

# Design and Basic Evaluation of Virtual IPv4 based CYPHONIC adapter

Ren Goto

Faculty of Information Science, Aichi Institute of Technology,  
1247 Yachigusa, Yakusa, Toyota, Aichi 470-0392, Japan

Taiki Yoshikawa

Graduate School of Business Administration and Computer Science, Aichi Institute of Technology,  
1247 Yachigusa, Yakusa, Toyota, Aichi 470-0392, Japan

Hijiri Komura

Graduate School of Business Administration and Computer Science, Aichi Institute of Technology,  
1247 Yachigusa, Yakusa, Toyota, Aichi 470-0392, Japan

Kazushige Matama

Faculty of Information Science, Aichi Institute of Technology,  
1247 Yachigusa, Yakusa, Toyota, Aichi 470-0392, Japan

Chihiro Nishiwaki

Graduate School of Business Administration and Computer Science, Aichi Institute of Technology,  
1247 Yachigusa, Yakusa, Toyota, Aichi 470-0392, Japan

Katsuhiro Naito

Faculty of Information Science, Aichi Institute of Technology,  
1247 Yachigusa, Yakusa, Toyota, Aichi 470-0392, Japan

## ABSTRACT

The rapid spread of cloud services and Internet of Things (IoT) leads to a request for secure communication between devices, called zero-trust security. However, security tends to be a low priority compared to the designated service because zero-trust security requires security knowledge. Therefore, a secure communication framework for developers' service development process is essential as the security measures. The authors have developed CYber PHysical Overlay Network over Internet Communication (CYPHONIC) for secure end-to-end communication between devices. Since the CYPHONIC provides secure communication, it also performs as the secure communication framework. The current implementation requires installing the device program into the end devices to join our overlay network. However, it should support general devices such as embedded devices or dedicated service servers even if they refuse to install the additional program. This paper proposes a new technology to support these general devices without installing the device program into the devices. We developed a CYPHONIC adapter to provide secure communication to the general devices. It shows that general devices can communicate over the overlay network through the proposed CYPHONIC adapter.

Keywords: IoT, Zero-trust security, Overlay network protocol

## 1. INTRODUCTION

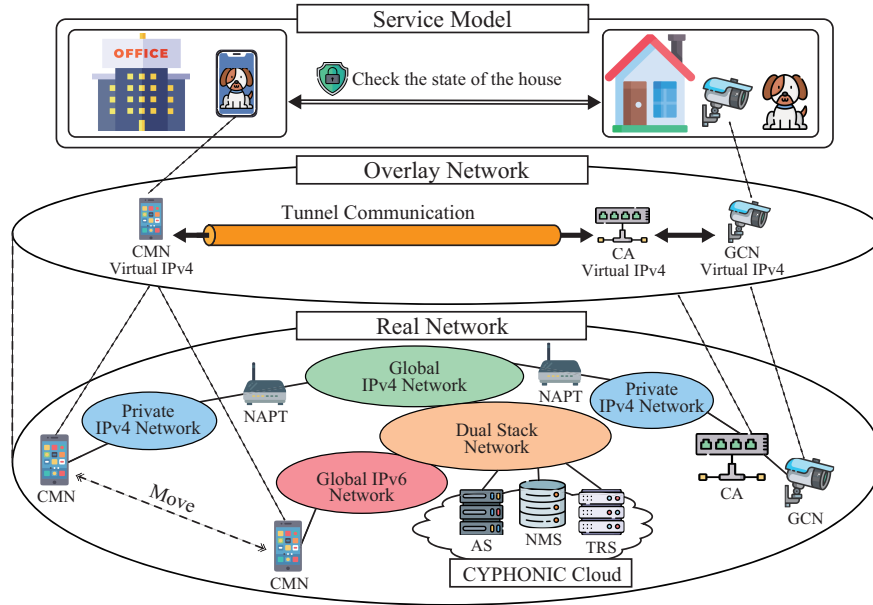
The zero-trust security model is the latest secure architecture to realize a more secure system by authorizing each endpoint. It requires all endpoints to be authenticated, authorized, and validated for security configuration, whether in or outside the

organization's network [1], [2]. Since many organizations use cloud systems to process data, a typical zero-trust security product considers that cloud systems manage each endpoint. As a result, almost all products rely on cloud systems to realize the security architecture [3].

