Secure Optical Transport Network

Tetsuya Okuda, Koji Chida, Daisuke Shirai, Sakae Chikara, Tsunekazu Saito, Misato Nakabayashi, Kazuki Yamamura, Yuri Tanaka, Katsuyuki Natsukawa, and Koichi Takasugi

Abstract

The implementation of an optical transport network, especially between datacenters, has been progressing. Similar to the Internet, communications on the optical transport network are protected by public-key cryptography and symmetric-key cryptography, but there are concerns that advances in the research and development of quantum computers will pose a risk to current cryptographic systems, public-key cryptography and key exchange in particular. In response to this problem, researchers at NTT Social Informatics Laboratories and NTT Network Innovation Laboratories are engaged in the research and development of safe key-exchange schemes to counter the cryptographic risks posed by quantum computers. They are also engaged in architecture design and tests with actual equipment with the aim of applying such key-exchange schemes to the optical transport network.

Keywords: optical transport network, quantum key distribution, post-quantum cryptography

1. Background

1.1 What does "transport" mean?

"Transport" is often defined as "carrying" (as in physical distribution) or "transmission" (as in communications). In other words, it generally refers to corporate distribution and transport services and to communication and transmission services. To make it easy to imagine the features of a secure optical transport network as a technology affixed with the label "transport," we begin our discussion using distribution and transport services as an example (**Fig. 1**).

What are the features of distribution and transport services by truck? Various images may come to mind, such as the carrying of many goods at one time and the prompt delivery of goods after orders are placed. We take up such features from the five viewpoints listed in **Table 1**.

First, in distribution and transport services, large capacity and low delay are features that are most important to customers and that give value to these services. Large capacity means a large number of trucks and low delay means short truck queuing time. From the viewpoint of running a distribution and transport business, efficient operations are essential, which can be expressed as the optimization of distribution and the economical management of daily operations. Many questions are now being asked about the social impact of services, so concerns about environmental load and safety have also become service features. Environmental load means low levels of exhaust gas/carbon dioxide (CO_2) and safety means correct delivery of goods and few traffic accidents.

What do these features mean in communication and transmission services? Large capacity and low delay are also the features that are the most important to customers and that give value to these services. Using terms from the field of communications, large capacity means high throughput and low delay means low latency. From the viewpoint of running a communication and transmission enterprise, efficient operations are likewise essential, which can be expressed as network efficiency in providing communication and transmission services. Finally, it is also true in the communications industry that the social impact of

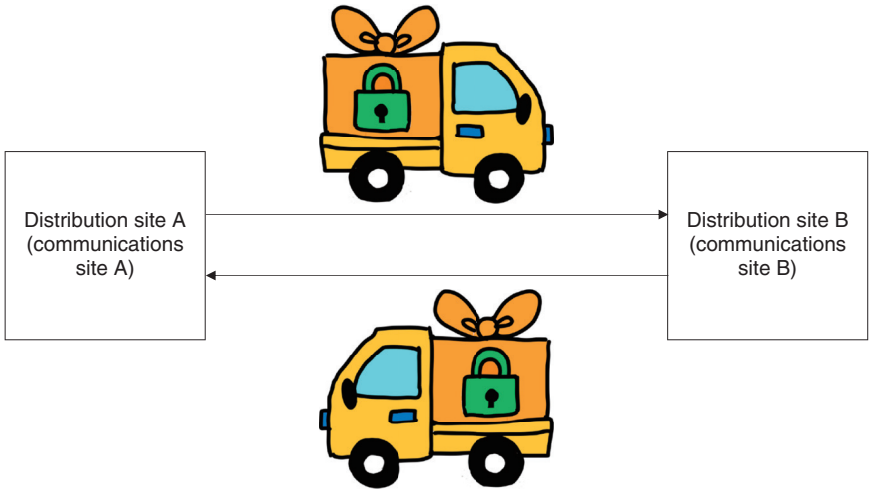


Fig. 1. What does “transport” mean?

Table 1. Comparison of distribution/transport and communication/transmission services.

