IEEE Transactions on Quantum Engineering

Received June 27, 2020; revised August 4, 2020; accepted August 24, 2020; date of publication August 26, 2020; date of current version September 16, 2020.

Digital Object Identifier 10.1109/TQE.2020.3019738

Programmable Quantum Networked Microgrids

ZEFAN TANG[1] (Student Member, IEEE), PENG ZHANG[1,2] (Senior Member, IEEE), WALTER O. KRAWEC[3], AND ZIMIN JIANG[1]

[1] Department of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY 11794-2350 USA
[2] Sustainable Energy Technologies Department, Brookhaven National Laboratory, Upton, NY 11973-5000 USA
[3] Department of Computer Science and Engineering, University of Connecticut, Storrs, CT 06269 USA

Corresponding author: Peng Zhang (p.zhang@stonybrook.edu).

This work was supported in part by the National Science Foundation under Grants OIA-2040599 and ECCS-1831811 and in part by the Office of the Vice President for Research, Stony Brook University.

ABSTRACT Quantum key distribution (QKD) provides a potent solution to securely distribute keys for two parties. However, QKD itself is vulnerable to denial of service (DoS) attacks. A flexible and resilient QKD-enabled networked microgrids (NMs) architecture is needed but does not yet exist. In this article, we present a programmable quantum NMs (PQNMs) architecture. It is a novel framework that integrates both QKD and software-defined networking (SDN) techniques capable of enabling scalable, programmable, quantum-engineered, and ultra-resilient NMs. Equipped with a software-defined adaptive post-processing approach, a two-level key pool sharing strategy and an SDN-enabled event-triggered communication scheme, these PQNMs mitigate the impact of DoS attacks through programmable post-processing and secure key sharing among QKD links, a capability unattainable using existing technologies. Through comprehensive evaluations, we validate the benefits of PQNMs and demonstrate the efficacy of the presented strategies under various circumstances. Extensive results provide insightful resources for building QKD-enabled NMs in practice.

INDEX TERMS Networked microgrids, quantum key distribution, software-defined networking.

I. INTRODUCTION

Major power outages in the United States in 2019, e.g., blackouts in Texas [1] and New York City [2], reveal that our existing power infrastructure is insufficient to sustain the ever-growing communities and increasingly deep integration of renewable energies. Microgrids, as a localized self-governing distribution network, are oriented to supply electricity for a local community, and have been proven to be potent for enhancing electricity resilience [3]. Networking a group of local microgrids greatly promotes the coordination of microgrids for achieving various benefits such as supporting smart city operations and helping sustain neighboring distribution grids during extreme events [4], [5].

Although microgrids are promising, transforming them into networked microgrids (NMs) remains prohibitively difficult [6]. Among various challenges, a critical one is the data breach issue in the face of a broader attack surface in today's power distribution where data flows are created between customers and utility control centers [7], [8]. The challenge continues escalating as malicious adversaries are more and more well-equipped and motivated [9].

Quantum key distribution (QKD) provides a potent solution to securely distribute keys for two parties [10]. It uses fundamental laws of quantum mechanics instead of relying on mathematical assumptions. Because those physics laws have been fairly heavily tested, they provide a more solid foundation [11]. However, QKD, even though commercially available in some cases, is not yet widely applied in real-world contexts. Real-world applications have begun, although they remain very limited (e.g., SK Telecom provides some interesting industrial applications). While QKD has been adopted in applications such as automated teller machine transactions [12], computer networks [13], online banking [14], and portable applications [15], the microgrid community is largely silent on the topic of developing quantum-secured NMs. In the context of NMs, the existing QKD systems cannot be directly applied. There are numerous communication channels existing in NMs, which typically have different data transmission requirements. For

instance, the control center in a single microgrid can communicate with different local controllers in the same microgrid; the control center in a microgrid can also communicate with those in other microgrids. These communications are subject to different conditions including distances and data transmission frequencies. The larger the data transmission frequency is, the sooner the keys (generated by a QKD system) will be consumed. Moreover, the data transmission frequency for a certain communication can vary due to the dynamic characteristics of each microgrid such as the plug-and-play of different loads and distributed energy resources (DERs). Therefore, while a QKD system with a certain configuration works for one communication channel, it can be infeasible (as keys are likely to be exhausted) for another communication; a QKD system working normally at a specific time moment may also fail to work later on. A testbed integrating QKD and NMs characteristics for evaluating the performance of QKD-enabled NMs in different situations is required but does not yet exist.

Further, it has been identified that QKD itself is vulnerable to denial of service (DoS) attacks [16]. Any attempt to learn keys on quantum optical equipment causes noise, potentially leading to the exhaustion of keys. As the data transmissions in NMs are continuous, and the data transmission frequencies for most communications in NMs are typically larger than those in many other networks, keys generated by QKD are more likely to be exhausted in NMs. While the key exhaustion is not a big issue in many other applications, it appears to be more serious in NMs. To manage QKD networks, many existing works [17]–[20] use the software-defined networking (SDN) due to its high flexibility and programmability. However, while SDN promises in managing resources for tasks such as the multitenant provisioning over QKD networks [18], those works are not for mitigating DoS attacks on QKD-enabled NMs.

There are several existing approaches relevant to the mitigation of DoS attacks in QKD-enabled applications. A simple and traditional one is to switch back to classical key distribution, which however loses unconditional security. Most research groups [21]–[24] focus on reselecting different quantum channels for two distant partners during DoS attacks. For instance, Hugues-Salas *et al.* [21] experimentally demonstrate the effectiveness of simply selecting an alternative path for a QKD-enabled optical network under DoS attacks. Wang *et al.* [22] present an adaptive key protection scheme to route and allocate keys for constructing a protection path against DoS attacks. However, all those methods are only applicable to QKD networks where multiple quantum paths exist between two nodes. In the context of QKD-enabled NMs, there is normally only one quantum channel between two microgrids for budgetary reasons. Other existing methods including reserving backup resources [25] and strengthening classical cryptographic systems [26] either are too expensive or fail to flexibly respond to different situations.

To bridge the gaps, we present a programmable quantum NMs (PQNMs) architecture in this article. This novel framework incorporates both QKD and SDN techniques. Because SDN is reaching maturity, the formally verified technical merits of SDN may be leveraged to enhance some immature aspects of QKD which helps promote wide adoptions of QKD in real-world applications. To mitigate the impact of DoS attacks on quantum channels, a software-defined adaptive post-processing (SDAPP) approach and a two-level key pool sharing (TLKPS) strategy are developed. Equipped with SDAPP, TLKPS, and an SDN-enabled communication scheme, PQNMs are capable of efficiently mitigating the impact of DoS attacks through programmable post-processing and secure key sharing among QKD links. The investigation in this article demonstrates the feasibility of QKD in NMs and benefits of SDN applications in quantum-secured NMs, and provides valuable insights for building PQNMs in practice. The main contributions of this article are fourfold:

1) It devises a novel PQNMs architecture supporting both quantum security and high programmability. The SDN functions for supporting the presented defending strategies are derived and deployed in the SDN controller.
2) The novel SDAPP and TLKPS strategies are developed to mitigate DoS attacks on quantum channels. Different with the existing methods in QKD networks, the presented strategies are well suited for quantum NMs.
3) It develops an SDN-enabled event-triggered communication scheme that not only maintains PQNMs's resilience, but also reduces the bandwidth consumption.
4) It builds a QKD and SDN-enabled NMs testbed in a Mininet environment incorporating both key generation and data transmission properties, providing valuable insights for constructing PQNMs in practice.

The rest of this article is organized as follows. Section II presents the PQNMs's architecture and the DoS attack. Our SDAPP and TLKPS strategies and event-triggered communication scheme are described in Sections III and IV, respectively. Section V provides the testbed design and the extensive evaluation results. Section VI concludes the article.

II. PQNMS UNDER DOS ATTACKS

In this section, we first introduce our design of PQNMs's architecture, and then describe the DoS attacks on PQNMs and the difficulties of using existing approaches.

A. ARCHITECTURE OF PQNMS

The architecture of PQNMs is illustrated in Fig. 1. It consists of two layers: 1) a physical layer where multiple quantum microgrids (QGrids) are interconnected, and 2) a cyber layer where SDN is utilized to manage the network.

