

Cooperative Resource Management in Quantum Key Distribution (QKD) Networks for Semantic Communication

Rakpong Kaewpuang, Minrui Xu¹, Graduate Student Member, IEEE, Wei Yang Bryan Lim², Member, IEEE, Dusit Niyato³, Fellow, IEEE, Han Yu⁴, Senior Member, IEEE, Jiawen Kang⁵, Member, IEEE, and Xuemin Shen⁶, Fellow, IEEE

Abstract—The increasing focus on privacy and security in 6G networks, which are intelligence-native, necessitates the use of quantum key distribution-secured semantic information communication (QKD-SIC) to protect confidential data. In QKD-SIC systems, edge devices connected via quantum channels can efficiently encrypt semantic information from the semantic source, and securely transmit the encrypted semantic information to the semantic destination. In this article, we consider an efficient resource (i.e., quantum key distribution (QKD) and KM wavelengths) sharing problem to support QKD-SIC systems under the uncertainty of semantic information generated by edge devices. In such a system, QKD service providers offer QKD services with different subscription options to the edge devices. The QKD services are envisioned to follow cloud computing that has the subscription in the reservation and on-demand options, i.e., for long and short (immediate) terms, respectively. As such, to reduce the cost for the edge device users, we propose a QKD resource management framework for the edge devices communicating semantic information. The framework is based on a two-stage stochastic optimization model to achieve optimal QKD deployment. Moreover, to reduce the deployment cost of QKD service providers, QKD resources in the proposed framework can be utilized based on efficient QKD-SIC resource management, including semantic information transmission among edge devices, secret-key provisioning, and cooperation formation

among QKD service providers. In detail, the formulated two-stage stochastic optimization model can achieve the optimal QKD-SIC resource deployment while meeting the secret-key requirements for semantic information transmission of edge devices. Moreover, to share the cost of the QKD resource pool among cooperative QKD service providers forming a coalition in a fair and interpretable manner, the proposed framework leverages the concept of Shapley value from cooperative game theory as a solution. Experimental results demonstrate that the proposed framework can reduce the deployment cost by about 40% compared with existing noncooperative baselines.

Index Terms—Cooperative resource management (CRM), game theory, quantum key distribution (QKD), semantic information communication (SIC), stochastic programming (SP).

I. INTRODUCTION

AS QUANTUM computers become a distinct possibility, they pose new potent threats to the traditional cryptographic security schemes. This has led to a revolution in the use of quantum channels for secret key distribution, i.e., quantum key distribution (QKD), for the transmission of confidential information [1], [2], [3], [4]. With the parallel processing of quantum computing, quantum computers can easily break the process of key exchanging in modern symmetric cryptography [5]. Fortunately, quantum channels based on the laws of quantum mechanics, such as Heisenberg's uncertainty principle and the no-cloning theorem, can perform data transmission, including symmetric key distribution, with provable security. In addition, QKD can enable information-theoretic security (ITS) for data transmission in classical data channels via the one-time pad (OTP) mechanism [6]. In intelligence-native 6G communications [7], security and privacy are critical requirements in distributed artificial intelligence (AI) training. In particular, the transmission of essential feature information in semantic communication makes 6G communications more demanding for security and privacy in semantic information communication (SIC) and networking.

SIC [8], [9], [10] refers to communication paradigms based on the concept of semantic-meaning transmission. SIC is a practical application of AI models for exchanging meaningful information obtained from transmission data with a minimum of communication resources. The main goal of semantic communication is to extract the meanings or features of the transmitted

Manuscript received 22 September 2022; revised 4 January 2023; accepted 22 July 2023. Date of publication 3 August 2023; date of current version 24 January 2024. This work was supported in part by NSFC under Grant 62102099; in part by the Pearl River Talent Recruitment Program under Grant 2021QN02S643; in part by the Guangzhou Basic Research Program under Grant 2023A04J1699; in part by the National Research Foundation, Singapore; in part by the Infocomm Media Development Authority under its Future Communications Research and Development Programme; in part by the DSO National Laboratories under the AI Singapore Programme (AISG) under Award AISG2-RP-2020-019; in part by the Energy Research Test-Bed and Industry Partnership Funding Initiative, Energy Grid (EG) 2.0 Programme; in part by the DesCartes and the Campus for Research Excellence and Technological Enterprise (CREATE) Programme; in part by the MOE Tier 1 under Grant RG87/22; in part by the Alibaba Group through Alibaba Innovative Research (AIR) Program and Alibaba-NTU Singapore Joint Research Institute (JRI); and in part by the Nanyang Technological University, Nanyang Assistant Professorship. (Corresponding author: Jiawen Kang.)

Rakpong Kaewpuang, Minrui Xu, Wei Yang Bryan Lim, Dusit Niyato, and Han Yu are with the School of Computer Science and Engineering, Nanyang Technological University, Singapore (e-mail: rakpong.kaewpuang@ntu.edu.sg; minrui001@e.ntu.edu.sg; bryan.limwy@ntu.edu.sg; dniyato@ntu.edu.sg; han.yu@ntu.edu.sg).

Jiawen Kang is with the School of Automation, Guangdong University of Technology, Guangzhou 510006, China (e-mail: kavinkang@gdut.edu.cn).

Xuemin Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: sshen@uwaterloo.ca).

Digital Object Identifier 10.1109/IJOT.2023.3301033

data (i.e., semantic information) from a semantic source and transmit the semantic information to a semantic destination, where it can be interpreted successfully. In the semantic communication system, we can consider that the semantic source and destination are semantic providers who execute intelligent algorithms (e.g., knowledge graphs and deep neural networks) autonomously. They can be edge devices or sensors with cognitive capabilities. In such a knowledge-based system, the semantic source and destination can establish and utilize their background knowledge bases (KBs) through online or offline training and inference. The KBs are typical models that the semantic source and destination can learn and validate in advance. For example, images, speeches, videos and texts are representative KBs. The semantic source uses an individual KB to extract the semantic information of the raw data, which is then transmitted to the semantic destination. When the semantic destination receives the semantic information, it uses its individual KB to interpret them.

Nevertheless, SIC provides a viable and intelligent way to exchange semantic information between the semantic source and the semantic destination. Regarding security, SIC faces confidentiality issues due to the eavesdropping risk in exchanging semantic information between the semantic source and the semantic target [11], [12], [13]. To ensure that the transmission of semantic information is secure, QKD is a promising mechanism to protect public keys from eavesdropping attacks.

To address the aforementioned issues, we propose a QKD-secured SIC (QKD-SIC) system to protect the semantic information and public keys from eavesdropping attacks. We consider the resource management problem that the secret keys are allocated to support the semantic information of edge devices in SIC. In addition, we consider that the amount of semantic information generated by edge devices is unpredictable. To optimize QKD resources when the amount of semantic information is unpredictable, QKD service providers can cooperate and establish a global resource pool. In particular, multiple QKD service providers can share their resources (i.e., QKD and key management (KM) wavelengths) in the pool. Therefore, the resources in the pool can be efficiently utilized by the QKD service providers. Nevertheless, three important questions arise in the context of this resource management.

- 1) What is an optimal resource allocation in the pool of SIC applications to minimize costs and satisfy the needs of edge devices?
- 2) How can the costs incurred by the resource pool be shared among cooperative QKD service providers?
- 3) Should QKD service providers cooperate or not in creating the resource pool?

To answer these questions for QKD service providers, we introduce a decision-making scheme with the components of resource allocation to SIC applications, cost management, and collaboration among QKD service providers in a QKD-SIC environment. The goal of the scheme is to make the best decisions for QKD service providers as they are rational and interested in minimizing their own costs. The main contributions of this article can be summarized as follows.

- 1) We introduce a hierarchical architecture for the QKD-SIC system, where resource allocation and routing decisions are coupled. To provide sufficient secret keys for semantic information transmission between virtual service providers (VSPs) and edge devices, the QKD network manager and controller allocate QKD resources (i.e., QKD and KM wavelengths) from QKD nodes and determine routing paths for QKD links.
- 2) We formulate and solve the stochastic programming (SP) model to obtain the optimal resource allocation decisions from a resource pool created by QKD service providers. The SP model requires the probability distributions of the random parameters, i.e., the secret-key rate (user demand) requirements. This model can be applied for the cooperative QKD service providers to make decisions in two stages. In the first stage, the QKD service providers make a resource reservation decision (i.e., QKD and KM wavelengths) based on the statistical information about users' demand. In the second stage, when QKD service providers know the exact level of users' demand, they make a decision to compensate for users' demand that cannot be satisfied when resources are insufficient.
- 3) We present a model to allocate the provisioning cost obtained from the resource pool among QKD service providers in a fair manner. In addition, we leverage Shapley values to determine fair and interpretable allocation of provisioning costs.
- 4) We introduce a cooperative game model for QKD service providers to decide whether they should cooperate and establish the resource pool or not. A stable cooperation strategy is the solution of the game model, which means that the rational QKD service providers do not want to change their decisions.

The remainder of this article is organized as follows. Section II presents related work. Section III describes the system model, the maritime case study, and the cost models. Section IV presents the SP model for resource allocation in QKD-SIC for a maritime application. Section V presents cost management model among QKD service providers. Section VI presents the cooperative game models for optimal cooperation formation for QKD service providers. Section VII presents the performance evaluation results. Section VIII concludes this article.

II. RELATED WORK

A. Semantic Information Communication

SIC significantly reduces the need for transmission resources, such as channels, by using AI to extract semantic features for the information between source and destination [14], [15]. Ng et al. [16] proposed an SIC in the metaverse between edge devices and the VSPs to reduce the size of transmitted data. In SIC, an edge device (e.g., a smartphone) can autonomously produce pictures (presemantic data) relevant to the interest of VSPs. The VSP can subscribe to edge devices that the VSP is interested in transmitting the semantic data to create the metaverse for supporting user

requests, where the user requests are considered as uncertainty. In [16], the stochastic semantic transmission scheme was proposed to minimize the transmission cost of VSPs. This scheme was formulated as a two-stage stochastic integer programming model under the uncertainty of user requests to achieve an optimal solution. The resource allocation for text SIC was proposed in [17] to maximize the overall semantic spectral efficiency in terms of channel utilization and the number of transmitted semantic symbols of all users. The deep learning-enabled SIC system for speech signals (DeepSC-S) was proposed in [18] to enhance the recovery accuracy of speech signals. Particularly, the joint semantic-channel coding was proposed to solve source distortions and channel effects. The squeeze-and-excitation network was employed in the proposed DeepSC-S to learn and extract speech semantic information. Xu et al. [19] provided a comprehensive overview of practical distributed edge learning (EL) techniques and introduced the interplay between EL and advanced communication optimization designs. The authors also provided the dual-functional performance metrics for learning and communication. In addition, the authors emphasized the potential benefits of learning-based communication systems (e.g., distributed goal-oriented semantic communication) and the necessity of resource allocation optimization for EL systems. Chen et al. [20] proposed a joint federated learning (FL) and wireless communication framework. In the proposed framework, the authors formulated the joint optimization problem that considers the resource allocation and user selection of FL to minimize the value of the FL loss function while satisfying the delay and energy consumption demands. To solve this problem, the authors derived a closed-form expression for the expected convergence rate of the FL algorithm under wireless medium constraints.

However, current SIC systems only leverage AI models to transmit necessary semantic information between the source encoder and the destination decoder, while the security issues in SIC systems are largely overlooked.

B. Quantum Internet

With the ability to provide ITS for communications, QKD and QKD-secured systems are expected to protect various 6G communications, such as optical, satellite, maritime, and their cross-layer communications [7], [21], [22]. Unlike traditional QKD protocols, such as Bennett-Brassard-1984 (BB84) [23], Bennett-Brassard-Mermin-1992 (BBM92) [1], and Grosshans-Grangier-2002 (GG02) [1], modern QKD protocols based on MDI technology can provide longer distribution distance and stronger security without assuming trusted relays [24]. To minimize the cost of deploying QKD resources in MDI-QKD, Cao et al. [25] proposed a static linear programming model and the CO-QBN algorithm to efficiently manage QKD networks. Kaewpuang et al. [26] proposed the resource allocation scheme for quantum-secured space-air-ground integrated networks (SAGINs) in which QKD services protect secure communications between space, aerial, and ground nodes by exchanging secret keys in quantum channels. Kaewpuang et al. [26] formulated and solved the SP model to achieve the optimal solution

for resource allocation (i.e., QKD and KM wavelengths) and routing under the uncertainties of secret-key rate requirements and weather conditions.

