A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security

Peng-Yong Kong, *Senior Member, IEEE*

***Abstract*—Smart grid depends on an advanced communication network to collect information from the power grid, and to disseminate control commands to the control devices. To safeguard the power grid, it is crucial to ensure information confidentiality in the communication networks. Quantum key distribution (QKD) protocols help in generating, and distributing secret keys between communication parties, and such secret keys are required in symmetric cryptography. The combination of QKD protocols, and symmetric cryptography are known to be unconditionally secure, which means information confidentiality can be guaranteed even against an eavesdropper, who has unlimited resources. This article provides a concise review of existing works on QKD protocols, and their applications in smart grid communications. Deploying QKD protocols in smart grid is challenging because distance between the control center, and control devices can be larger than the limits of existing protocols. Also, QKD protocols require an expensive quantum channel between each pair of sender, and receiver nodes, and there is large number of control devices with diverse capabilities in smart grid. We have classified existing works based on the challenges they have dealt with. Compared to the rich literature on QKD protocols in general, there are significantly fewer works in the specific context of smart grid. This can be an indication for opportunity to make a significant contribution. We have also identified a few research challenges that can be potential future works.**

***Index Terms*—Communication network, communication security, confidentiality, cryptography, network security, quantum key distribution (QKD), smart grid.**

I. Introduction

SMART grid is a state-of-the cyber-physical system, which integrates advanced information and communication technologies with the traditional power grid [1]. In smart grid, power generation, storage, and dispatch are dynamically controlled in response to some changes in electricity demand, distributed renewable generation output, and storage facility utilization [2]–[4]. For example, the power output from a wind turbine is intermittent and not controllable. When the wind flow is strong but the electricity demand is weak, the smart grid can dynamically reduce the power dispatch and direct the overly produced power to energy storage facility. In some cases, such as the dynamic thermal rating of overheard power transmission lines, the dynamic control mechanism also requires accurate information on weather conditions, such as sun shine, atmospheric humidity, and ambient temperature, which may affect ampcity of the transmission lines. Such dynamic control is necessary because an excessive power input–output gap or an operating point beyond technical limits, will lead to catastrophic failures in the entire power grid. With the dynamic control capability, compared to the traditional power grid, smart grid can maintain stability at the same time of achieving a higher operation efficiency, where the efficiency is gained by safely operating the existing infrastructure closer its technical limits.

The smart grid dynamic control system requires the support of an advanced communication network [5]–[7]. Through the network, the control center can collect information from remotes sensors, which are installed at various locations throughout the power grid [8]. Based on the collected information, the control center must decide on suitable control actions to continuously match power output and input, while keeping the operating points within some acceptable limits. The decided control commands are disseminated through the communication network to remote actuators in the power grid [9]. While a communication network is an inseparable and a critical component of a smart grid, it can also make the smart grid more vulnerable by expanding its exposure to malicious attacks. Specifically, in addition to directly attack a power grid infrastructure, the grid can be indirectly destroyed by attacking its communication network. With the high level of interdependence between power grid and communication network in a smart grid [10]–[12], it is crucial to ensure the communication network robustness and security.

Communication security is essential in ensuring the overall robustness of a smart grid [13]. For example, malicious attacks on sensor data transmissions can mislead the power grid control algorithms. This can result in catastrophic consequences such as blackouts in large geographic areas. According to the National Institute of Standards and Technology (NIST) [14] and the European Network and Information Security Agency (ENISA) [15], confidentiality, integrity, authenticity, functionality, and availability are the most critical communication security aspects in a smart grid. Among these different security aspects, our concern is to ensure confidentiality and integrity. We want to maintain communication confidentiality such that data from remote sensors are kept secret from illintentioned adversaries. This is important to prevent unauthorized profiling on the intimate details

Manuscript received May 29, 2020; revised August 10, 2020 and September 1, 2020; accepted September 9, 2020. Date of publication October 2, 2020; date of current version March 24, 2022.

The author is with the Electrical Engineering and Computer Science Department, Khalifa University, Abu Dhabi, UAE (e-mail: pengyong.kong@ku.ac.ae).

Digital Object Identifier 10.1109/JSYST.2020.3024956

of smart grid operation and consumer lifestyle. We also want to protect communication integrity such that the control commands cannot be illegitimately modified in transit. In general, data integrity can be verified using checksums. In the context of smart grid dynamic control under the malicious insidious attack, the integrity of control commands can be assured as long as they are kept confidential. This is because an attacker must first learn about the system behaviors, and know the original command before modifying it to gradually harm the system without being easily detected. For example, the attacker can modify the control commands to successively move the smart grid's operating point dangerously close to its technical limits. As such, the attack may go on undetected with the smart grid remains operational, but the system is exposed to failures, which are triggered by natural fluctuations in operating conditions. Therefore, we will focus on communication confidentiality hereafter.

In smart grid, communication confidentiality can be achieved through cryptography. Currently, there is no industrial standard that is specifically designed for cryptographic systems of a smart grid communication network. Existing cryptographic algorithms, such as advanced encryption standard (AES) [16] and Rivest–Shamir–Adleman (RSA) [17], which have not been designed especially for smart grid, can be used in smart grid communications. Compared to AES and RSA, one-time-pad (OTP) is a simpler symmetric cryptographic algorithm, which requires the secret encryption keys never be reused in whole or in part, and OTP has been proofed to be unconditionally secure. Symmetric cryptographic algorithms depend on key distribution protocols to disseminate secret keys, which are used to encrypt communications between the control center and control devices. Here, for brevity, a control device refers to both a sensor and an actuator, as well as a smart meter in a power transmission and distribution network. Recently, there is an increasing interest in using quantum key distribution (QKD) protocols for the secret key distribution in smart grid [18]. Compared to classical key distribution, QKD protocols can better protect secrecy of the distributed secret keys, by not relying on the barrier of computational complexity in solving some intractable mathematical problems. Instead, QKD protocols are based on the laws of physics that govern the emerging quantum communication technologies. More specifically, QKD protocols exploit the fact that classical information can be encoded into quantum states, quantum state cannot be cloned and decoding a quantum state will change the state itself. As such, QKD protocols ensure that a compromised secret key can be identified and discarded, before use.

The European Space Agency has completed a project in January 2020 to show the feasibility of using a satellite based QKD protocol to protect confidentiality of messages exchanged between 60 ground control nodes, which include transformer stations in a smart grid [19]. According to [20], in March 2020, a power utility company in Tennessee, USA, has experimented with a QKD protocol in distributing secret keys that are used in encrypting control messages to dispatch and control the flow of electricity. In [21], a European Union level quantum communication infrastructure has been articulated. The infrastructure will initially provide QKD services to safeguard critical infrastructures, which include electric power grid. In 2017, a quantum communication network with QKD protocols has been implemented in Jinan, China, where the first users are government agencies, the military, finance, and electricity sectors that require secure communications [22]. In this implementation, the power grid's existing optical ground wire lines are used as the quantum communication channels. Here, QKD protocols coupled with symmetric cryptography can guarantee the confidentiality and integrity of the data being exchanged and stored in a smart grid. In [23], QKD protocols are used to provide symmetric encryption keys in protecting confidentiality of the bid prices in power market operation and the usage schedules in a demand response application.

There are a number of existing surveys on QKD protocols [24]–[26]. However, none of these existing surveys has focused on the context of smart grid communications. In this article, we aim to provide a concise review of existing QKD protocols and their applications for secure communications in smart grid. We have prepared this article for communication system engineers. Therefore, we have consciously avoided excessive fine details in fundamental physics and quantum mechanics. Instead, we have focused on the description of higher-level protocol details in the context of a smart grid communication network. While the protocols and their basis in quantum physics are not covered in detail here, those interested can find further reading in [27]–[31]. As preliminaries, Section II describes the basic operation of QKD protocols, discusses the suitability of QKD protocols for smart grid communications, and explains the technical challenges in deploying QKD protocols in smart grid. Section III classifies existing works from the literature before reviewing them in detail. Some open research challenges are presented in Section IV as potential future works, before this article ends with concluding remarks in Section V.

QKD protocols can only help in distributing secret encryption keys for cryptographic algorithms, but performing the encryption itself. Other aspects of quantum cryptography, such as quantum secret sharing [32], [33], quantum signatures [34]–[36], and quantum data locking [37] are not covered in this article. For ease of reference, we summarize the key findings in this article as follows.

1) Deployment of QKD protocols in smart grid faces a few technical challenges. Transmission networks of a power grid may span across a few hundred kilometers, and this exceeds the key distribution distance limit of existing protocols. Apart from the distance limitation, power distribution networks consist of a large number of control devices, such as sensors, actuators, and smart meters, with diverse capabilities [38]. QKD protocols require quantum channels, but it is too costly to have a quantum channel to each control device. Also, QKD protocols need to support different smart grid applications that have different communication quality of service requirements.
2) Existing works in the literature can be classified into the following three groups:
   a) facilitate QKD protocols deployment over a large geographical area;

b) efficient QKD protocols deployment with a large number of control devices;
c) authentication of QKD nodes through quantum channels.

