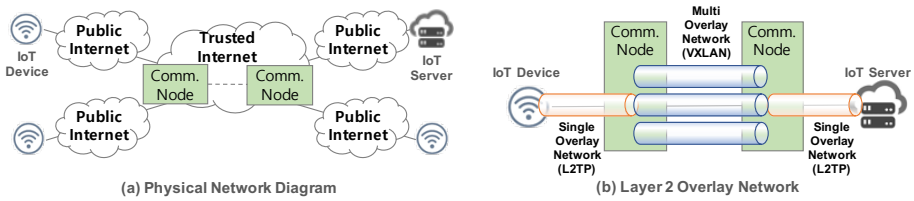

Fig. 2: Overview Diagram of SSI: CN is built on the trusted Internet such as AWS, Azure, and GCP. CN bridges the L2TP tunnel to the VXLAN tunnel.

4.2 L2TP And VXLAN Based Overlay Network

The overlay network of SSI provides network separation and layer 2 network without limiting the distance between IoT devices and servers. The network segment (between IoT device and CN) that is connected to various IoT endpoints and does not require network separation is configured as a single overlay network using the L2TP protocol. However, the communication node, which is the connection hub of SSI, provides a sufficient number of overlay networks using VXLAN to relay many separated networks. Figure 2(b) shows that the communication node (CN) bridges the L2TP tunnel and the VXLAN tunnel.

For example, if IoT devices are assigned the same VNID (VXLAN ID) from each CN, they are connected to the same VXLAN tunnel and belong to a single broadcast domain. In other words, the IoT device and IoT server assigned the same VNID can be connected to the same broadcast domain regardless of their location.

4.3 End-to-End Encryption Using MACsec

Data may be exposed outside the transmission path in the overlay network of SSI where encryption is not applied. Even if L2TP/IPsec is applied, encryption is not applied to the multiple tunnels communicating with VXLAN. In this case, encryption for VXLAN should be added.

We applied the MACsec protocol to improve the security vulnerability of the overlay network using L2TP and VXLAN. In the network to which MACsec is applied, only the hosts that have been authenticated are subject to MACsec Key Agreement (MKA). If a host connected to the VTEP has not been authenticated by the authentication server, the MKA protocol does not proceed normally, so SAK (Secure Association Key) transmission will be blocked. In Figure 3, a connectivity association key (CAK) is delivered to the approved CN via 802.1X authentication server, and CN shares CAK only for the supplicant who has completed authentication. Even though a rogue VTEP establishes a normal VTEP and VXLAN tunnel, IoT devices belonging to the Rogue VTEP cannot join MACsec communication because CAK is not provided.

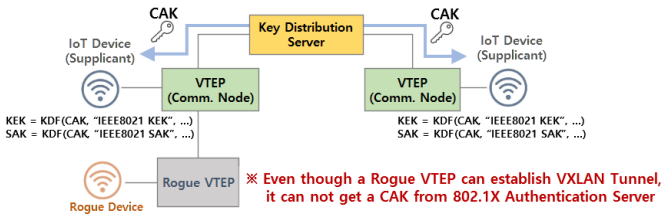

Fig. 3: CAK Delivery using 802.1X authentication server: IoT devices that do not complete 802.1X authentication cannot get a CAK for MACsec encryption.

MACsec uses the AES-GCM algorithm, and the symmetric key (SAK) used in the encryption algorithm is periodically generated in the host. SAK is encrypted using a key encrypting key (KEK) that is shared between hosts. AES-GCM algorithm is widely used for the data encryption required fast processing cause of supporting the parallel encryption method [17]. KEK, which encrypts SAK as a symmetric key continuously generated by the host, minimizes computing resources in contrast to the asymmetric key algorithm. Therefore, MACsec is considered a suitable encryption protocol for an IoT device.