Service features	Distribution/transport services	Communication/transmission services
Large capacity	Number of trucks	Throughput
Low delay	Truck queuing time	Latency
Efficient operations	Distribution optimization	Communication network optimization
Environmental load	Exhaust gas/CO_2	Power consumption
Safety	Correct delivery of goods Few traffic accidents	Few communication failures High level of security

services has come under the spotlight, so environmental load and safety have also become of concern. In this industry, environmental load means low power consumption and safety means few network failures and a high level of security.

Among the five viewpoints listed in Table 1, the Innovative Optical and Wireless Network (IOWN) and All-Photonics Network (APN) under research and development at NTT aim for services that take into account the three points of large capacity, low delay, and low environmental load that appeal most to customers [1]. The first step in adding the viewpoint of “safety = security” to IOWN/APN is the secure optical transport network proposed in this article.

1.2 Necessity of an optical transport network

Many people have come to appreciate how their lives have become more convenient thanks to the proliferation of mobile phones and smartphones and the expansion of the large-capacity and low-latency fifth-generation mobile communications system (5G). Large capacity and low latency are also desirable features in communication and transmission services targeting corporate customers. Customer needs have come to focus on datacenter interconnect services envisioning the need for datacenter disaster recovery as well as on uncompressed video transmission services for remote production to enable simultaneous and parallel work between a video production site in the field and an editing site. Transmitting such large-capacity data with low latency in real time to the extent possible requires the application of optical transport [2]. This article introduces our efforts in adding security to optical transport.

2. Current technologies

2.1 Internet standards

To add security to communication and transmission services, we can expect the application of current technologies used on the Internet to be effective and to mature in terms of evaluating security the longer

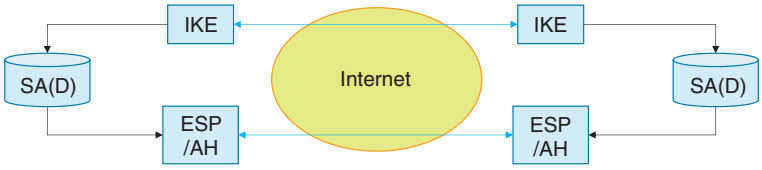


Fig. 2. IPsec architecture.

they stay in use.

On the Internet, Secure Sockets Layer/Transport Layer Security (SSL/TLS) and Security Architecture for Internet Protocol (IPsec) are typical protocols used for configuring safe communication paths (secure channels). SSL/TLS is a standard protocol for configuring a secure channel between a web server and client. IPsec is a standard protocol for configuring secure channels between sites such as between a company's main office and its branch offices. It is a technology used in virtual private network services. The secure optical transport network introduced in this article is a communication and transmission service operating between sites.

2.2 IPsec

IPsec for configuring a secure channel between sites is specified by the Internet Engineering Task Force (IETF), an organization that formulates de facto Internet standards. The IPsec specifications are organized into architecture, encryption, authentication, and key exchange [3].

IPsec's architecture features the following mechanisms: Internet key exchange (IKE) that exchanges keys, encapsulated security payload (ESP) that performs encryption and authentication, authentication header (AH) that performs authentication, and security association database (SAD) that conveys the keys agreed upon in IKE via ESP or AH (**Fig. 2**). "Authentication" includes message authentication and entity authentication, which test the validity of a message delivered from a communication destination and that of the communication destination, respectively.

Next, we discuss how this IPsec configuration might change in a secure optical transport network.

3. Issues and proposals (I): Possibility of advances in quantum computers

3.1 Possibility of advances in quantum computers

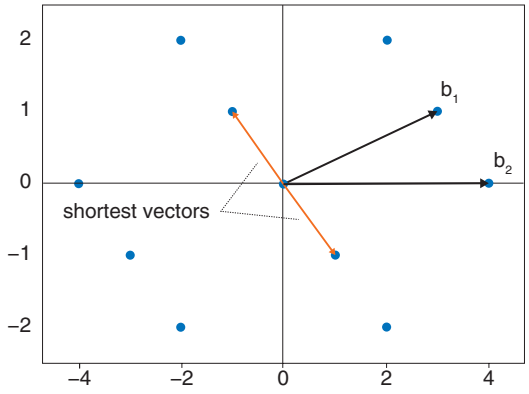
Current communications on the Internet and other networks use key exchange based on public-key cryptography, which uses a problem that is difficult to solve mathematically as a basis for ensuring security. For example, the Rivest-Shamir-Adleman (RSA) cryptosystem uses the fact that factoring the product of two large prime numbers takes an extremely long amount of time as a basis for security. However, if a genuine quantum computer having error resilience could be achieved, factoring the product of two large prime numbers could be performed in a relatively short time. If so, the RSA cryptosystem could no longer be called secure. To solve this problem, we have been researching and developing a key-exchange scheme that cannot be broken by a quantum computer.