Each QGrid contains a microgrid control center (MGCC) along with numerous loads and DERs, i.e., photovoltaics (PVs), wind turbines, and battery storages. The MGCC is responsible for collecting information from loads and sending control signals to local controllers for some DERs. As building a quantum channel is costly, QKD is established

IEEE Transactions on Quantum Engineering

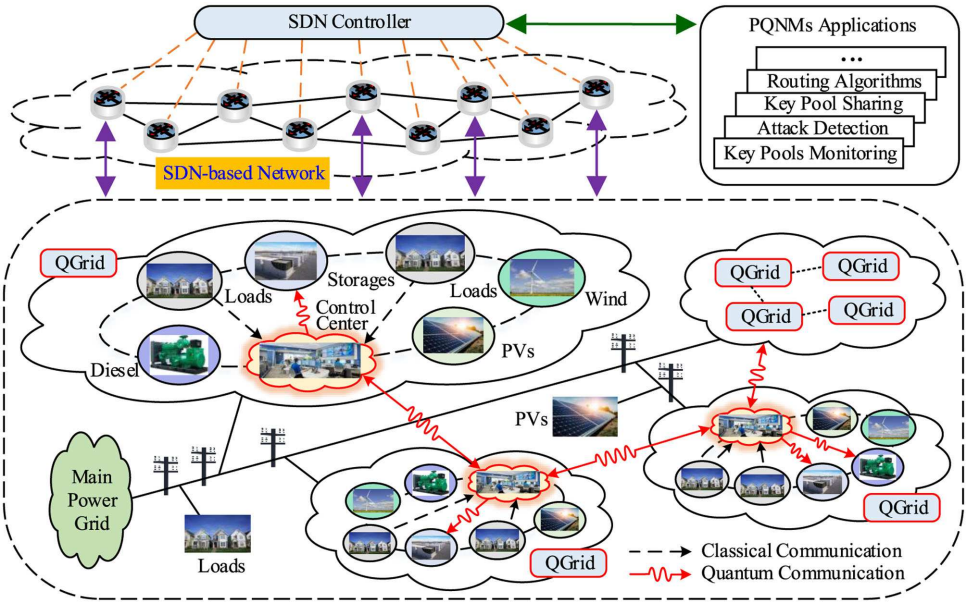


FIGURE 1. Architecture of PQNMs.

only for critical communications in this framework. Specifically, in each QGrid, the communications between MGCC and local controllers are established over quantum channels (typically using optical fibers to transfer quantum signals), and the communications between MGCC and loads are established over classical channels. Note that this arrangement is reasonable, because the data from different loads will be dealt with by some anomaly detection methods [27] when received by the MGCC. When malicious data are identified in the MGCC, various countermeasures can be carried out to minimize the impact on microgrid. Further, within a single microgrid, there are many loads distributed around, introducing numerous communications between the control center and different loads.

Note that microgrids accept different communication technologies: wired or wireless. Wired technologies commonly use the medium access control protocol as the data layer protocol which assigns addresses for connected communication devices. If optical fibers are used for wired communications, typically the wave division multiplexing (WDM) or synchronous optical network will be used as the physical layer protocol [28]. Note that there are some existing works on quantum-classical signal coexistence in the same fiber. Some existing methods include the multistage band-stop filtering, spaced channel configuration, and time-scheduled QKD-over-WDM [29]. A more general way for communication is, however, the use of wireless technologies due to the low cost, easy installation, and acceptable transmission speed. For wireless technologies, the long-term evolution (LTE) is typically used when the fourth-generation (4G) cellular networks are employed. Generally, if wireless technologies are used for microgrid classical communications, the optical fiber is only used for QKD. If optical fiber technologies are used for microgrid communications, one optical fiber can be used as the quantum channel and another fiber can be the classical one; or the quantum and classical signals can be in the same fiber with relevant techniques adopted. In this study, we consider that optical fibers are only used for QKD.

Keys used for communications between two MGCCs in different QGrids are also generated using QKD. Keys generated by different quantum channels are stored in separate key pools (KPs). In general, the receiver is relatively more expensive and more vulnerable to attacks than the transmitter in a QKD system. We therefore place the receiver within the MGCC, and the transmitter in each DER, as the MGCC has a high security level in microgrid and it becomes cost-effective for DERs to deploy QKD devices. This network design guarantees both secrecy and data integrity of critical communications through the use of keys produced by QKD. It also ensures that QKD devices, which are costly, are only allocated on critical levels of communications, and leaving others secured through post-quantum cryptographic systems. This architecture is expansible to support more quantum devices.

To enable intelligent and programmable networking in the communication network, SDN is employed in this architecture [30]. SDN is an innovative technique where the SDN controller manages flow controls with a specific protocol such as OpenFlow [31], making network switches become simple forwarding devices. By decoupling control and data planes and centralizing the control logic in the SDN controller, the controller obtains a global knowledge of network states, enabling the development of sophisticated applications. Note that the SDN network and QKD systems operate independently. The SDN controller only communicates with either MGCCs or DERs without affecting QKD operations. The keys generated by a QKD system can be managed with the help of a local key management system.

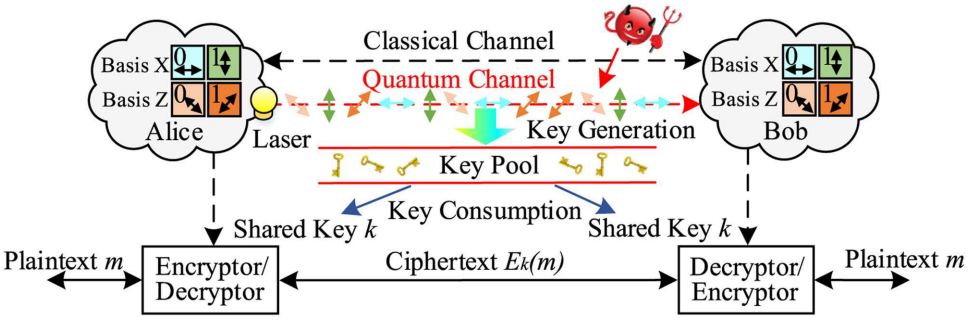


FIGURE 2. General setting of a QKD-based communication system.

B. DOS ATTACKS ON QKD SYSTEMS

The general setting of a QKD-based communication system is illustrated in Fig. 2. It consists of a quantum channel and a classical one, the functions of which are described as follows.

1) The quantum channel allows two parties to share quantum bits, i.e., qubits, for generating secure *raw keys*.
2) The generated raw keys are processed through post-processing over the classical channel to produce *secure keys* used for tasks such as encryption and authentication.
3) The produced secure keys are stored in a KP.

Keys produced by QKD are unconditionally secure because by using different, randomly chosen bases to encode classical bits, an adversary with little knowledge on the basis choices cannot truly obtain the information being transmitted. Further, any eavesdropping attack on the quantum channel causes noise which can be detected by the two parties.

However, this inevitably introduces DoS attacks. Any DoS attack on quantum optical equipment increases noise and causes key establishment sessions in a QKD system to be aborted, potentially leading to the exhaustion of keys.

Note that for detecting attacks on quantum channels, as far as the authors are aware, there is no "standard" way. One could imagine if the traffic is "stable," then an attack would cause a sudden drop of the key rate beyond normal limits. This can be used as a warning that the link is under attack. But there is no good solution to distinguish that from the low volume in the KP due to other reasons. Luckily, this does not matter—if the KP has a low volume, the exact cause does not matter so much as long as we have a way to actively compensate for the key loss.

C. DIFFERENCE BETWEEN QKD NETWORKS AND QUANTUM NMs

There are existing works on mitigating DoS attacks for QKD networks. However, while the approaches are applicable for QKD networks, they are not suited for quantum NMs. The difference between QKD networks and quantum NMs is illustrated in Fig. 3. As shown in Fig. 3(a), in a QKD network, multiple QKD paths exist between two nodes, and hence,

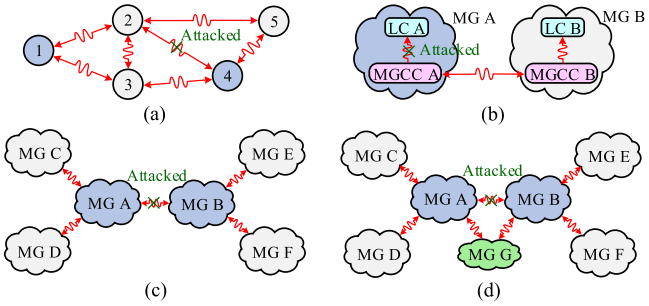


FIGURE 3. Difference between QKD networks and quantum NMs. (a) A typical QKD network. (b) Scenario 1: Attack within a single microgrid. (c) Scenario 2: Attack between two microgrids without an alternative QKD path. (d) Scenario 3: Attack between two microgrids with an alternative QKD path.

when one path is attacked, an alternative path can be switched to. For instance, Nodes 1 and 4 can select not only Paths 1–2–4, but also Paths 1–3–4, 1–2–3–4 and 1–3–2–4 to distribute keys between them.