In Equation 1, the context is obtained from the bitwise operation of KS-nonce generated from a key server (KS), 32bit-value provided by member identifier (MI), and counter number maintained by KS. In Equation 2,3, key derivation function (KDF) generates SAK and KEK using a pseudorandom function [5,6].

$$Context = KS\text{-}nonce|MI\text{-}value\,list|Key\text{-}number \tag{1}$$

$$SAK = KDF(CAK, \text{“}IEEE8021\,SAK'', Context, SAK\,length) \tag{2}$$

$$KEK = KDF(CAK, \text{“}IEEE8021\,KEK'', Keyid, length) \tag{3}$$

4.4 Network Architecture

SSI consists of a communication node (CN) that mediates different types of overlay networks, a CN controller that controls these CNs, and an authentication server that provides authentication and authorization. The L2TP authentication server provides the initial authentication and minimum information for configuring the L2TP tunnel, and the 802.1X authentication server provides VNID for relay to the VXLAN tunnel and CAK for MACsec encryption. CN bridges the L2TP tunnel to which the IoT device is connected to the VXLAN by referring to the VNID. After authentication and authorization of an IoT device and tunnel bridging of the CN, the IoT device uses CAK to apply MACsec encryption to end-to-end communication. Figure 4 shows the architecture where each element is connected and the logical network separation. Because the global IaaS such as AWS, Azure, and GCP has a dedicated Internet backbone for the stable and secure service when interworking between global regions, we use AWS IaaS for the trusted Internet. Besides, if you use IaaS compute nodes, you can quickly and build a communication node on the trusted Internet at low cost, and you can conveniently expand the scale.

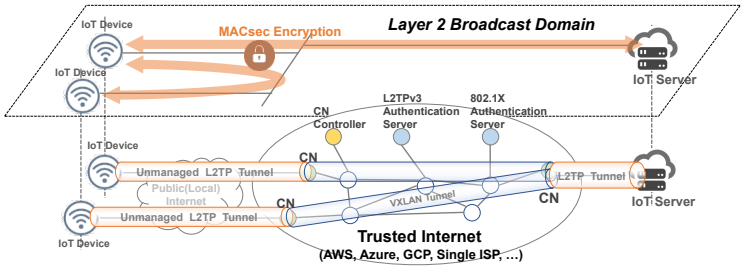

Fig. 4: SSI Platform using Global IaaS : The SSI platform built using the global IaaS provides the same layer 2 network and MACsec encryption to IoT devices and IoT servers (or another IoT devices).

Figure 5 explains the data transaction between SSI components divided by each step.

Step 1: IoT device authentication - After the permission of the L2TP authentication server, IoT devices receive session information to connect to the IoT network platform.

Step 2: L2TP tunnel with communication node (CN) - IoT devices (or local gateways) establish a tunnel with the nearest CN using L2TP session information.

Step 3: 802.1X authentication/authorization - IoT devices access the communication node through the L2TP tunnel and perform 802.1X authentication. After the authentication server's permission, CN receives attribute value pairs (AVPs) (e.g., VXLAN ID (VNID), connectivity association key (CAK)).