3.2 Quantum key distribution

Quantum key distribution (QKD) is a mechanism for distributing keys by quantum physics. It shares information on a secret key via quantum states on a quantum channel that can transmit quantum states. The most outstanding feature of QKD is the ability to detect eavesdropping by a third party when sharing the secret key. This originates in a property unique to quantum mechanics that measuring a quantum state changes the state. If a third party is attempting to eavesdrop, that is, to carry out measurements while two parties are sending and receiving a quantum state, the sent quantum state and received quantum state will differ. Consequently, if the two parties should then check with each other on their sent and received states and find that they differ, they would be able to detect that a third party is eavesdropping. Performing this process of sending/receiving quantum states and checking for eavesdropping repeatedly increases accuracy and eventually enables the two parties to share a secret key.

3.3 Post-quantum cryptography-based key distribution

Post-quantum cryptography (PQC) is a public-key-cryptography and key-distribution mechanism in which problems that are mathematically difficult to



Two-dimensional lattice vectors (blue points) generated by basis vectors {b_1, b_2} = {(3, 1), (4, 0)}. The shortest vectors in this lattice are (1, -1) and (-1, 1). The shortest vector problem—a major lattice problem—consists of finding the shortest vectors when given basis vectors {b_1, b_2}.

Fig. 3. Example of a lattice problem difficult for quantum computers.

solve provide a basis for security. In particular, problems that are assumed to be difficult even for a quantum computer to solve are used as grounds for security. In lattice-based cryptography, for example, it is assumed that finding the lattice points closest to the origin in a given set of lattice points is a difficult problem to solve even for a quantum computer, thereby providing a basis for security.

At NTT, research and development in this area is centered about NTRU, a type of PQC lattice-based cryptography incorporated in technology developed by a team including NTT (**Fig. 3**).

We generically refer to QKD and PQC-based key distribution (PQKD) as xKD.

4. Issues and proposals (II): Countermeasures against new attackers in architecture design

4.1 Countermeasures against attackers in a zero trust network

Designs that envision attackers in a zero trust network, which, as the name indicates, is a closed network that cannot be trusted [4] have become widespread. In this architecture design, it is necessary to assume attackers on all types of networks including telecommunications carrier networks and intra-site networks. In a telecommunications carrier network, it is assumed that an attacker will be intercepting communications by physically connecting to optical fiber, while in an intra-site network, it is assumed that an attacker intercepting communications has access rights in that network.

We first consider an attacker attempting to intercept communications by physically connecting to optical fiber in a telecommunications carrier network. A defense can be mounted through *hop-by-hop encryption* such as OTNsec, a protocol that protects Layer 1 (physical layer), and MACsec, a protocol that protects Layer 2 (data link layer). Implementing encryption functions in lower layers in this manner should enable the addition of security without hindering the low-latency feature of IOWN/APN.

Next, to defend against an attacker who is attempting to intercept communications within an intra-site network while having access rights in that network, architecture design for inter-site communications typified by IPsec must be reviewed from the bottom up. In the secure optical transport network, key exchange equivalent to IPsec/IKE described above will correspond to xKD equipment, and encryption equivalent to ESP/AH in IPsec will correspond to an optical transponder or white-box switch. Given the trend toward a disaggregated architecture described later, it must be assumed that separate devices will perform key exchange and transmission and that the key exchange and encryption functions that were integrated in IPsec will take on a separated configuration (**Figs. 4**, **5**, and **6**). As a result, key information corresponding to SA(D) in IPsec will circulate in a network external to the device, which means that new measures

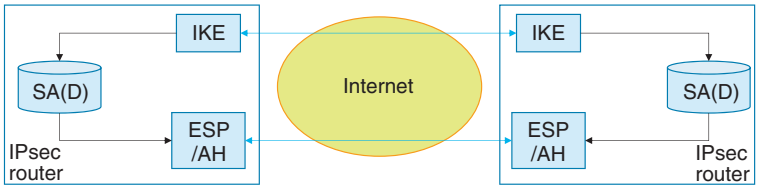


Fig. 4. Ordinary IPsec equipment configuration.