However, a quantum NMs system typically has only one quantum path between two communicating parties, i.e., a MGCC and a local controller, or two neighboring MGCCs. Based on the NMs topology and location of the attack on the system, three cases exist as follows.

1) Scenario 1: The KP that lacks key bits is within a single microgrid, i.e., between a MGCC and a local controller.
2) Scenario 2: The KP that lacks key bits is between two microgrids that do not have an alternative QKD path.
3) Scenario 3: The KP that lacks key bits is between two microgrids with an alternative QKD path.

Most communications in NMs fall under Scenarios 1 and 2 as shown in Fig. 3(b) and (c), where there is only one QKD path between two communicating nodes. The traditional method for QKD networks, i.e., reselecting an alternative QKD path, is however infeasible in these cases. Generally, few situations are under Scenario 3 when an alternative QKD path exists between MGCCs A and B (i.e., MGCC A–G–B) as shown in Fig. 3(d).

III. DEFENDING STRATEGIES ENABLED BY SDN

To mitigate the impact of DoS attacks on PQNMs, we present an SDAPP approach and a TLKPS strategy. Specifically, SDAPP is launched to improve QKD's performance during the DoS attack, and TLKPS is performed when the number of bits in a KP is below a predetermined threshold. To demonstrate the defending strategies, without loss of generality, a practical decoy-state QKD protocol [32] is considered in this study. Note that other QKD protocols can also be used where the principles can be easily extended.

A. QKD MODELING AND THE SDAPP APPROACH

In our testbed, we simulate QKD's performance using Python and integrate the QKD simulator into microgrid simulator, i.e., Matlab/Simulink. This testbed thus incorporates both key generation and data transmission properties, providing valuable resources for evaluating PQNMs's performance in different situations. Simulating a QKD system requires mathematical modeling of the QKD protocol. In this subsection, we briefly present the modeling of the decoy-state protocol.

The idea of this protocol is as follows: One party, commonly named Alice, randomly selects a classical bit from 0 and 1, and a quantum encoding basis X or Z (with probabilities p_x and $1-p_x$, respectively). Alice then uses the selected basis to encode the selected bit for preparing a quantum bit (i.e., qubit), and sends the qubit to the other party (named Bob) through the quantum channel. Weak coherent laser pulses are used to implement qubits, and the diagonal and horizontal polarizations of each photon are utilized as the X and Z bases, respectively. The intensity of each laser pulse varies from three intensities k_1, k_2, and k_3 with probabilities p_{k_1}, p_{k_2}, and $p_{k_3} = 1 - p_{k_1} - p_{k_2}$, respectively. For each qubit Bob receives, he randomly selects a basis from X and Z with probabilities p_x and $1-p_x$, respectively, and decodes the qubit with the selected basis. When a block size (N_b) of bits are received by Bob, the two parties share a raw key.

The number of signals actually sent by the laser for generating N_b correctly received signals can be expressed as

$$N_a = \frac{N_b}{R_s} \tag{1}$$

where R_s is the rate of correctly received raw-key signals.

Let v_a be the speed of the laser sending signals, a constant value assumed in this study. Then, N_a can be expressed as

$$N_a = v_a \Delta t \tag{2}$$

where Δt is the time required to send N_a signals by the laser. From (1) and (2), Δt can be obtained as

$$\Delta t = \frac{N_b}{R_s v_a}. \tag{3}$$

In practice, N_b is a user-specified parameter. From (3), with the constant R_s and v_a, the larger the N_b, the larger the Δt.

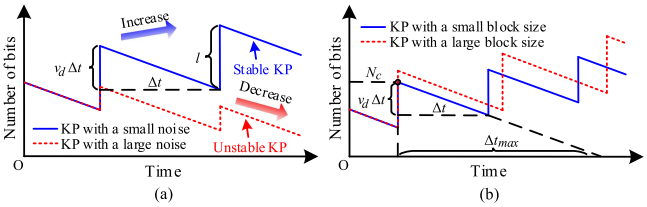


FIGURE 4. QKD's performance with different noises and block sizes. (a) KP's performance with different noises and (b) KP's performance with different block sizes.

When N_b signals have been received by Bob, the post-processing starts. The key extracted after the post-processing (which is called the secure key) will be unconditionally secure, the length (ℓ) of which has been found as follows [32]:

$$\ell = \left\lfloor \zeta_{X,0} + \zeta_{X,1} - \zeta_{X,1} h(\theta_X) - \beta_c - 6\log_2 \frac{21}{p_d} - \log_2 \frac{2}{p_f} \right\rfloor \tag{4}$$

where $\zeta_{X,0}$, $\zeta_{X,1}$, and θ_X are the number of vacuum events, the number of single-photon events, and the phase error rate associated with the single-photon events in the raw key from Alice's side, respectively. $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. p_d is the probability that the keys at the two sides are not identical, and p_f is the maximum failure probability, a user-specified value. β_c specifies the amount of information leaked during error correction. It is set to $n_X \eta_c f(\theta_X)$, where n_X is the number of bits with X bases in the raw key from Alice's side, and η_c is the error correction's efficiency.

By using the decoy-state protocol, the above parameters can be bounded, and their deviations can be found in [32].

In our architecture, we assume a standard fiber channel and practical settings for devices. In this case, the probability of having a bit error for intensity k, δ_k, is as follows [33]:

$$\delta_k = p_{dc} + e_{\text{mis}}(1 - e^{-\tau_r k}) + \frac{p_{ap} d_k}{2}, \ \forall k \in \{k_1, k_2, k_3\} \tag{5}$$

where p_{dc} and p_{ap} are the dark count and after-pulse probabilities, respectively. e_{mis} is the error (mainly caused by optical errors) rate. The attack on a quantum channel can be modeled by setting a large e_{mis}. τ_r is the transmittance that is related to the fiber length L as follows:

$$\tau_r = 10^{-\alpha L/10} \tag{6}$$

where the fibers are assumed to have an attenuation coefficient $\alpha = 0.2$ dB/km. In (5), d_k is the expected detection rate (excluding after-pulse contributions), and can be calculated as follows:

$$d_k = 1 - (1 - 2p_{dc}) e^{-\tau_r \eta_r k}, \ \forall k \in \{k_1, k_2, k_3\} \tag{7}$$

where η_r is the receiver's detection efficiency.

Fig. 4 gives an example of QKD's performance with different noises e_{mis}'s and block sizes N_b's, where v_d is the key consumption speed. This figure is not from simulation or experiment, but for an illustration of the impacts of the noise

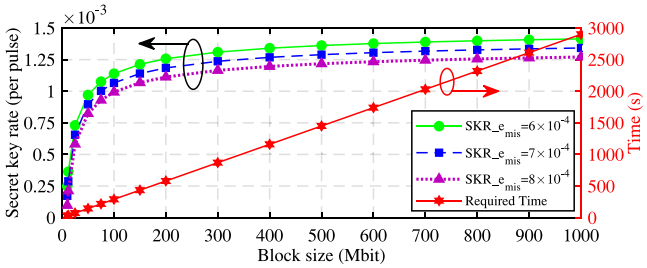


FIGURE 5. Secret key rate and time needed for generating the secret key of size ℓ with different block sizes.

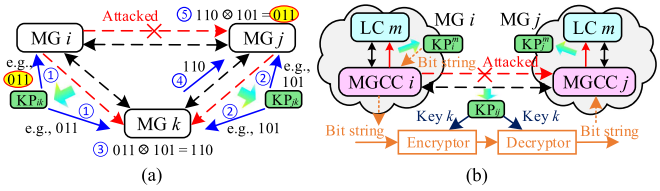


FIGURE 6. Illustration of the TLKPS strategy. (a) The first level of TLKPS and (b) The second level of TLKPS.

and block size. The QKD's performance in different situations (i.e., with difference noises and block sizes) is evaluated with our testbed as will be shown later. Within Δt, when the time increases, the number of bits in the KP continues decreasing before a certain number of bits are generated (i.e., for a discrete-variable QKD system). This key bit consumption is caused by the continuous data transmission in NMs, as each data packet transmission leads to the consumption of a certain number of bits in the KP (i.e., when one-time pads are used as the encryption method). For a discrete-variable QKD system, after a given time (i.e., Δt), a certain number (ℓ) of bits will be generated.

