Joint Server, Source Rate, and Link Allocation Strategy for Semi-QKD in Power Systems

1st Mariam Gado
Department of Computer Science
Tennessee Technological University
Cookeville, Tennessee, USA
mmgado42@tntech.edu
ORCID: 0000-0001-9249-3794

2nd Muhammad Ismail
Department of Computer Science
Tennessee Technological University
Cookeville, Tennessee, USA
mismail@tntech.edu

***Abstract*—Semi-quantum key distribution (Semi-QKD) can generate unconditionally secure keys between the substations and control center in power systems. These keys can be used to encrypt and decrypt measurements and control commands. This paper studies the problem of allocating a minimal number of quantum servers with optimal source rates and fiber links on a pre-existing cyber layer of power systems to satisfy the minimum required key rate under an attacker's presence. We formulate the problem as a binary optimization problem to upgrade the cyber layer of power system to supports semi-QKD. We use genetic algorithm to develop an optimal allocation strategy due to the complexity of the allocation problem. We examine the proposed allocation strategy on the cyber layer of the IEEE 14-bus and the IEEE 39-bus test systems. Our results demonstrate that the target key rate can be achieved at different attack levels with a number of quantum servers and fiber links that is 70% and 31%, respectively, less than the results of a benchmark for the IEEE 14-bus system. Also, we obtained a number of quantum servers and fiber links that is 66.67% and 17%, respectively, less than the result of a benchmark for the IEEE 39-bus system. Our results demonstrate that the proposed solution requires 80% and 97% less quantum server upgrades compared with QKD for the IEEE 14-bus and the IEEE 39-bus test systems, respectively.**

***Index Terms*—Quantum key distribution, SQKD, smart grid, power system, genetic algorithms, and secret key generation.**

I. Introduction

False data and command injection attacks threaten the security of power systems. These attacks can be mitigated using encryption algorithms such as the advanced encryption system (AES) [1]. Secret keys can support encryption and decryption of data, which can be shared between parties using key-sharing mechanisms. Two of the most used key-sharing mechanisms are Rivest-Shamir-Adleman (RSA) [2] and Diffie-Hellman key exchange [3], which depend on the mathematical problem complexity to secure the keys [4]. These problems can not be solved in a reasonable time using classical computers. However, quantum computers have the capability to solve them, revealing the secret keys and compromising the security of the system [5]. Post-quantum key exchange strategies were proposed to solve this challenge, achieving system security against both classical and quantum adversaries under computational assumptions. On the other hand, quantum key distribution (QKD) and SQKD have the unique advantage of generating unconditionally secure keys, following the laws of quantum mechanics.

Breaching the security of the power system can lead to blackouts, which leads to severe consequences varying from financial losses to threatening the human lives. Quantum servers are used to support QKD and SQKD by generating, measuring, and manipulating quantum bits (qubits). Fiber optical links are also needed to transmit qubits between nodes. However, the cyber layer of the power system is not prepared with the necessary equipment for these capabilities. Hence, it is needed to explore the upgrade solutions of the cyber layer of power systems by equipping it with quantum servers and fiber links to support QKD or SQKD.

A. Related Works

In a recent work, QKD is used for secret key sharing and data authentication in power systems [6]. Two of the most used QKD protocols are BB84 protocol [7] and B92 protocol [8]. Both protocols require all the cyber nodes in the cyber layer to be upgraded to fully quantum servers with full quantum capabilities, i.e., qubit generation, transmission, and measurement in the Z or the X bases. On the other hand, SQKD has the advantage of sharing unconditionally secure keys between nodes that are not fully quantum servers unlike QKD [9]. In SQKD, a few number of nodes have to be upgraded to fully quantum servers, while the remaining nodes have limited quantum capabilities, e.g., transmit and measure qubits only in the Z basis. Several SQKD protocols have been proposed in the literature [9]. The mirror protocol is considered as one of the most robust SQKD protocols against noiseless attacks, which can be applied in practice [10]. Practical collective attacks on the mirror protocol were studied in [11], while the remaining study of general attacks is still an open research problem. The work in [12] proposed a greedy algorithm to upgrade a pre-existing fiber-based cyber layer in power system to support SQKD.