Xu et al. [12] proposed the QKD-based secure FL scheme to support the FL model encryption against eavesdropping attacks on FL networks. Particularly, the resource allocation scheme for QKD resources (i.e., wavelengths) to support FL networks was proposed to minimize the overall deployment cost under the uncertainty of the number of FL workers associated with the secret-key rate requirements. The concept of QKD over SAGIN was proposed to achieve secure communications with global coverage and reconfigurable since QKD over SAGIN are supplementary options to alleviate the limitation in the distance of the optical fiber-based QKD [22], [27]. Xu et al. [22] proposed the QKD service provisioning framework to establish secure communications in quantum-secured SAGIN. The two-stage SP was formulated to minimize the provisioning cost under the uncertainty of secret-key rates. Kaewpuang et al. [13] proposed the hierarchical architecture for QKD-secured FL systems. In [13], the QKD resource management was formulated, which is based on the two-stage SP, to minimize the deployment cost under the uncertainty of the secret-key rate requirements from FL applications.

C. Game-Based Resource Allocation

Güler et al. [28] proposed a game-based resource allocation framework for SIC system, where the semantic content of a message to be transmitted over a noisy channel was taken into consideration to optimize the performance of a communication system. In addition, the impact of social influence on how the messages were translated by considering the influence of the agent in the communication network. The agent had an influence on the receiver, i.e., how to decode the received messages by providing side information. The influence of the agent can be adversarial or helpful to the communicating parties. Therefore, the authors considered the SIC problem with social influence as a Bayesian game with incomplete information and investigated the conditions under which a Bayesian Nash equilibrium exists.

Nevertheless, the existing works in the literature do not consider the uncertainty of secret-key requirements from SIC. In addition, the works in the literature do not consider the problem of optimizing the resource allocation to semantic applications, cost management, and cooperation formation for QKD service providers under uncertainty.

III. SYSTEM MODEL AND CASE STUDY

We list the abbreviations and their definitions used in this article in Table I. We propose a three-layer QKD-SIC architecture illustrated in Fig. 1. The architecture consists of the QKD layer, the QKD management and control layer, and the semantic layer. In the QKD layer, there are three types of nodes and two types of links. The three types of nodes are QKD nodes, trusted relays, and untrusted relays. In QKD-SIC, there are KM links and QKD links. Each KM link consists of a classical channel that is a logical link implemented by one wavelength channel [R1]. Each QKD link consists of a classical channel

TABLE I
 LIST OF KEY ABBREVIATIONS

Abbreviations	Definitions
BB84	Bennett-Brassard-1984
BBM92	Bennett-Brassard-Mermin-1992
BERT	Bidirectional Encoder Representations from Transformers
CRM	Cooperative Resource Management
CO-QBN	Cost-Optimized QKD Backbone Networking
DeepSC-S	Deep learning-enabled SIC system for Speech signals
GG02	Grosshans-Grangier-2002
GKS	Global Key Server
ITS	Information-Theoretic Security
KB	Knowledge base
KM	Key Management
LKM	Local Key Manager
MDI	Measurement-Device-Independent
MDI-QRx	MDI-QKD Receiver
MDI-QTx	MDI-QKD Transmitter
MUX/DEMUX	Multiplexing/Demultiplexing
OTP	One-Time Pad
QKD	Quantum Key Distribution
SAGIN	Space-Air-Ground Integrated Networks
SI	Security Infrastructure
SIC	Semantic Information Communication
VSO	Virtual Service Operator
VSP	Virtual Service Provider

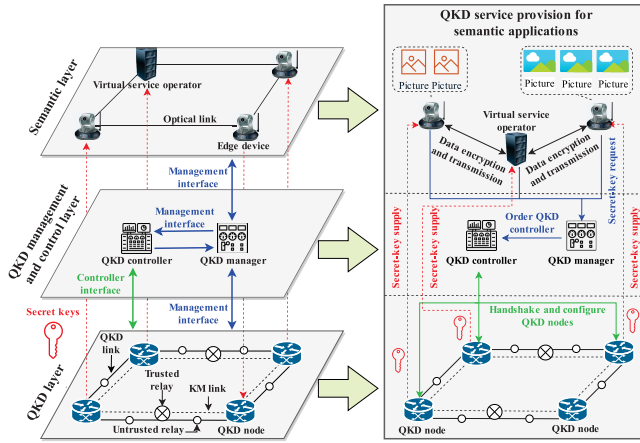


Fig. 1. QKD-SIC architecture.

and a quantum channel. The classical channel is a logical link that is implemented by two or more wavelength channels for synchronization, distillation, and so forth [R1]. In addition, the quantum channel is a physical link that is implemented by one wavelength channel for quantum information transmission [R1]. We consider that QKD nodes are co-located with SIC nodes, which can be edge servers or quantum secure end users. The links (i.e., QKD, KM, and optical links) are multiplexed within a single fiber by MUX/DEMUX components [R1]. Therefore, the network topology for the QKD layer is the same as that for the semantic layer. Hence, SIC nodes in the semantic layer can use KM and QKD links (i.e., classical and quantum channels) via the fiber for quantum-secured communications. Let \mathcal{N} and \mathcal{E} denote the set of SIC/QKD nodes and the set of fiber links between SIC/QKD nodes, respectively.

A QKD node supplies secret keys to its co-located SIC node. The trusted relay and the untrusted relay are located between the QKD nodes. The QKD node consists of a global key server (GKS), a local key manager (LKM), a security infrastructure (SI), and components of trusted/untrusted relays. A trusted

relay consists of two or multiple transmitters of MDI-QKD (MDI-QTx), LKM, and SI, while an untrusted relay consists of one or multiple receivers of MDI-QKD (MDI-Rxs). An MDI-QRx must be located between two MDI-QTx to generate local secret keys. An LKM is used to obtain and store the local secret keys from the connected MDI-QTx, and LKM performs secret key propagation via the OTP method [25] to generate global secret keys between QKD nodes. The SIs are applied to ensure that trusted relays work in a secure manner. In the QKD layer, the QKD links are used to connect between MDI-QTx and MDI-QRx, while the KM links are used to connect between LKMs. The QKD link contains quantum and classical channels, while the KM link contains a classical channel implemented by wavelengths.

In the semantic layer, an SIC node can be an edge device (e.g., a smartphone and surveillance camera) or a virtual service operator (VSO) (i.e., semantic receiver). Each edge device in different areas has different views for locations, as shown in Fig. 1. Edge devices can capture pictures and extract the corresponding semantic information (i.e., snapshots) from the pictures. Then, the edge device transmits the semantic information via the classical channel of optical fibers to the respective VSO, which uses this data to create the virtual environment for a particular application, for example, transportation and education. Before the semantic information transmission between the edge device and the VSO happens, the VSO has to subscribe to the respective edge devices.

When the VSO subscribes to the respective edge devices, the respective edge devices will request secret keys from the QKD manager based on their security requirements for encrypting their semantic information. When the QKD manager receives the request, the QKD manager responds by checking the available secret keys. Suppose the secret keys are available to support the request, and thus the QKD manager will order the QKD controller to select the suitable QKD nodes to provide the secret keys in a suitable format for semantic information encryption. If the secret keys are unavailable to support the request, the edge devices and the VSO will wait until the secret keys are available. Then, the edge devices encrypt the semantic information via the secret keys and transmit the encrypted semantic information to the semantic receiver. The amount of semantic information (i.e., snapshots) of each edge device directly depends on the available secret-key resources in the QKD layer as well as the security requests in the semantic layer. Therefore, it has a tradeoff between the QKD resources and the requests from edge devices.

A. Cooperation Among QKD Service Providers and Pooling of QKD Resources

To minimize the deployment costs, the QKD service providers can cooperate and establish a QKD resource pool that comprises QKD and KM wavelengths to support the security demand. The set of cooperative QKD service providers that agree to cooperate and establish the QKD resource pool is represented by \mathbb{C} . It could have many coalitions. Therefore, let $\Upsilon = \{\mathbb{C}_1, \mathbb{C}_2, \mathbb{C}_3, \dots, \mathbb{C}_{|\Upsilon|}\}$ denote a set of all coalitions (i.e., cooperation structure or coalitional structure) where

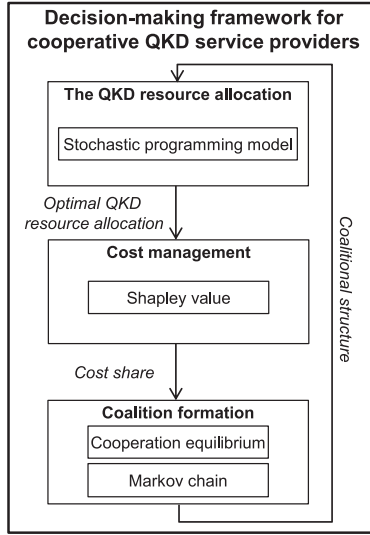


Fig. 2. Components of the decision-making framework for QKD service providers.

$\mathbb{C}_i \in \Upsilon$. Each coalition i (\mathbb{C}_i) has its own QKD resource pool that is created by the cooperative QKD service providers in the coalition i . Given a coalition \mathbb{C} , $W_{ij}^{\text{qkd}}(\mathbb{C})$ denotes available QKD wavelengths on the QKD link between SIC/QKD nodes i and j in the corresponding resource pool. $W_{ij}^{\text{km}}(\mathbb{C})$ denotes available KM wavelengths on the KM link between SIC/QKD nodes i and j in the corresponding resource pool. The cost generated from the QKD resource pool will be shared by all cooperative QKD service providers in the coalition.

With the collaboration among the QKD service providers, we introduce a framework that comprises three main components:

- 1) *QKD Resource Allocation for QKD Service Providers:* With cooperative QKD service providers, the objective of QKD resource allocation is to procure the optimal numbers of QKD and KM wavelengths while the deployment cost of the cooperative QKD service providers is minimized. Hence, we formulate an optimization problem based on SP. The probability distributions of random parameters in the SP model are taken into consideration.
- 2) *Cost Management:* Given a coalition of QKD service providers and the optimal QKD resource allocation, we apply the concept of Shapley value to obtain the share of deployment cost for each cooperative QKD service providers.
- 3) *Coalition Formation:* We analyze the stable cooperation strategy among QKD service providers by using the cooperation formation model. The dynamics of coalition formation are analyzed by Markov chain models.

The interactions among the three components are illustrated in Fig. 2. The coalition formation is first performed to achieve the coalition structure and then the coalition structure is applied by the QKD resource allocation. The optimal QKD resource allocation of the SP model is used by the cost management in which the Shapley value is applied to allocate the incurred deployment cost to QKD service providers. The

QKD service providers alter their coalition formation strategies accordingly when they obtain their costs.

B. Network Model

In the QKD-SIC model, let \mathcal{F} and $f(s_f, d_f, P_f(\cdot)) \in \mathcal{F}$ denote the set of QKD-SIC chain requests and a QKD-SIC chain request of SIC nodes, respectively. s_f and d_f are the source node and destination node of QKD-SIC chain request f , respectively. Let K_D denote the maximum achievable secret-key rate at a distance D . The number of parallel QKD-SIC links $P_f(\cdot)$ to satisfy the security demand (secret-key rate) of SIC transmission between s_f and d_f is expressed as follows:

$$P_f(\tilde{\omega}) = \left\lceil \frac{\tilde{k}_f}{K_D} \right\rceil \quad (1)$$

where f is the QKD-SIC chain request and \tilde{k}_f is a random variable of secret-key rate requirement of request f . D is a distance between two connected MDI-QTxS, which can be expressed as follows:

$$D \approx 2\phi \quad (2)$$

where ϕ is the distance between the MDI-QRx connecting to the MDI-QTx.

C. Cost Model

We adopt the costs of the QKD network components and the links from [25] to support the deployment of QKD with hybrid trusted/untrusted relays on the existing optical backbone network. The QKD network components include MDI-QTxS, MDI-QRxS, LKMs, SIs, and multiplexing/demultiplexing (MUX/DEMUX) components. The links include QKD links and KM links. The components and links can be described as follows.

