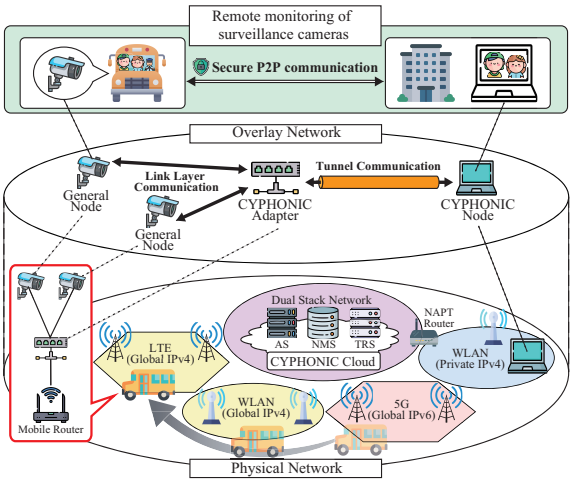
CYPHONIC Adapter: Enabling Secure P2P Connectivity for Diverse IoT Devices

Ren Goto*, Kazushige Matama*, Ryouta Aihata†, Michiyo Suda†, Hidekazu Suzuki‡, Katsuhiro Naito†,
*Graduate School of Business Administration and Computer Science, Aichi Institute of Technology, Toyota, Aichi, Japan
†Faculty of Information Science, Aichi Institute of Technology, Toyota, Aichi, Japan
‡Faculty of Information Engineering, Meijo University, Nagoya, Aichi, Japan
Email: r0719en, matama, sonarait, flower87@pluslab.org, hsuzuki@meijo-u.ac.jp, naito@pluslab.org

***Abstract*—Peer-to-Peer (P2P) communication emerges as a potent paradigm in distributed processing models. However, network accessibility challenges and inherent limitations in existing solutions have impeded the full realization of P2P's potential. To address these issues, we've developed CYber PHysical Overlay Network over Internet Communication (CYPHONIC), an innovative solution enabling P2P-based direct device-to-device communication while ensuring robust zero-trust security. Additionally, we introduce the concept of a gateway device equipped with a CYPHONIC adapter to cater to conventional devices, often referred to as general nodes. Our paper focuses on implementing a remote camera monitoring solution, providing secure access to surveillance cameras. We aim to demonstrate that our overlay network seamlessly connects all CYPHONIC clients, including general nodes. We also present a comprehensive case study centered on remote camera monitoring. This case study showcases the effortless connectivity enabled by our overlay network, highlighting how CYPHONIC clients, including general nodes, can efficiently interconnect.**

***Index Terms*—Remote camera monitoring solution, Seamless connectivity, Overlay network, Zero-trust security, Peer-to-Peer communication**



AS: Authentication Service NMS: Node Management Service TRS: Tunnel Relay Service
NAPT: Network Address Port Translation

Fig. 1. Overview of CYPHONIC

I. Introduction

Distributed processing models, predominantly based on Peer-to-Peer (P2P) architecture, have gained considerable prominence for their ability to enhance data processing efficiency and bolster service resilience in complex network environments [1]. However, the widespread depletion of global IPv4 addresses has compelled organizations to implement solutions such as Network Address Port Translation (NAPT) and IPv6. Although practical, NAPT can introduce access restrictions for hidden nodes behind it due to inbound traffic limitations, while IPv6 is unique. At the same time, the format can pose interoperability challenges, especially in dual-stack networks [2].

In response to the network accessibility challenges often associated with P2P communication, the authors have developed CYber PHysical Overlay Network over Internet Communication (CYPHONIC) [3]. CYPHONIC offers a streamlined solution to enhance direct device-to-device communication within P2P frameworks while incorporating robust zero-trust security measures.

Traditionally, the integration of CYPHONIC required the installation of a client program on all end devices, presenting a significant adoption barrier. This requirement posed challenges for devices like the Internet of Things (IoT), embedded systems, and dedicated service servers, which tend to resist additional program installations due to resource constraints and concerns about system reliability. To address this challenge, we introduce the innovative concept of the CYPHONIC adapter [4]. This adapter is a gateway device, enabling general nodes to seamlessly harness CYPHONIC's capabilities without requiring extensive modifications.

This paper primarily focuses on showcasing the practical application of our solution in the context of remote camera monitoring. Specifically, we aim to demonstrate how CYPHONIC clients, including general nodes and surveillance cameras, can seamlessly communicate over our overlay network. This demonstration emphasizes how our solution effectively addresses the network-related challenges associated with P2P models, enabling secure and efficient interconnections among diverse end devices.

II. CYPHONIC

Fig. 1 presents an overview of CYPHONIC, which facilitates secure and efficient communication among networked devices. CYPHONIC addresses the need for enhanced connectivity by seamlessly bridging the gap between IPv4 and IPv6 communication protocols while gracefully handling NAPT

traversal. This innovative solution offers a robust framework for device interconnection. Furthermore, it leverages zero-trust security principles and encryption techniques to ensure the utmost security for all networked devices.