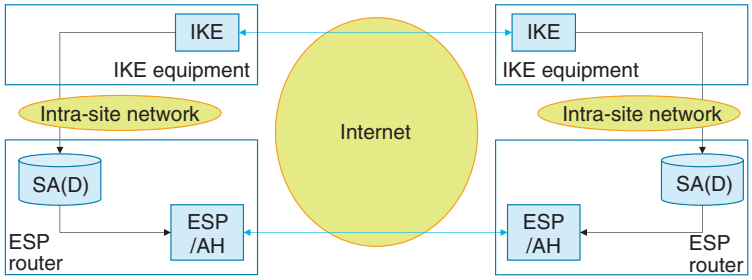


Fig. 5. Configuration with IPsec equipment separated.

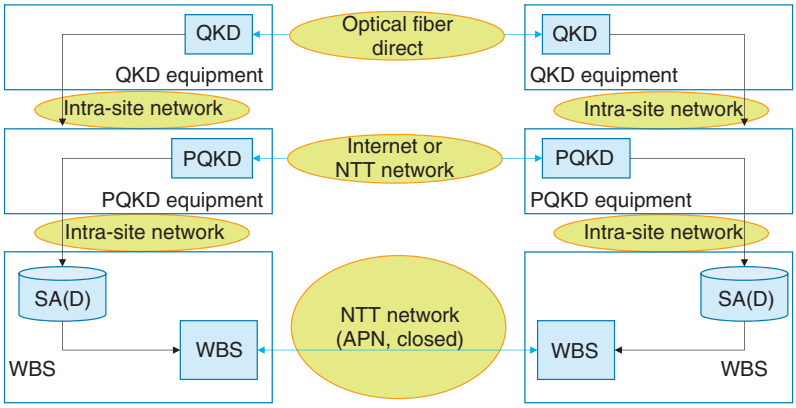


Fig. 6. Configuration with equipment of secure optical transport network separated.

must be studied for protecting communications on any type of network assuming a zero trust network. Specifically, it will be necessary to design a secure method for key distribution from xKD equipment to the optical transponder and a secure method for equipment authentication between xKD equipment and the optical transponder. For details on these studies, the reader is asked to consult a previously published paper [5].

4.2 Necessity of architecture and equipment that can be tested from the outside

In a zero trust network, the ability to test the reliability of architecture, protocol, equipment, etc. from the outside is required. The ability to make updates separately to architecture, protocol, equipment, etc. is also required as a fundamental security measure in anticipation of some type of danger. For architecture design, protocol design, and equipment selection described in this article, we adopted formal verification