As shown in Fig. 4(a), a small noise on the quantum channel can eventually increase the number of bits in the KP, and the KP remains "stable." A larger noise does not affect Δt, but reduces ℓ. The KP can become "unstable"—that is, the number of bits in the KP gradually decreases and eventually reaches zero. To avoid keys being exhausted, the following condition should be satisfied:

$$\ell \geq v_d \Delta t. \tag{8}$$

In practice, people are often interested in the secret key rate (SKR), which is defined as follows:

$$\text{SKR} = \frac{\ell}{N_a}. \tag{9}$$

From (2), (8), and (9), SKR should satisfy

$$\text{SKR} \geq \frac{v_d}{v_a}. \tag{10}$$

Fig. 5 gives the performance of the SKR and Δt under different N_b's, where N_b is tuned from 10 Mbits to 1000 Mbits and e_{mis} is set at 6×10^{-4}, 7×10^{-4}, and 8×10^{-4}, respectively. Other parameters of the QKD system are the same as in [32]. It can be seen that, with a given e_{mis}, the larger the N_b, the larger the SKR. It indicates that, to satisfy the condition in (10), a larger N_b should be selected.

However, N_b should not be too large, because a larger N_b also leads to a larger Δt [refer to (3)]. As shown in Fig. 4(b), the maximum Δt can be obtained as follows:

$$\Delta t_{\max} = \frac{N_c}{v_d} \tag{11}$$

where N_c is the current number of bits in the KP. Substituting (3) into (11), N_b should satisfy the following condition:

$$N_b \leq \frac{N_c R_s v_a}{v_d}. \tag{12}$$

The idea of the SDAPP approach is as follows.

1) When the KP is stable, no action is needed.
2) When the KP becomes unstable, the two parties increase N_b, while (12) is satisfied.
3) When the TLKPS is triggered, the SDN controller sends control signals to related QKD nodes to increase N_b's for corresponding QKD systems.

Note that the photon loss in a quantum channel is a fundamental limitation on the key-generation rate of any QKD protocol, even augmented with unlimited two-way classical communication [34], [35]. In fact, the so-called PLOB bound, named for the authors of [35], shows that the key rate of a QKD protocol is proportional to $-\log_2(1-\tau_r)$, where τ_r is the transmittance of the channel [see (6)]. This rate may be overcome through the use of quantum repeaters or through twin-field QKD (TF-QKD) [36], [37]. Thus, quantum repeaters could improve the distance limitation of QKD networks, and we leave an exact study of how this would affect SKRs in our simulations as future work.

B. SDN-ENABLED TLKPS STRATEGY

When an attack on the quantum channel is detected, the microgrid operator can check the status of the system and clear the attack within a certain time. If the attack is cleared before keys are exhausted, normal data transmissions will not be affected because they are performed over classical channels. However, if the number of bits in the KP is below a certain level, data transmissions are likely to be affected. To tackle this issue, the TLKPS strategy is established.

An example of this strategy is illustrated in Fig. 6. In general, this strategy contains two levels. A threshold T_h is first determined to restrict the minimum number of bits in a KP, meaning if the number of bits in a KP is below T_h, a given number (N_s) of bits will be shared from other KPs through either the first or the second level of TLKPS, the selection of which is determined by the SDN controller depending on the scenario. Only when the KP is between two microgrids with an alternative QKD path where sufficient keys exist, the first level of TLKPS is implemented; otherwise, the second level of TLKPS is performed. Let KP_{ij} be the KP between MGCC

i and MGCC j, N_{ij} the number of bits in KP_{ij}, KP_i^t the KP between MGCC i and the tth local controller within MG i, and N_i^t the number of bits in KP_i^t.

When there exists a microgrid, namely MG k, that establishes KPs with both MG i and MG j, and the numbers of bits in KP_{ik} and KP_{jk} are both above $(T_h + N_s)$, N_s bits can be shared to KP_{ij} using the first layer of TLKPS. In this case, MG k is utilized as an intermediate node to distribute keys for MG i and MG j. As illustrated in Fig. 6(a), MG k and MG i both extract a string of bits from KP_{ik}, and MG k and MG j both extract the same number of bits from KP_{jk}. MG k then XORs the extracted two-bit strings, and sends the result to MG j. MG j XORs the received bit string with the bit string extracted previously from KP_{jk}. The result obtained by MG j will be exactly the same as the bit string extracted by MG i from KP_{ik}. In this way, a string of bits is securely transferred from KP_{ik} and KP_{jk} to KP_{ij}. Note that this first level of TLKPS still maintains information-theoretic security, and is thus given the first priority in TLKPS.

However, in most cases, there is no such intermediate node, or attacks are performed on multiple links, making intermediate microgrids fail to share enough bits. The second level of TLKPS is thus established. As shown in Fig. 6(b), when N_{ij} is below T_h, KP_i^m is utilized to share bits for KP_{ij}. Note that 1) when the KP that lacks bits is between two microgrids, the selection is completed by the SDN controller; and 2) when the KP that lacks bits is within a single microgrid, this selection can be achieved by the MGCC. A bit string is first extracted from KP_i^m, and is then used as a plaintext, encrypted by MGCC i via Advanced Encryption Standard (AES) with a key extracted from KP_{ij} (note there are still some keys left in KP_{ij}), and sent to MGCC j. MGCC j uses the same key from KP_{ij} to decrypt the received message and obtains the bit string. A bit string is thus transferred from KP_i^m and is securely shared to KP_{ij}. Note that this AES-based key distribution is given the second priority in TLKPS because it loses information-theoretic security; but it is still better than relying on public key systems because AES is considered quantum-secure [38].

There exists a body of literature on QKD resource management for the QKD networks. For instance, Cao *et al.* [29] present a time-scheduled QKD-over-WDM scheme for key pool management where either uniform or nonuniform time slots are allocated for the construction of different KPs. However, this method is different with the TLKPS strategy in that TLKPS does not require time slots and utilizes the existing secret keys which is more time-efficient. Wang *et al.* [39] present three secret-key recovery strategies, namely the one-path recovery method, multipath recovery method, and time window-based recovery method. However, these methods are infeasible in NMs where generally limited QKD paths exist between two communicating parties.

IV. SDN-ENABLED COMMUNICATION SCHEME

Each microgrid has its own information such as the number of KPs it connects and the number of bits in each KP. It is, however, typically unconscious of the information owned by other microgrids. The SDN controller is thus established to manage the network by collecting information from each microgrid and providing the optimal decision unattainable by a single microgrid. In this study, SDAPP and TLKPS are enabled by SDN to mitigate DoS attacks under various circumstances. Specifically, the SDN controller has the following functions.

1) It monitors the information of KPs including the number of KPs each MGCC possesses and symbols indicating whether each KP is willing to share bits for other KPs. It updates the information periodically.
2) If faced with a DoS attack, it determines which case it is and tells corresponding MGCCs which layer of the TLKPS strategy should be implemented.
3) It provides parameters modification for each KP enabling a resilient, flexible, and economical NMs system.

As the TLKPS strategy is only required when the number of bits in a KP is lower than a threshold T_h, an event-triggered communication scheme is established to reduce the communication bandwidth while still maintaining the system resiliency.

A. KPS MONITORING

The SDN controller is a logically centralized network controller that has access to all the SDN switches. It can communicate with all the MGCCs to collect KPs' information. In the presented scheme, the SDN controller periodically sends requests to all the MGCCs. Once receiving a request, each MGCC sends corresponding information to the SDN controller. It is thus important for the SDN controller to identify each MGCC and corresponding local controllers. Using the IP protocol as an example, each MGCC or local controller has a unique IP address. The information sent from each MGCC to the SDN controller includes the following.

1) IP addresses of all the local controllers that have established KPs with the MGCC. By knowing the local controllers' IP addresses, the SDN controller not only obtains the number of KPs inside each microgrid, but also identifies those KPs.
2) IP addresses of all the neighboring MGCCs that have established KPs with the MGCC. Similarly, the SDN controller obtains the number of KPs the MGCC connects outside the microgrid and identifies those KPs. Importantly, the SDN controller obtains a global overview of the KPs, with which it can determine if there is an alternative QKD path between two microgrids.
3) A symbol (i.e., 0 or 1) for each KP indicating whether the MGCC is willing to share bits from this KP to other KPs at this moment. With this information, the SDN controller determines which KPs should be utilized to

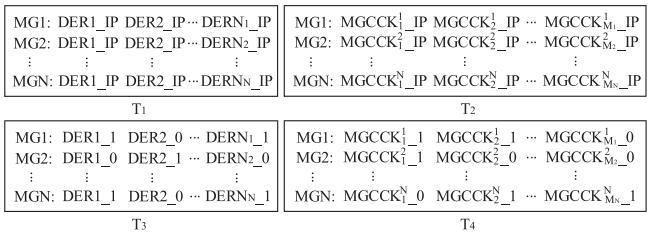


FIGURE 7. Lookup tables in the SDN controller.