3) There are still various open research problems for widespread and cost-efficient QKD protocol deployment in smart grid communication networks. Over an extended geographical area, existing QKD protocols are not truly end-to-end between control center and control devices. For a large of number of control devices, there is a need to develop a framework to systematically tradeoff between the security risk and system scalability. Currently available QKD protocols generate secret keys at a rate, which is much slower compared to typical data communication rates. As a result, these existing protocols are not capable of supporting real-time communications in data channel, which is essential to some smart grid applications.

II. QKD Protocols: Fundamentals, Suitability, and Challenges

Communication confidentiality can be achieved through cryptography, which is the art of encrypting messages using a secret key by a sender in a way that the messages become unintelligible for those not knowing the secret key. This is because the secret key must be used to decrypt the messages. As such, only authorized receivers who know the secret key, can read the messages. Cryptographic algorithms can be broadly divided into two major groups, namely symmetric cryptography and asymmetric cryptography.

Asymmetric cryptographic algorithms, such as RSA, are also knows as public key cryptographic algorithms, for the fact that each communication node has a public key in addition to a private key. The private key must remain known only to its owner, while the public key can be freely disseminated to all the key owner's communication counterparts. In such a cryptographic system, a sender can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted by the receiver using its own private key. The security strength of public key cryptography relies on some unproven assumptions of the mathematical complexity and the irrational amount of time needed to perform integer factorization or to solve some discrete logarithm problems. This means that public key cryptographic algorithms are potentially vulnerable to improvements in computational power or discovery of efficient algorithms to solve discrete logarithm problems. Shor [39], has proposed an algorithm to factorize large integer numbers and to solve discrete logarithm problems in polynomial time by using the principles of quantum computing. Grover [40], has proposed another quantum computing algorithm that allows for secondary acceleration when calculating inverse hash function. With rapid advancement in computing technologies, a traditionally secure public key cryptographic system may not be secure anymore in the not-too-distant future [41]. In view of the threats posed by quantum computing, postquantum cryptography has been developed, and is being standardized [42]. These are asymmetric cryptographic algorithms that are designed to be safe against quantum computing attacks. However, postquantum cryptography may not completely solve the problem because there may be undiscovered quantum algorithms that will easily break the security of the new postquantum cryptographic systems. In other words, postquantum cryptography is likely to offer only a partial and temporary solution to the threats posed by quantum computing. In contrast to classical asymmetric cryptography, most current symmetric cryptographic algorithms are relatively secure against attacks by quantum computers. While the Grover's quantum computing algorithm does speed up computational attacks against symmetric cryptographic algorithms, doubling the secret key length may effectively block these attacks.

In symmetric cryptographic algorithms such as AES and OTP, both the sender and receiver must use a same secret key to encrypt and decrypt their messages. Among various existing symmetric cryptographic algorithms, OTP has a low computational complexity as it simply pairs a plaintext with a secret key. Specifically, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the secret key using modular addition. If the secret key is truly random, at least as long as the plaintext, never be reused in whole or in part, and is kept completely secret, then there exist an information theoretic proof that the resultant ciphertext will be impossible to crack by any third party who may have unlimited resources, including access to a quantum computer. This desirable status is called unconditional security and it is the ultimate guarantee to communication confidentiality in smart grid.

To implement a symmetric cryptographic system in smart grid, the control center and a control device must somehow agree first on a common secret key. This secret key can be a preshared key or a key that is distributed by a trusted courier. Apart from these two methods, the Diffie–Hellman scheme is a well-known key distribution protocol that allows a pair of communication parties (Alice and Bob) that have no prior knowledge of each other to jointly establish a symmetric cryptographic secret key over an insecure channel. A simple example of the Diffie–Hellman implementation involves Alice and Bob to publicly agree to use two integer numbers, says p and g, where g is a primitive root modulo p. Alice chooses randomly a secret integer a and sends to Bob $(g^a \bmod p)$. Bob chooses randomly a secret integer b and sends to Alice $(g^b \bmod p)$. Alice and Bob compute separately their secret keys as $[(g^b \bmod p)^a \bmod p]$ and $[(g^a \bmod p)^b \bmod p]$, respectively. The two keys are identical although they are generated locally using information received from the other party. To steal the secret key, eavesdropper Eve must solve a discrete logarithm problem. For example, Eve needs to find a given only p, g, and $(g^a \bmod p)$. Similar to public key cryptography, the ability of Diffie–Hellman scheme in keeping its secret key confidential to only Alice and Bob, relies on an expectation of a long time needed in solving the discrete logarithm problem for a large value p of a few hundred digits. Unfortunately, there is no theoretical proof that the Diffie–Hellman scheme can unconditionally protect the secret key from an eavesdropper with unlimited quantum computing resources. In view of the challenge, QKD protocols have emerged as an alternative to the classical key distribution protocols in

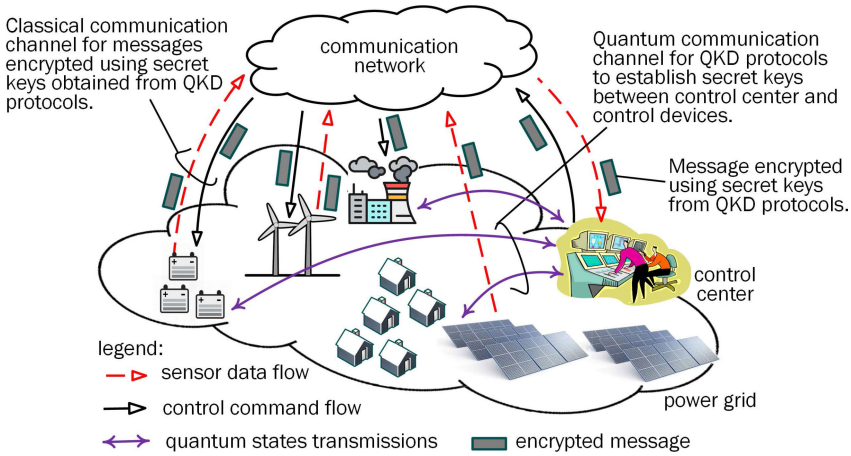

Fig. 1. Illustration of a smart grid system with integrated power grid and communication network. Notice that QKD protocols are only used to establish secret keys for encryption, but not to encrypt the messages. There are two types of communication channels, namely classical channel and quantum channel. The quantum channel is a necessity to QKD protocols.

symmetric cryptographic systems for smart grid communications [43]. While postquantum cryptography may be used to strengthen Diffie–Hellman scheme, this article reviews QKD protocols, which protect secret key through the fundamentals of physics, but not the barriers erected by computational complexity. Also, instead of a one-off secret key generation for a communication session, QKD protocols can provide a continuous stream of new secret key bits for OTP, which demands secret key never be reused in whole or in part.

QKD protocols help in securely establishing the symmetric cryptographic secret key between a pair of communication devices that have no prior knowledge of each other. The additional process of making sure that the communication counterpart is indeed who they claim they are, is called authentication. Although it is reasonable for a node to authenticate its communication counterpart before establishing a mutual secret key, QKD protocols do not require authentication. Users remain free to add authentication mechanisms of their choice on top of a QKD protocol. Despite the use of term "distribution," typically, the key is created jointly and simultaneously at both the control center and a control device, but not first created by one party to be distributed to the other party. As illustrated in Fig. 1, QKD protocols are not used to encrypt the messages, but they are used to establish the secret keys, which are then used to encrypt the messages. The encrypted messages are transmitted through classical communication channels, which can appear in the forms of any existing wired or wireless communication channels, such as the Internet. In addition to the classical channel, Fig. 1 shows that QKD protocols require an additional quantum communication channel to transmit quantum states in establishing the secret keys. Currently, the quantum channel can exist as an optical fiber or a free-space wireless channel.

As depicted in Fig. 2, QKD protocols are designed to establish a secret key only between a pair of sender and receiver nodes, which are directly connected through a quantum channel without any intermediate node. As such, they are peer-to-peer or point-to-point protocols, although the classical channel between the sender and receiver may not be a direct link. The classical

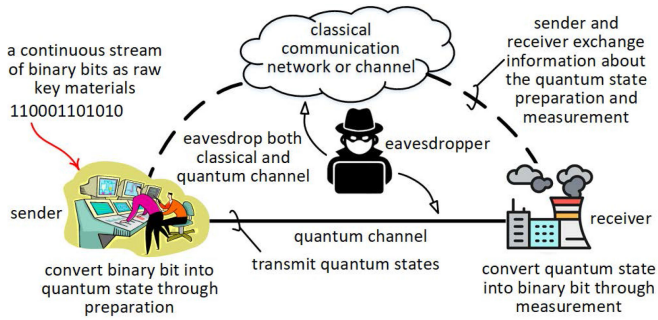

Fig. 2. QKD protocols establish secret keys between a pair of sender and receiver nodes, which are directly connected through a quantum channel. A classical communication channel, which can be multi-hop is also required. The eavesdropper may observe both quantum channel and classical channel.

channel is used to transmit classical information, such as the typical binary 1 or 0. On the other hand, the quantum channel is used to transmit quantum state, which is the value of a quantum particle's properties, and a quantum particle can be a single photon [44]. In quantum physics, a quantum state is a vector with complex coefficients and unit length in a Hilbert space. We can encode classical information into a quantum particle by changing its quantum state before sending it over a distance and thus, turn the quantum particle into an information carrier for the purpose of communications. This leads to quantum communication, which is quite different from classical communication. In quantum communications, the process of information encoding and decoding at the sender and receiver, are called quantum state preparation and measurement, respectively. After preparation, we can only know the exact value of a quantum state by measuring it, and the measurement process itself will change the state, such that the new state will have completely no memory of it previous state. As such, a transmitted information can be correctly read only once, and if the information has been eavesdropped, it will appear as an error at the receiver.