The number of IoT devices is increasing rapidly. The resource of the IoT devices is extensive computational resources. Therefore, cooperated IoT devices can realize a single service by performing distributed computation [4], [5]. The zero-trust security model is also essential to realize the service because each IoT device typically exists in different areas or networks [6]. It requires IoT devices to realize secure end-to-end communication even if they connect to any network systems. On the contrary, typical developers of IoT devices concentrate on their service, not the security model. As a result, they may often handle security as a low priority function compared to the designated service functions [7]. Therefore, a secure communication framework is essential for developers to help their service development process without any knowledge of the zero-trust security model.

Since each IoT device exists in distributed networks, the framework should support several network types such as IPv4 global addresses, IPv4 private addresses, and IPv6 addresses. Typically, these techniques are supposed to be network accessibility issues [8], [9]. As the solution, several technologies have been proposed [10], [11]. However, conventional methods require developers to understand the details of the technologies.

Cellular systems are also spreading globally and are the main access network for IoT devices. As a result, IoT devices may change access networks according to the service condition of the



AS: Authentication Service NMS: Node Management Service TRS: Tunnel Relay Service  
 CA: CYPHONIC Adapter CMN: CYPHONIC Mobile Node GCN: General Correspondent Node

Fig. 1. Overview of CYPHONIC

cellular or Wi-Fi service [12]. Therefore, the framework should handle the change of IP address due to the change of access networks. IP mobility technologies are well-known solutions for this situation [13], [14]. However, conventional technologies focus on IPv6 networks because IPv6 is designed to support mobility. Finally, developers require a more packaged solution to realize their service on the zero-trust security model.

The authors have proposed and developed CYber PHysical Overlay Network over Internet Communication (CYPHONIC) as a technology that can comprehensively solve these issues [15]–[17]. CYPHONIC provides secure end-to-end communication for any application by inserting the new overlay network layer between the network and transport layers. As a result, developers can use the zero-trust security model by focusing on their services.

The current CYPHONIC system requires a device to install the program for the CYPHONIC communication function. On the contrary, some conventional devices (General Node), such as IoT devices, embedded devices, and dedicated servers, tend to avoid the additional installation of the device program due to the limitation of system and hardware resources or the effect on the system reliability [18].

This paper proposes an adapter device called CYPHONIC adapter to provide a function to join the CYPHONIC network for general nodes. The CYPHONIC adapter is a new technology to support these general nodes without installing the device program into the devices. We developed a CYPHONIC adapter to provide secure communication over our overlay network to the general nodes. It shows that general devices can communicate over the overlay network through the proposed CYPHONIC adapter.

## 2. CYPHONIC

CYPHONIC uses virtual IP addresses to enable secure end-to-end communication over an overlay network unaffected by the physical network environment. Fig. 1 shows the overview of CYPHONIC. CYPHONIC comprises a cloud service and CYPHONIC nodes, end devices equipped with CYPHONIC. CYPHONIC nodes enable secure end-to-end communication between devices in cooperation with cloud services. The cloud service consists of three types of services: Authentication Service (AS), Node Management Service (NMS), and Tunnel Relay Service (TRS). AS performs the authentication process to verify that the CYPHONIC node is a valid user. Additionally, it assigns a Fully Qualified Domain Name (FQDN) as the identifier of the CYPHONIC node. It distributes an encryption key to encrypt the NMS and the CYPHONIC node communication. NMS assigns a unique virtual IP address to the CYPHONIC node, which remains even when the node changes an access network. Additionally, it manages network information such as the real IP addresses of CYPHONIC nodes and the existence of NAPT. It also selects an optimal route according to the network environment of both CYPHONIC nodes and instructs the construction procedure to establish secure communication. TRS relays the data between devices when direct communication is difficult due to the different protocol versions between IPv4/IPv6 networks or the rejection of incoming packets due to NAPT mechanisms.

The CYPHONIC node authenticates to AS at the service startup and registers its network location information to NMS. NMS assigns a virtual IP address to the CYPHONIC node as the response message. NMS instructs the appropriate communication path for both CYPHONIC nodes so that bidirectional communication is always available even when there is a

NAPT mechanism on the communication path or both nodes use different protocol versions such as IPv4 and IPv6. The CYPHONIC node performs secure communication with the virtual IP address and encapsulates packets for the secure communication into User Datagram Protocol (UDP) datagrams with an actual IP address. Additionally, CYPHONIC nodes exchange an encryption key to secure communication by encrypting all packets in UDP datagrams. Therefore, CYPHONIC can provide a secure communication mechanism for developers without special security knowledge.