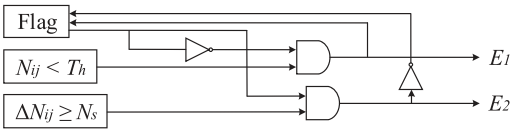


FIGURE 8. Logic diagram of the event detection.

share bits in TLKPS. Compared with sending the number of bits in each KP, the confidentiality is improved.

Once the SDN controller receives the above information, it updates the lookup tables, i.e., T_1–T_4 as shown in Fig. 7. Specifically, tables T_1 and T_2 store IP addresses of local controllers and neighboring MGCCs that have established KPs with each MGCC, respectively. Tables T_3 and T_4 store the binary bits for KPs established inside each microgrid and between two microgrids, respectively. "1" indicates that the KP is willing to share bits for other KPs, and "0" means the KP refuses to share bits for other KPs. These tables will be checked when an event occurs and a request from any MGCC is received by the SDN controller.

B. EVENT-TRIGGERED COMMUNICATION

To reduce the network bandwidth consumption (corresponding to the achieved throughput, i.e., the average rate of successful data transfer through a communication path), an event-triggered communication scheme is developed. E_1 and E_2 are two events defined in this scheme where E_1 refers to the bit-sharing request from any MGCC to the SDN controller and E_2 is the request clearance after bit sharing is completed. These events are detected by each MGCC. The logic diagram of the event detection is illustrated in Fig. 8.

Specifically, an E_1 event is triggered when the number of bits in a KP between two microgrids (i.e., N_{ij}) is detected to be lower than the threshold T_h. Note that if the KP between any MGCC and a local controller lacks bits, the MGCC can implement the second layer of TLKPS directly because it has control of all the KPs surrounding itself. E_2 is triggered only after E_1 is triggered and when the given number (i.e., N_s) of bits have been shared to the KP. This detection sequence can be achieved by setting a flag which is initialized at zero.

When an E_1 event is triggered, the MGCC sends the E_1 request including its own IP address and the IP address of the other MGCC (with which the KP is established) to the SDN controller. Assume the index numbers of the two MGCCs

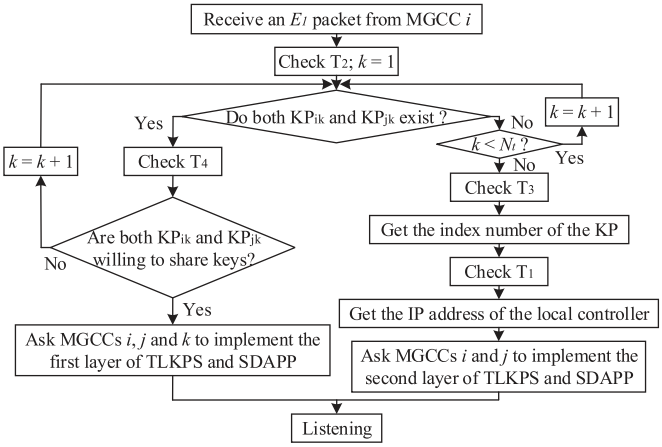


FIGURE 9. Flow chart of the SDN controller for the E_1 event.

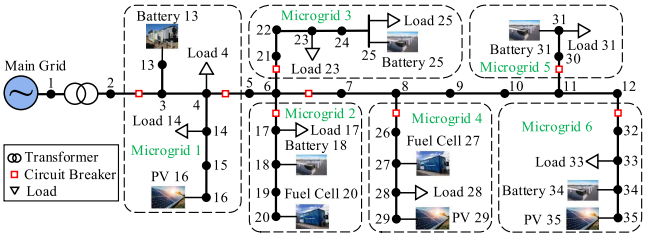


FIGURE 10. One-line diagram of the NMs model.

are i and j, respectively. Upon receiving the request, the SDN controller checks T_2 to determine whether there are any MGCCs that have established KPs with both MGCCs i and j. The procedures are shown in Fig. 9, where N_t refers to the total number of microgrids, and are also summarized below.

1) If there exists one MGCC k (checked in T_2) and the bits for both N_{ik} and N_{jk} are 1 (checked in T_4), the SDN controller sends control signals to MGCCs i, j, and k to implement the first layer of TLKPS and the SDAPP.
2) Otherwise, the SDN controller checks T_3 to select a KP from all KPs within MGs i and j that are willing to share keys. With the index number of the selected KP, the SDN controller checks T_1 to obtain the local controller's IP address, and sends it to MGCCs i and j to implement the second layer of TLKPS and the SDAPP.

Note that the SDAPP is implemented not only for attacked KPs but also for KPs that will share bits to attacked KPs. When an E_2 event is triggered, the SDN controller sends control signals to corresponding MGCCs to finish the sharing.

V. TEST AND VALIDATION

A typical NMs system shown in Fig. 10 is used to evaluate the performance of PQNMs in this study. This system is based on the NMs model from [40] with control centers and varying loads added. It contains six microgrids, and can operate in either grid-connected or islanded mode depending on whether

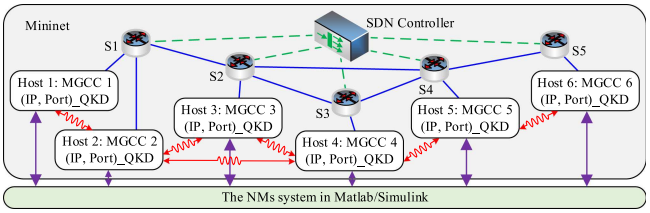


FIGURE 11. Testing environment in this study.

the circuit breaker between buses 2 and 3 is closed or open. The DERs in this NMs system include three PV systems, two fuel cells, and five battery storages. More details on the system can be found in [40].

In this study, the NMs operate in the way below. The NMs system works in islanded mode, meaning the circuit breaker between buses 2 and 3 is open. Each MGCC receives not only load information from different loads within the same microgrid, but also packets from other MGCCs. It sends control signals to corresponding DERs within the same microgrid to regulate their power outputs. Note that information exchange between two microgrids is needed because the power generated from DERs in a single microgrid can oftentimes reach a capacity limit. A negative value in the packet sent from one MGCC to a neighboring MGCC refers to the active power requested to be sent by the neighboring microgrid. A positive value indicates that the power generated by DERs is sufficient to support all the loads within the same microgrid and a certain amount of active power can be provided for other microgrids; this power can be the difference between the sum of DERs' capacity limits and the sum of loads within the single microgrid. In this study, without loss of generality, each fuel cell in Fig. 10 uses P–Q control to regulate its power output, whose active power reference is received from the MGCC, while the PVs (which use MPPT control) and batteries (which use v/f control) do not establish communication channels with MGCCs.

Fig. 11 illustrates the testing environment where the NMs system is modeled in Matlab/Simulink and the SDN network is running in Mininet, a network simulator equipped with virtual hosts, switches, and links running on a Linux kernel. In this study, each MGCC is modeled using a Mininet host, which is a virtual server with a user-specified IP address and port capable of communicating with not only other hosts but also the NMs in Simulink. Five switches are created, the connection of which is also given in Fig. 11. An SDN OpenFlow controller Ryu is used to manage the network. In Simulink, the whole NMs system has one IP address with different ports assigned to loads and DERs. Note that in this case, the SDN controller stores each DER's port in its lookup tables; in reality, each DER can have a different IP address. User Datagram Protocol (UDP) is adopted to transmit data packets, meaning any UDP packet whose destination IP address and port match those of the server will be received by the server. The simulation time step is set at 50 μs, and the bandwidth for each communication link is set at 1 Gbps.

TABLE 1. QKD systems' initial configurations in the testbed

KP	From	To	L (km)	e_{mis}
KP_{12}	MGCC 1	MGCC 2	5	6×10^{-4}
KP_{23}	MGCC 2	MGCC 3	10	5×10^{-4}
KP_{24}	MGCC 2	MGCC 4	10	5×10^{-4}
KP_{34}	MGCC 3	MGCC 4	10	5×10^{-4}
KP_{45}	MGCC 4	MGCC 5	12	6×10^{-4}
KP_{56}	MGCC 5	MGCC 6	7	6×10^{-4}
KP_2^1	MGCC 2	Fuel Cell 20	5	5×10^{-4}
KP_4^7	MGCC 4	Fuel Cell 27	5	5×10^{-4}

QKD systems are simulated using Python in this study, and run on Mininet hosts. The QKD simulator simulates the occurrence probabilities of various events including multiphoton emission, phase errors, photons being lost in the channel, and imperfections of the detector. Time is used as the indicator to determine whether a sufficient number of key bits have been received such that post-processing can start. When the simulator is called, it determines the number of signals that have been sent from the last call, the choices of the user for those signals, and whether a measurement outcome was obtained by the receiver. More details of the QKD simulator can be found in our prior work [9]. The generated key bits are stored in separate KPs, and when there is a need to send a packet, a certain number (i.e., 64 in this study) of bits are consumed from the corresponding KP. This testbed design integrates both key generation (from QKD systems) and key consumption (from data transmission) properties, thus providing valuable resources for evaluating PQNMs's performance in different situations. In this testbed, eight QKD systems are established. Their connections and initial configurations are given in Table 1. Other parameters of each QKD system are initially the same as in [9].