B. Limitations, Challenges, and Contributions

The aim of this paper is to enable substations in power systems to share unconditionally secure keys to secure mea-

This work was supported by NSF award #2220346.

surements and control commands. However, the works in the literature to secure power grids e.g., [6], [13], and [12], using QKD suffer from the following limitations:

- The studied power systems consider a small number of closely located power substations, where the scalability of these QKD solutions is not guaranteed for larger transmission power systems.
- The QKD-based solutions in the literature require the upgrade of all cyber nodes in the cyber layer to fully quantum servers, which increase the upgrading cost.
- There is only one existing work in the literature [12] that considers upgrading the cyber layer of power systems to support SQKD to reduce the cost compared with QKD solutions. However, this work assumes the existence of a fiber-based cyber layer to be upgraded to support SQKD, such assumption is not supported in existing power systems [14]. Instead, existing power systems are equipped with a mixture of classical links (e.g., radio, microwave, etc.) and fiber links.

Hence, there is a need for a cost-effective solution to support SQKD by upgrading a pre-existing cyber layer in a larger transmission power system. The solution should enable these features: (a) the proposed solution should require the upgrade of a minimal number of cyber nodes to quantum servers, where the selected quantum servers have the least possible source rates and a minimal number of link upgrades to fiber links. The quantum servers have full quantum capabilities, while the remainder of cyber nodes have limited quantum capabilities; (b) The proposed solution should satisfy the target key rate for long distances on a large-scale transmission power system.

Toward this objective, we carried out the following:

- We formulated a binary optimization problem for allocating a minimal number of quantum servers with the least source rates and fiber links, thus, upgrading the classical cyber layer of power system to support SQKD to satisfy the minimum target key rate under the presence of an attacker who controls the noise in the quantum channel. To solve the formulated problem, we propose an allocation strategy based on a genetic optimization algorithm given the computational complexity.
- We examined the proposed allocation strategy on the cyber layer of the IEEE 14-bus and the IEEE 39-bus test systems. Our results demonstrate a quantum server number reduction of 70% and 50% compared with a source rate benchmark solution of 10^7 photon per second (pps) in the benchmark for the IEEE 14-bus and the IEEE 39-bus test systems, respectively. Also, our results demonstrate a quantum server number reduction of 80% and 97% compared with QKD for the IEEE 14-bus and the IEEE 39-bus test systems, respectively. The number of fiber link upgrades has a reduction of 31% and 17% compared with a benchmark and QKD for the IEEE 14-bus and the IEEE 39-bus test systems, respectively.

The rest of this paper is organized as follows. Section II reviews quantum systems and SQKD. Section III illustrates the system model. Section IV presents the problem formulation and the proposed allocation strategy. Section V introduces the numerical results. Section VI concludes our paper.

II. Preliminaries

This section gives a brief background about quantum systems and SQKD.

A. Quantum States and Measurements

Quantum systems use qubits as the basic building blocks of information. Photons are used to represent qubits in the SQKD systems, and the polarization of the photon(s) represents a quantum state. We consider two polarization bases in this paper as follows: the Z basis (i.e., computational basis) and the X basis (i.e., diagonal basis). The Z basis has two states $|0\rangle$ and $|1\rangle$, and the X basis has two states $|+\rangle$ and $|-\rangle$, where the state $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and the state $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. To receive the corresponding information, both the sender and the receiver must agree on the same basis for encoding and decoding the qubits in quantum systems. In the Z basis, the classical bits 0 and 1 are received when measuring $|0\rangle$ and $|1\rangle$, respectively. In the X basis, the classical bits 0 and 1 are received when measuring $|+\rangle$ and $|-\rangle$, respectively.