### 3. CYPHONIC ADAPTER

#### 3.1. Concept design

Since an end node must install the unique device program called CYPHONIC Daemon to support secure communication, it also requires flexible specification to accept the additional installation into the end node. On the contrary, some end nodes for IoT or embedded devices limit device resources. Therefore, it may be difficult for these devices to install the CYPHONIC Daemon. Additionally, some particular server tends to refuse the additional installation because they have concerned about the effect on the stability and reliability of their service. As a result, CYPHONIC should support these general nodes without installing the CYPHONIC Daemon.

This paper proposes an adapter device called CYPHONIC adapter to provide a function to join the CYPHONIC network for general nodes. General nodes can be connected to adjacent CYPHONIC adapters to communicate over our overlay network without installing CYPHONIC Daemon. Since the CYPHONIC adapter performs processing for CYPHONIC communication instead of the general nodes, it interconnects the general nodes and CYPHONIC end nodes. We also develop a prototype implementation of the CYPHONIC adapter to evaluate the fundamental evaluation for secure communication.

#### 3.2. System model

Fig. 2 shows the system model of the proposed CYPHONIC adapter. The CYPHONIC adapter needs to have the ability to manage general nodes and the CYPHONIC communication function. The CYPHONIC Daemon performs as a background process in the device's user space and provides the necessary functionality to communicate over our overlay network. The CYPHONIC Daemon has functions for signaling with each cloud service and handling Domain Name System (DNS) messages for FQDN queries. Additionally, it has functions to encapsulate, decapsulated, encrypt, and decrypt virtual IP packets into CYPHONIC packets.

The CYPHONIC adapter utilizes the conventional CYPHONIC Daemon functionality as a communication function. Then, it is implemented as an Adapter Daemon to manage the information for general nodes and handle the communication between general nodes and CYPHONIC nodes. The management function obtains the pair of a virtual IP address and an FQDN for each general node because CYPHONIC identifies an end node based on FQDN. Additionally, it also assigns the virtual IP address to the general nodes. The communication handling

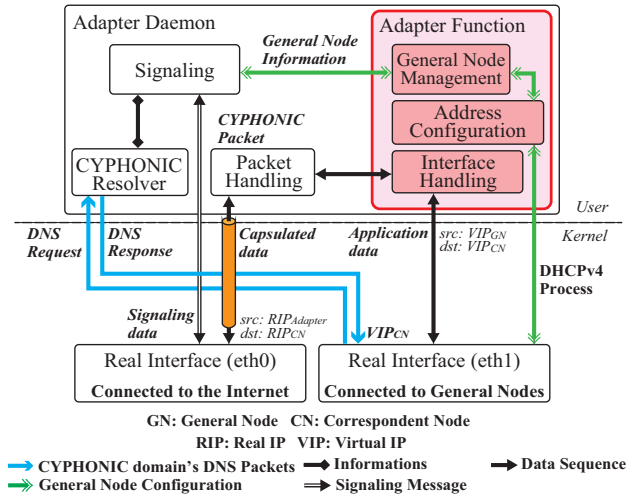


Fig. 2. System model of CYPHONIC adapter

function acquires packets from general nodes, performs signaling with cloud services, and encrypts and decrypts messages.

#### 3.3. Component function

The CYPHONIC adapter extends the implementation of the conventional CYPHONIC Daemon to support management and transportation functions for general nodes. It has two physical Network Interface Cards (NICs), one is bridged to the general node, and the other is connected to a network. The conventional CYPHONIC Daemon has Signaling Module, CYPHONIC Resolver Module, and Packet Handling Module. Signaling Module performs signaling with each cloud service. The CYPHONIC adapter obtains the information necessary for general nodes to communicate with the peer node from the cloud service. CYPHONIC Resolver Module processes DNS packets for FQDN queries. It responds to a DNS Request received from a general node by generating a DNS Response containing the virtual IP address of the peer node. Packet Handling Module realizes secure communication by encryption, calculation, decapsulation, and decryption of virtual IP packets. The general node does not encrypt the virtual IP packets. The CYPHONIC adapter encrypts the virtual IP packets and encapsulates them into CYPHONIC encapsulated packets. It utilizes the functions in the CYPHONIC Daemon to realize these operations.