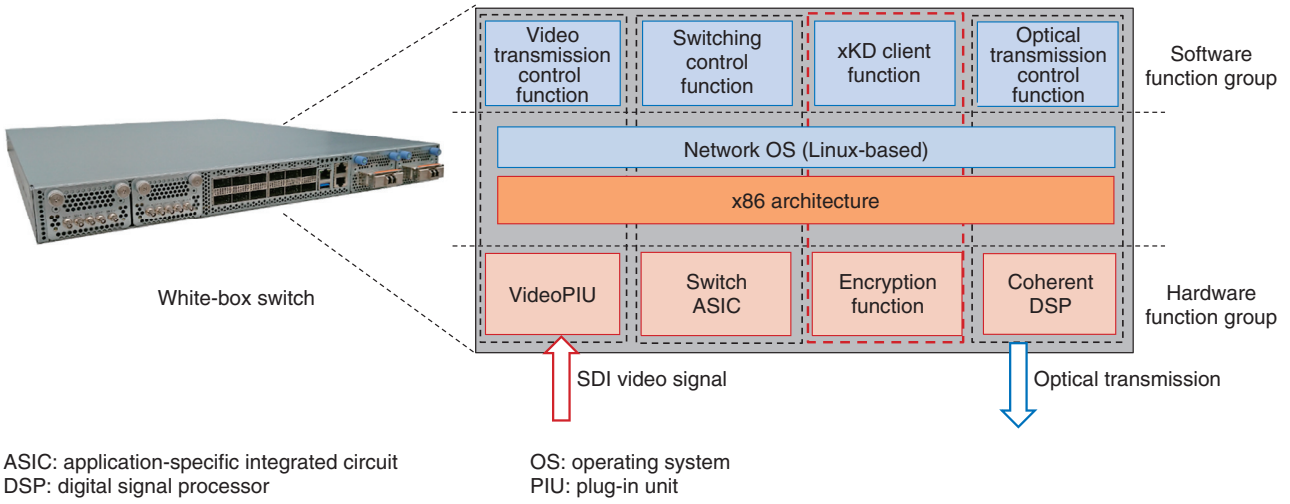


Fig. 7. Disaggregated architecture of white-box switch.

and the white-box switch as technologies for testing reliability from the outside and making updates separately.

4.3 Formal verification

At the time of protocol design including cryptography, there is a need for testing that can mathematically guarantee security as in maintaining the confidentiality of secret information within a protocol and ensuring the integrity of messages. In this regard, formal verification technology has been used for testing the safety of protocols such as SSL/TLS and IPsec that serve as transport layers and for testing the safety of authentication protocol on the 5G standard. Formal verification is a technology that describes a system and the properties that the system must satisfy in a formal language and that tests whether the system is satisfying those properties on the basis of logical reasoning. In formal verification, there are many components that can be automated by computer, so this technology excels in testing results from the outside including checking for reproducibility and in adaptively retesting in the face of protocol updates. For the secure optical transport network introduced in this article, we designed an IPsec-based protocol that combines xKD equipment with an optical transponder and tested its security using the ProVerif formal verification tool [6].

4.4 White-box switch

Transmission equipment for optical-transport purposes had been provided in a form that integrated optical modules and various functions. In contrast, there is also equipment that adopts technology that enables flexible configuration changes, the addition of new functions, cost reductions, etc. by separating the various functions of the transmission equipment and controlling them by standardized interfaces in a disaggregated architecture. This equipment is called a white-box switch or white-box transponder. In our current research, we have taken a white-box switch and added an xKD client function for obtaining an encryption key from xKD equipment in the software function group in order to set the key and control the encryption function of the hardware function group (**Fig. 7**). We also added a function for directly inputting an SDI (serial digital interface) signal (video signal) and showed that uncompressed 8K60P video in excess of 40 Gbit/s could be securely transmitted with ultra-low latency using this function. Therefore, we have demonstrated the feasibility of secure optical transport linking xKD equipment and optical transponders.

5. Toward the future

In this article, we introduced a secure optical transport network as an initiative to add security functions to IOWN/APN now being researched and developed at NTT. We also introduced key issues and proposals in relation to this initiative. We consider our efforts to be one step in our ongoing plan to contribute to the provision of safe and secure technologies and services.

References

[1] Website of NTT R&D, IOWN, https://www.rd.ntt/e/iown/

[2] M. Tomizawa, A. Kaneko, and S. Kimura, "Device Technology Development for Beyond 100G Optical Transport Network," NTT Technical Review, Vol. 14, No. 9, 2016. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201609fa1.html

[3] IETF, "Security Architecture for the Internet Protocol," RFC 4301, https://datatracker.ietf.org/doc/rfc4301/
IETF, "Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 7296, https://datatracker.ietf.org/doc/rfc7296/
IETF, "IP Encapsulating Security Payload (ESP)," RFC 4303, https://datatracker.ietf.org/doc/rfc4303/
IETF, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," RFC 6071, https://datatracker.ietf.org/doc/rfc6071/

[4] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST SP 800-207, Aug. 2020.

[5] S. Maeda, M. Nakabayashi, and T. Okuda, "Architecture Design and Security Evaluation with Formal Verification for Secure Optical Transport Network," 95th Conference of the Special Interest Group on Computer Security (IPSJ-CSEC), Nov. 2021.

[6] B. Blanchet, "Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif," Foundations of Security Analysis and Design VII, pp. 54–87, Springer, 2013.