B. Semi-Quantum Key Distribution Protocol

We adopt the mirror protocol [10] for SQKD since its security was proven to be robust against all noiseless attacks and a set of practical attacks [11]. The mirror protocol defines Bob as the fully quantum node, while Alice is defined as the semi-quantum node with limited quantum capabilities. The steps of the SQKD mirror protocol are as follows:

1) Bob prepares a $|+\rangle$ state and sends it to Alice.
2) Alice receives the $|+\rangle$ state and applies one of the following steps randomly:
   a) Alice leaves all photons undisturbed and transmits them back (reflects) towards Bob without measuring them. This is called a test round.
   b) Alice reflects all the photons in the $|1\rangle$ state and measures all the photons in the $|0\rangle$ state. This is called a raw key round.
   c) Alice reflects all the photons in the $|0\rangle$ state and measures all the photons in the $|1\rangle$ state. This is called a raw key round.
   d) Alice measures all the photons and does not reflect any photons towards Bob. This is called a swap-all round.
3) Bob receives the state from Alice if any and measures it either in the Z basis or in the X basis randomly.

In the raw key rounds, Alice and Bob can share a qubit if Alice chooses 2b) or 2c) while detecting no photon after she applies measurements on the state she received. Simultaneously, Bob has to choose the Z basis for measurement in order for them to share a qubit. We refer the reader to [10] for more information about the mirror protocol. We assume the existence of an insider attacker Eve between Alice and Bob who controls the communication channel's noise by

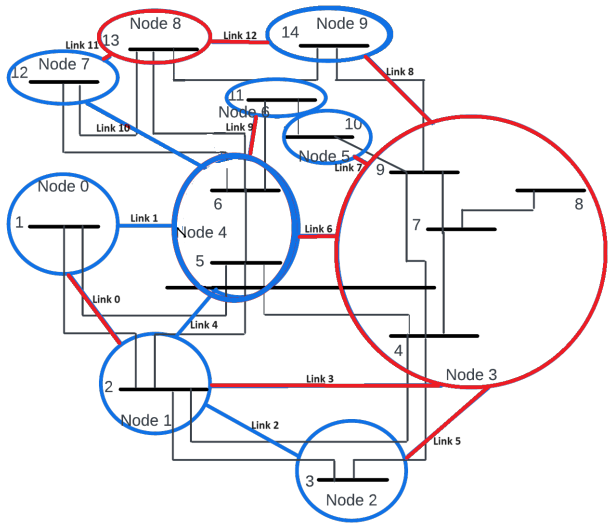

Fig. 1: Physical layer of the IEEE 14-bus system (in black) and the cyber layer (in blue). The cyber layer is based on [15]. The full quantum nodes and fiber links are represented in red. Semi-quantum nodes are represented in blue.

performing no attack or a single attack represented by a noise injection level.

III. System Model

The physical and cyber layers of the power system are described in this section along with the design requirements.

A. Physical Layer

The physical layer consists of a set of generation and load buses (substations) that are connected using transmission lines. Each substation is connected to sensing devices, which monitor and measure active and reactive powers, three-phase voltages, etc.

The quantum servers in the physical model are the local controllers, where the substations send their measurements and receive the control commands from the local controllers via a wide-area network.

We use the IEEE 14-bus and the IEEE 39-bus test systems for performance evaluation of the proposed allocation strategy.

B. Cyber Layer

The local controllers are connected to the power substations in the cyber layer via a set of routers and links. The cyber layer of the IEEE 14-bus test system based on [15] is illustrated in Fig. 1. The majority of links are classical in the classical networks according to [14], hence, in this work we assume that there are no fiber links in the cyber layer for both of the considered test systems.

This work aims to define the quantum server and fiber link upgrades (i.e., red circles and lines in Fig. 1, respectively) of the cyber layer to support SQKD between the local control centers and the power substations. The remaining of the cyber nodes will be semi-quantum servers with limited quantum capabilities, and the rest of the links are not going to be upgraded. The generated unconditionally secure keys will be used for encryption and decryption of measurements and control signals between the local control centers and the power substations.