In quantum physics, the no-cloning theorem indicates that it is impossible to create an identical copy of an arbitrary

unknown quantum state, while keeping the original quantum state intact [45]. This no-cloning theorem coupled with the measurement process in information decoding, has formed the foundation for QKD protocols to unconditionally guarantee confidentiality of the secret keys even in the presence of very powerful eavesdroppers. There are two types of QKD protocols, namely prepare-and-measure (PM) protocols and entanglement based (EB) protocols.

The first ever PM protocol is BB84 [46], and it is also the foundation for many other PM and EB protocols. BB84 is comprised of three steps, namely the raw key exchange, key sifting and key distillation. In the raw key exchange step, with reference to Fig. 2, the sender first creates a random sequence of binary bits as the raw materials, based on which a secret key can be produced for symmetric cryptography. For each binary bit, the sender randomly selects one of its two Hilbert space bases, namely rectilinear and diagonal, and use the selected basis to encode the bit by preparing a corresponding quantum state. For example, if rectilinear basis is selected, bit 0 is encoded into vertical polarization of a photon. On the other hand, if diagonal basis is selected, the same bit 0 is encoded into 45° polarization of a photon. The sender transmits the prepared quantum state to the receiver using the quantum channel. This process is repeated for each bit of the random sequence, with the sender recording the bit, basis and time of each transmitted quantum state. Upon receiving the quantum states from the sender, the receiver does not know the basis the photons have been encoded in. For each received quantum state, the receiver randomly selects one of the two bases and uses the selected basis to decode the quantum state through measurement. If the selected basis is identical to the basis the sender has used in preparing the quantum state, the measurement is correct. Otherwise, the measurement indicates the correct bit only half of the times. The receiver records the selected basis, measurement outcome and time of each measurement.

The key sifting step begins immediately after the receiver has measured all the received quantum states. In this step, the receiver first informs the sender over a classical channel the list of its measurement bases. In return, the sender also informs the receiver over the classical channel its list of selected bases. After comparing the received list of bases with the local list, both the sender and receiver will separately discard from their own local list, all entries with different bases. If the eavesdropper does not exist and there is no communication channel error, the remaining sequence of binary bits is identical at both sides. Then, this binary sequence is the secret key generated by BB84. Unfortunately, this is usually not the case because errors can still occur due to component imperfections and environmental perturbations in the quantum channel.

Due to eavesdropping and channel errors, at the end of key sifting step, the binary bit sequences at the sender and receiver may not be identical. Hence, the key distillation step postprocesses the potentially erroneous binary sequences to turn them into usable secret key. The key distillation step consists of two substeps, namely key reconciliation and privacy amplification. The key reconciliation substep performs error detection and correction, by using a classical error correction protocol to ensure the binary sequences are identical at both the sender and receiver. Through the error detection and correction, this substep can also estimate the actual error rate. With the assumption that all errors are due to only eavesdropping, the estimated error rate provides an indication on the amount of information the eavesdropper may have on the secret key. If the error rate is above an acceptable threshold, both the sender and receiver will discard their secret keys and restart the process. Otherwise, the protocol enters the privacy amplification substep to reduce the partial information, the eavesdropper has obtained about the secret key. The knowledge of eavesdropper can be eliminated by compressing the key using an appropriate factor to produce a shorter key. The compression factor depends on the error rate detected earlier in key reconciliation. A higher error rate implies a more severe leakage of information to the eavesdropper and, therefore, requires a higher compression factor to ensure the eavesdropper has only negligible information about the final key. At the end of privacy amplification, the shorter key is the final secret key to be used in symmetric cryptography.

In the literature, E91 is the first ever EB protocol [47]. Similar to BB84, E91 consists of three steps. But, E91 uses a different method to encode classical binary bits into quantum states in the raw key exchange step and a different approach to detect eavesdropper in the key distillation step. In the raw key exchange step, a sequence of entangled quantum particle pairs are produced by a specialized photon source. From each pair, the sender and receiver each receives one photon through the quantum channel. The sender will first randomly choose a basis to measure its photon. Due to quantum entanglement [48], this measurement by the sender on one member of the entangled pair is equivalent to preparing the other member in a random state on the result of the measurement. The sender records the time, the measurement basis, and the measurement outcome. At about the same time but after the sender's measurement, the receiver also randomly and independently chooses a basis to measure its photon. Similar to the sender, the receiver records the time, the measurement basis, and the measurement outcome. The raw key exchange step ends when all the produced entangled quantum particle pairs have been transmitted and measured. Immediately after the raw key exchange step, key sifting step begins with the sender and receiver exchange their records through the classical channel. Subsequently, the sender and receiver discard all the bits that are not measured using a same basis at both sides. After completing the key sifting, in the key reconciliation step, E91 uses the Bells inequality test to detect the presence of eavesdropper. The privacy amplification step in E91 may be the same as in BB84.

Compared to EB protocols, PM protocols can achieve a higher secret key rate but a shorter key distribution distance. The secret key rate is the rate at which a stream of secret key bits can be established between a pair of sender and receiver nodes. The key rate depends mainly on the efficiency of the photon source and detector, the quantum channel loss and the vulnerability to various types of security attacks. The key distribution distance is the geographical range within which the QKD protocols can achieve a desirable secret key rate. Currently, there is no feasible QKD protocol that can operate beyond a distribution

TABLE I
USE OF PM AND EB PROTOCOLS IN SMART GRID

References	Remarks
[19]	Satellite based PM protocol, without disclosing protocol specifications.
[20], [65]	Single-photon based PM protocol, implemented using infrared light source over some spare optical fibers.
[22]	EB protocol, no technical detail has been provided.
[55]	BB84 with decoy state between a control center and multiple substations in a dynamic control scenario.
[66]	PM protocol over optical fibers, satellite links and terrestrial mobile communication networks for smart grid.
[68]	A combination of continuous variable and discrete variable PM protocols.
[71]	EB QKD using a ping-pong protocol.
[23], [53], [69], [73], [74], [76], [77]	Mention or use BB84 and/or PM protocol in general.

distance of 300 km using an optical fiber for secret key rate more than 100 kb/s. For example, experimental measurements in [49] and [50] have achieved a secret key rate of less than 1 b/s at a distance of just beyond 300 km. Separately, a secret key rate of 3.18 b/s at 307 km has been achieved by [51] using ultralow loss optical fibers with its receiver operated at a low temperature of 153 K.

The communication environment in a power system can be noisy. In such a noisy environment, Sharma *et al.* [52] showed that EB protocols can perform better than PM protocols. Separately, Fang-Yi *et al.* [53] have proposed a modified PM protocol with phase coding to eliminate additional errors due to disturbance on quantum channel, which is an open-air optical fibers. As shown in Table I, regardless of the strengths and weaknesses, almost all the existing works in smart grid have used PM protocols.

Compared to classical key distribution protocols such as the Diffie–Hellman scheme, applying QKD protocols in smart grid has the following advantages.

1) *Future proof:* QKD protocols do not depend on the barrier of computational complexity for its security and, thus, are not at risk of becoming obsolete in face of the rapidly increasing computing power.
2) *Unconditional and immediate security:* The secret key distributed by QKD protocols are unconditionally secure through the use of some unique quantum physics axioms that allow the immediate detection of the presence of any eavesdropper. Without such immediate eavesdropper detection, a compromised secret key can be in use for some times until well after serious damage has occurred.
3) *Practical implementation:* QKD protocols require transmissions of quantum particles through quantum channels. Practically, these quantum particles can be photons and the quantum channels are optical fibers. These optical fibers are readily available since optical communications have become popular in connecting control center and substations in smart grid [54]. According to [55], 100% of all 220 kV substations and 92% of all 110 kV substations in China are already connected with optical fibers. These existing optical fibers can be used as quantum channels for QKD protocols, and there is no need to particularly lay additional optical fibers. As demonstrated in [56] and [57], QKD protocols can also share a physical optical fiber with classical optical communication transmissions.

Despite the superior security characteristics of QKD protocols, applying them in smart grid faces a few technical challenges as follows.