The CYPHONIC adapter should manage the connected general nodes. Therefore, it introduces General Node Management Module. General Node Management Module manages the virtual IP addresses, MAC addresses, and FQDNs of the connected general nodes. Additionally, encryption keys are generated and managed for each communication process of general nodes to achieve secure communication. When the general node communicates, the encryption key is transferred to Packet Handling Module. Since general nodes typically use a dynamic assignment of IP addresses, it also introduces Address Configuration Module for assigning virtual IP addresses to the general nodes. Address Configuration Module executes the Dynamic Host Configuration Protocol (DHCP) process for connected general nodes. It assigns a virtual IP address based

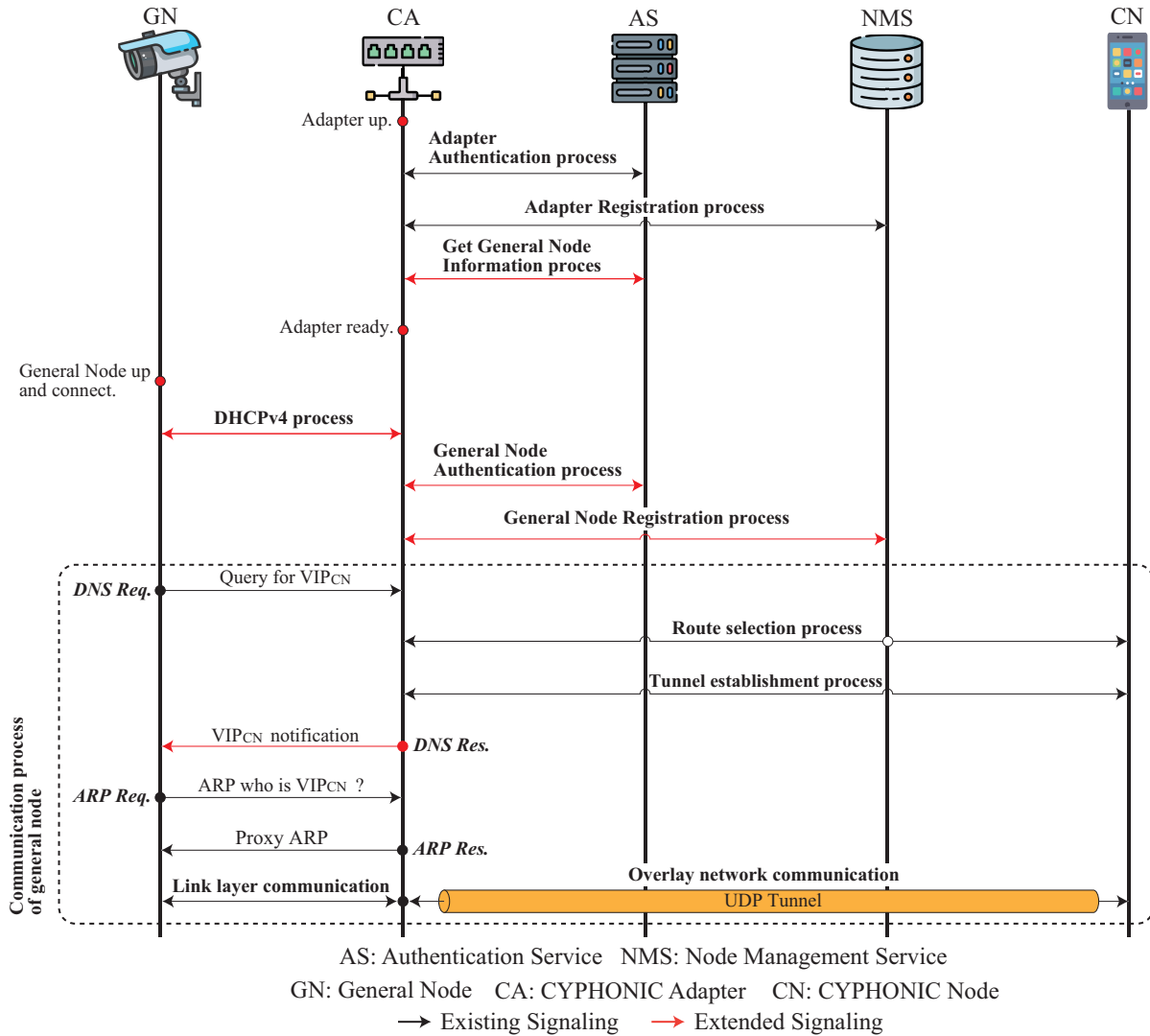


Fig. 3. Communication sequence using CYPHONIC adapter

on the MAC address of a general node. It notifies the virtual IP address, the default gateway address, and the IP address of the DNS server at the same time. When a general node is activated, it can obtain a virtual IP address by a general DHCP service. This paper assumes that Address Configuration Module assigns a virtual IPv4 address to a general node because the mainstream IP protocol is still IPv4. The CYPHONIC adapter also handles virtual IP packets from and to general nodes to interconnect to the CYPHONIC network. Therefore, Interface Handling Module hooks packets from general nodes and forwards them to Packet Handling Module to process CYPHONIC operations. The CYPHONIC adapter also decapsulates and decrypts packets by Packet Handling Module in the case of backward communication. Then, it forwards the virtual IP packets to the general node by Interface Handling Module. As a result, the CYPHONIC adapter can interconnect between the general node and correspondent nodes.