C. SQKD Rate

To support a key distribution rate $r_{n,n'}$ between a fully quantum server at n and a semi-quantum server at n', an optimal number and locations of quantum servers and fiber links are required. A set of intermediate fiber links $\mathcal{E}_{n,n'}$ is used between nodes n and n'. This set is a collection of all fiber links in the path between nodes n and n' to generate $r_{n,n'}$, which satisfy the minimum required key generation rate $r_{\min}$. The channel between n and n' is noisy reducing the attained key rate $r_{n,n'}$, where the noise is indicating the existence of an attacker E.

The works in [11] and [12] describe the attained key rate $r_{n,n'}$ in bits per second (bps) as follows:

$$r_{n,n'} = r_n \times M_{n,n'} \times (S(n'|E) - H(n'|n)), \tag{1}$$

where r_n represents the source rate of the fully quantum server in pps. In (1), $M_{n,n'}$ is the probability a raw key bit is generated between nodes n and n' successfully, which is described as [11]

$$M_{n,n'} = \frac{1}{2} \times 10^{\frac{-2\alpha L_{n,n'}}{10}}, \tag{2}$$

where α denotes the fiber link attenuation loss per kilometer and $L_{n,n'}$ is the fiber link length between nodes n and n' in kilometer, which is the summation of the lengths of all fiber links in $\mathcal{E}_{n,n'}$. The right-hand side term in (1) represents the difference between two terms. The first term is the Von Neuman entropy $S(n'|E)$ between n' and the attacker E. The second term is the entropy $H(n'|n)$ between n and n'. The reader is referred to [11] for more information about the calculation of the key rate of the SQKD protocol.

IV. The Allocation of Different Quantum Servers and Fiber Links

In this section, we formulate the problem to minimize the upgrading cost of the cyber layer of the power system to support the generation of unconditionally secure keys. Then, we illustrate our proposed allocation strategy based on genetic optimization.

A. Problem Formulation

The cyber layer is modeled as an undirected, connected, weighted, acyclic graph $G(\mathcal{N}, \mathcal{E})$. $\mathcal{N}$ represents the set of cyber nodes in the classical cyber layer and $\mathcal{E}$ represents the set of classical links between nodes, which can be microwave, radio, etc. The cyber layer does not have any fiber links. The set $\mathcal{E}$ has its corresponding weights based on the lengths of each link. The allocation problem identifies the minimum number of cyber nodes $\in \mathcal{N}$ to be upgraded to fully quantum servers belonging to a discrete set of source rates $\mathcal{K}$. The set

$\mathcal{E}$ of the links to be upgraded to fiber links is also identified by the allocation problem.

There are three constraints in the allocation problem, the first constraint is achieving the minimum required key generation rate $r_{\min}$. The second constraint ensures that a link is upgraded to a fiber link only if it is part of a path between n and n'. The third constraint ensures that only one quantum server is allocated at a given upgraded cyber node. We describe the allocation problem as follows

$$\begin{aligned} \min_{x_{n,k}, y_{i,j}} \quad & \sum_{n=1}^{N} x_{n,k} + \sum_{i=1}^{N}\sum_{j=1}^{N} y_{i,j} \\ \text{s.t.} \quad & r_{n,n'} \geq r_{\min} \\ & y_{i,j} \in \mathcal{E}_{n,n'}, \\ & \sum_{k=1}^{\mathcal{K}} x_{n,k} = 1 \ \forall n \\ & \qquad \forall n \in \hat{\mathcal{N}}, n' \in \mathcal{N}/\hat{\mathcal{N}}, \\ & \qquad \forall i, j \in \mathcal{N} \\ & \qquad i \neq j, n \neq n', \\ & \qquad x_{n,k}, y_{i,j} \in \{0,1\}, \end{aligned} \tag{3}$$