1) *Extended coverage area:* Based on the topological data of an actual national power grid in [58]–[60], the transmission line network can extend to cover an area which is more than 200 km away from the generator. Currently, QKD protocols can provide a secret key rate of about 1 Mb/s over a key distribution distance of 50 km. The secret key rate drops to about 10 kb/s when the distance grows to 100 km. There is no existing protocol that can operate over 300 km using an optical fiber for secret key rate over 100 kb/s. Thus, multihop relaying over quantum channel is needed for an extended distance. However, such relaying solution does not provide end-to-end security and is highly dependent on the trustworthiness of the relays.
2) *Large number of end nodes:* Smart grid consists of a larger number and types of end nodes with diverse capabilities. Apart from a control center, smart grid has many sensors, actuator, data storage and processors, transformer substations, renewable energy generators, energy storage, etc. Also, each consumer in the distribution network of a power grid is installed with a smart meter. QKD protocols are originally designed to operate on a point-to-point basis between a pair of communication nodes. The challenge is for QKD protocols to distribute secret keys to a large number of nodes with unequal capabilities, and are not directly connected through an optical fiber. It is too costly to have a quantum channel to each control device.
3) *Real-time communications:* Smart grid supports a myriad of applications, such as dynamic pricing, demand response, load shedding, and remote meter reading. Some of these applications, such as substation protection mechanisms require a communication delay not exceeding 4 ms [61]. But, the process of distributing a secret key through QKD protocols can take hundreds of miliseconds depending on the key length. The challenge is for QKD protocols to support real-time communications.
4) *Big amount of data:* Some smart grid equipments, such as the synchronous phase measurement units, may generate a continuous stream of data. Depending on the sampling interval and data accuracy requirements, the data stream may be a few Mb/s. This is probably not a high data rate considering the terabits per second capacity of optical fibers or the gigabit per second capacity of 5G cellular networks. However, QKD protocols can generate secret key at a rate of about 1 Mb/s over 50 km. It is not uncommon for QKD implementations to produce secret key at about 10 kb/s beyond 100 km. With the use of OTP

TABLE II
FACILITATE QKD PROTOCOLS DEPLOYMENT OVER A LARGE GEOGRAPHICAL AREA

References	Remarks
[65]	Use trusted relay to extend key distribution distance in 2-hop configuration. Relay performs key switching transformation to support heterogeneity in QKD protocols among different operators.
[66]	Use trusted relay over optical fiber to extend key distribution distance for upto 3k KV transmission network, and satellite as quantum channel for ultra high voltage transformer stations. Relay and satellite relays original secret key, but not data.
[68]	Use discrete variable QKD (DV-QKD) to reach a longer key distribution distance in wide area networks.

symmetric cryptographic algorithm, the data rate cannot exceed the secret key rate. The challenge is for QKD protocols to support the data rate required by various smart grid applications.

In addition to the challenges given earlier, we should take note that fully device-independent QKD protocols provide the highest level of quantum security but they are characterized by very low secret key rates and are very demanding in implementation. Most practical QKD protocols are not fully device-independent. They are theoretically secure, but may not be secure in real world implementations. This is because security model may not capture all features of a real device and practical implementations are prone to side-channel attacks [62]–[64]. This type of attacks exploit secondary variations in hardware information, such as the execution time, power consumption, power dissipation, and electromagnetic interference produced by electronic devices throughout the key distribution process, to derive knowledge of the actual secret key. For example, the leakage of light from photodetectors may reveal useful information about the quantum polarization to an observing attacker. However, we believe that none of these side-channel attacks is nonredeemable if we know its existence.

III. QKD PROTOCOLS AND THEIR APPLICATIONS IN SMART GRID COMMUNICATIONS

Among the large number of publications that deal with QKD protocols, there is only a small subset that have focused on smart grid. In Section II, we have presented some technical challenges in implementing QKD protocols in smart grid. We notice that not all these challenges have been worked on by the existing literature. For ease of exposition, we have classified the existing works into three groups depending on the challenge that they have dealt with. The first group of works have developed methods to facilitate QKD protocol deployment over a large geographical area. Works in the second group have enabled QKD protocols to efficiently cover a larger number of control devices. In the third group, several methods have been proposed to authenticate the pair of sender and receiver nodes, which are involved in establishing secret keys through QKD protocols, or using the secret keys, which have been established earlier by QKD protocols. In the rest of this section, we will review these existing works in separate subsections. We have created a forth subsection called "other works," to collect existing research works, which do not fit into the three groups. In practice, a single paper may have worked on multiple issues and thus, its classification into a group should not be perceived as an exclusivity but it is rather for a better presentation flow.

A. Facilitate QKD Protocols Deployment Over a Large Geographical Area

Existing works in facilitating QKD protocols deployments over a large geographic area are summarized in Table II. As discussed earlier, a transformer substation can be more than 200 km away from the generator and control center, but the secret key rate of existing QKD protocols will drop to 10 kb/s at 100 km. To achieve a desirable secret key rate, the key distribution distance has to be limited. In [65], trusted relays are used between the control center and control devices, such that the secret keys are being regenerated every few tens of km, over a necessary operating distance. With such intermediate relay nodes, a single-hop link is turned into a multihop connection, where QKD protocol is performed separately at each hop. Consider a simple case with only a single relay between the control center and a control device, in a 2-hop configuration. The relay needs to execute QKD protocols to separately establish a secret key with the control center and control device. In this case, the relay trustworthiness is utmost important because it will decrypt a message from the control center, before encrypting it again using a different secret key for delivery to the control device. While this relaying approach is common for QKD protocols outside the context of smart grid, the scheme in [65] is unique in the sense that it considers heterogeneity in the system. Specifically, the control center may communicate with another control center or a control device, which belongs to another operator and thus, using a different QKD protocol. In this scenario, Long [65] has proposed a key switching operation that enables the trusted relay to transform an incoming encrypted message to an outing message encrypted using the destination secret key, without the need to first decrypt the incoming message.

The work [66] has considered an entire smart grid that has a power transmission network and a distribution network with wide area awareness capability. To cover geographical areas with different sizes, Jia *et al.*[66] proposed to use optical fibers and satellite communications, as well as terrestrial wireless cellular networks. Specifically, a QKD protocol is performed over optical fibers, which connect substations up to 35 kV. When there is a need, trusted relays are added to the optical fiber connections. Here, each trusted relay encrypts the control center secret key as its payload so that the original key can reach the intended control device. For wide area awareness of ultrahigh-voltage (a few hundred, e.g., 345 kV) transmission lines and transformer

TABLE III
EFFICIENT QKD PROTOCOLS DEPLOYMENT WITH A LARGE NUMBER OF CONTROL DEVICES

References	Remarks
[55]	Use PON to connect a large number of smart meters to the control center for cost efficiency and high bandwidth. QKD protocol execution requires perfect clock synchronization to extract correct quantum states from downstream broadcast.
[66], [67]	QKD protocols are executed between the control center and a co-located key management device. Generated secret keys are physically transported to end devices through dongles and thus, eliminate the need of expensive quantum channels.
[68]	Use the lower cost continuous variable QKD (CV-QKD) protocols between end devices and an aggregator, but discrete variable QKD (DV-QKD) over a longer distance between aggregator and the control center.
[69]	A group of end devices share a common secret key to reduce the number of quantum channels and QKD protocols deployment to save cost.
[70]	Divide a limited number of original QKD generated secret keys into segments, and recompose the segments to form a large pool of secret keys, one for each end devices.

stations, satellite links are used as the quantum channels for QKD protocols.

B. Efficient QKD Protocols Deployment With a Large Number of Control Devices

Existing works on efficient QKD protocols deployment with a large number of control devices are summarized in Table III. In a dynamic control application, the control devices are sensors and actuators. On the other hand, in an advanced metering infrastructure, the control devices are smart meters. With the continuous upgrading of metering infrastructure, there will be a large number of control devices. In [55], passive optical network (PON) is used to connect smart meters to the control center, because PON offers high bit rates and excellent cost efficiency. A PON uses only passive components and each smart meter can see the entire downstream broadcast from the control center. If there is a synchronized clock between the control center and smart meters in PON, Zhang and Chen[55] further suggest that QKD protocols can be performed separately between the control center and each smart meter, with the smart meter picking a correct quantum state from the broadcast to distill an individual secret key.

To support a large number of smart meters, the work in [67] seems to have an interesting solution. Here, QKD protocols are performed between the control center and a colocated key management device. Multiple secret keys can be generated at the key management device, one for each smart meter. There is no communication connection between the key management device and smart meters. A dongle, which is called a quantum key mobile storage device, is used to physically transport the secret key to a smart meter. There is one dongle for each smart meter. Each dongle copies and stores its corresponding secret key from the key management device. Upon insertion into the smart meter, the dongle provides a dedicated secret key for secure communication between the smart meter and the control center. After all the stored secret key bits are consumed, the dongle must be removed from the smart meter and to return to the key management device for more secret key bits. As a practical consideration, the storage capacity of the dongle must be large enough to store a sufficiently many secret key bits to last for a long time. This idea of physical secret key transportation can eliminate the need of a quantum channel between the control center and each smart meter. However, it should be noted that the QKD protocol stops at the key management device and there is no QKD operation with the smart meters. As such, the dongle practically acts as a trusted courier in physically transporting secret keys with associated implications in terms of key freshness, system scalability and security. This same idea of using a physical dongle for key transportation has also been presented in [66], where smart meters are connected to the control center through an existing terrestrial cellular network. It is a practical solution for [66] because cellular channels are currently not feasible quantum channels.