1) *MDI-QTxS and MDI-QRxS:* The MDI-QKD process requires two MDI-QTxS and one MDI-QRx and therefore the number of MDI-QTxS ($A_{\text{tx}}^f(\cdot)$) and MDI-QRxS ($A_{\text{rx}}^f(\cdot)$), which satisfy the QKD-SIC chain request f , are expressed in (3) and (4), respectively

$$A_{\text{tx}}^f(\tilde{\omega}) = \sum_{i \in \mathcal{N}_f} \sum_{j \in \mathcal{N}_f} 2P_f(\tilde{\omega}) \left\lceil \frac{e_{(i,j)}}{D} \right\rceil \quad (3)$$

$$A_{\text{rx}}^f(\tilde{\omega}) = \sum_{i \in \mathcal{N}_f} \sum_{j \in \mathcal{N}_f} P_f(\tilde{\omega}) \left\lceil \frac{e_{(i,j)}}{D} \right\rceil. \quad (4)$$

$e_{(i,j)}$ is the distance of physical fiber link between nodes i and j . \mathcal{N}_f is set of nodes having the fiber links on the route of request f .

2) *Local Key Managers:* For the QKD-SIC chain request f , the required number of LKMs ($A_{\text{km}}^f(\cdot)$) is expressed as follows:

$$A_{\text{km}}^f = \sum_{i \in \mathcal{N}_f} \sum_{j \in \mathcal{N}_f} \left\lceil \frac{e_{(i,j)}}{D} + 1 \right\rceil. \quad (5)$$

3) *Security Infrastructures:* The required number of SIs ($A_{\text{si}}^f(\cdot)$) to satisfy the QKD-SIC chain request f is expressed as follows:

$$A_{\text{si}}^f = \sum_{i \in \mathcal{N}_f} \sum_{j \in \mathcal{N}_f} \left\lceil \frac{e_{(i,j)}}{D} - 1 \right\rceil. \quad (6)$$

4) *MUX/DEMUX Components*: The required number of MUX/DEMUX component pairs (A_{md}^f) for the QKD-SIC chain request f is expressed as follows:

$$A_{\text{md}}^f = \sum_{i \in \mathcal{N}_f} \sum_{j \in \mathcal{N}_f} \left\lceil \frac{e_{(i,j)}}{D} \right\rceil + \sum_{i \in \mathcal{N}_f} \sum_{j \in \mathcal{N}_f} \left\lceil \frac{e_{(i,j)}}{D} - 1 \right\rceil. \quad (7)$$

5) *QKD and KM Links*: Three wavelengths and one wavelength are occupied by the QKD link and the KM link, respectively [29]. The link cost for the QKD-SIC chain request f is expressed as follows:

$$A_{\text{ch}}^f(\tilde{\omega}) = \sum_{i \in \mathcal{N}_f} \sum_{j \in \mathcal{N}_f} (3P_f(\tilde{\omega})e_{(i,j)} + e_{(i,j)}) \quad (8)$$

where the physical lengths of QKD links and KM links are denoted by $3P_f(\tilde{\omega})e_{(i,j)}$ and $e_{(i,j)}$, respectively.

D. Cooperation Cost

We consider the cooperation cost of QKD service providers when the providers decide to share the resources (i.e., QKD and KM wavelengths) in the resource pool. The costs of QKD and KM wavelengths to be shared in the pool can be expressed in

$$C_s^{\text{qkd}}(s) = W_s^{\text{qkd}} C_s^{\text{qkd}} \quad (9)$$

$$C_s^{\text{kmw}}(s) = W_s^{\text{kmw}} C_s^{\text{kmw}}. \quad (10)$$

W_s^{qkd} and W_s^{kmw} are the number of QKD wavelengths and the number of KM wavelengths shared in the pool by QKD service provider s , respectively. C_s^{qkd} and C_s^{kmw} are the costs of shared QKD and KM wavelengths to be charged by QKD service provider s , respectively. In addition, let C_s^{coc} denote the fixed cooperation cost that will be charged when QKD service provider s is in cooperation. This cost can incur due to the communication and computation overhead and other security management tasks, which is typically incurred when independent providers interact with each other.

E. Case Study (Maritime Transportation Surveillance Over QKD)

In the case study of maritime transportation surveillance in QKD-SIC, we give an overview of maritime transportation and highlight the semantic requirements (i.e., semantic information) of maritime transportation applications.

Maritime transportation, where goods or people are transported via sea routes, is introduced as a case study. In this example, we consider maritime transportation from the perspective of a VSO, i.e., semantic receiver, who participates in the virtual environment [8]. It is challenging for new employees to practically sail ships since they are unfamiliar with locations and procedures. This may cause accidents with employees and boatmen. Therefore, a virtual environment for maritime applications is a promising solution. The VSO can create a virtual environment of maritime applications for practicing employees.

In Fig. 3, there are two VSOs and two edge devices in the system. We consider that the VSOs are maritime shipping companies to provide the services of autonomous maritime

ships. The VSO can set up simulated environments in the virtual environment in which the VSO can deploy their employee to use the virtual environment and experiment with the autonomous maritime ships. To create the maritime virtual environment, the VSO has to subscribe to edge devices to request the semantic information. Before subscribing to edge devices, the VSO uses bidirectional encoder representations from transformers (BERTs) [30] with the average similarity score of the category of each semantic information that generated by edge devices. For example, in Fig. 3, edge devices send the sample data and the average category similarity scores to VSOs. When VSOs receive the sample data and the average category similarity scores, VSOs extract the semantic information (i.e., snapshots of boats) in categories and then compare their interest (i.e., boats) with the similarity scores. As shown in Fig. 3, the average similarity score of semantic information of edge device 1 is the highest score (i.e., 0.95). Therefore VSOs subscribe edge device 1 to transmit the semantic information.

The VSO can create and provide a real-time virtual environment for maritime applications to support its users. The virtual environment of maritime applications can interact with edge devices by transmitting semantic information back and forth since the VSO can build the details of the virtual environment. The edge devices can be considered to be surveillance cameras or smartphones that are located in different areas. The edge devices and VSO are connected with the optical fibers. The edge devices generate the semantic information by using the semantic segmentation modules. In the semantic segmentation module, the pretrained machine learning models are applied, e.g., you only look once (YOLO) [31]. The snapshots from edge devices are considered to be the semantic information of interest to the VSO. When the VSO receives the semantic information, the VSO uses this semantic information to build the virtual environment of maritime applications for users.

Therefore, to prevent eavesdropping attacks, the QKD is promising for providing proven secure key distribution schemes for the semantic information transmitting between edge devices and the VSO by facilitating public key and data encryption. In this article, we consider that the number of secret-key rate requirements in the QKD layer directly depends on the number of snapshots captured by edge devices. However, the number of snapshots of each edge device cannot be known in advance since the number of snapshots which are generated by the semantic segmentation module is relevant to the interest of VSO. Therefore, the number of snapshots of each device becomes an uncertain parameter.

The QKD resource allocation for maritime transportation applications from the QKD resource pool that is created by QKD service providers in coalition \mathcal{C} is formulated as the two stages of the SP model. Fig. 4 illustrates the two stages of the SP model for maritime transportation applications given the QKD resource pool that is conceived by cooperative QKD service providers in coalition \mathcal{C} . In the first stage, decisions of provisioning QKD and KM wavelengths, and a decision of the routing according to the semantic requirements (i.e., from the semantic source node to destination node) are made. In the second stage, when the semantic requirements (i.e., the number

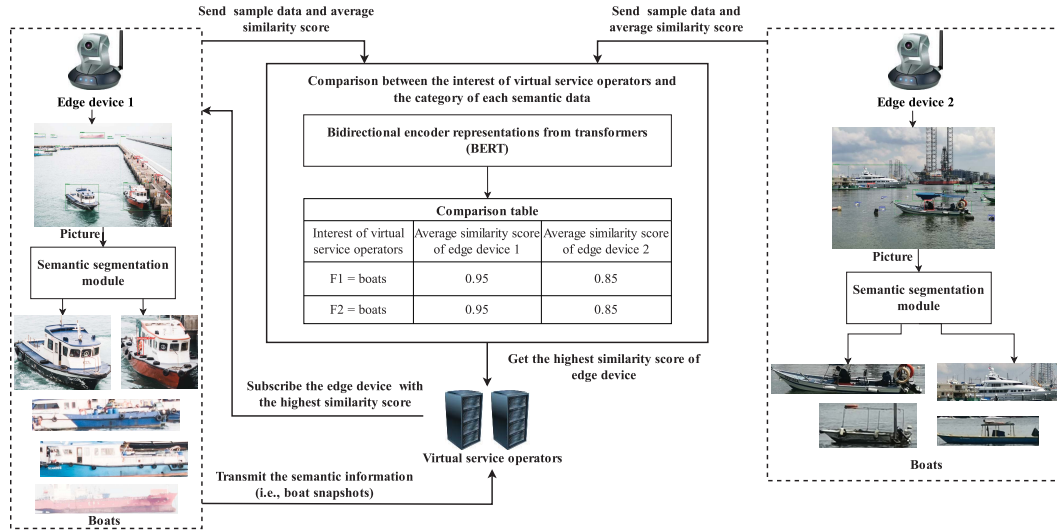


Fig. 3. Example of maritime transportation surveillance semantic information transfer.

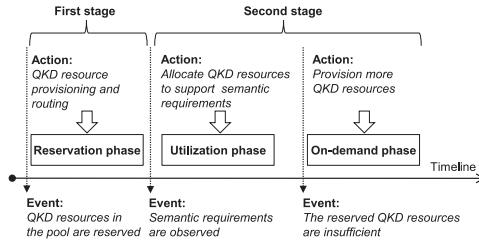


Fig. 4. Two-stage SP.

of snapshots generated by an edge device) are observed, the QKD and KM wavelengths that are provisioned in the first stage will be allocated to satisfy the semantic requirements. If the numbers of reserved QKD and KM wavelengths in the first stage are not enough, the QKD and KM wavelengths in the on-demand phase are provisioned.

IV. OPTIMIZATION FORMULATION

In this section, we first describe sets, constants, and decision variables of the SP model in Table II. We next present the SP model from the QKD resource pool created by the cooperative QKD service providers in coalition \mathbb{C} . Finally, we present the deterministic equivalent formulation to achieve the solution of the SP model.

A. Stochastic Programming Formulation

We first propose a QKD resource allocation scheme based on a two-stage SP model [32] among cooperative QKD service providers in coalition structure \mathbb{C} . The resource allocation decisions in the proposed scheme are conducted in two stages according to the result of the SP model

$$v(\mathbb{C}) = \min \sum_{f \in \mathcal{F}} \sum_{n \in \mathcal{N}} \sum_{i \in \mathcal{I}_n} \left(B_{n,f}^{\text{eng}} x_{i,n,f} + \left(\frac{1}{3} (A_{\text{tx}}^f(\tilde{\omega}) \beta_{\text{tx}}^r + A_{\text{rx}}^f(\tilde{\omega}) \beta_{\text{rx}}^r) \right) y_{i,n,f}^r \right)$$