### 3.4. Communication sequence

Fig. 3 shows the communication sequence of the CYPHONIC adapter. CYPHONIC executes five processes for end-to-end communication using overlay networks: authentication, registration, route selection, tunnel establishment, and data communication. AS performs the authentication process of end nodes to join the overlay network and assigns a virtual IP address. NMS handles the registration process from end nodes to obtain access network environment. It also manages the route selection process to select an adequate signaling process to establish secure communication according to the access network environment of both end nodes. Both end nodes perform the tunnel establishment process to establish secure communication by exchanging an encryption key directly.

Since the CYPHONIC adapter obtains the information of general nodes from the cloud service, it performs the authentication and registration processes instead of general nodes. The first process assigns the virtual IP address through the DHCP process

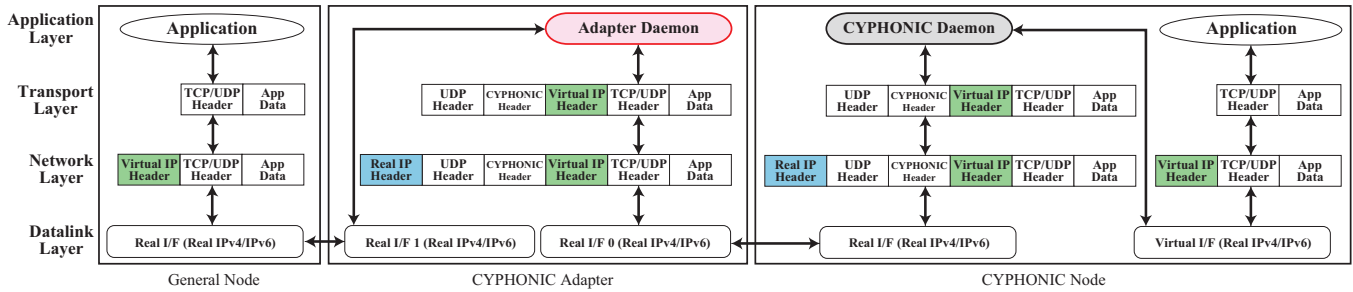


Fig. 4. Packet flow of General Node

according to the information of general nodes because general nodes may be offline. After that, the CYPHONIC adapter performs the authentication process and registration process of the general node to AS.

CYPHONIC identifies each end node by FQDN. Therefore, the initial communication trigger is a DNS query message including FQDN. Since the CYPHONIC adapter provides a DNS function to general nodes, it can receive DNS query messages. As a result, it performs the tunnel establishment process when the DNS query message arrives at the CYPHONIC adapter. NMS selects a communication pattern to establish a tunnel according to the network information of each end node. It also notifies the selected pattern to both end nodes. As CYPHONIC supports secure communication, each end node should exchange an encryption key. Therefore, the CYPHONIC adapter also exchanges an encryption key for each tunnel. Finally, it generates a DNS response message, including the correspondent node's virtual IP address. It should receive packets from the general node even if the destination IP address of the packets is the virtual address of the correspondent node. Therefore, it uses the Proxy Address Resolution Protocol (ARP) mechanism to transmit an ARP reply message to the ARP request for the virtual address. As a result, it receives the packets instead of the correspondent node and performs the CYPHONIC communication.