where $x_{n,k}$ is a binary quantum server allocation decision variable such that $x_{n,k} = 1$ indicates that the cyber node n is to be upgraded to a quantum server, where k belongs to the pps set $\mathcal{K}$, $\hat{\mathcal{N}}$ is the set of quantum servers, and $n \in \hat{\mathcal{N}}$. Otherwise, $x_{n,k} = 0$ and the node n is to be considered as a semi-quantum server, where $\mathcal{N}/\hat{\mathcal{N}}$ is the set of semi-quantum servers, where $y_{i,j}$ is defined as a binary fiber link allocation decision variable. $y_{i,j} = 1$ indicates that this link is to be upgraded to a fiber link to support SQKD, where $y_{i,j}$ directly connects nodes i and j. Otherwise, $y_{i,j} = 0$ and this link will not be upgraded. The allocation problem maintains the minimum required key rate $r_{\min}$ in the first constraint in (3), where $r_{n,n'}$ is calculated from (1). The second constraint ensures that $y_{i,j}$ is only upgraded if it is part of a path in $\mathcal{E}_{n,n'}$ between n and n'. The third constraint ensures that there is only one quantum server that is allocated at n.

The allocation problem introduced in (3) is an NP-complete binary program [12]. Hence, we propose a genetic algorithm-based allocation strategy due to the complexity of finding an optimal solution to (3).

B. Proposed Allocation Strategy

We use genetic algorithm (GA)-based approach to solve the allocation problem since GA solves optimization problems with lower complexity [16]. GA is a metaheuristic algorithm whose operations follow the nature evolution such as selection, mutation, and crossover.

The key distribution rate between a semi-quantum node (Alice) and a quantum server (Bob) is affected by the distance between these two nodes and the used source rate to generate the photons assuming the other algorithm's variables in (1) are fixed. Each cyber node is a candidate to be upgraded to one of the k quantum servers. Similarly, each link/edge is a candidate to be upgraded to a fiber link. The solution is modeled as a variant of the one-max problem [17] in which a chromosome has the length of the summation of the number of cyber nodes, k times the number of cyber nodes (for k distinct source rates) and the number of links between nodes. We construct the population using the chromosome length, population size, crossover rate, number of iterations, mutation rate, and the objective function. Three constraints are checked after constructing a quantum network graph G' based on the chromosome for a feasible solution. This allows us to construct a feasible search space that allows the objective function value to be minimized. The three constrains are: (a) minimum required key rate satisfaction $r_{\min}$, which is checked using the first constraint in (3), (b) graph connectivity, which is checked using the second constraint in (3), (c) quantum server exclusivity, which is checked by the third constrain in (3).

Algorithm 1 illustrates the steps of the proposed allocation strategy, where the inputs are as follows: the minimum required key rate $r_{\min}$, the cyber layer topology $G(\mathcal{N}, \mathcal{E})$, the number of iterations $iter$, chromosome length $lenc$, population size $psize$, crossover probability $pcross$, and mutation probability $pmut$. The **Construct-Pop**$(lenc, psize)$ generates a population size $psize$ of chromosomes with a length of $lenc$. **Construct**(c) function checks the number and locations of 1s the chromosome and constructs the graph G'. **C-Rate**(G') function has two aims. The first aim is to assign a quantum server with its corresponding source rate for each semi-quantum node in the graph, which generates the largest key generation rate for this semi-quantum node. The second aim is to check if all nodes can obtain the minimum key generation rate $r_{\min}$ for the chromosome. **C-Con**(G') function uses Dijkstra's algorithm to check if the graph G' is connected through checking the connectivity of each node to all other nodes in the graph. **C-Server**(G') function ensures that only one quantum server is installed in a specific node. The outputs of the three functions are binary. **UpgradesN**(c) function calculates the score of the chromosome only if all outputs of the three previously mentioned binary functions are 1s, otherwise, the score of the chromosome is infinity and it does not represent a feasible solution. The score is calculated using the summation of quantum servers and fiber links according to the following weights, where $k \in \{10^7, 10^8, 10^{10}\}$ in this paper: the weight of the 10^7 pps server or a fiber link is 1, the weight of 10^8 pps server is 2, and the weight of 10^{10} pps server is 4 since higher source rates cost more than lower source rates. The function **Construct-npop**$(pop, scores, pcross, pmut)$ generates a new population $npop$ from the inputs as follows: the previous population pop, previous population scores $scores$, the crossover probability $pcross$, and the probability of mutation $pmut$. The output of Algorithm 1 is the chromosome solution to the allocation problem, where it defines the number of each quantum servers, their locations, and the number and locations of fiber links.