TABLE II
LIST OF KEY NOTATIONS

Notations	Definitions
\mathcal{N}	Set of all SIC/QKD nodes in the network
\mathcal{O}_n	Set of outgoing links from node $n \in \mathcal{N}$
\mathcal{I}_n	Set of incoming links to node $n \in \mathcal{N}$
\mathcal{F}	Set of QKD-SIC chain requests in the network
$\tilde{\omega}$	Random variable of secret-key rate requirement of request
W_f^{qkd}	Three wavelengths of QKD link of request f satisfying the secret-key rate [25]
W_f^{km1}	One wavelength of KM link of request f satisfying the secret-key rate [25]
$B_{n,f}^{\text{eng}}$	Amount of energy required for transferring traffic of request f through node n
$x_{i,j,f}$	Binary decision variable indicating whether request $f \in \mathcal{F}$ will take a route with the link from node $i \in \mathcal{N}$ to node $j \in \mathcal{N}$ or not
$y_{i,n,f}^r$	Decision variable indicating the wavelength channels for QKD link in the reservation phase
$z_{i,n,f}^r$	Decision variable indicating the wavelength channels for KM link in the reservation phase
$y_{i,n,f,\omega}^e$	Decision variable indicating the utilized wavelength channels for QKD link under scenario ω
$z_{i,n,f,\omega}^e$	Decision variable indicating the utilized wavelength channels for KM link under scenario ω
$y_{i,n,f,\omega}^o$	Decision variable indicating the wavelength channels for QKD link in the on-demand phase under scenario ω
$z_{i,n,f,\omega}^o$	Decision variable indicating the wavelength channels for KM link in the on-demand phase under scenario ω

$$+ (A_{\text{km}}^f \beta_{\text{km}}^r + A_{\text{si}}^f \beta_{\text{si}}^r + A_{\text{md}}^f \beta_{\text{md}}^r) z_{i,n,f}^r + e_{(i,n)} (y_{i,n,f}^r + z_{i,n,f}^r) \beta_{\text{ch}}^r + \mathbb{E}_{\Psi} \left[\mathcal{C} (x_{i,n,f}, y_{i,n,f}^r, z_{i,n,f}^r, \tilde{\omega}) \right] \quad (11)$$

where

$$\begin{aligned} & \mathcal{C} (x_{i,n,f}, y_{i,n,f}^r, z_{i,n,f}^r, \tilde{\omega}) \\ &= \min_{x_{i,n,f}, y_{i,n,f}^e, z_{i,n,f}^e} \sum_{f \in \mathcal{F}} \sum_{n \in \mathcal{N}} \sum_{i \in \mathcal{I}_n} \left(\left(\frac{1}{3} (A_{\text{tx}}^f(\tilde{\omega}) \beta_{\text{tx}}^e + A_{\text{rx}}^f(\tilde{\omega}) \beta_{\text{rx}}^e) \right) y_{i,n,f,\omega}^e \right. \\ & \quad + (A_{\text{km}}^f \beta_{\text{km}}^e + A_{\text{si}}^f \beta_{\text{si}}^e + A_{\text{md}}^f \beta_{\text{md}}^e) z_{i,n,f,\omega}^e \\ & \quad + e_{(i,n)} (y_{i,n,f,\omega}^e + z_{i,n,f,\omega}^e) \beta_{\text{ch}}^e \\ & \quad \left. + \left(\frac{1}{3} (A_{\text{tx}}^f(\tilde{\omega}) \beta_{\text{tx}}^o + A_{\text{rx}}^f(\tilde{\omega}) \beta_{\text{rx}}^o) \right) y_{i,n,f,\omega}^o \right) \end{aligned}$$

$$\begin{aligned}
 & + \left(A_{\text{km}}^f \beta_{\text{km}}^o + A_{\text{si}}^f \beta_{\text{si}}^o + A_{\text{md}}^f \beta_{\text{md}}^o \right) z_{i,n,f,\tilde{\omega}}^o \\
 & + e_{(i,n)} \left(y_{i,n,f,\tilde{\omega}}^o + z_{i,n,f,\tilde{\omega}}^o \right) \beta_{\text{ch}}^o \quad (12)
 \end{aligned}$$

$$\text{s.t.} \quad \sum_{j' \in \mathcal{O}_{S_f}} x_{S_f,j',f} - \sum_{i' \in \mathcal{I}_{S_f}} x_{i',S_f,f} = 1, f \in \mathcal{F} \quad (13)$$

$$\sum_{i' \in \mathcal{I}_{D_f}} x_{i',D_f,f} - \sum_{j' \in \mathcal{O}_{D_f}} x_{D_f,j',f} = 1, f \in \mathcal{F} \quad (14)$$

$$\begin{aligned}
 & \sum_{j' \in \mathcal{O}_n} x_{n,j',f} - \sum_{i' \in \mathcal{I}_n} x_{i',n,f} = 0 \\
 & f \in \mathcal{F}, n \in \mathcal{N} \setminus \{S_f, D_f\} \quad (15)
 \end{aligned}$$

$$\sum_{j' \in \mathcal{O}_n} x_{n,j',f} \leq 1, n \in \mathcal{N}, f \in \mathcal{F} \quad (16)$$

$$\sum_{f \in \mathcal{F}} (y_{i,j,f,\tilde{\omega}}^e x_{i,j,f}) \leq W_{i,j}^{\text{qkd}}(\mathbb{C}), i, j \in \mathcal{N} \quad (17)$$

$$\sum_{f \in \mathcal{F}} (z_{i,j,f,\tilde{\omega}}^e x_{i,j,f}) \leq W_{i,j}^{\text{kml}}(\mathbb{C}), i, j \in \mathcal{N} \quad (18)$$

$$y_{i,n,f,\tilde{\omega}}^e x_{i,j,f} \leq y_{i,n,f}^r x_{i,j,f}, i, n \in \mathcal{N}, f \in \mathcal{F} \quad (19)$$

$$z_{i,n,f,\tilde{\omega}}^e x_{i,j,f} \leq z_{i,n,f}^r x_{i,j,f}, i, n \in \mathcal{N}, f \in \mathcal{F} \quad (20)$$

$$\begin{aligned}
 & \left(y_{i,n,f,\tilde{\omega}}^e x_{i,j,f} \right) + y_{i,n,f,\tilde{\omega}}^o \geq P_f(\tilde{\omega}) W_f^{\text{qkd}} x_{i,n,f} \\
 & i, n \in \mathcal{N}, f \in \mathcal{F} \quad (21)
 \end{aligned}$$

$$\begin{aligned}
 & \left(z_{i,n,f,\tilde{\omega}}^e x_{i,j,f} \right) + z_{i,n,f,\tilde{\omega}}^o \geq P_f(\tilde{\omega}) W_f^{\text{kml}} x_{i,n,f} \\
 & i, n \in \mathcal{N}, f \in \mathcal{F} \quad (22)
 \end{aligned}$$

$$W_{i,j}^{\text{qkd}}(\mathbb{C}) \leq W_{\text{max}}^{\text{qkd}}, i, j \in \mathcal{N} \quad (23)$$

$$W_{i,j}^{\text{kml}}(\mathbb{C}) \leq W_{\text{max}}^{\text{kml}}, i, j \in \mathcal{N} \quad (24)$$

$$x_{i,n,f} \in \{0, 1\}, i, n \in \mathcal{N}, f \in \mathcal{F} \quad (25)$$

$$\begin{aligned}
 & y_{i,n,f}^r, y_{i,n,f,\tilde{\omega}}^e, y_{i,n,f,\tilde{\omega}}^o, z_{i,n,f}^r, z_{i,n,f,\tilde{\omega}}^e, \\
 & z_{i,n,f,\tilde{\omega}}^o \in \{0, 1, 2, \dots\}, i, n \in \mathcal{N}, f \in \mathcal{F}. \quad (26)
 \end{aligned}$$

In the proposed system, QKD resources (i.e., QKD and KM wavelengths) are allocated by QKD service providers to SIC applications in the QKD network. In the first stage, QKD resources are allocated in the resource pool of QKD nodes. The actual number of QKD resources in the resource pool is determined in the second stage. The SP model considers the uncertainties (i.e., the number of *scenarios*), including the number of QKD devices required by the SIC nodes. In the QKD network, the secret-key rates are uncertain. Let $\tilde{\kappa}_f$ denote a random variable representing the secret-key rate required for the QKD-SIC chain request f . Let φ denote the size of the scenario spaces \mathcal{K}_f . Let $\tilde{\omega}$ denote a random variable associated with the secret-key rate requirement, i.e., $\tilde{\omega} \in \{\tilde{\kappa}_f | \tilde{\kappa}_f \in \mathcal{K}_f\}$ where $\mathcal{K}_f = \{\tilde{\kappa}_{f1}, \tilde{\kappa}_{f2}, \tilde{\kappa}_{f3}, \dots, \tilde{\kappa}_{f\varphi}\}$.

The objective of the SP model for QKD resource allocation under uncertainty expressed in (11) is to minimize the total cost of deploying QKD resources, including MDI-QTxS, MDI-QRxS, LKMs, SIs, MUX/DEMUX components, and QKD and KM links. The term $\mathbb{E}_{\Psi}[\mathcal{C}(x_{i,n,f}, y_{i,n,f}^r, z_{i,n,f}^r, \tilde{\omega})]$ in (11) is the expected secret-key rate requirements for encrypting semantic information, which is a key property of the SP model.

Constraint (13) ensures that the number of outgoing routes is larger than the number of incoming routes when the node

is the source node S_f of the QKD-SIC chain request f . Constraint (14) ensures that the number of incoming routes is larger than the number of outgoing routes if the node is the destination node D_f of the QKD-SIC chain request f . Constraint (15) ensures that the number of outgoing routes must equal the number of incoming routes if the node is the intermediate node of the QKD-SIC chain request f . Constraint (16) ensures that there is no loop for any QKD-SIC chain request, meaning that there is only one outgoing route for the QKD-SIC chain request of any node. Constraint (17) ensures that the QKD wavelengths of all QKD-SIC chain requests of any node must not exceed the available QKD wavelengths in the QKD resource pool [i.e., $W_{i,j}^{\text{qkd}}(\mathbb{C})$]. Constraint (18) ensures that the KM wavelengths of all QKD-SIC chain requests from any node must not exceed the available KM wavelengths in the QKD resource pool [i.e., $W_{i,j}^{\text{kml}}(\mathbb{C})$].

Constraint (19) ensures that the number of QKD wavelengths utilized is less than or equal to the number of QKD wavelengths reserved. Constraint (20) ensures that the number of KM wavelengths utilized is less than or equal to the number of KM wavelengths reserved. Constraint (21) ensures that the number of QKD wavelengths used plus the number of on-demand QKD wavelengths must satisfy the security requirements (i.e., secret-key rates). Constraint (22) ensures that the number of KM wavelengths used plus the number of on-demand KM wavelengths must satisfy the requirements. Constraints (23) and (24) ensure that the QKD and KM wavelength resource pools do not exceed the maximum available QKD and wavelength resource pools, respectively. Constraints (25) and (26) are the binary and integer variables, respectively.

B. Deterministic Equivalent Formulation

The SP with the random variable $\tilde{\omega}$ in (11)–(26) can be transformed into the deterministic equivalence problem [32] as expressed in (29)–(36). The random variable $\tilde{\omega}$ can be represented by a scenario. The scenario is a realization of a random variable, which is denoted by ω . The value of the random variable can be taken from a set of scenarios. Let Ψ and Ω_f as defined in (27) and (28), respectively, be the set of all scenarios of each requirement (i.e., a scenario space) and the set of all scenarios of request f , respectively. Let K denote the maximum required secret-key rate of the request f

$$\Psi = \prod_{f \in \mathcal{F}} \Omega_f = \Omega_1 \times \Omega_2 \times \dots \times \Omega_{|\mathcal{F}|} \quad (27)$$

$$\Omega_f = \{0, 1, 2, \dots, K\}. \quad (28)$$

The expectation $\mathbb{E}[\cdot]$ of the SP in (11) can be represented by the weighted sum of scenarios and their probabilities $\mathbb{P}_f(\omega)$.

The objective function (29) is to minimize the deployment cost. The decision variables $y_{i,n,f,\omega}^e, y_{i,n,f,\omega}^o, z_{i,n,f,\omega}^e$, and $z_{i,n,f,\omega}^o$ are under ω (i.e., $\omega \in \Omega_f$) which implies that the values of demands are available when ω is observed. Constraints (30) and (31) guarantee that the utilization of QKD and KM

wavelengths does not exceed the QKD and KM wavelength capacity, which are similar to (17) and (18). Constraints (32) and (33) guarantee that the expended QKD and KM wavelengths, respectively, must not exceed the reserved QKD and KM wavelengths, which have the same meanings as (19) and (20). Constraints (34) and (35) guarantee that all demands are satisfied, which are similar to (21) and (22), respectively. Constraint in (36) indicates that all decision variables are nonnegative integers.