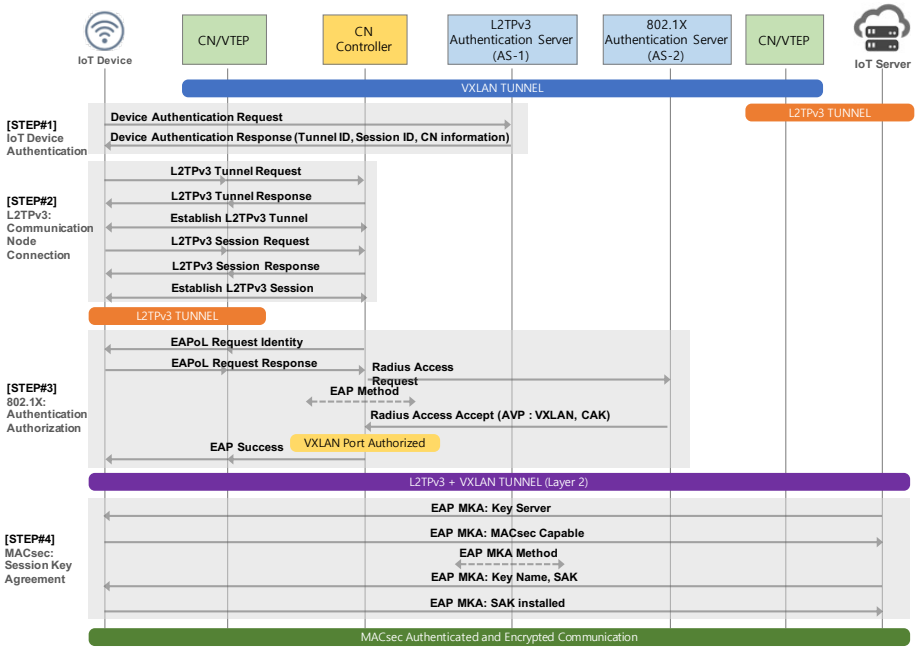

Fig. 5: SSI Platform Process : IoT device authentication → L2TP tunneling → 802.1X authentication → MACsec Key Agreement → Encrypted Communication

※ *Through the process up to this point, the IoT device can communicate with other devices in the same layer 2 network. However, for MACsec communication, the process of synchronizing the secure association key (SAK) must be finally performed.*

Step 4: MACsec session key agreement - The symmetric key is shared within the same VXLAN domain using the EAP protocol and is used for MACsec encryption.

In the surveys about IoT security [2,8,9], authentication, access control, network separation (or secure routing), encryption, detection, and SDN are represented as security aspects of IoT network. In Table 2, SSI supports all security aspects except detection. Detection can be easily applied without affecting the response time by mirroring traffic through CN.

5 Evaluation

The experiment environment is configured to measure the response time, CPU usage, and speed delay due to the application of an encryption algorithm. We use a Raspberry Pi 3B+ as an IoT device and AWS EC2 as an IoT server to build the experiment environment. Amazon AWS is used for the trusted Internet to examine the effect of speed improvement. The average response time between EC2s, located in Seoul, South Korea, and Ohio, US, shows 180 to 190

Table 2: Security function comparison with previous IoT platforms

Function	SSI	Linda et al. (2018) [21]	Kumar et al. (2019) [14]	McCormack et al. (2020)[16]
Layer 2 Communication	Yes	No	No	No
Net Separation	Yes	Yes	No	No
Authentication	Yes	No	Yes	No
Access Control	Yes	Yes	No	Yes
Enc.(End-to-End)	Yes	No	Yes	No
Enc.(Many-to-Many)	Yes	No	Yes	No
Encryption(Datalink)	Yes	No	No	No
SDN	Yes	Yes	No	Yes
Detection	No	No	No	Yes

Table 3: Evaluation Case: Case type was chosen to compare the effects of the overlay network (1-3, 2-4) and VPN protocol (4-5-6).
Since OpenVPN does not support AES-GCM in PSK mode, AES-128-CBC is used

Case	VPN Type	Network	Cipher Algorithm
1	None	No Overlay	None
2	OpenVPN	No Overlay	AES-128-CBC
3	SSI (No Encrypted)	L2TP + VXLAN	None
4	OpenVPN	L2TP + VXLAN	AES-128-CBC
5	IPsec	L2TP + VXLAN	AES-128-GCM
6	SSI (Encrypted)	L2TP + VXLAN	AES-128-GCM

ms. We compared the Network performance and CPU usage of SSI with IPsec (Strongswan) and OpenVPN.

Network performance is measured in the six VPN test cases depending on whether the overlay network and the encryption. To verify the performance of encryption, we use OpenVPN, IPsec, and MACsec protocols. We do not include the WireGuard, because it does not support the AES algorithm. MACsec and IPsec use the AES-GCM cipher algorithm. However, the AES-GCM algorithm of OpenVPN cannot be applied with a pre-shared key similar to the key exchange of SSI, so the AES-CBC algorithm is applied. IPsec of Strongswan and OpenVPN are evaluated to be very stable and fast in the layer 3 VPN. Table 3 shows the classification of 6 test environments. First, case 2 is a typical VPN using OpenVPN. Next, Case 3 shows the test case to evaluate the performance of overlay network using L2TP and VXLAN. Lastly, cases 4, 5, and 6 are the comparison of each VPN performance.