CYPHONIC's architecture comprises three essential cloud services: the Authentication Service (AS), the Node Management Service (NMS), and the Tunnel Relay Service (TRS). These services collectively manage device authentication, configuration, and protocol-specific IP datagram conversion. Alongside these cloud services, CYPHONIC nodes, equipped with CYPHONIC client programs, form the solution's core. To cater to the diverse landscape of networked devices, we introduce the CYPHONIC adapter, a vital component specifically tailored to support general nodes, which may face challenges installing the client program.

Each CYPHONIC node has a unique, Fully Qualified Domain Name (FQDN) for precise identification and a virtual IP address for overlay network communication. The client program within these nodes retrieves application data, generates virtual IP packets through an internal virtual interface, and secures these packets via encryption using pre-shared keys. This process establishes User Datagram Protocol (UDP) tunneling on the physical network, enabling seamless communication.

The CYPHONIC adapter serves as an intermediary, intercepting application data from general nodes through physical interfaces and effectively handling the functions delegated by the CYPHONIC client program. It assumes the responsibility of managing FQDNs and virtual IP addresses for general nodes. General nodes can effortlessly harness the secure communication services of CYPHONIC by establishing direct connections with the CYPHONIC adapter.

III. Demonstration

Through our innovative overlay network, this paper showcases the practicality and value of the CYPHONIC adapter in facilitating P2P communication among client devices, including CYPHONIC nodes and general nodes. CYPHONIC ensures transparent application communication, connecting devices seamlessly, even when behind NAPT or operating with different IP versions.

We provide a concise demonstration overview in Fig. 2. Two general nodes utilizing IPv4 are connected to the CYPHONIC adapter. Each general node runs an HTTP Live Streaming (HLS) application responsible for streaming camera images. On the other side, peer CYPHONIC nodes on various IPv4 and IPv6 networks subscribe to the streaming feeds from the general nodes.

The magic of the CYPHONIC adapter lies in its ability to bridge the IP version disparities within the real network seamlessly. As a result, both CYPHONIC nodes can effortlessly access the general node, offering a hassle-free and straightforward communication experience. Through a collaborative effort between the CYPHONIC node and the CYPHONIC adapter, application data is efficiently forwarded into our overlay network. This abstraction effectively shields the intricacies of the real-world network environment from the applications

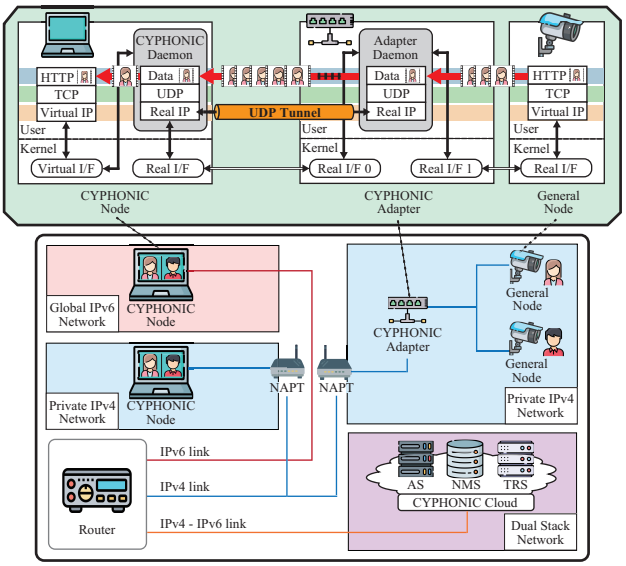


Fig. 2. Overview of demonstration scheme

running on end devices. Our demonstration perfectly illustrates how CYPHONIC enables seamless communication of nodes across diverse networks.

IV. Conclusions

CYPHONIC's innovative approach enhanced device-to-device communication while incorporating robust zero-trust security measures. Introducing the CYPHONIC adapter bridged the gap for conventional devices, removing the need for extensive modifications. The demonstration underscored the seamless interconnectivity of CYPHONIC clients, including general nodes and surveillance cameras. By resolving network issues associated with P2P models, our solution paved the way for secure and efficient connections among diverse end devices.

Acknowledgment

This work is supported in part by Grant-in-Aid for Scientific Research (C)(21K11877), the Japan Society for the Promotion of Science (JSPS), the Cooperative Research Project of the Research Institute of Electrical Communication, Tohoku University, and the collaborative research project with Ultimatrust Co., Ltd., Japan, and AIM Japan.

References

[1] A. Alhussain, H. Kurdi, and L. Altoaimy, "Managing Trust and Detecting Malicious Groups in Peer-to-Peer IoT Networks," Sensors, 10.3390/s21134484, June 2021.

[2] B. M. Kamel, P. Ligeti, A. Nagy, and C. Reich, "Distributed Address Table (DAT): A Decentralized Model for End-to-End Communication in IoT," Peer-to-Peer Networking and Applications, 10.1007/s12083-021-01221-3, January 2022.

[3] 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 International Conference on Consumer Electronics (ICCE), 10.1109/ICCE53296.2022.9730323, January 2022.

[4] R. Goto, T. Yoshikawa, H. Komura, K. Matama, C. Nishiwaki, and K. Naito, "Design and Basic Evaluation of Virtual IPv4-based CYPHONIC adapter," Journal of Systemics, Cybernetics and Informatics (JSCI), 10.54808/JSCI.20.03.55, October 2022.