Algorithm 1 Proposed Allocation Strategy

Input: $r_{\min}$, $G(\mathcal{N}, \mathcal{E})$, $iter$, $lenc$, $psize$, $pcross$, $pmut$
Initialize: Empty lists pop, $npop$
min $\rightarrow \infty$
pop = $npop$ = **Construct-Pop**($lenc$, $psize$)
for $i \in iter$ **do**
  $pop = npop$
  $scores$ = []
  for $c \in psize$ **do**
    G' =**Construct**(c)
    con1 = **C-Rate**(G')
    con2 = **C-Con**(G')
    con3 = **C-Server**(G')
    if con1 = con2 = con3 = 1 **then**
      score = **UpgradesN**(c)
    else
      score = ∞
    end if
    $scores$.add($score$)
    if $score \leq$ min **then**
      solution = c
    end if
  end for
  $npop$ = **Construct-npop** (pop, $scores$, $pcross$, $pmut$)
end for
Output: Allocation solution

V. Numerical Results

The numerical results of the allocation strategy are represented in this section on the cyber layer of the IEEE 14-bus test system as illustrated in Fig. 1 [15] and the cyber layer of the IEEE 39-bus test system [18]. Link distances are extracted from the technical notes in [19] and [18] for the IEEE 14-bus and the IEEE 39-bus test systems, respectively. The attenuation coefficient α in this work is set to 0.2 dB/km [20]. Algorithm 1 is used as the allocation strategy, where the following values are the inputs: $r_{\min} = 256$ (for AES standard), $iter = 1000$, $lenc = 53$ (10 servers $+13$ edges $+3\times10$), $lenc = 203$ for the IEEE 14-bus and the IEEE 39-bus test systems, respectively, $psize = 200$, $pcross = 0.9$ and $pmut = 1/23$. We consider three distinct source rates, i.e., $k \in \{10^7, 10^8, 10^{10}\}$.

A. IEEE 14-bus Test System

The numerical results of using Algorithm 1 on the IEEE 14-bus test system are shown in this subsection.

The numerical results of the allocation strategy on the cyber layer of the IEEE 14-bus test system are shown in Fig. 2, where we compare the number and the source rate of the quantum servers and the number of fiber links. Fig. 2 shows that at least 2 nodes are required to be upgraded to fully quantum servers, one with source rates of 10^7 pps and the other with a source rate of 10^8 pps in order to satisfy $r_{\min} = 256$ bps under the presence of an attacker with a noise level up to 11%, which is the maximum achieved resistance by the SQKD algorithm in [10]. The work in literature [12] shows that at least 10, 3 and 2 nodes are required to be upgraded to fully quantum servers of source rate of 10^7 pps, 10^8 pps and 10^{10} pps, respectively. The number of links to be upgraded to fiber links is 9 using the proposed allocation strategy, while the benchmark in [12] requires a fully fiber network of 13 fiber links. The results demonstrate a reduction of 33% in the number of quantum servers compared with the source rate solution of 10^8 pps and also a source rate reduction of one server to 10^7 pps for both the benchmark solutions in [12] of 10^8 pps and 10^{10} pps. The results also show a reduction of 70% and 80% in the number of quantum servers for 10^7 pps and full QKD solutions, respectively. The number of link upgrades is reduced by 31% compared with both of the QKD and the benchmark in [12].