Fig. 4 shows the packet flow when the general node communicates with a CYPHONIC node. Since the general node performs standard IP-based communication with virtual IP addresses, the IP header of the packets from the general nodes includes the virtual IP addresses. The CYPHONIC adapter performs secure communication processing. It encrypts and encapsulates the incoming packets, including the virtual IP addresses. As a result, it transmits the capsulated packets with physical IP addresses.

The CYPHONIC node receives the incoming capsulated packets from the CYPHONIC adapter. It decapsulates and decrypts the packets to retrieve the inner IP packets, including the virtual IP addresses. Since it has a virtual network interface, the application receives the decapsulated packets through the virtual network interface.

#### 4. EVALUATION

We have developed a prototype implementation of the CYPHONIC adapter on Linux OS. Since the CYPHONIC Daemon uses Golang to implement the functions, the prototype also

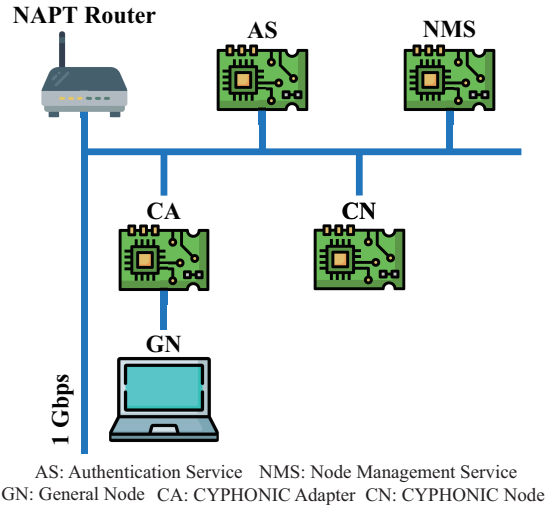


Fig. 5. Evaluation model

TABLE I  
SPECIFICATIONS OF THE MEASURING DEVICES

CYPHONIC Cloud	
Machine	Raspberry Pi 4 Model B
OS	Raspbian GNU/Linux 10.0 (Buster)
CPU	Quad Core 1.5GHz Broadcom BCM2711 64bit
Memory	4GB RAM
CYPHONIC Node / CYPHONIC Adapter	
Machine	Raspberry Pi 4 Model B
OS	Raspbian GNU/Linux 10.0 (Buster)
CPU	Quad Core 1.5GHz Broadcom BCM2711 64bit
Memory	8GB RAM
General Node	
OS	macOS Big Sur Version 11.5
CPU	Dual Core 2.20GHz Intel(R) Core i7-5650U 64bit
Memory	8GB RAM

employs Golang to extend the functions. Fig. 5 shows the verification environment in this evaluation. Table I shows the device specification used for the verification. The CYPHONIC adapter and the conventional CYPHONIC node communicate over the proposed overlay network in the evaluation environments.

TABLE II  
ROUND TRIP TIME

CYPHONIC Adapter		CYPHONIC Node	
RTT average	RTT max	RTT average	RTT max
3.272ms	9.271ms	3.271ms	9.133ms

TABLE III  
UDP THROUGHPUT PERFORMANCE

Traffic	CYPHONIC Adapter		CYPHONIC Node	
	Throughput	Jitter	Throughput	Jitter
10Mbps	10Mbps	0.32ms	10Mbps	0.52ms
20Mbps	19.9Mbps	0.15ms	20Mbps	0.66ms
30Mbps	29.6Mbps	0.26ms	30Mbps	0.55ms
40Mbps	39.7Mbps	0.30ms	40Mbps	0.29ms
50Mbps	49.5Mbps	0.23ms	50Mbps	0.27ms

The first evaluation is the reachability between nodes. We have used the ping tool to check the reachability. Table II shows the RTT for communication between general nodes and CYPHONIC nodes and communication between CYPHONIC nodes. The evaluation results showed that the Round Trip Time (RTT) is almost the same in the CYPHONIC adapter and the CYPHONIC node. Therefore, the proposed mechanisms do not have a significant overhead for processing.

The second evaluation is the throughput between nodes. We have used the iperf tool to measure the throughput. Table III shows the communication throughput in UDP. All measurements are averages of 10 measurements taken in one minute. The results showed that the CYPHONIC adapter's throughput is slightly lower than that of the CYPHONIC node. But, the prototype has enough throughput performance required by high throughput applications such as streaming, etc [19], [20].