ICMP Response Time, File Download time, and Packet loss ratio are adopted as performance measurement items. First, while packets of 1508 bytes are transmitted from the IoT device to the IoT server 1000 times, we measured the ICMP response time to measure the Round Trip Time and the packet loss ratio. In Table 4, the overlay network has a similar response time compared to the public

Table 4: Network performance Comparison: The cases of 1-3 and 2-4 show that overlay network can improve the network performance. Moreover, the cases of 4-5-6 show that SSI's VPN is better than IPsec and OpenVPN.

Case	ICMP Response Time (ms)			Packet Loss (%)	Download Speed (MB/sec)
	min	avg	max		
1	185	187	197	0.1	1.89 (0.0%)
2	212	213	254	0.8	1.48 (-21.7%)
3	191	193	215	0	2.07 (+9.5%)
4	210	211	228	0.3	1.92 (+1.6%)
5	194	198	383	0	1.63 (-13.8%)
6	192	193	205	0	1.94 (+2.6%)

network, but it shows stable network performance without any packet loss. Next, download speed is measured. The download speed of each case is the average speed of downloading 10 files with different file sizes from 10MB to 100MB.

We have confirmed that the performance is improved by applying the overlay network in the evaluation results. The MACsec algorithm has a lower CPU usage rate than IPsec. In the comparison of networks without data encryption in Table 4, the download speed of overlay network is improved by 10% compared to the public Internet, and no packet loss occurred. The download time of the SSI is improved by 31% compared to the public Internet applying OpenVPN. In addition, we compared the number of packets and data size transmitted when SSI, IPsec, and OpenVPN are applied on the overlay network. In transmitting a 10MByte file, we have confirmed that MACsec transmitted 11.2MB with 11,968 packets, IPsec transmitted 11.9MB with 11,815 packets, and OpenVPN transmitted 12.0MB with 19,842 packets. When comparing the total data transmission size and the number of packets, MACsec of SSI has worth considering communication efficiency.

We can confirm that the MACsec algorithm is more suitable for IoT than IPsec and OpenVPN in terms of CPU usage. Figure 6 graph shows the CPU usage while an IoT device (Raspberry Pi 3B+) downloads a 100MB file. In the encrypted communication, the file download time of SSI and OpenVPN is the same at 51 seconds, and IPsec takes 56 seconds. During the download time, the average CPU usage of OpenVPN is 27.5%, IPsec is 21.4%, and SSI is the lowest at 18.8%. When considering that most IoT devices provide low power and low computing resources, MACsec applied to SSI is considered to be a very suitable cipher algorithm for IoT.

6 Conclusion

We expect that SSI effectively blocks MITM, route tampering, and privacy breaches occurring in the open IoT network by using an overlay network and many-to-many and end-to-end encryption. In addition, the MACsec encryption

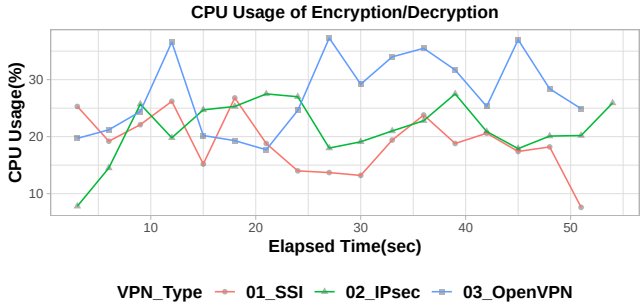

Fig. 6: CPU Usage for Data Transfer:
(SSI: Avg 18.8%, IPsec: Avg 21.4%, OpenVPN: Avg 27.5%)

algorithm is effective for IoT devices due to low CPU usage, and the layer 2 overlay network helps to use various communication protocols. The experiment environment installed from the IoT device located in Seoul, South Korea to the IoT server located in Ohio, US, has verified that the network speed has improved by 30% and the CPU usage rate of the IoT device has decreased by 31.6%.

Since CNs are installed on the trusted public cloud, they are convenient to control and scale compared to a local network environment. Various NFVs of SDN and middleboxes requiring high availability can be applied to the SSI's CN. In other words, SSI is more efficient in providing flexible computing resources than installing a security gateway on the local edge network close to IoT devices.