A unique benefit of this testbed is that it combines quantum key generation with classical NMs data transmission. For a QKD system, keys are continuously generated and stored into a KP. When a classical data packet needs to be transferred, a certain number of key bits need to be consumed (when the one-time pad is used as the encryption method). With this unique feature, various research works can be conducted to evaluate the performance of the QKD-enabled NMs, and thus one can obtain valuable insights unattainable by other existing NMs testbeds. This testbed offers a more realistic environment for evaluating either the QKD performance under different NMs conditions (e.g., with different data transmission speeds), or the NMs performance with different QKD configurations (e.g., how the NMs performs when keys are exhausted, when keys in a QKD system will be exhausted under different conditions, etc.).

A. QKD PERFORMANCE WITH DIFFERENT FIBER LENGTHS AND NOISES

The QKD's performance with different fiber lengths L's and noise levels e_{mis}'s is evaluated using the testbed. In this case, the number of bits in KP_2^1 is recorded. L for this KP is set at 5, 7, and 10 km, respectively, and e_{mis} is 6×10^{-4}, 7×10^{-4}, and 8×10^{-4}, respectively. Note that a microgrid

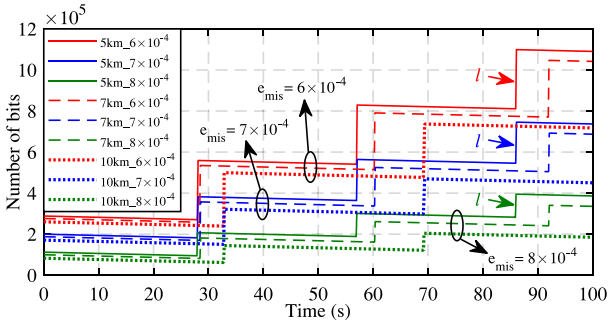


FIGURE 12. QKD performance under different fiber lengths and noise levels.

is a small-scale localized distribution network, the size of which is small. In NMs, only two neighboring microgrids typically require communication to share power with each other. Two microgrids with a large distance commonly do not share power with each other (and therefore do not require communication) mainly because 1) large electrical distance would prevent power transfer between the microgrids and 2) long-distance reactive power delivery would cause high power losses and voltage issues. For an unrepeatered QKD system, the distance between two communicating nodes can be as large as hundreds of kilometers. In microgrids or NMs, it is normally not necessary to use quantum repeaters due to the small scale. However, quantum repeaters will be needed for a quantum-secure regional power grid or even a larger national grid with a much larger distance between two communicating parties.

In this test case, the data transmission speed for the classical communication is set at 10 packets/s. As mentioned, when a data packet is received by the MGCC, 64 bits are deducted from the corresponding KP. The comparison results are shown in Fig. 12.

It can be observed that 1) a larger L greatly increases the time required to produce the key of size ℓ, and only slightly decreases the value of ℓ (see the lines with the same colors in Fig. 12); and 2) e_{mis} does not affect the time required to produce the key of size ℓ; but a larger e_{mis} greatly reduces the value of ℓ. A strong DoS attack on quantum channel can severely decrease the quantum key generation speed, potentially leading to the exhaustion of keys in a KP.

B. BASELINE TEST: PQNMS PERFORMANCE IN NORMAL SITUATIONS

This subsection evaluates the PQNMs's performance in normal situations when there is no attack. The QKD systems' configurations are given in Table 1. At time $t = 1$ s, a time-varying load with a magnitude of 100 kW and a frequency of 1 Hz is added to Load 4 (which is initially zero). A packet containing the value of this load is continuously sent from Load 4 to MGCC 1, and is forwarded by MGCC 1 to MGCC 2, requesting that a certain amount of power be generated by Microgrid 2 to support the load variation in Microgrid 1. When MGCC 2 receives the packet from MGCC 1, it

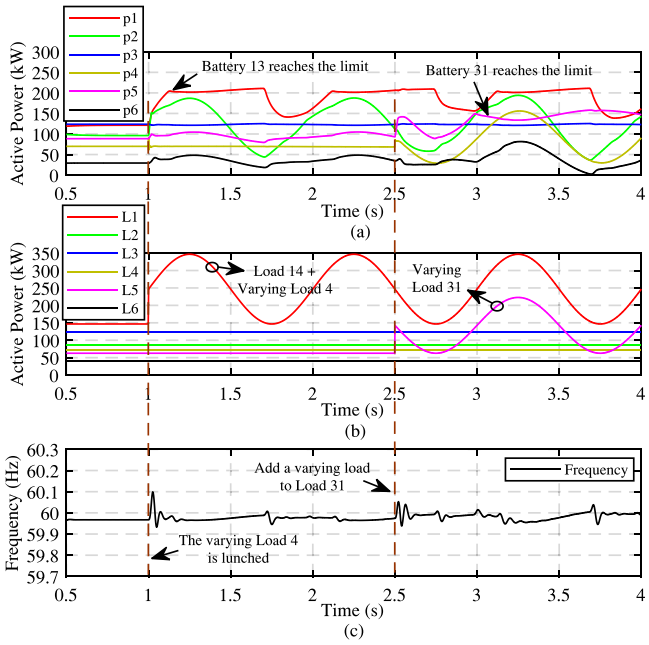


FIGURE 13. System response with varying loads added and communications enabled in normal situations without attack. (a) The total active power generated in each microgrid, (b) The sum of loads in each microgrid, and (c) The system frequency.

sends the active power reference to Fuel Cell 20 to regulate its power output. If there are enough keys in KP_{12}, the communication between MGCCs 1 and 2 remains normal; otherwise, the communication will be interrupted.

At time $t = 2.5$ s, another time-varying load with a magnitude of 80 kW and a frequency of 1 Hz is added to Load 31 (which is initially 62.75 kW). Similarly, a packet containing the variation of this load is continuously sent from Load 31 to MGCC 5, and is forwarded by MGCC 5 to MGCC 4, requesting that a certain amount of power be generated by Microgrid 4 to support the load variation in Microgrid 5. When MGCC 4 receives the packet from MGCC 5, it sends the active power reference to Fuel Cell 27 to regulate its power output.

The responses of the total active power generated in each microgrid, the sum of loads in each microgrid, and the system frequency are illustrated in Fig. 13. It can be seen that, when a varying load is added to Load 4 at time $t = 1$ s, the active power generated from Microgrid 1 quickly reaches the capacity limit (which is set at 200 kW). Meanwhile, extra power is generated in Microgrid 2 to support the load variation in Microgrid 1. Similarly, at time $t = 2.5$ s, the active power generated from Microgrid 5 reaches the capacity limit and extra power is generated in Mirogrid 4 to support the load variation in Microgrid 5. The effectiveness of the data transmission in the PQNMs is validated.

C. PQNMS PERFORMANCE AFTER KEYS ARE EXHAUSTED

The performance of PQNMs after keys are exhausted in a KP is evaluated in this subsection. Fig. 14 illustrates the active

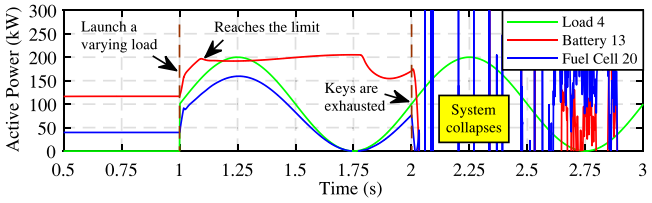


FIGURE 14. Performance of the PQNMs before and after keys are exhausted.

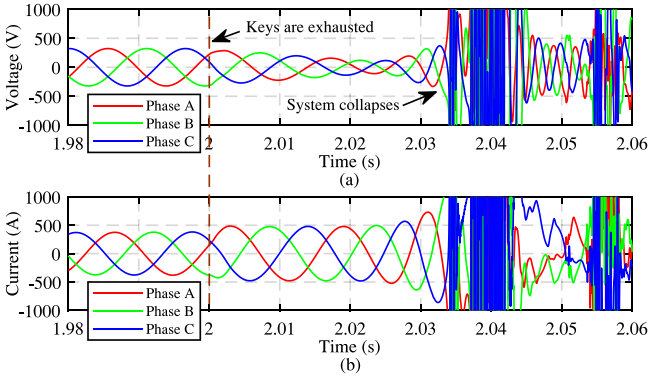


FIGURE 15. Voltage and current at bus 13 before and after keys are exhausted. (a) Voltage response of bus 13 before and after keys are exhausted and (b) Current response of bus 13 before and after keys are exhausted.