The optimal solutions of the SP model and the deterministic equivalent formulation can be attained based on [32, Ths. 8 and 9]. In addition, the complexity of the proposed models depends on the number of SIC/QKD nodes in the system since the computational time of finding the optimal route for request f dominates when the number of SIC/QKD nodes increases. Therefore, we can conclude that the computational time of the proposed model increases significantly when the number of SIC/QKD nodes increases. In addition, the complexity of the proposed model [33] is $\mathcal{O}(|\mathcal{N}|^2)$ where $\mathcal{O}(\cdot)$ and $|\mathcal{N}|$ are big \mathcal{O} notation and the number of SIC/QKD nodes, respectively

$$\begin{aligned}
 v(\mathbb{C}) = & \min_{x_{i,n,f}, y_{i,n,f}^r, z_{i,n,f}^r} \sum_{f \in \mathcal{F}} \sum_{n \in \mathcal{N}} \sum_{i \in \mathcal{I}_n} \left(B_{n,f}^{\text{eng}} x_{i,n,f} \right. \\
 & + \left(\frac{1}{3} (A_{\text{tx}}^f(\bar{\omega}) \beta_{\text{tx}}^r + A_{\text{rx}}^f(\bar{\omega}) \beta_{\text{rx}}^r) \right) y_{i,n,f}^r \\
 & + (A_{\text{km}}^f \beta_{\text{km}}^r + A_{\text{si}}^f \beta_{\text{si}}^r + A_{\text{md}}^f \beta_{\text{md}}^r) z_{i,n,f}^r \\
 & \left. + e_{(i,n)} (y_{i,n,f}^r + z_{i,n,f}^r) \beta_{\text{ch}}^r \right) \\
 & + \sum_{f \in \mathcal{F}} \mathbb{P}_f(\omega) \sum_{n \in \mathcal{N}} \sum_{i \in \mathcal{I}_n} \left(\left(\frac{1}{3} (A_{\text{tx}}^f(\omega) \beta_{\text{tx}}^e + A_{\text{rx}}^f(\omega) \beta_{\text{rx}}^e) \right) y_{i,n,f,\omega}^e \right. \\
 & + (A_{\text{km}}^f \beta_{\text{km}}^e + A_{\text{si}}^f \beta_{\text{si}}^e + A_{\text{md}}^f \beta_{\text{md}}^e) z_{i,n,f,\omega}^e \\
 & + e_{(i,n)} (y_{i,n,f,\omega}^e + z_{i,n,f,\omega}^e) \beta_{\text{ch}}^e \\
 & + \left(\frac{1}{3} (A_{\text{tx}}^f(\omega) \beta_{\text{tx}}^o + A_{\text{rx}}^f(\omega) \beta_{\text{rx}}^o) \right) y_{i,n,f,\omega}^o \\
 & + (A_{\text{km}}^f \beta_{\text{km}}^o + A_{\text{si}}^f \beta_{\text{si}}^o + A_{\text{md}}^f \beta_{\text{md}}^o) z_{i,n,f,\omega}^o \\
 & \left. + e_{(i,n)} (y_{i,n,f,\omega}^o + z_{i,n,f,\omega}^o) \beta_{\text{ch}}^o \right) \quad (29)
 \end{aligned}$$

s.t. (13)–(16) and (23)–(25)

$$\sum_{f \in \mathcal{F}} (y_{i,j,f,\omega}^e x_{i,j,f}) \leq W_{ij}^{\text{qkd}}(\mathbb{C}) \quad (30)$$

$$\sum_{f \in \mathcal{F}} (z_{i,j,f,\omega}^e x_{i,j,f}) \leq W_{ij}^{\text{kml}}(\mathbb{C}) \quad (31)$$

$$i, j \in \mathcal{N} \quad \forall \omega \in \Omega_f \quad (32)$$

$$y_{i,n,f,\omega}^e x_{i,j,f} \leq y_{i,n,f}^r x_{i,j,f} \quad (33)$$

$$z_{i,n,f,\omega}^e x_{i,j,f} \leq z_{i,n,f}^r x_{i,j,f} \quad (34)$$

$$\begin{aligned}
 & i, n \in \mathcal{N}, f \in \mathcal{F} \quad \forall \omega \in \Omega_f \\
 & (y_{i,n,f,\omega}^e x_{i,j,f}) + y_{i,n,f,\omega}^o \\
 & \geq \sum_{\omega \in \Omega_f} (P_f(\omega) W_f^{\text{qkd}} x_{i,n,f}), i, n \in \mathcal{N}, f \in \mathcal{F} \quad (35)
 \end{aligned}$$

$$\begin{aligned}
 & (z_{i,n,f,\omega}^e x_{i,j,f}) + z_{i,n,f,\omega}^o \\
 & \geq \sum_{\omega \in \Omega_f} (P_f(\omega) W_f^{\text{kml}} x_{i,n,f}), i, n \in \mathcal{N}, f \in \mathcal{F} \quad (36)
 \end{aligned}$$

$$\begin{aligned}
 & y_{i,n,f}^r, y_{i,n,f,\omega}^e, y_{i,n,f,\omega}^o, z_{i,n,f}^r, z_{i,n,f,\omega}^e, z_{i,n,f,\omega}^o \\
 & \in \{0, 1, 2, \dots\}, i, n \in \mathcal{N}, f \in \mathcal{F} \quad \forall \omega \in \Omega_f. \quad (37)
 \end{aligned}$$

V. COST MANAGEMENT AMONG QKD SERVICE PROVIDERS

When the QKD resource allocation for maritime transportation applications is performed, the cooperative QKD service providers in coalition \mathbb{C} share the deployment cost created from satisfying the semantic requirements. In this section, we present the cost management to apply the concept of Shapley value to determine the deployment cost-sharing that each of cooperative QKD service providers will obtain.

A. Shapley Value

The concept of Shapley value [34] is applied to determine the deployment cost-sharing among cooperative QKD service providers.¹ The cooperative providers form a coalition to establish the shared QKD resource pool. Given the characteristic function $v(\cdot)$ in (11) and (29), the Shapley value of QKD service provider s is expressed in as follows:

$$\vartheta_s(v) = \sum_{\mathbb{D} \subseteq \mathbb{C} \setminus \{s\}} \frac{|\mathbb{D}|! (|\mathbb{C}| - |\mathbb{D}| - 1)!}{|\mathbb{C}|!} (v(\mathbb{D} \cup \{s\}) - v(\mathbb{D})). \quad (37)$$

The cost management of the cooperative QKD service providers in coalition \mathbb{C} based on the Shapley value can achieve four desirable properties as follows.

- 1) *Efficiency*: It is $\sum_{s \in \mathbb{C}} \vartheta_s(v) = v(\mathbb{C})$ which means that the sum of deployment cost of all cooperative QKD service providers is minimum.
- 2) *Symmetry*: $\vartheta_s(v)$ is equal to $\vartheta_l(v)$ if $v(\mathbb{D} \cup \{s\}) = v(\mathbb{D} \cup \{l\})$ contains all QKD service providers s and l given all coalitions \mathbb{D} of other cooperative QKD service providers. This means that the cost shared between QKD service providers s and l is equal if they make an identical contribution to the coalition.
- 3) *Dummy*: $\vartheta_s(v)$ is 0 if $v(\mathbb{D}) = v(\mathbb{D} \cup \{s\})$ contains all coalitions \mathbb{D} of all cooperative QKD service providers except provider s . This means that the cost shared by QKD service provider s is zero if QKD service provider s does not make a contribution to the total cost of the coalition.
- 4) *Additivity*: $\vartheta(u + v) = \vartheta(v + u) = \vartheta(u) + \vartheta(v)$ if u and v are the characteristic functions.

With the Shapley value, individual fairness is achieved [34]. In particular, the cost shared by the cooperative QKD service provider is not more than the cost of the QKD service provider who does not cooperate with other QKD service providers [i.e., $\vartheta_s(v) \leq v(\{s\})$]. In addition, the uniqueness of the Shapley value is ensured [34].

¹In the remainder of this article, “QKD service provider” and “provider” are used interchangeably.

The complexity of the Shapley value depends on the number of QKD service providers in a coalition \mathbb{C} , which means that the computational time of the Shapley value in the proposed model increases dramatically when the number of providers increases. This is due to the fact that theoretically, the complexity of the Shapley value [35] is $\mathcal{O}(|\mathbb{G}|^2)$ where $\mathcal{O}(\cdot)$ and $|\mathbb{G}|$ are big \mathcal{O} notation and the number of providers in a coalition \mathbb{C} , respectively. Therefore, the complexity of the Shapley value directly affects the performance of the proposed model.

VI. COOPERATION FORMATION AMONG QKD SERVICE PROVIDERS

In this section, we investigate the condition that QKD service providers aim to minimize their own costs. Therefore, QKD service providers may form a coalition and create a resource pool (i.e., QKD and KM wavelengths). We analyze the cooperation formation of QKD service providers by considering their individual costs.

A. Cooperation Model

We detail the model of cooperation formation of the QKD service providers with the following information. Let a set of all providers (i.e., players) be denoted by \mathbb{G} . There is an agreement among providers in \mathbb{C} on cooperation (i.e., $\mathbb{C} \subseteq \mathbb{G}$). \mathbb{C} is a set of cooperative providers such that the characteristic function of cooperative providers is $v(\mathbb{C})$, which is given by (29). For example, given three providers, a set of providers is $\mathbb{G} = \{1, 2, 3\}$. The cooperation can be defined as $\mathbb{C} \in \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. The coalition game with a set of players that are providers can be defined as $(\mathbb{G}, \delta_s(\cdot))$. Therefore, we can formulate a coalition game to model and obtain the equilibrium strategies. The strategy of each provider is to cooperate with other providers. Let $p_{s,l}$ denote the cooperation. If $p_{s,l} = 1$ which means that providers s and l cooperate, and $p_{s,l} = 0$ otherwise. Let $\mathbf{p}_s \in \mathcal{P}_s$ denote the strategy of provider s . Let $\mathbf{p}_s^* \in \mathcal{P}_s$ denote the cooperation equilibrium strategy. Let $\mathbf{p}_{-s}^* \in \prod_{l \in \mathbb{G} \setminus \{s\}} \mathcal{P}_l$ denote the cooperation equilibrium strategies of all providers except the strategy of provider s . Therefore, the strategy space of provider s cooperating with other providers is expressed in (38). The cooperation structure \mathbb{C} is expressed in (39). Therefore, the cooperation equilibrium of the cooperation formation of providers is expressed in (40)

$$\mathcal{P}_s = \left\{ (p_{s,1}, \dots, p_{s,l-1}, p_{s,l}, p_{s,l+1}, \dots, p_{s,|\mathbb{G}|}) \mid p_{s,l} \in \{0, 1\}, l \in \mathbb{G} \setminus \{s\} \right\} \quad (38)$$

$$p_{s,l} = \begin{cases} 1, & \text{if } s \in \mathbb{C} \text{ AND } l \in \mathbb{C} \\ 0, & \text{if } s \notin \mathbb{C} \text{ OR } l \notin \mathbb{C} \end{cases} \quad (39)$$

$$\delta_s(\mathbf{p}_s^*, \mathbf{p}_{-s}^*) \leq \delta_s(\mathbf{p}_s, \mathbf{p}_{-s}^*) \quad \forall s. \quad (40)$$

$\delta_s(\cdot)$ is the cost of provider s received from the QKD resource allocation and cost management, i.e., $\delta_s(\cdot) = \vartheta_s$ in (37).

B. Dynamics of Coalition Formation

The cooperation formation equilibrium among providers is determined based on best response dynamics. In particular,

the provider iteratively makes a decision to form a cooperation. The decision iteration is denoted by σ (i.e., $\sigma = 1, 2, 3, \dots, N$) where N is a maximum number of iterations. The strategy of provider s in the decision iteration σ is denoted by $\mathbf{p}_s(\sigma)$. The strategies of all providers except the strategy of provider s in decision iteration $\sigma - 1$ are denoted by $\mathbf{p}_{-s}(\sigma - 1)$. In each decision iteration, the provider assesses the new strategy and then changes to the new strategy with the lowest cost. The strategy of provider s in decision iteration σ [i.e., $\mathbf{p}_s(\sigma)$] can be determined as follows:

$$\mathbf{p}_s(\sigma) \in \arg \min_{\mathbf{p}_s \in \mathcal{P}_s} \delta_s(\mathbf{p}_s, \mathbf{p}_{-s}(\sigma - 1)). \quad (41)$$

In (41), given the knowledge of strategies of other providers in the prior decision iteration [i.e., $\mathbf{p}_{-s}(\sigma - 1)$], the best new strategy is selected by the provider s . However, the provider may make a mistake with a small probability (i.e., \aleph).