### 5. CONCLUSION

This paper has proposed the adapter device called CYPHONIC adapter to provide a function to join the CYPHONIC network for general nodes such as IoT devices, embedded devices, and dedicated servers. The CYPHONIC adapter is a new technology to support these general nodes without installing the device program into the devices. Therefore, the conventional general nodes can quickly join the secure overlay network. We have developed the prototype of the CYPHONIC adapter to provide secure communication over our overlay network to the general nodes. It shows that general devices can communicate over the overlay network through the proposed CYPHONIC adapter without significant overhead.

### ACKNOWLEDGMENT

This work is supported in part by the collaborative research project with Mobiline Co., Ltd., Japan and Grant-in-Aid for Scientific Research (C)(21K11877), Japan Society for the Promotion of Science (JSPS).

### REFERENCES

[1] A. Iftekhhar, N. Tahmin, U. Sultana, and T. Kazi, "Protection of Sensitive Data in Zero Trust Model," 10.1145/3377049.3377114, January 2020.

[2] Y. Qigui, W. Qi, Z. Xiaojian, and F. Jiakuan, "Dynamic Access Control and Authorization System based on Zero-trust architecture," 10.1145/3437802.3437824, October 2020.

[3] H. Sufian, K. Faraz, and H. Bilal, "Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review," 10.1155/2019/9629381, January 2019.

[4] B. Joharan, "A fair survey on Internet of Things (IoT)," 10.1109/ICETETS.2016.7603005, February 2016.

[5] S. Khaitan and J. McCalley, "Design Techniques and Applications of Cyberphysical Systems: A Survey," 10.1109/JSYST.2014.2322503, June 2015.

[6] L. Shancang, "Editorial: Zero Trust based Internet of Things," 10.4108/eai.5-6-2020.165168, June 2020.

[7] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," 10.1016/j.comnet.2014.11.0088, January 2015.

[8] C. Huang and S. Hwang, "The asymmetric NAT and its traversal method," 10.5555/1689139.1689175, April 2009.

[9] P. Wu, Y. Cui, J. Wu, J. Liu, and C. Metz, "Transition from IPv4 to IPv6: A state-of-the-art survey," 10.1109/SURV.2012.110112.00200, January 2013.

[10] A. Keränen, C. Holmberg, and J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal," 10.17487/RFC8445, July 2018.

[11] W. Jianing, Z. Shilong, and J. Lurong, "Research and application of related technologies of new generation network communication protocol IPv6," 10.1109/ICMCCE51767.2020.00479, May 2015.

[12] B. Feng, C. Zhang, J. Liu, and Y. Fang, "D2D Communications-Assisted Traffic Offloading in Integrated Cellular-WiFi Networks," 10.1109/JIOT.2019.2922550, October 2019.

[13] S. Ghaleb, S. Subramaniam, Z. Zukarnain, and A. Muhammed1, "Mobility management for IoT: a survey," 10.1186/s13638-016-0659-4, July 2016.

[14] A. Hussain, S. Nazir, F. Khan, L. Nkenyereye, A. Ullah, S. Khan, S. Verma, and Kavita, "A Resource Efficient hybrid Proxy Mobile IPv6 extension for Next Generation IoT Networks," 10.1109/JIOT.2021.3058982, February 2021.

[15] T. Yoshikawa, S. Isomura, H. Komura, S. Kubota, C. Nishiwaki and K. Naito, "Performance evaluation of shared library supporting multi-platform for overlay network protocol," 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE), October 2020.

[16] T. Yoshikawa, H. Komura, C. Nishiwaki, R. Goto, K. Matama, and K. Naito, "Evaluation of new CYPHONIC: Overlay network protocol based on Go language," 2022 IEEE 40th International Conference on Consumer Electronics (ICCE), January 2022.

[17] T. Yoshikawa, H. Komura, R. Goto, K. Matama, C. Nishiwaki, and K. Naito, "Demonstration of video conferencing tool with overlay network protocol," 2022 IEEE 19th Consumer Communications & Networking Conference (CCNC), January 2022.

[18] A. Musaddiq, Y. Zikria, O. Hahm, H. Yu, A. Bashir, S. Kim, "A Survey on Resource Management in IoT Operating Systems," 10.1109/ACCESS.2018.2808324, February 2018.

[19] S. Tavakoli, "Subjective QoE Analysis of HTTP Adaptive Streaming Applications," December 2015.

[20] A. Biernacki and K. Tutschku, "Performance of HTTP video streaming under different network conditions," 10.1007/s11042-013-1424-x, September 2014.