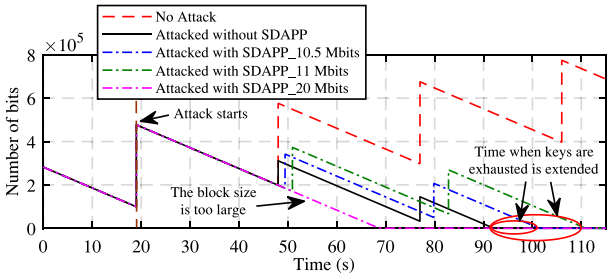


FIGURE 16. Effectiveness of the SDAPP with different block sizes under attacks.

powers of Load 4, Battery 13, and Fuel Cell 20 before and after keys are exhausted in KP_{12}, and the voltage and current responses are given in Fig. 15.

It can be observed that 1) before keys are exhausted (i.e., $t < 2$ s), the power generated by Battery 13 reaches the capacity limit (i.e., 200 kW); however, the system remains stable; and 2) when keys are exhausted in KP_{12} at time $t = 2$ s, the system eventually collapses in a short time.

D. VALIDATION OF SDAPP

The effectiveness of the SDAPP is validated in this subsection. The number of bits in KP_2^1 is recorded where the initial block size is set at 10 Mbits. e_{mis} for this KP is set at 5×10^{-4} and 8×10^{-4} for no attack and strong attack, respectively. Other parameters are the same as shown in Table 1. Fig. 16 illustrates the comparison results of the numbers of bits in KP_2^1 with and without SDAPP, where the block size for the

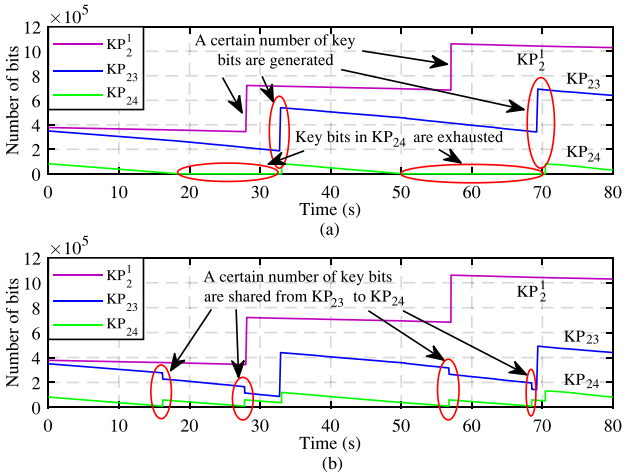


FIGURE 17. Numbers of bits in KP_2^1, KP_{23}, and KP_{24} with and without TLKPS when the quantum channel between MGCCs 1 and 2 is attacked. (a) Comparison results of different KPs' sizes without TLKPS and (b) Comparison results of different KPs' sizes with TLKPS.

SDAPP is set at 10.5, 11, and 20 Mbits, respectively. It can be seen that 1) a slightly larger block size extends the time when keys are exhausted during the attack (see the blue and green lines); and 2) a block size that is too large causes keys to be exhausted sooner (see the purple line).

E. VALIDATION OF TLKPS

To validate the effectiveness of TLKPS, the quantum channel between MGCCs 2 and 4 is attacked, i.e., e_{mis} for KP_{24} is set at 8×10^{-4}. Other parameters are the same as shown in Table 1. For the TLKPS strategy, the threshold is set at 10,000, meaning that once the number of bits in any KP is below 10 000, a given number (which is set at 50 000) of bits will be shared to that KP.

The comparison results of the numbers of bits in KP_2^1, KP_{23}, and KP_{24} with and without TLKPS are given in Fig. 17. It can be seen that 1) without TLKPS, there is a shortage of bits in KP_{24} while other KPs do not have shortage issues; and 2) with TLKPS, the shortage issue can be well solved; whenever the number of bits in KP_{24} is below 10 000, 50 000 bits are sent from KP_{23} to KP_{24}.

F. EFFECTIVENESS OF SDN-ENABLED COMMUNICATION

This subsection validates the effectiveness of the SDN-enabled event-triggered scheme. Specifically, the SDN controller receives 10 data packets from each MGCC per second to update the information. When an E_1 event occurs, the speed for the E_1 packets transmission from the MGCC to the SDN controller is set at 100 packets/s. At time $t = 20$ s, the number of bits in KP_2^1 is below the threshold and E_1 packets are sent from MGCC 2 to the SDN controller. At time $t = 55$ s, both KP_2^1 and KP_4^1 lack bits and E_1 packets are sent from MGCCs 2 and 4 to the SDN controller. When an E_1 packet is received by the SDN controller, the TLKPS

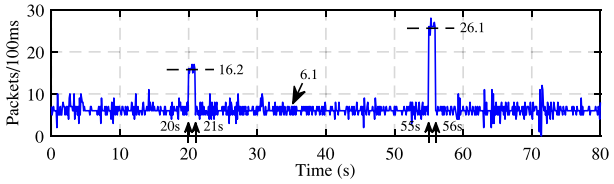


FIGURE 18. Data packets received by the SDN controller during two events.

is implemented and is completed in 1 s. The data packets received by the SDN controller are monitored using Wireshark, and the results are illustrated in Fig. 18.

It can be observed that the throughput increases to 16.2 packets/100 ms from 20 to 21 s, and 26.1 packets/100 ms from 55 to 56 s, signaling that the SDN controller has received the packets during E_1 events. Compared with continuous data transmissions, this scheme requires a shorter period, greatly reducing the usage of communication bandwidth.

VI. CONCLUSION

This article presents a novel PQNMs architecture incorporating both QKD and SDN techniques. Defending strategies including the SDAPP and TLKPS are designed to mitigate DoS attacks. This is an important step toward constructing resilient, flexible, and quantum-secured NMs in practice. With the presented techniques and progresses, more research work could be done in the future. For instance, it is reasonable to move forward to architect a quantum-secured regional power grid, or even a larger national grid. The QKD-enabled NMs testbed will be beneficial for not only power industry but also quantum community for evaluating the performance of more advanced and practical QKD protocols.

REFERENCES

[1] R. Owens, "More than 200,000 Dallas-area customers still without power Monday night; Oncor asks for patience," *CBS DFW News*, 2019. [Online]. Available: https://dfw.cbslocal.com/2019/06/10/dallas-customers-without-power-oncor-patience/

[2] J. Barron and M. Zaveri, "Power restored to Manhattan's west side after major blackout," *The New York Times*, 2019. [Online]. Available: https://www.nytimes.com/2019/07/13/nyregion/nyc-power-outage.html

[3] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh, and R. Jin, "Enabling resilient microgrid through programmable network," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2826–2836, Nov. 2016, doi: 10.1109/TSG.2016.2589903.

[4] P. Zhang and B. Wang, "Enabling reliable networked microgrids for distribution grid resiliency," *Proposal for Grant No. ECCS-1611095, U.S. National Science Foundation*, Nov. 2015.

[5] Z. Tang *et al.*, "Extreme photovoltaic power analytics for electric utilities," *IEEE Trans. Sustain. Energy*, vol. 11, no. 1, pp. 93–106, Jan. 2018, doi: 10.1109/TSTE.2018.2884500.

[6] M. N. Alam, S. Chakrabarti, and X. Liang, "A benchmark test system for networked microgrids," *IEEE Trans. Ind. Inform.*, vol. 16, no. 10, pp. 6217–6230, Oct. 2020, doi: 10.1109/TII.2020.2976893.

[7] Z. Tang, J. Jiao, P. Zhang, M. Yue, C. Chen, and J. Yan, "Enabling cyberattack-resilient load forecasting through adversarial machine learning," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, 2019, pp. 1–5, doi: 10.1109/PESGM40551.2019.8974076.

[8] L. Chen, D. Yue, C. Dou, J. Chen, and Z. Cheng, "Study on attack paths of cyber attack in cyber-physical power systems," *IET Gener. Transmiss. Distrib.*, vol. 14, no. 12, pp. 2352–2360, 2020, doi: 10.1049/iet-gtd.2019.1330.

[9] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure microgrid," *IEEE Trans. Power Syst.*, to be published, doi: 10.1109/TPWRS.2020.3011071.

[10] E. Y.-Z. Tan, C. C.-W. Lim, and R. Renner, "Advantage distillation for device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 124, no. 2, 2020, Art. no. 020502, doi: 10.1103/PhysRevLett.124.020502.