From (41), discrete-time Markov chain can be applied to model the strategy adaptation of the cooperation formation [36]. Under all cooperations of all providers, the finite state space of the Markov chain is expressed as $\Theta = \prod_{s \in \mathbb{G}} \mathcal{P}_s = \mathcal{P}_1 \times \dots \times \mathcal{P}_{|\mathbb{G}|}$. It is assumed that it has symmetric cooperation which is $p_{s,l} = p_{l,s}$. The strategy $\mathbf{p}_s(\cdot)$ in (41) contains the cooperations of provider s and is part of the state τ , i.e., $\tau \in \Theta$. For the transition probability of Markov chain, τ and τ' are the current state and the next state, respectively. Let $\tau = (p_{s,1}, \dots, p_{s,l}, \dots, p_{s,|\mathbb{G}|})$, $\tau \in \Theta$ denote the current state. Let $\tau' = (p'_{s,1}, \dots, p'_{s,l}, \dots, p'_{s,|\mathbb{G}|})$, $\tau' \in \Theta$ denote the next state. The set of providers associated with the state change from τ to τ' is defined in

$$\mathcal{Z}_{\tau,\tau'} = \{s \mid p_{s,l} \neq p'_{s,l}, s \neq l, s, l \in \mathbb{G}\}. \quad (42)$$

The transition probability from τ to τ' is expressed in

$$\mathbf{T}_{\tau,\tau'} = \lambda^{|\mathcal{Z}_{\tau,\tau'}|} (1 - \lambda)^{|\mathbb{G}| - |\mathcal{Z}_{\tau,\tau'}|} \prod_{s \in \mathcal{Z}_{\tau,\tau'}} \Xi_s(\tau, \tau') \quad (43)$$

where λ is the probability of the provider updating the strategy in an iteration of the decision. The probability of changing the strategy of provider s in an iteration of the decision is expressed in (44). Let $\delta_s(\tau)$ denote the cost that is the function of the strategies of all providers. In (44), the provider can change to the strategy that produces lower cost [i.e., $\delta_s(\tau') < \delta_s(\tau)$]. However, the provider may irrationally change to the new strategy with probability \aleph

$$\Xi_s(\tau, \tau') = \begin{cases} 1 - \aleph & \text{if } \delta_s(\tau') < \delta_s(\tau) \\ \aleph, & \text{otherwise.} \end{cases} \quad (44)$$

VII. PERFORMANCE EVALUATION

In this section, we perform experiments with the following considerations. First, we consider that the proposed SP model can obtain the efficient routing to satisfy the QKD-SIC chain requests.² Each routing consists of QKD and KM wavelengths in the reservation and the on-demand phases of the SP model. The routing results are shown in Section VII-B1. Second, we

²In the remainder of this article, “QKD-SIC chain request” and “QKD chain request” are used interchangeably.

consider that the deployment cost can be decreased by optimally reserving the number of QKD and KM wavelengths in advance. The results are presented in Section VII-B2.

Third, we show the upper and lower bounds of the SP model with the consideration that if the gap between the solutions of the bound and the solution of the SP model is small enough, we can apply the upper and lower bounds to obtain the satisfied solutions instead of the SP model. This is due to the fact that formulations of the upper and lower bounds are much lower complexity than the formulation of SP model since the numbers of variables and constraints of formulations of the upper and lower bounds are less than that of formulation of SP model. In addition, we compare the SP model with the CO-QBN algorithm [25] with different quantitative analyzes to show the performance of the SP model. The results are shown in Section VII-B3. Fourth, we show the SP model with a cooperative game and examine the impact of shared QKD and KM wavelengths. In this experiment, we consider that, with a large number of secret-key rates, the costs of cooperative providers are significantly lower than that of noncooperative providers. The results are shown in Section VII-B4.

Finally, we investigate and show how the coalition structure affects the costs of QKD service providers. The stable coalition structure, which is a solution to the cooperative game (i.e., the cooperation equilibrium), can be determined by the Shapley value, a fair cost-sharing concept. In addition, we investigate how the cost of shared QKD and KM wavelengths and cooperation affect the stable cooperative structure. The reason for this is that we want to know where the cooperation structure is stable when the cost increases. The results are shown in Section VII-B5.

A. Parameter Setting

We consider the SIC over QKD networks as shown in Fig. 1. Specifically, there are three QKD service providers. Providers 1, 2, and 3 have 10, 15, and 20 available QKD wavelengths, respectively. Providers 1, 2, and 3 have 40, 55, and 65 available KM wavelengths, respectively. We perform experiments using the NSFNET and USNET topologies [25]. The distance D between two QTxs is set to 160 km [25]. We set $W_{\max}^{\text{qkd}} = 1,000$ and $W_{\max}^{\text{kml}} = 300$ for the maximum number of wavelengths for a QKD link between node i and node j and the maximum number of wavelengths for a KM link between node i and node j , respectively. We consider the Shapley value for cost-sharing between providers. We implement and solve the SP model using the GAMS/CPLEX solver [37].

For the SP model, we consider the random number of secret-key rates with uniform distribution for ease of presentation. We consider the cost values of five QKD network components which are composed of MDI-QTXs, MDI-QRXs, LKMs, SIs, MUX/DEMUX components, and QKD and KM links. For the reservation phase, we apply these cost values from [25]. The cost values of the components can be presented in Table III.

B. Numerical Results

1) *Routing*: Fig. 5 illustrates the solutions of the SP model that satisfy three QKD-SIC chain requests. In the solutions,

TABLE III
RESERVATION, UTILIZATION, AND ON-DEMAND COST VALUES

Notations	Values(\$)	Notations	Values(\$)	Notations	Values(\$)
$\beta_{\text{tx}}^r, \beta_{\text{rx}}^e$	1,500	$\beta_{\text{tx}}^r, \beta_{\text{rx}}^e$	2,250	$\beta_{\text{km}}^r, \beta_{\text{km}}^e$	1,200
$\beta_{\text{si}}^r, \beta_{\text{si}}^e$	150	$\beta_{\text{md}}^r, \beta_{\text{md}}^e$	300	$\beta_{\text{ch}}^r, \beta_{\text{ch}}^e$	1
β_{tx}^o	6,000	β_{rx}^o	9,000	β_{km}^o	3,000
β_{si}^o	500	β_{md}^o	900	β_{ch}^o	4

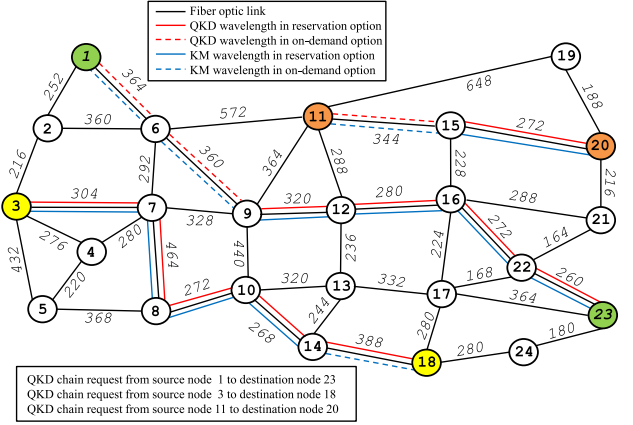


Fig. 5. Example of three QKD-SIC chain requests in USNET topology.

the SP model can allocate QKD and KM wavelengths (i.e., resources) in reservation and on-demand phases for the requests in fiber optic networks. In Fig. 5, each request (i.e., a route) utilizes QKD and KM wavelength within a fiber optic link. To obtain the optimal deployment cost, it is interesting to mention that both QKD and KM wavelengths in reservation and on-demand phases are utilized along the routes. For example, with the QKD-SIC chain request from source node 1 to destination node 23, the optimal deployment cost can be obtained from the route consisted of nodes $1 \rightarrow 6 \rightarrow 9 \rightarrow 12 \rightarrow 16 \rightarrow 22 \rightarrow 23$. In particular, QKD and KM wavelengths in the on-demand phase are utilized from node 1 to node 6 (i.e., $1 \rightarrow 6$) and from node 6 to node 9 (i.e., $6 \rightarrow 9$) while the rest of the route utilize the QKD and KM wavelengths in the reservation phase.

2) *Cost Structure Analysis*: In Fig. 6(a), we examine the performance of the SP model in obtaining an optimal solution. In the first stage, we vary the number of reserved QKD wavelengths and fix the number of reserved KM wavelengths. Then, we present the optimal solution obtained by the SP model and the effect of reserved QKD wavelengths on the solution. In Fig. 6(a), when the number of reserved QKD wavelengths increases, the first-stage cost increases significantly. However, the second-stage cost decreases dramatically when the secret-key rates check. The reason is that the QKD wavelength in the on-demand phase (i.e., the second stage) is forced to be minimum by utilizing the cheaper QKD wavelength in the reservation phase (i.e., the first stage). As a result, at 150 QKD wavelengths reserved, the optimal solution can be achieved, and the second-stage cost is 0. This is because the reserved QKD wavelengths meet demands (i.e., secret-key rates), and therefore the on-demand QKD wavelengths in the second stage are not utilized. After this point, the total cost and the first-stage cost increase since it has a penalty cost for an excess of

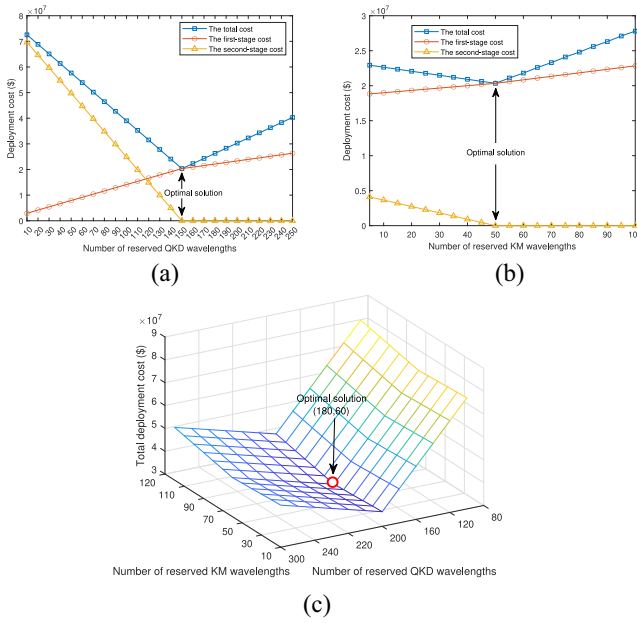


Fig. 6. (a) Optimal solution under different reserved QKD wavelengths, (b) optimal solution under different reserved KM wavelengths, and (c) optimal solution under different reserved QKD and KM wavelengths.

reserved QKD wavelength to be charged. For Fig. 6(a), we can mention that over- and under-provision of QKD wavelengths affect the high-total cost significantly.

In a similar way to the investigation above, in Fig. 6(b), we vary the number of KM wavelengths in the first stage and fix the number of QKD wavelengths to show the optimal solution obtained by the SP model. In Fig. 6(b), clearly, the first-stage cost increases steadily while the second-stage cost decreases. However, the optimal solution is achieved when the number of reserved KM wavelength is 50. The reason is that the reserved KM wavelengths of 50 successfully satisfy the demands. After this point, the total cost and the first-stage cost increase since the penalty cost of an excess of reserved KM wavelengths is charged. Therefore, we can explain that the high cost is affected by not only the reserved QKD wavelengths but also the reserved KM wavelengths. In addition, we vary the number of QKD and KM wavelengths to show the optimal solution obtained by the SP model. In Fig. 6(c), apparently, the optimal deployment cost can be achieved (i.e., the numbers of reserved QKD and KM wavelengths being 180 and 60, respectively) when the number of QKD and KM wavelengths increases.

Fig. 7(a) illustrates the number of QKD and KM wavelengths (i.e., resources) in reservation and on-demand phases under different secret-key rates. In the reservation phase, the numbers of QKD and KM wavelengths rise steeply until the secret-key rates are 5 and 3 Kb/s, respectively. This is because the reserved QKD and KM wavelengths are completely utilized at the secret-key rates of 5 and 3 Kb/s, respectively. After these points, both QKD and KM wavelengths are constant since the capacities of QKD and KM wavelengths are limited. The capacities of QKD and KM wavelengths in the reservation phase are constrained by the QKD service provider. As a result, to satisfy the high-secret-key rates, the QKD and KM wavelengths in the on-demand phase are more utilized.