It is straightforward to connect directly each control device to the control center, but this approach is not scalable with respect to an increasing number of control devices. For a scalable deployment, apart from the control center and smart meters, the communication network should also have some data aggregators. As illustrated in Fig. 3, these aggregators collect data from multiple smart meters and combine the data, before sending them to the control center. Such aggregation reduces the number of connections that the control center needs to manage, and also helps in avoiding network traffic congestion. The existence of data aggregator may require additional considerations in QKD protocols. In [68], all smart meters within a domain are connected to a data aggregator through a neighborhood area network, and all data aggregators from different domains are connected to the control center through a wide area network. With this system model, Bebrov *et al.* [68] have proposed to use continuous variable QKD (CV-QKD) protocols in the neighbor area networks, but to use discrete variable QKD (DV-QKD) protocols in the wide area network. This is because there is a large number of smart meters and PM CV-QKD protocols can be implemented using lower cost homodyne or heterodyne detectors. If PM DV-QKD protocol is used in connecting smart meters directly to data aggregator, each smart meter will need an expensive single-photon detector. Since DV-QKD can achieve a higher secret key rate at a longer transmission distance, it is selected for implementation in the wide area network where the distance between the data aggregators and the control center can be larger. Since single-photon detectors are probably the most costly components in a PM QKD system, Bebrov *et al.* [68] have further proposed to implement both the DV and CV QKD protocols in a 2-hop topology with a single relay sitting between a pair of sender and receiver nodes. In such a topology, both the sender and receiver are photon sources, and the relay node is the only photon detector. Hence, the number of

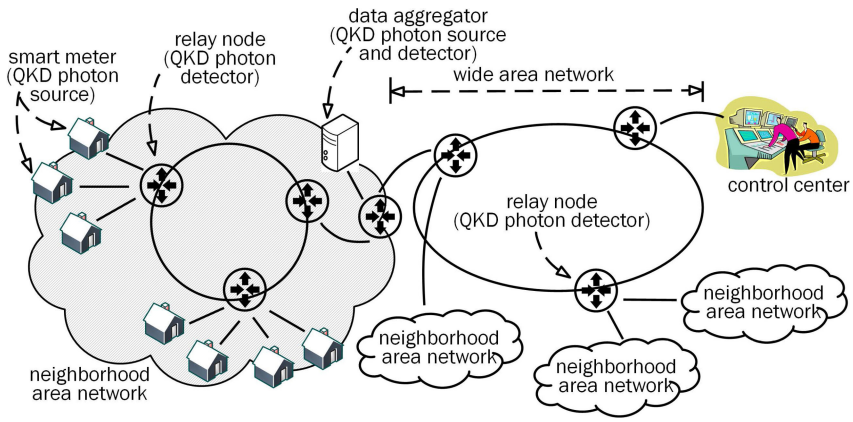

Fig. 3. Smart grid communication system model with a hierarchical architecture. CV-QKD protocols are used in neighborhood area networks and DV-QKD protocols are used in wide area networks. In the figure, only quantum channels are illustrated.

TABLE IV
AUTHENTICATION OF QKD NODES

References	Remarks
[71]	Key server keeps an authentication key for each pair of sensor and receiver nodes. Transmit authentication key and secret key through a quantum channel using an EB based ping-pong QKD protocol.
[73]	Divide each BB84 generated secret key into 3 parts, for encryption, authentication and confirmation, respectively. Need only a star topology for quantum channels while classical communication networks can be as complex as a mesh topology.
[74]	Divide each BB84 generated secret key into 2 parts, for authentication and encryption, respectively. Authentication is performed through quantum channel where the key is used to set the bases in preparing quantum states.

single-photon detectors can be reduced to achieve a lower system cost.

For cost efficiency, a group of smart meters which are connected to a same aggregator may share a single quantum channel and a same QKD-generated secret key [69]. However, this will compromise the unconditional security strength brought by QKD protocols, because each individual secret key is known by more than a single pair of sender and receiver nodes. This issue of secret key sharing has been studied in [70], where the aggregator may compose a large number of new secret keys from only a limited number of original QKD-generated secret keys. In [70], original secret keys are first divided into small segments. Then, two or three segments can be combined to form a new key for a smart meter. As such, a large pool of secret keys can be generated from a limited number of QKD terminals with quantum channels. However, the security implications of such secret key generation has not been presented.

C. Authentication of QKD Nodes

While establishing a secret key between a pair of sender and receiver nodes, QKD protocols do not demand a built-in mechanism to authenticate that the sender and receiver nodes are really who they claim to be. If there is a need for node authentication, we are free to choose any scheme we like. There are various existing generic authentication schemes that may work together with QKD protocols. In this section, as summarized in Table IV, we have selectively surveyed only authentication schemes that involve quantum channels. The work [71] has proposed a method to authenticate both the sender and receiver nodes, during the key distribution process of an EB protocol. The authentication is achieved through the verification of an additional authentication key which is kept at a trusted key server. Each authentication key is unique to a pair of sender and receiver nodes. According to our understanding in reading the published paper, it is indeed necessary to have an authentication key for each pair of communication nodes. The key distribution process begins when the ith smart meter sends a request to the key server to ask for its unique authentication key, a_i. While it is not explicitly stated, transmissions of authentication key is done in a classical channel and must be encrypted for confidentiality. Upon receiving a_i, the meter generates a random number r_i using quantum generator and then, creates a session key k_i, which is a concatenation of a_i, r_i, and i, such that $k_i = a_i \| r_i \| i$, where $\|$ represents the concatenation operator. We want to highlight that the session key k_i is transmitted as plaintext to control center using the ping-pong protocol [72] through a quantum channel. At the control center, the arrival of a session key triggers a request to the key server for the corresponding authentication key. If the received authentication key from key server matches that in the received session key, the control center proceeds to extract r_i from the session key k_i and use it as the secret key for symmetric cryptography in subsequent communications over classical channel. After completing the current communication session, the session k_i is turned into the authentication key $a_i = k_i \oplus k_i$ for the next session. While this proposed method is indeed unique as described earlier, there are a few parts that may require further clarification. Specifically, for the ith smart meter to send its session key to the control center using a ping-pong protocol, the control center must initially create and transmit

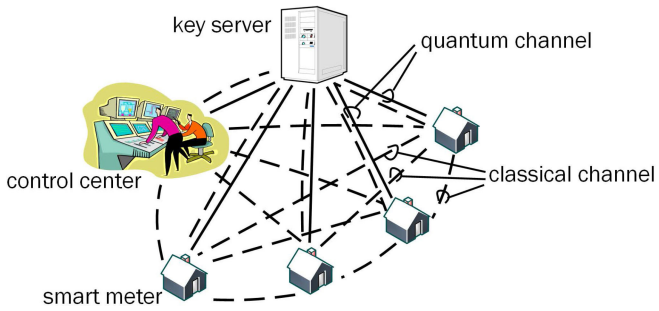

Fig. 4. Smart grid communication system model with star quantum channel topology and mesh classical channel topology.

sufficient number of entangled photon pairs for encoding by the meter. Clarification is needed on how this process is done in the context of the proposed method, and the duration to transmit a session key. Most importantly, reliability of this method depends on capability of the key server in initially authenticating all nodes and later, in protecting the authentication keys.

The joint consideration of both node authentication and secret key distribution in [71] is also addressed by [73], but in a different way. In [73], BB84 is first used to generate a secret key s_i between the key server and the ith nodes in the communication network. Let index 0 refer to the control center, and other nodes are smart meters. Only the key server has all the secret keys, while each node knows only its own key. The secret key s_i is divided into three parts, namely k_i, a_i, and d_i, where each part has 256 b. For each pair of secret keys s_i and s_j, the key server publishes an authentication key $p_{i,j} = a_i \oplus k_j$ and a confirmation key $q_{i,j} = H(k_j \| d_i)$, where $H(\cdot)$ a cryptographic hash function such as SHA-256. The ith smart meter can now obtain k_0 of the control center by calculating $k_0 = p_{i,0} \oplus a_i$. The same smart meter confirms that the obtained k_0 is correct by calculating $H(p_{i,0} \oplus a_i \| d_i)$ and verifying that it is equals to the value $q_{0,i}$ published by the key server. This key confirmation step is essential for security against malicious manipulation of $p_{i,j}$. After the confirmation, the ith smart meter can now encrypt its messages using k_0, which can be decrypted only by the control center. As illustrated in Fig. 4, this secure communications can be extended beyond control center and smart meter pairs, to peer-to-peer communications between smart meters. When control center and smart meters are connected through a mesh topology, this method can generate a secret key for any pair of nodes, without expanding the number of quantum channels. For example, in a network of N nodes, the scheme can generate a secret key for each of the $N(N-1)/2$ pairs of nodes, with the number of quantum channels remains at N. This is a great advantage as it avoids the need to laying addition optical fibers, which are not usually available in a mesh topology. However, the key server must be a completely trusted party. While this method helps end devices to authenticate to each other after secret keys are established through QKD protocols, there is no effort to initially authenticate a node prior to performing QKD.