[11] 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, doi: 10.1109/TCOMM.2020.2978071.

[12] D. Graham-Rowe, "Quantum ATM brings gold standard security to the masses," *NewScientist*, vol. 196, pp. 30–31, 2007, doi: 10.1016/S0262-4079(07)62851-6.

[13] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Multi-tenant provisioning for quantum key distribution networks with heuristics and reinforcement learning: A comparative study," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 2, pp. 946–957, Jun. 2020, doi: 10.1109/TNSM.2020.2964003.

[14] A. Rastogi and S. Sharma, "Quantum cryptography in online banking," EasyChair, Tech. Rep., 2020.

[15] S. Cobourne *et al.*, *Quantum Key Distribution Protocols and Applications*. Surrey, England, U.K., 2011. [Online]. Available: https://www.ma.rhul.ac.uk/static/techrep/2011/RHUL-MA-2011-05.pdf

[16] F. Gao, S.-J. Qin, F.-Z. Guo, and Q.-Y. Wen, "Dense-coding attack on three-party quantum key distribution protocols," *IEEE J. Quantum Electron.*, vol. 47, no. 5, pp. 630–635, May 2011, doi: 10.1109/JQE.2011.2107889.

[17] A. Aguado *et al.*, "The engineering of software-defined quantum key distribution networks," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 20–26, Jul. 2019, doi: 10.1109/MCOM.2019.1800763.

[18] Y. Cao, Y. Zhao, X. Yu, and J. Zhang, "Multi-tenant provisioning over software defined networking enabled metropolitan area quantum key distribution networks," *J. Opt. Soc. Amer. B*, vol. 36, no. 3, pp. B31–B40, 2019, doi: 10.1364/JOSAB.36.000B31.

[19] A. Aguado *et al.*, "Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources," *J. Lightw. Technol.*, vol. 35, no. 8, pp. 1357–1362, 2017, doi: 10.1109/JLT.2016.2646921.

[20] A. Aguado *et al.*, "Quantum-aware software defined networks," in *Proc. Int. Conf. Quantum Cryptography*, 2016. [Online]. Available: http://oa.upm.es/id/eprint/46651/contents

[21] E. Hugues-Salas *et al.*, "Experimental demonstration of DDoS mitigation over a quantum key distribution (QKD) network using software defined networking (SDN)," in *Proc. Optical Fiber Commun. Conf. Expo.*, 2018, pp. 1–3. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8385709

[22] H. Wang *et al.*, "Protection schemes for key service in optical networks secured by quantum key distribution (QKD)," *J. Opt. Commun. Netw.*, vol. 11, no. 3, pp. 67–78, 2019, doi: 10.1364/JOCN.11.000067.

[23] E. Hugues-Salas, F. Ntavou, D. Gkounis, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Monitoring and physical-layer attack mitigation in SDN-controlled quantum key distribution networks," *J. Opt. Commun. Netw.*, vol. 11, no. 2, pp. A209–A218, 2019, doi: 10.1364/JOCN.11.00A209.

[24] Y. Li, P. Huang, S. Wang, T. Wang, D. Li, and G. Zeng, "A denial-of-service attack on fiber-based continuous-variable quantum key distribution," *Phys. Lett. A*, vol. 382, no. 45, pp. 3253–3261, 2018, doi: 10.1016/j.physleta.2018.09.027.

[25] N.-H. Bao, D.-Y. Luo, and J.-B. Chen, "Reliability threshold based service bandwidth recovery scheme for post-disaster telecom networks," *Opt. Fiber Technol.*, vol. 45, pp. 81–88, 2018, doi: 10.1016/j.yofte.2018.06.008.

[26] T. Jennewein *et al.*, "Quantum cryptography with entangled photons," *Phys. Rev. Lett.*, vol. 84, no. 20, p. 4729, 2000, doi: 10.1103/PhysRevLett.84.4729.

[27] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011, doi: 10.1109/TSG.2011.2159406.

[28] S. Marzal, R. Salas, R. González-Medina, G. Garcerá, and E. Figueres, "Current challenges and future trends in the field of communication architectures for microgrids," *Renewable Sustain. Energy Rev.*, vol. 82, pp. 3610–3622, 2018, doi: 10.1016/j.rser.2017.10.101.

[29] Y. Cao, Y. Zhao, Y. Wu, X. Yu, and J. Zhang, "Time-scheduled quantum key distribution (QKD) over WDM networks," *J. Lightw. Technol.*, vol. 36, no. 16, pp. 3382–3395, 2018, doi: 10.1109/JLT.2018.2834949.

[30] D. Kreutz *et al.*, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2014, doi: 10.1109/JPROC.2014.2371999.

[31] N. McKeown *et al.*, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, 2008, doi: 10.1145/1355734.1355746.

[32] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Phys. Rev. A*, vol. 89, no. 2, 2014, Art. no. 022307, doi: 10.1103/PhysRevA.89.022307.

[33] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New J. Phys.*, vol. 12, no. 6, 2010, Art. no. 063027, doi: 10.1088/1367-2630/12/6/063027.

[34] M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nature Commun.*, vol. 5, no. 1, pp. 1–7, 2014, doi: 10.1038/ncomms6235.

[35] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Commun.*, vol. 8, no. 1, pp. 1–15, 2017, doi: 10.1038/ncomms15043.

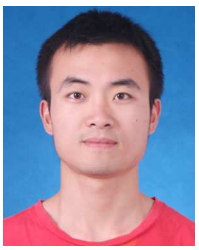
[36] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, 2018, doi: 10.1038/s41586-018-0066-6.

[37] S. Wang *et al.*, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," *Phys. Rev. X*, vol. 9, no. 2, 2019, Art. no. 021046, doi: 10.1103/PhysRevX.9.021046.

[38] L. Chen *et al.*, "Report on post-quantum cryptography," Nat. Inst. Standards Technol., Bethesda, MD, USA, Rep. NISTIR 8105, 2016.

[39] H. Wang *et al.*, "Resilient quantum key distribution (QKD)-integrated optical networks with secret-key recovery strategy," *IEEE Access*, vol. 7, pp. 60079–60090, 2019, doi: 10.1109/ACCESS.2019.2915378.

[40] Y. Li, Y. Qin, P. Zhang, and A. Herzberg, "SDN-enabled cyber-physical security in networked microgrids," *IEEE Trans. Sustain. Energy*, vol. 10, no. 3, pp. 1613–1622, Jul. 2018, doi: 10.1109/TSTE.2018.2889451.



Zefan Tang (Student Member, IEEE) received the B.S. degree in mechanical engineering from Zhejiang University, Zhejiang, China, in 2014, and the M.S. degree in electrical and computer engineering from the University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai Jiao Tong University, Shanghai, China, in 2017. He is currently working toward the Ph.D. degree in electrical engineering at Stony Brook University, Stony Brook, NY, USA.

His research interests include quantum security, quantum key distribution, quantum networking, cyber-physical security for electric power networks, and microgrids.

Peng Zhang (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of British Columbia, Vancouver, BC, Canada, in 2009.

He is a SUNY Empire Innovation Professor with Stony Brook University, Stony Brook, NY, USA. He has a joint appointment with Brookhaven National Laboratory as a Staff Scientist. Previously, he was a Centennial Associate Professor and a Francis L. Castleman Associate Professor with the University of Connecticut, Storrs, CT, USA. He was a System Planning Engineer with BC Hydro and Power Authority, Canada, during 2006–2010. His research interests include quantum security, quantum computing, programmable microgrids, networked microgrids, power system stability and control, cyber security, formal methods and reachability analysis, and software-defined networking.

Dr. Zhang is an individual member of CIGRÉ. He is an Editor for the IEEE TRANSACTIONS ON POWER SYSTEMS, the IEEE TRANSACTIONS ON SUSTAINABLE ENERGY, and the IEEE POWER AND ENERGY SOCIETY LETTERS, and an Associate Editor for the IEEE JOURNAL OF OCEANIC ENGINEERING.

Walter O. Krawec received the M.A. degree in mathematics from the State University of New York at Albany (SUNY), Albany, NY, USA in 2010 and the Ph.D. degree in computer science from the Stevens Institute of Technology, Hoboken, NJ, USA, in 2015.

He is currently an Assistant Professor of Computer Science and Engineering with the University of Connecticut, Storrs, CT, USA. His research interests include quantum cryptography and quantum information theory.

Zimin Jiang received the B.S. degree in electrical engineering from Shandong University, Jinan, China, in 2015, where he is working toward the Ph.D. degree.

He is currently a Research Support Specialist with the Department of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY, USA. His research interests include power system stability and control, microgrids, cyber security, renewable energy integration, and grid interconnection testing.