In the on-demand phase, the numbers of QKD and KM wavelengths start rising dramatically at 5 and 3 Kb/s, respectively, due to the limited capacities of QKD and KM wavelengths in the reservation phase.

Fig. 7(b) illustrates subpath utilization according to the QKD-SIC chain request (i.e., from a source to a destination) of QKD and KM wavelength in reservation and on-demand phases under the different costs of QKD and KM links. The full path in Fig. 7(b) is $1 \rightarrow 6 \rightarrow 9 \rightarrow 12 \rightarrow 16 \rightarrow 22 \rightarrow 23$, which consists of six subpaths. Source and destination nodes are 1 and 23, respectively. In Fig. 7(b), it is straightforward to mention that when the cost of QKD and KM links increases, the number of utilized subpaths of both QKD and KM wavelengths in the reservation phase changes to that of both QKD and KM wavelengths in the on-demand phase. For example, with QKD and KM link cost $< 50\$$, the subpaths of KM wavelengths in reservation and on-demand phases are utilized. However, with QKD and KM link cost $= 50\$$, the subpaths of KM wavelength in the on-demand phase are completely utilized (i.e., six subpaths). To obtain the optimal deployment cost, the subpath utilization in the reservation phase is completely changed to the subpath utilization in the on-demand phase by the SP model.

3) *Performance Evaluation under Various Parameters:* We first evaluate the performance of the SP model by comparing it with the *cooperative resource management (CRM) over the expected value deterministic* and the *deterministic equivalent formulation*. In the case of CRM over the expected value deterministic, the secret-key rates (i.e., demands) in the first stage are considered to be the expected demands. On the other hand, the secret-key rates are considered as the exact demands in the case of the deterministic equivalent formulation. The former formulation is used to find the values of the upper bound, while the latter formulation is used to find the values of the lower bound.

In Fig. 7(c), the CRM over the expected value deterministic and deterministic equivalent formulation yield the solutions that are the upper bound and lower bound of the SP model, respectively. We observe that the gap to the upper bound is sufficiently small. This result implies that using the expected value of secret-key rates can achieve a satisfactory solution (i.e., close to the optimal solution of the SP model). Then, we compare the SP model with the CO-QBN algorithm [25]. Fig. 7(d) illustrates a performance comparison of the SP model and CO-QBN algorithm by varying the number of QKD-SIC chain requests. In Fig. 7(d), both the SP model and CO-QBN algorithm can decrease the deployment cost when the QKD-SIC chain requests increase. However, in comparison with the CO-QBN algorithm, the SP model can significantly achieve a lower deployment cost under different QKD-SIC chain requests.

4) *Impact of Available QKD and KM wavelengths:* We consider a situation that the QKD service providers 1 and 2 cooperate to share the QKD and KM wavelengths. Fig. 8(a) illustrates the total deployment cost when provider 2 shares the number of QKD and KM wavelengths. It is clear to explain that, with the high demands, the total deployment cost increases if provider 2 performs over-sharing wavelengths

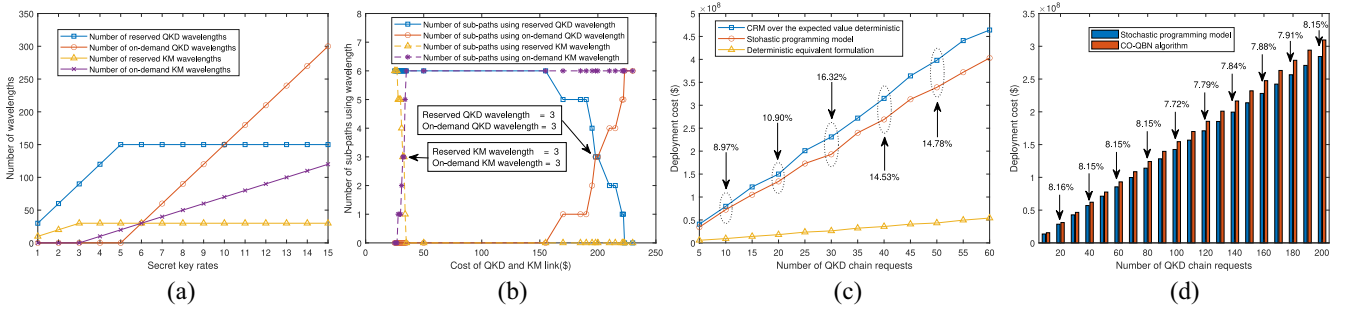


Fig. 7. (a) Numbers of QKD and KM wavelengths in reservation and on-demand phases under different secret-key rates, (b) numbers of QKD and KM wavelengths in reservation and on-demand phases under the different costs of QKD and KM links, (c) bounding of the objective value from the SP model, and (d) cost comparison between the SP model and the CO-QBN algorithm.

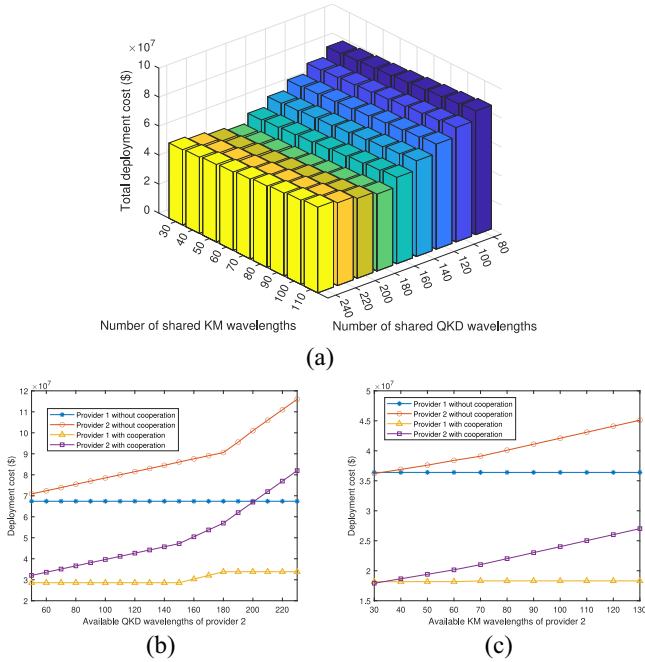


Fig. 8. (a) Deployment cost under different number of shared QKD and KM wavelengths of provider 2, (b) costs of providers 1 and 2 with and without cooperation under different available QKD wavelengths of provider 2, and (c) costs of providers 1 and 2 with and without cooperation under different available KM wavelengths of provider 2.

and under-sharing wavelengths. Fig. 8(b) and (c) illustrate the optimal deployment cost obtained from the SP model when provider 2 increases the number of shared QKD and KM wavelengths. The main observation is that the providers experience lower costs when they are in cooperation. This is due to the fact that the providers can utilize the available resources of each other. As illustrated in Fig. 8(b) and (c), when the QKD and KM wavelengths of provider 2 increase, provider 1 receives a benefit from using the extra QKD and KM wavelengths of provider 2 and provider 2 can utilize QKD and KM wavelengths shared in the resource pool by provider 1. On the other hand, without cooperation, the QKD and KM wavelength resources cannot be shared. Hence, increasing the available QKD and KM wavelengths of provider 2 does not have an effect on the deployment cost of provider 1. Another observation is that, with cooperation, the cost of provider 1 can slightly increase when the QKD and KM wavelengths

of provider 2 increase. This is because provider 1 does not contribute more to the QKD and KM wavelength resource pool. Therefore, the cost-sharing of provider 1 increases when provider 2 contributes more resources.

5) Cooperation Formulation and Impact of Cooperation Cost: We evaluate the cooperation formation behavior of the three providers and then scrutinize the cooperation costs which comprise shared QKD wavelength [i.e., $C^{\text{qkd}}(s)$], shared KM wavelength [i.e., $C^{\text{kmw}}(s)$], and cooperation (i.e., C_s^{coc}). Table IV illustrates the Shaplye values (i.e., the cost of each provider), which is $\vartheta_s(v) = \vartheta_s(v) + C^{\text{qkd}}(s) + C^{\text{kmw}}(s) + C_s^{\text{coc}}$, for the QKD and KM wavelength resource allocation. With cost management and QKD and KM wavelength allocation based on the SP model, the stable coalition structure of the QKD wavelength pool is obtained to be \mathbb{C}_2^* (i.e., providers 1 and 2 cooperate). \mathbb{C}_2^* is a stable coalition structure since providers 1 and 2 achieve the lowest cost, while provider 3 does not have a better choice to decrease its cost. In addition, the stable coalition structure of KM wavelength pool is obtained to be \mathbb{C}_5^* (i.e., providers 1, 2, and 3 cooperate). \mathbb{C}_5^* is a stable coalition structure since providers 1, 2, and 3 achieve a lower cost compared with other coalition structures.

We investigate how the costs of parameters (i.e., shared QKD and KM wavelengths, and cooperation) affect the stable cooperation structure. In Fig. 9(a)–(c), the major observation is that the cooperation structure will move toward $\{\{1\}, \{2\}, \{3\}\}$ which means that providers work separately when the costs of shared QKD wavelength [i.e., $C^{\text{qkd}}(s)$], shared KM wavelength [i.e., $C^{\text{kmw}}(s)$], and cooperation (i.e., C_s^{coc}) increase. The reason is that, without cooperation, the providers mainly utilize the resources (i.e., QKD and KM wavelengths) in reservation and on-demand phases to obtain the minimum cost. When the costs increase, it is not worth for the provider to cooperate and increase their resources to accommodate demands. Alternatively, it is more beneficial for the provider to work separately.

Fig. 9(d) illustrates the adaptation of the stable coalitions under different sharing costs of QKD and KM wavelengths. With a large number of secret-key rates (i.e., demands), each provider tends to move to the coalition structure $\mathbb{C}_5 = \{\{1, 2, 3\}\}$ when the sharing cost of QKD and KM wavelengths is low. For example, with the sharing cost of QKD and KM

TABLE IV
PAYOFF MATRIX FOR THREE COALITION GAME

The Shapley value						
Cooperation structure	QKD wavelength pool			KM wavelength pool		
	Provider 1	Provider 2	Provider 3	Provider 1	Provider 2	Provider 3
$C_1 = \{\{1\}, \{2\}, \{3\}\}$	3,271,643.12	2,998,812.40	2,725,981.68	35,647,210.00	35,260,720.00	35,131,890.00
$C_2 = \{\{1, 2\}, \{3\}\}$	2,562,990.84*	2,890,160.12*	2,725,981.68*	32,199,190.00	37,227,700.00	35,131,890.00
$C_3 = \{\{1, 3\}, \{2\}\}$	2,562,990.84	2,998,812.40	3,217,329.40	32,263,605.00	35,260,720.00	40,773,285.00
$C_4 = \{\{2, 3\}, \{1\}\}$	3,271,643.12	3,026,575.48	3,353,744.76	35,647,210.00	37,485,360.00	40,966,530.00
$C_5 = \{\{1, 2, 3\}\}$	2,108,660.56	2,572,245.20	2,899,414.48	26,300,931.67*	31,522,686.67*	35,068,271.67*

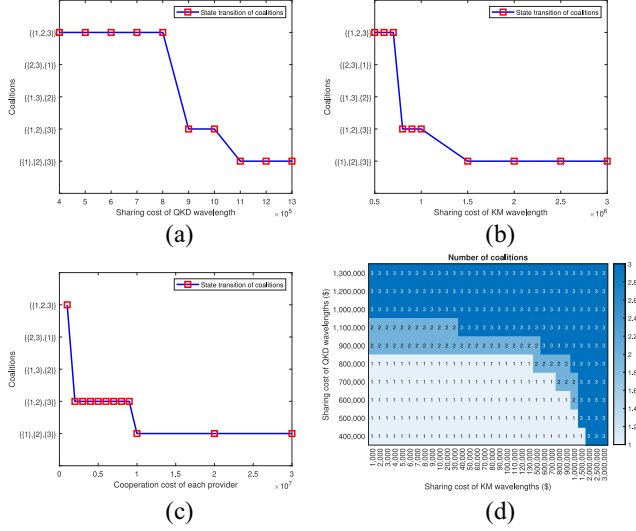


Fig. 9. (a) and (b) transition cooperation structure under different cost of QKD wavelength and under different cost of KM wavelength, respectively, (c) transition cooperation structure under different cooperation cost of each provider, and (d) stable coalitions under different sharing costs of QKD and KM wavelengths.

wavelengths being \$600 000 and \$10 000, respectively, the stable coalition is $C_5 = \{\{1, 2, 3\}\}$ which is indicated by “1” in Fig. 9(d). This is because each provider obtains the lowest cost, and the resource can be better utilized with more providers in the coalition. However, when the sharing cost of QKD and/or KM wavelengths increases, the stable coalition tends to move to the coalition $C_1 = \{\{1\}, \{2\}, \{3\}\}$ which is indicated by “3” in Fig. 9(d). This is due to the fact that each provider obtains a high cost when they cooperate to share their QKD and/or KM wavelengths. As a result, there are no QKD and KM wavelength pools, and each provider separately supports the demands.