The work [74] uses part of a currently generated secret keys as authentication keys for the next iteration of QKD protocols, although this is not typical in the popular Kerberos like authentication algorithms [75], which focus more on confirming the identify of a communication node. Here, BB84 first generates a secret keys, and the key is divided into two parts. The first part is used for authentication and the second part is used for data encryption. After the encryption keys are exhausted, the next iteration of BB84 is needed to produce more secret key. Before the next iteration can start, authentication is carried out. The authentication is done through quantum channel, where the authentication key sets a sequence of bases which are used in preparing quantum states. Identity of the sender is confirmed if all the quantum states are correctly measured using the same bases. After the authentication is completed, the typical BB84 is performed to generate the next secret key. It is more secure to perform authentication through a quantum channel, as compared to a classical channel. However, the challenge is in producing and protecting the initial authentication key, before the first BB84 iteration starts. Also, consuming part of the QKD-generated secret key bits for subsequent authentication will further reduce the secret key rate for data encryption.

D. Other Works

Through an advanced meeting infrastructure, the control center can collect usage data from each smart meter. If the data are encrypted using secret keys, which are established directly between the control center and smart meter, it can be kept confidential from eavesdroppers. However, there is another issue of protecting consumer privacy from the control center. Reasonably, the control center should be able to determine a dynamic control action based on the aggregate value of electricity consumption, and there is no need for fine grain data of individual consumers. As such, Borges *et al.* [76] have proposed a scheme that allows the control center to retrieve only an aggregate value from a number of individually encrypted data. In [76], BB84 is used to establish a different secret key between the control center and each smart meter. Let s_i be the secret key with the ith smart meter. Each smart meter knows only its individual secret key, while the control center knows all the secret keys. Let $m_i \in [0, M-1]$ be the integer-valued sensor data from the ith smart meter. Consider the system model as depicted in Fig. 5, meter i generates an encrypted message e_i using the Claude Castelluccia's symmetric homomorphic encryption technique. Specifically, $e_i = m_i + (\bar{s}_i \bmod M) + e_{i-1}$, where $\bar{s}_i \in [0, M-1]$ is the integer-valued representation of s_i. As illustrated in the figure, the encrypted message e_i is then directly transmitted to the subsequent $(i+1)$th meter. Says, there are a total of K smart meters. The Kth meter sends its encrypted message e_K to the control center. At the control center, the sum of all the data value $m = \sum_{i=1}^{K} m_i$ can be retrieved from e_K by performing $\bar{m} = e_K - (\bar{s} \bmod M)$, where $\bar{s} = \sum_{i=1}^{K} \bar{s}_i$. As long as the secret key distributed by BB84 is secure, the confidentiality of individual data is guaranteed, because the control can read only the consolidated data, which is the sum of all original data from a set of meters.

Similar to [76] and [69] wants to protect the data privacy of individual consumers, but for the case where smart meters

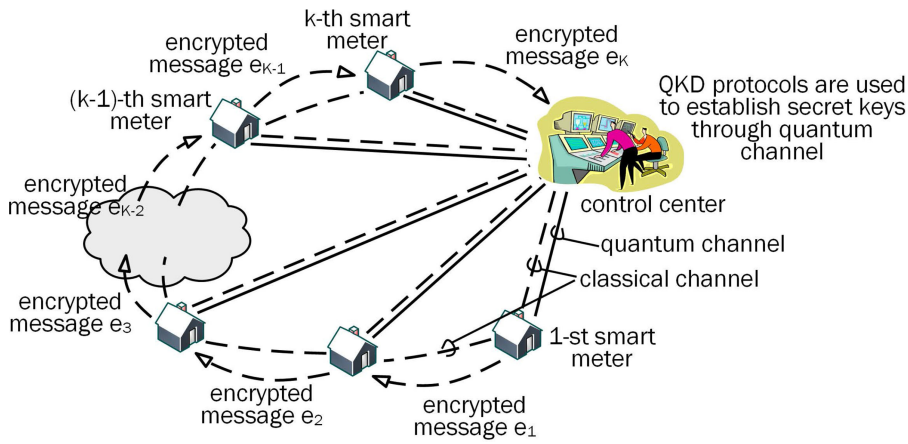

Fig. 5. QKD protocols are used to establish directly a secret key between each smart meter and the control center. But, the control center can only retrieve the aggregate meter readings. Individual meter values are hidden from the control center.

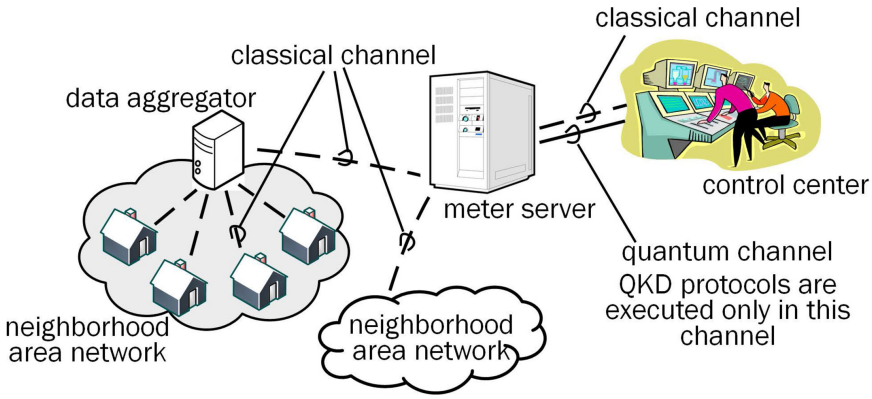

Fig. 6. Smart grid communication system model with a single secret key shared by multiple smart meters.

are not connected directly to the control center. In [69], smart meters are organized into multiple groups, where all smart meters within a group are connected directly only to a data aggregator. As illustrated in Fig. 6, the aggregator is further connected to a meter server, which is a proxy to the control center. Following the same choice of [76], the method proposed in [69] uses BB84 to establish a secret key between the control center and a meter server. Then, the meter server shares the same secret key with all its smart meters only, while keeping the key unknown to the aggregator. Within a domain, different smart meters use a same secret key to encrypt their individual messages before sending them to the aggregator. Then, the aggregator uses the same symmetric homomorphic encryption as in [76] to add multiple encrypted messages before sending the combined message to the meter server. Without knowing the secret key, the aggregator cannot decrypt the message. Upon reception, the combined message is further forwarded to the control center. With knowledge of the secret key, control center can decrypt the message to retrieve the value of the aggregate data, but not individual data of each smart meter. By limiting QKD protocol operations to only between control center and meter server, a clear advantage of this approach is a significant reduction in the use of expensive single-photon detectors. However, in the absence of quantum channels between the meter server and smart meters, it is unclear how secret key can be secured distributed to all meters. Compared to [76] and [69] is less secure because it has contradicted the fundamental of QKD security, where a secret key can only be known by a pair of communicating nodes. With multiple smart meters knowing a same secret key, it is easier for at least one of the them to turn adversary or to disclose the key and thus, compromise the entire system.

For the purpose of evaluating QKD protocols and their applications in smart grid, Lardier *et al.* [77] have developed an open-source cosimulation platform. Compared to other existing simple QKD simulator [78], the platform has been built on Mosaik framework [79] and it can simulate electricity flows in a power grid together with information flow in a communication network. With the platform, QKD protocol is used to distribute secret key before information can be encrypted using OTP or AES-256. The platform has implemented three different PM protocols, such as BB84 and SARG04 [80]. Some case studies have been presented to demonstrate how the platform enables quick configuration of a low-voltage distribution grid for a given topology and a communication network for a desired QKD protocol. The configuration has been evaluated for both efficiency and security against man-in-the-middle attacks.

IV. Research Challenges

So far in this article, we have presented all the existing works that we can find regarding QKD protocols for smart grid communications. While there is a very rich existing literature on QKD protocols in general, there are significantly fewer works on QKD protocols with focus on smart grid communication networks. This implies a good opportunity to make a contribution in this important research area. In the rest of this section, we highlight a few research problems for potential future works.

A. System Scalability

Smart grid communication networks are often characterized as having a larger number of control devices, such as sensors, actuators, and smart meters in the access network. This is a different scenario from which QKD protocols are usually considered for. Typically, QKD protocols are used to secure only a few communication nodes in the core or backbone networks. QKD protocols are not designed to handle a large number of nodes because they work only on a point-to-point basis and each realization requires both a quantum channel and a classical channel. When the number of communication nodes increase even in a simple topology, but not necessarily mesh topology, the system complexity and cost may increase significantly faster. It is not scalable nor reasonable to have QKD protocols implemented in every tiny sensors. We need a scalable architecture that allows sharing of a limited number of quantum channels by a large population of nodes. This means some secret key generated by QKD protocols through quantum channel may be distributed through classical channel. This necessitates developing a hybrid quantum-classical networks that support many users. However, the hybrid key distribution protocols can compromise the prized unconditional security of QKD protocols. Thus, there is a need to develop a hybrid quantum-classical framework to assist in a systematic tradeoff between security requirements and system scalability.