Tetsuya Okuda
Research Engineer, NTT Social Informatics Laboratories.
He received a B.S. and M.S. from the University of Tokyo in 2009 and 2011. Since 2011, he has been engaged in research & engineering on security protocol at NTT. He is a member of Information Processing Society of Japan (IPSJ). He received the IPSJ/Computer Security Symposium Student Paper Award in 2019.

Koji Chida
Senior Research Engineer, Supervisor, NTT Social Informatics Laboratories.
He received a B.S., M.S., and Dr.Eng. from Waseda University, Tokyo, in 1998, 2000, and 2006. Since 2000, he has been engaged in research on cryptography and privacy-enhancing technologies at NTT. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and IPSJ. He received the IPSJ Best Paper Award in 2012.

Daisuke Shirai
Senior Research Engineer, Supervisor, Frontier Communication Laboratory, NTT Network Innovation Laboratories.
He received a B.E. in electronic engineering, M.E. in computer science, and Ph.D. in media design from Keio University, Kanagawa, in 1999, 2001, and 2014. He pioneered the world's first 4K JPEG 2000 codec system, which enables low latency 4K60p video transmission on a Gigabit network. He has applied his expertise across multiple domains through his study of practical applications in digital audio and video broadcasting technology, image coding, information theory, networking, human-computer interaction, and software architecture. His current research topics include remote video production network, ultra-low latency visual communication and its security over optical transport networks.

Sakae Chikara
Senior Research Engineer, Information Security Technology Research Project, NTT Social Informatics Laboratories.
He received a B.E. and M.E. in electrical and electronic engineering, system of electronic from Tokyo Institute of Technology in 1988 and 1990. He joined NTT Telecommunication Networks Laboratory in 1990 and studied network architecture, network management systems, and distributed computing systems. He also joined the projects of ITS (intelligent transport systems), development of cryptographic systems, and information security systems. His current interests are secure network systems, especially quantum computing systems, post quantum computing systems, and fiber optical network systems. He is a member of IEICE.

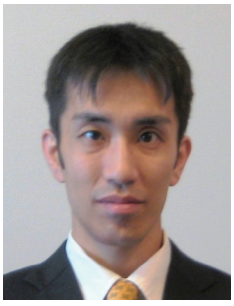
Tsunekazu Saito
Senior Research Engineer, NTT Social Informatics Laboratories.
He received a B.S. and M.S. from Waseda University, Tokyo, in 2006 and 2008 and Ph.D. in mathematics from Kyushu University, Fukuoka, in 2011. Since 2011, he has been engaged in research on elliptic curve cryptography and post-quantum cryptography at NTT.

Misato Nakabayashi
Information Security Technology Research Project, NTT Social Informatics Laboratories.
She received an M.Sc. from Tohoku University, Miyagi, in 2019 and joined NTT the same year. Her current research interest is in formal verification.

Kazuki Yamamura
Information Security Technology Research Project, NTT Social Informatics Laboratories.
He received an M.S. from Japan Advanced Institute of Science and Technology (JAIST), Ishikawa, in 2021. Since 2021, he has been engaged in research on cryptography at NTT.

Yuri Tanaka
NTT Social Informatics Laboratories.
She received a B.E. and M.E. from Keio University, Kanagawa, in 2019 and 2021. Since joining NTT Secure Platform Laboratories in 2020, she has been engaged in research on quantum security and computing. She is a member of the Physical Society of Japan.

Katsuyuki Natsukawa
Executive Research Engineer, Supervisor, NTT Social Informatics Laboratories.
He received an M.E. from Nara Institute of Science and Technology in 1996. He joined NTT the same year and is currently conducting R&D on data protection technologies centered on cryptography.



Koichi Takasugi
Executive Research Engineer, Director, Head of Frontier Communication Laboratory, NTT Network Innovation Laboratories.
He received a B.E. in computer science from Tokyo Institute of Technology, M.E. from JAIST, and Ph.D. in engineering from Waseda University, Tokyo, in 1995, 1998, and 2004. He was involved in the design and standardization of the Next Generation Network architecture. He has implemented and installed super high-density Wi-Fi systems in several football stadiums. He was also active in the artificial intelligence field, such as diagnosing diabetes by machine learning. He is currently leading research on the network architecture and protocols in optical and wireless transport networks.