VIII. CONCLUSION

In the proposed QKD-SIC system, edge devices will need security requirements in QKD nodes. Therefore, the QKD service providers must provide QKD resources to achieve the minimum deployment cost. We have proposed a decision-making scheme for QKD service providers in QKD-based SIC. The proposed scheme comprises methods for resource allocation to secure semantic information transmission of edge devices, cost management, and cooperation among QKD service providers. In particular, the QKD service providers can cooperate and establish the QKD resource pool. For the resource allocation, we have applied the two-stage SP to

resolve the solutions of the QKD service providers to support edge devices to transmit the semantic information that utilizes resources in the resource pool. For cost management, we have incorporated Shapley values to share the deployment cost that is received from the resource pool with cooperative QKD service providers in a fair and interpretable manner. For the coalition formation among QKD service providers, we have achieved the cooperation equilibrium solutions for the cooperative QKD service providers who contribute to the resource pool.

REFERENCES

- [1] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, “The evolution of quantum key distribution networks: On the road to the QInternet,” *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2nd Quart., 2022.
- [2] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, “Quantum Internet: Networking challenges in distributed quantum computing,” *IEEE Netw.*, vol. 34, no. 1, pp. 137–143, Jan./Feb. 2020.
- [3] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, “When entanglement meets classical communications: Quantum teleportation for the quantum Internet,” *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3808–3833, Jun. 2020.
- [4] J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, “Quantum Internet protocol stack: A comprehensive survey,” *Comput. Netw.*, vol. 213, Aug. 2022, Art. no. 109092.
- [5] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O’Brien, “Quantum computers,” *Nature*, vol. 464, no. 7285, pp. 45–53, 2010.
- [6] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
- [7] X. You et al., “Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts,” *Sci. China Inf. Sci.*, vol. 64, no. 1, pp. 1–74, 2021.
- [8] X. Luo, H.-H. Chen, and Q. Guo, “Semantic communications: Overview, open issues, and future research directions,” *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 210–219, Feb. 2022.
- [9] W. Yang et al., “Semantic communications for 6G future Internet: Fundamentals, applications, and challenges,” 2022, *arXiv:2207.00427*.
- [10] Z. Qin, X. Tao, J. Lu, W. Tong, and G. Y. Li, “Semantic communications: Principles and challenges,” 2022, *arXiv:2201.01389*.
- [11] A. J. Blesswin, C. Raj, R. Sukumaran, and M. G. Selva, “Enhanced semantic visual secret sharing scheme for the secure image communication,” *Multimedia Tools Appl.*, vol. 79, pp. 17057–17079, Jun. 2020.
- [12] M. Xu et al., “Stochastic resource allocation in quantum key distribution for secure federated learning,” in *Proc. IEEE GLOBECOM*, 2022, pp. 4377–4382.
- [13] R. Kaewpuang, M. Xu, D. Niyato, H. Yu, and Z. Xiong, “Adaptive resource allocation in quantum key distribution (QKD) for federated learning,” in *Proc. IEEE ICNC*, 2023, pp. 71–76.
- [14] T. Zaarour, A. Bhattacharya, and E. Curry, “OpenPubSub: Supporting large semantic content spaces in peer-to-peer publish/subscribe systems for the Internet of Multimedia Things,” *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17640–17659, Sep. 2022.
- [15] B. Kim, S. Heo, J. Lee, S. Jeong, Y. Lee, and H. Kim, “Compiler-assisted semantic-aware encryption for efficient and secure serverless computing,” *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5645–5656, Apr. 2021.

- [16] W. C. Ng, H. Du, W. Y. B. Lim, Z. Xiong, D. Niyato, and C. Miao, "A stochastic approach for semantic-enabled transmission in the meta-verse," unpublished.
- [17] L. Yan, Z. Qin, R. Zhang, Y. Li, and G. Y. Li, "Resource allocation for text semantic communications," *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1394–1398, Jul. 2022.
- [18] Z. Weng and Z. Qin, "Semantic communication systems for speech transmission," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, pp. 2434–2444, Aug. 2021.
- [19] W. Xu, Z. Yang, D. W. K. Ng, M. Levorato, Y. C. Eldar, and M. Debbah, "Edge learning for B5G networks with distributed signal processing: Semantic communication, edge computing, and wireless sensing," 2022, *arXiv:2206.00422*.
- [20] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, "A joint learning and communications framework for federated learning over wireless networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 269–283, Jan. 2021.
- [21] C. Zhang, Z. Liu, Y. Chen, J. Lu, and D. Liu, "A flexible and generic gaussian sampler with power side-channel countermeasures for quantum-secure Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8167–8177, Sep. 2020.
- [22] M. Xu et al., "Quantum-secured space-air-ground integrated networks: Concept, framework, and case study," *IEEE Wireless Commun.*, early access, Oct. 10, 2022, doi: [10.1109/MWC.008.2200163](https://doi.org/10.1109/MWC.008.2200163).
- [23] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014.
- [24] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, 2012, Art. no. 130503.
- [25] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 9, pp. 2701–2718, Sep. 2021.
- [26] R. Kaewpuang, M. Xu, D. Niyato, H. Yu, and Z. Xiong, "Resource allocation in quantum key distribution (QKD) for space-air-ground integrated networks," in *Proc. IEEE CAMAD*, 2022, pp. 71–76.
- [27] H. Cui et al., "Space-air-ground integrated network (SAGIN) for 6G: Requirements, architecture and challenges," *China Commun.*, vol. 19, no. 2, pp. 90–108, Feb. 2022.
- [28] B. Güler, A. Yener, and A. Swami, "The semantic communication game," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 4, pp. 787–802, Dec. 2018.
- [29] A. Wonfor et al., "Field trial of multi-node, coherent-one-way quantum key distribution with encrypted 5×100G DWDM transmission system," in *Proc. 45th Eur. Conf. Opt. Commun. (ECOC)*, 2019, pp. 1–4.
- [30] H. Xie, Z. Qin, G. Y. Li, and B.-H. Juang, "Deep learning enabled semantic communication systems," *IEEE Trans. Signal Process.*, vol. 69, pp. 2663–2675, Apr. 2021.
- [31] J. Redmon and A. Farhadi, "YOLOv3: An incremental improvement," 2018, *arXiv:1804.02767*.
- [32] J. R. Birge and F. Louveau, *Introduction to Stochastic Programming*. New York, NY, USA: Springer, 2011.
- [33] J. K. Lenstra and A. H. G. R. Kan, "Complexity of vehicle routing and scheduling problems," *Networks*, vol. 11, no. 2, pp. 221–227, 1981.
- [34] B. Peleg and P. Sudhölter, *Introduction to the Theory of Cooperative Games*, vol. 34. Heidelberg, Germany: Springer, 2007.
- [35] X. Deng and C. H. Papadimitriou, "On the complexity of cooperative solution concepts," *Math. Oper. Res.*, vol. 19, no. 2, pp. 257–266, 1994.
- [36] S. Goyal and F. Vega-Redondo, "Network formation and social coordination," *Games Econ. Behav.*, vol. 50, no. 2, pp. 178–207, 2005. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0899825604000296>
- [37] "GAMS solvers." GAMS. Accessed: Jul. 17, 2022. [Online]. Available: <https://www.gams.com/>



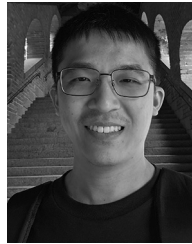
Rakpong Kaewpuang received the M.Eng. degree from the Department of Computer Engineering, Kasetsart University, Bangkok, Thailand, in 2010.

He is a Research Associate with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests are logistics and supply chain management, cloud computing, and smart grid systems.



Minrui Xu (Graduate Student Member, IEEE) received the B.S. degree from Sun Yat-sen University, Guangzhou, China, in 2021. He is currently pursuing the Ph.D. degree with the School of Computer Science and Engineering, Nanyang Technological University, Singapore.

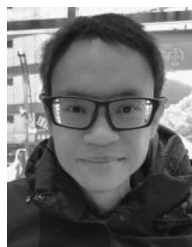
His research interests mainly focus on metaverse, deep reinforcement learning, and mechanism design.



Wei Yang Bryan Lim (Member, IEEE) received the Ph.D. degree from Nanyang Technological University (NTU), Singapore, in 2022, under the Alibaba Ph.D. Talent Programme.

He is currently an Assistant Professor with the School of Computer Science and Engineering, NTU. He was a Visiting Scholar with institutions, such as KTH Royal Institute of Technology, Stockholm, Sweden, and the University of Sydney, Sydney, NSW, Australia.

Dr. Lim won the "Most Promising Industrial Postgraduate Programme Student" Award under the Alibaba Ph.D. Talent Programme. His works have won best paper awards, including the IEEE Wireless Communications and Networking Conference, IEEE Asia Pacific Board Outstanding Paper Award, and the IEEE SPCC Technical Committee Best Paper Award. He regularly serves as the Technical Programme Committee Member in flagship conferences; is a part of the Guest Editor Team of special issues such as the *IEEE Wireless Communication Magazine*; and is currently the Review Board Member of IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS.



Dusit Niyato (Fellow, IEEE) received the B.Eng. degree from King Mongkuts Institute of Technology Ladkrabang, Bangkok, Thailand, in 1999, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Winnipeg, MB, Canada, in 2008.

He is a Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests are in the areas of sustainability, edge intelligence, decentralized machine learning, and incentive mechanism design.



Han Yu (Senior Member, IEEE) received the Ph.D. degree from the School of Computer Science and Engineering, Nanyang Technological University (NTU), Singapore, in 2014.

He is a Nanyang Assistant Professor with the School of Computer Science and Engineering, NTU. He held the Prestigious Lee Kuan Yew Postdoctoral Fellowship from 2015 to 2018. He has published over 200 research papers and book chapters in leading international conferences and journals. He is a Coauthor of the book *Federated Learning*—the first

monograph on the topic of federated learning. His research focuses on federated learning and algorithmic fairness.

Dr. Yu's research works have won multiple awards from conferences and journals. He is a Senior Member of CCF.



Jiawen Kang (Senior Member, IEEE) received the Ph.D. degree from Guangdong University of Technology, Guangzhou, China, in 2018.

He has been a Postdoctoral Fellow with Nanyang Technological University, Singapore, from 2018 to 2021. He currently is a Professor with Guangdong University of Technology. His research interests mainly focus on blockchain, security, and privacy protection in wireless communications and networking.



Xuemin (Sherman) Shen (Fellow, IEEE) received the B.Sc. degree in electrical engineering from Dalian Maritime University, Dalian, China, in 1982, and the M.Sc. and Ph.D. degrees in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1987 and 1990, respectively.

He is a University Professor in Electrical and Computer Engineering. His research focuses on wireless communication networks, including capacity analysis, mobility and radio resource management, Quality-of-Service provisioning, wireless/Internet interworking, network modeling, and stability and performance analysis. In addition, he has been investigating and developing algorithms and protocols for wireless network security and privacy preservation. His research findings have been applied to vehicular networks, wireless body area networks and remote e-healthcare systems, wireless ad hoc and sensor networks, and smart grid.

Prof. Shen received the R.A. Fessenden Award in 2019 from IEEE Canada; the James Evans Avant Garde Award in 2018 from the IEEE Vehicular Technology Society; the Joseph LoCicero Award in 2015; and the Education Award in 2017 from the IEEE Communications Society. He has also received the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award five times from the University of Waterloo.