B. End-to-End Security Over Long Distance

Smart grid can cover a large geographical area. For example, the power generator can be located more than 200 km away from the population center as well as the control center. It is not unusual that the control center is situated more than 100 km away from a control device. Recall that QKD protocols work on a point-to-point basis, and cannot reach a key distribution distance beyond 300 km using an optical fiber for secret key rate over 100 kb/s. To establish a secret key over a long distance, current QKD protocols require the use of trusted intermediate nodes to relay the secret keys because reliable and practical quantum repeaters are still nonexistence. In existing multihop implementations, QKD protocols are performed independently on each hop, where each pair of consecutive relay nodes has a separate secret key. Specifically, each relay node will generate a separate secret key with its next relay node. At a relay node, an incoming message is encrypted using the secret key with its upstream relay node. This encrypted message will be decrypted before being encrypted again using the secret key with its downstream relay node. This process of decryption and re-encryption at an intermediate node does not offer a truly end-to-end security to the exchanged messages. This is because the original message and secret keys are exposed in transit even though such exposure is only to some trusted relay nodes. Therefore, there is a need to develop a QKD protocol that can establish an end-to-end secret key without needing the intermediate node to decrypt the messages. This can probably be achieved by considering some practical operating procedures in smart grid context. For example, it is reasonable to assume control devices can be registered and physically coupled with the control center before being brought to installation at a remote location.

C. Real-Time Communications

Secret key rate decreases rapidly with an increase in transmission distance. While most smart grid applications do not produce a large amount of data and, thus, may not require a high key rate, QKD protocols must be able to support real-time dynamic control with short communication latency. Since QKD protocols cannot produce secret keys in real time, such key may be generated long before the initiation of a real-time communication session. This is different from the typical QKD usage scenario, where a generated secret key is used immediately in a communication session. While waiting to be used, a secret key is exposed to peeking. The risk of being stolen increases with the length of waiting time. Also, there is a possibility of losing key synchronization while waiting and maintaining synchronization without data will also consume precious secret key bits. Hence, there is a need to develop a framework to tradeoff between the need to support real-time communications and the risk of secret key being exposed or unsynchronized in waiting.

V. Conclusion

We have presented the needs to safeguard information confidentiality in smart grid and have proposed to do so by using QKD protocols to distribute secret key for OTP symmetric cryptography. To assist readers in appreciating technical details of QKD protocols, we have provided a concise overview on quantum communications. We have also reviewed some QKD protocols that have been used by existing works in securing smart grid communication networks. We have reviewed all the publications that we can find regarding QKD protocols and their applications in smart grid. These existing works deal with effective aggregation of data, authentication of communicating parties, cost-efficient and scalable QKD protocol implementations, etc. For scalability and cost efficiency, sharing of some secret keys by a larger group of communication nodes are often required in these existing works. We have found that there are only a small number of existing publications on QKD protocols in the specific context of smart grid communications, and thus, there is a good opportunity to make some significant contributions in the research area. We have identified a few research challenges, which include connection for a larger number of control devices, truly end-to-end secret key distributions and provision for real-time communications.

REFERENCES

[1] R. Atat, L. Liu, H. Chen, J. Wu, H. Li, and Y. Yi, "Enabling cyber-physical communication in 5G cellular networks: Challenges, spatial spectrum sensing, and cyber-security," *IET Cyber-Phys. Syst.: Theory Appl.*, vol. 2, no. 1, pp. 49–54, Apr. 2017.

[2] P.-Y. Kong, "Multicell D2D communications for hierarchical control of microgrid system," *IEEE Syst. J.*, to be published, doi: 10.1109/jsyst.2020.2990466.

[3] P.-Y. Kong and Y. Song, "Joint consideration of communication network and power grid topology for communications in community smart grid," *IEEE Trans. Ind. Informat.*, vol. 16 , no. 5, pp. 2895–2905, May 2020.

[4] P.-Y. Kong, "Distributed management scheme for energy storage in smart grid with communication impairments," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1392–1402, Apr. 2018.

[5] I. Stoyanov, T. Iliev, G. Mihaylov, E. Ivanova, and P. Kogias, "Smart grid communication protocols in intelligent service for household energy use," in *Proc. Comput. Methods Syst. Software*, Sep. 2017, pp. 380–389.

[6] Y. Song, P.-Y. Kong, Y. Kim, S. Baek, and Y. Choi, "Cellular-assisted D2D communications for advanced metering infrastructure in smart grid," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1347–1358, Jun. 2019.

[7] P.-Y. Kong, "Effects of communication network performance on dynamic pricing in smart power grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 533–541, Jun. 2014.

[8] P.-Y. Kong, "Radio resource allocation scheme for reliable demand response management using D2D communications in smart grid," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2417–2426, May 2020.

[9] P.-Y. Kong, "Wireless neighborhood area networks with QoS support for demand response in smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1913–1923, Jul. 2016.

[10] P.-Y. Kong, "Routing in communication networks with interdependent power grid," *IEEE/ACM Trans. Netw.*, vol. 28, no. 4, pp. 1899–1911, Aug. 2020.

[11] P.-Y. Kong, "Optimal configuration of interdependence between communication network and power grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4054–4065, Jul. 2019.

[12] P.-Y. Kong, "Cost efficient data aggregation point placement with interdependent communication and power networks in smart grid," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 74–83, Jan. 2019.

[13] K. Hamedani, L. Liu, R. Atat, J. Wu, and Y. Yi, "Reservoir computing meets smart grids: Attack detection using delayed feedback networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 734–743, Feb. 2018.

[14] National Institute of Standards and Science, *"Guidelines for Smart Grid Cybersecurity*," National Institute of Standards and Science, Gaithersburg, MD, USA, Rep. NISTIR 7628 revision 1, Sep. 2014.

[15] European Network and Information Security Agency, *Smart grid security, Annex II - Security aspects of the smart grid*, Heraklion, Greece, Apr. 2012.

[16] "Announcing the Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, United States National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Nov. 2001.

[17] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[18] M. Kaur and S. Kalra, "Security in IoT-based smart grid through quantum key distribution," *Adv. Intell. Syst. Comput.*, vol 554, pp. 523–530, Sep. 2017.

[19] QKD4ECI—Quantum Key Distribution for European Critical Infrastructure, Jan. 2020. [Online]. Available: https://artes.esa.int/projects/qkd4eci

[20] D. Flessnerm, "Tennessee utility uses quantum tech for cybersecurity," *Chattanooga Times*, Mar. 2020.

[21] A. M. Lewis and M. Travagnin, "A secure quantum communications Infrastructure for Europe," European Commissions Science and Knowledge Service Joint Research Center, Brussels Belgium, Tech. Rep. JRC116937, Jul. 2019,

[22] Z. Zhihao, "Quantum tech to link Jinan governments," *China Daily*, Jul. 2017. [Online]. Available: http://www.chinadaily.com.cn/china/2017-07/11/content_30065215.htm

[23] X. Zhang, Z. Y. Dong, Z. Wang, C. Xiao, and F. Luo, "Quantum cryptography based cyber-physical security technology for smart grids," in *Proc. Int. Conf. Adv. Power Syst. Control, Oper. Manage.*, Nov. 2015, pp. 1–6.

[24] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surveys Tut.*, vol. 21, no. 1, pp. 881–919, First Quarter 2019.

[25] L. Jian *et al.*, "A survey on quantum cryptography," *Chin. J. Electron.*, vol. 27, no. 2, pp. 223–228, Mar. 2018.

[26] A. I. Nurhadi and N. R. Syambas, "Quantum key distribution (QKD) protocols: A survey," in *Proc. Int. Conf. Wireless Telematics*, Jul. 2018, pp. 1–5.

[27] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, Mar. 2010.

[28] S. Imre, "Quantum communications: Explained for communication engineers," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 28–35, Aug. 2013.

[29] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *Quantum Inf.*, vol. 2, Nov. 2016, Art. no. 16025.

[30] A. Sharma and A. Kumar, "A survey on quantum key distribution," in *Proc. Int. Conf. Issues Challenges Intell. Comput. Techniques*, Sep. 2019, pp. 1–4.

[31] G. Arun G and V. Mishra, "A review on quantum computing and communication," in *Proc. Int. Conf. Emerg. Technol. Trends Electron., Commun. Netw.*, Dec. 2014, pp. 1–5.

[32] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, no. 3, pp. 1829–1834, Mar. 1999.

[33] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, "Long-distance measurement-device-independent multiparty quantum communication," *Phys. Rev. Lett.*, vol. 114, no. 9, pp. 090–501, Mar. 2015.

[34] H.-J. Ding *et al.*, "280-km experimental demonstration of a quantum digital signature with one decoy state," *Opt. Lett.*, vol. 45, no. 7, pp. 1711–1714, Apr. 2020.