We expect that SSI can provide a VPN network environment to collaborate with offices from outside. In further research, we plan to conduct research to develop a secure and scalable VPN for the business collaboration between telecommuting users through the improvement of SSI.

References

1. L2VPN (L2TPv3) (2020), `https://www.yamaha.com/products/en/network/techdocs/vpn/l2tpv3/`
2. Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F.: Internet of Things security: A survey. Journal of Network and Computer Applications **88**, 10–28 (2017)
3. Bello, O., Zeadally, S., Badra, M.: Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT). Ad Hoc Networks **57**, 52–62 (2017)
4. Bradley, J., Loucks, J., Noronha, A., Macaulay, J., Buckalew, L.: Internet of Everything (IoE) (2013), `https://www.ciosummits.com/IoE_-_Top_10_Insights_from_Cisco_s_IoE_Value_Index_Survey.pdf`
5. Chen, L.: Nist special publication 800-108. Recommendation for Key Derivation Using Pseudorandom Functions (Revised), http://csrc.nist.gov/publications/nistpubs/800-108/sp800-108.pdf (2009)
6. Craig Hill, S.O.: Introduction to WAN MACsec (2018), `https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKRST-2309.pdf`

7. Donenfeld, J.A.: WireGuard: Next Generation Kernel Network Tunnel. In: NDSS (2017)
8. Farris, I., Taleb, T., Khettab, Y., Song, J.: A survey on emerging SDN and NFV security mechanisms for IoT systems. IEEE Communications Surveys & Tutorials **21**(1), 812–837 (2018)
9. Hassan, W.H., et al.: Current research on Internet of Things (IoT) security: A survey. Computer networks **148**, 283–294 (2019)
10. Hei, I., Špeh, I., Šarabok, A.: IoT network protocols comparison for the purpose of IoT constrained networks. In: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). pp. 501–505. IEEE (2017)
11. Hippold, S.: Gartner 2020 Hype Cycle for Supply Chain Strategy Shows Internet of Things is Two to Five Years Away from Transformational Impact (2021), `https://www.gartner.com/en/newsroom`
12. Hwang, Y.H.: IoT security & privacy: threats and challenges. In: Proceedings of the 1st ACM workshop on IoT privacy, trust, and security. pp. 1–1 (2015)
13. Khan, M.A., Salah, K.: IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems **82**, 395–411 (2018)
14. Kumar, S., Hu, Y., Andersen, M.P., Popa, R.A., Culler, D.E.: {JEDI}: Many-to-Many End-to-End Encryption and Key Delegation for IoT. In: 28th {USENIX} Security Symposium ({USENIX} Security 19). pp. 1519–1536 (2019)
15. Lau, J., Townsley, M., Goyret, I.: Layer two tunneling protocol-version 3 (l2tpv3). RFC 3931 (2005)
16. McCormack, M., Vasudevan, A., Liu, G., Echeverría, S., O'Meara, K., Lewis, G., Sekar, V.: Towards an Architecture for Trusted Edge IoT Security Gateways. In: 3rd {USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 20) (2020)
17. McGrew, D., Viega, J.: The galois/counter mode of operation (gcm). submission to NIST Modes of Operation Process **20**, 10 (2004)
18. OWASP IoT Security Team: OWASP IOT Top 10 2018 (2020), `https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf`
19. Robin Shahan, Phil Meadows, B.L.: IoT security architecture (2018), `https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture`
20. Ryoo, J., Kim, S., Cho, J., Kim, H., Tjoa, S., Derobertis, C.: IoE security threats and you. In: 2017 International Conference on Software Security and Assurance (ICSSA). pp. 13–19. IEEE (2017)
21. Shif, L., Wang, F., Lung, C.H.: Improvement of security and scalability for IoT network using SD-VPN. In: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. pp. 1–5. IEEE (2018)
22. Simpson, A.K., Roesner, F., Kohno, T.: Securing vulnerable home iot devices with an in-hub security manager. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). pp. 551–556. IEEE (2017)