[35] H.-L. Yin, Y. Fu, and Z.-B. Chen, "Practical quantum digital signature," *Phys. Rev. A*, vol. 93, no. 3, pp. 032–316, Mar. 2016.

[36] R. Amiri, P. Wallden, A. Kent, and E. Andersson, "Secure quantum signatures using insecure quantum channels," *Phys. Rev. A*, vol. 93, no. 3, pp. 032–325, Mar. 2016.

[37] S. Pirandola *et al.*, "Advances in quantum cryptography," Jun. 2019, *arXiv:1906.01645v1*.

[38] S. Chen *et al.*, "Internet of things based smart grids supported by intelligent edge computing," *IEEE Access*, vol. 7, pp. 74089–74102, Jun. 2019.

[39] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[40] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. ACM Symp. Theory Comput.*, May 1996, pp. 212–219.

[41] D. Bruss, G. Eedelyti, T. Meyer, T. Riege, and J. Rothe, "Quantum cryptography: A survey," *ACM Comput. Surveys*, vol. 39, no. 2, pp. 1–27, Jun. 2007.

[42] "Status report on the second round of the NIST post-quantum cryptography standardization process," National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Rep. NISTIR 8309, Jul. 2020.

[43] H.-L. Yin *et al.*, "Long-distance measurement-device-independent quantum key distribution with coherent-state superpositions," *Opt. Lett.*, vol. 39, no. 18, pp. 5451–5454, 2014.

[44] H.-L. Yin, Y. Fu, Y. Mao, and Z.-B. Chen, "Security of quantum key distribution with multiphoton components," *Sci. Rep.*, vol. 6, 2016, Art. no. 29482.

[45] W. K. Wootters and W. Hubert, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[46] C. Bennett and G. Brassard, "Quantum cryptography: Key distribution and coin tossing," in *Proc. Int. Conf. Comput., Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 175–179.

[47] A. K. Ekert, "Quantum cryptography based on Bells' theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–553, Aug. 1991.

[48] A. Einstein, B. Podolsky, and N. Rosen, "Can qantummechanical description of physical reality be considered complete?" *Phys. Rev.*, vol. 47, pp. 777–780, May 1935.

[49] H.-L. Yin *et al.*, "Measurement device independent quantum key distribution over 404 km optical fibre," *Phys. Rev. Lett.*, vol. 117, no. 19, Nov. 2016, Art. no. 190501.

[50] J.-P. Chen *et al.*, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, no. 7, pp. 070–501, Feb. 2020.

[51] B. Korzh *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photon.*, vol. 9, pp. 163–168, Feb. 2015.

[52] V. Sharma, K. Thapliyal, A. Pathak, and S. Banerjee, "A comparative study of protocols for secure quantum communication under noisy environment: Single-qubit-based protocols versus entangled-state-based protocols," *Quantum Inf. Process.*, vol. 15, no. 11, pp. 4681–4710, Jul. 2016.

[53] L. Fang-Yi *et al.*, "Effect of electromagnetic disturbance on the practical QKD system in the smart grid," *Chin. Physics B*, vol. 23, no. 12, Oct. 2014, Art. no. 12401.
[54] S. F. Bush, S. Goel, and G. Simard, *IEEE Vision for Smart Grid Communications: 2030 and Beyond Roadmap*, pp. 1–19, Sep. 2013, doi: 10.1109/IEEESTD.2013.6690098.
[55] R. Zhang and X. Chen, "Prospects of fiber quantum key distribution technology for power systems," in *Proc. Int. Conf. Elect. Distrib.*, Jun. 2013, pp. 1–4.
[56] K. A. Patel *et al.*, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X*, vol. 2, no. 4, Nov. 2012, Art. no. 41010.
[57] Y. Ma, X. Wang, and D. Cui, "Secure communication mechanism for smart distribution network integrated with subcarrier multiplexed quantum key distribution," *Power Syst. Technol.*, vol. 37, no. 11, pp. 3214–3220, Nov. 2013.
[58] P.-Y. Kong, K.-S. Tseng, J.-A. Jiang, and C.-W. Liu, "Robust wireless sensor networks for transmission line monitoring in Taiwan," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technologies Smart Grids*, Oct. 2018, pp. 1–6.
[59] P.-Y. Kong, C.-W. Liu, and J.-A. Jiang, "Cost efficient placement of communication connections for transmission line monitoring," *IEEE Trans. Ind. Electron.*, vol. 64, no. 5, pp. 4058–4067, May 2017.
[60] P.-Y. Kong *et al.*, "An adaptive packets hopping mechanism for transmission line monitoring systems with a long chain topology," *Int. J. Elect. Power Energy Syst.*, vol. 124, 106–394, Jan. 2021.
[61] S. Fuloria, R. Anderson, K. McGrath, K. Hansen, and F. Alvarez, "The protection of substation communications," 2009. [Online]. Available: http://www.cl.cam.ac.uk/rja14/Papers/S4-2010.pdf
[62] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: Real implementation problems," *Theor. Comput. Sci.*, 560, pp. 27–32, Sep. 2014.
[63] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, pp. 130–503, Mar. 2012.
[64] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Phys. Rev. Lett.*, vol. 111, no. 13, pp. 130–501, Sep. 2013.
[65] A. Long, "Trustworthy relay node networking," *Cybersecurity for Energy Delivery Systems Peer Review*, Los Alamos National Laboratory, Los Alamos, NM, USA, Nov. 2018.
[66] G. Jia, W. Ni, and J. Wu "Research and applications of key technologies of quantum secure communication in energy Internet," in *Proc. Int. Conf. Intell. Green Building Smart Grid*, Sep. 2019, pp. 54–60.
[67] Z. Yan, Q. Zhang, Y. Song, and J. Yuan, "Quantum key interaction mechanism for power communication access network," in *Proc. IEEE Int. Conf. Commun. Technol.*, Oct. 2018, pp. 941–945.
[68] G. Bebrov, R. Dimova, and E. Pencheva, "Quantum approach to the information privacy in smart grid," in *Proc. Int. Conf. Optim. Elect. Electron. Equipment*, May 2017, pp. 971–976.
[69] R. C. Diouvu and J. T. Agee, "Enhancing the security of a cloud-based smart grid AMI network by leveraging on the features of quantum key distribution," *Trans. Emerg. Telecommun. Technologies*, vol. 30, no. 6, pp. 1–21, Jun. 2019.
[70] L. Wang, D. Wang, J. Gao, C. Huo, H. Bai, and J. Yuan, "Research on multi-source data security protection of smart grid based on quantum key combination," in *Proc. IEEE Int. Conf. Cloud Comput. Big Data Anal.*, Apr. 2019, pp. 1–5.
[71] Y. Li, P. Zhang, and R. Huang, "Lightweight quantum encryption for secure transmission of power data in smart grid," *IEEE Access*, vol. 7, pp. 36285–36293, Apr. 2019.
[72] K. Bostrom and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, no. 18, pp. 187–902, Oct. 2002.
[73] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, "Network-centric quantum communications with application to critical infrastructure protection," May 2013, *arXiv:1305.0305*.
[74] S. Zhang, X. Liu, and B. Wang, "An applied research of improved BB84 protocol in electric power secondary system communication," in *Proc. Int. Conf. Electron. Eng., Commun. Manage.*, Dec. 2011, pp. 545–550.
[75] L. Zhu and B. Tung, "Public key cryptography for initial authentication in Kerberos (PKINIT)," Internet Engineering Task Force (IETF), RFC 4556, Jun. 2006.
[76] F. Borges, R. A. M. Santos, and F. L. Marquezino, "Preserving privacy in a smart grid scenario using quantum mechanics," *Secur. Comm. Netw.*, vol. 8, no. 12, pp. 2061–2069, Aug. 2015.
[77] W. Lardier, Q. Varo, and J. Yan, "Quantum-Sim: An open-source co-simulation platform for quantum key distribution-based smart grid communications," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technologies Smart Grids*, Oct. 2019, pp. 1–6.
[78] QKD simulator. Accessed: Mar. 31, 2020. [Online]. Available: https://qkdsimulator.com
[79] MOSAIK "A Flexible Smart Grid Co-Simulation Framework," May 2020. [Online]. Available: https://mosaik.offis.de/
[80] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, Feb. 2004, Art. no. 57901.

Peng-Yong Kong (Senior Member, IEEE) received the B.Eng. (first class honours) degree in electrical and electronic engineering from the Universiti Sains Malaysia, George Town, Malaysia, and the Ph.D. degree in electrical and computer engineering from the National University of Singapore, Singapore.

He is currently an Associate Professor with the Electrical Engineering and Computer Science Department, Khalifa University, Abu Dhabi, UAE. He was previously an Adjunct Assistant Professor with the Electrical and Computer Engineering Department, National University of Singapore, Singapore, concurrent to the appointment of a Research Scientist with the Institute for Infocomm Research, Agency for Science, Technology and Research, Singapore. He was an Engineer with the Intel Malaysia. His research interests are in the broad area of computer and communication networks, as well as cyber-physical systems.