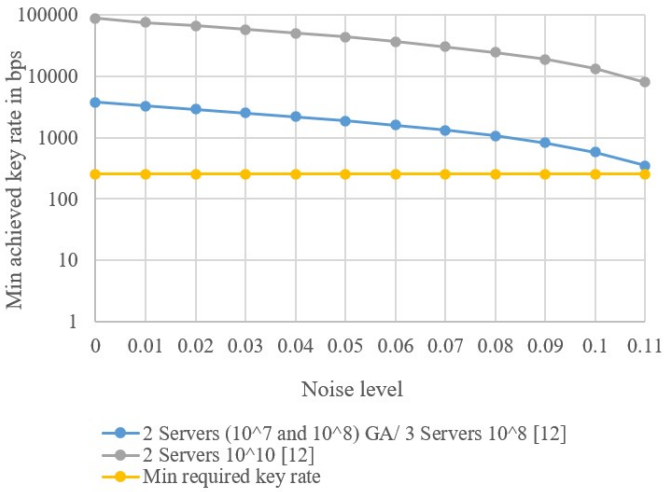

Fig. 2: Comparison of the minimum achieved key rate $r_{n,n'}$ and the number and source rate of quantum servers on the cyber layer of the IEEE 14-bus test system between the proposed allocation strategy (GA) and the benchmark in [12] for an attack level up to 11%.

B. IEEE 39-bus Test System

The numerical results of using Algorithm 1 on the IEEE 39-bus test system are shown in this subsection.

The numerical results of the allocation strategy on the cyber layer of the IEEE 39-bus test system, where we compare the number and the source rate of the quantum servers and the number of fiber links. Fig. 3 shows that at least 1 node is required to be upgraded to a fully quantum server with a source rate of 10^8 pps in order to satisfy $r_{\min} = 256$ bps under the presence of an attacker with a noise level up to 11%. The work in literature [12] shows that at least 4, 3 and 1 nodes are required to be upgraded to fully quantum servers of source rate of 10^7 pps, 10^8 pps and 10^{10} pps, respectively. The number of links to be upgraded to fiber links is 39 using the proposed allocation strategy, while the benchmark in [12] requires a fully fiber network of 47 fiber links. The results demonstrate

a reduction of 50% and 66.67% in the number of quantum servers compared with the source rate solution of 10^7 pps and 10^8 pps, respectively, and also a source rate reduction of one server to 10^8 pps for the 10^{10} pps benchmark solution in [12]. The results also show a reduction of 97% in the number of quantum servers compared with QKD solutions. The number of link upgrades is reduced by 17% compared with full QKD and the benchmark in [12].

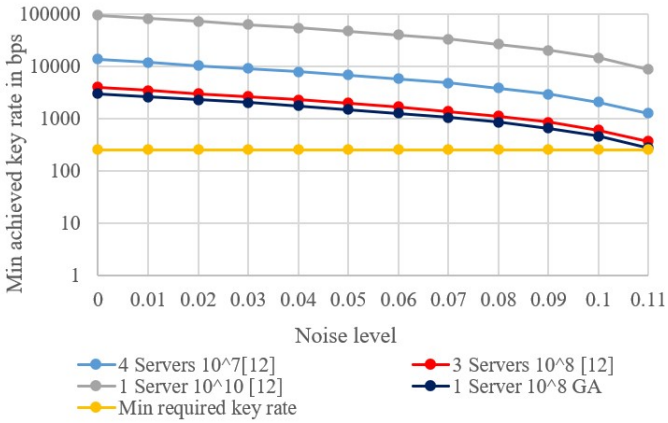

Fig. 3: Comparison of the minimum achieved key rate $r_{n,n'}$ and the number and source rate of quantum servers on the cyber layer of the IEEE 39-bus test system between the proposed allocation strategy (GA) and the benchmark in [12] for an attack level up to 11%.

VI. Conclusion

The problem of upgrading a pre-existing cyber layer of power systems to support the generation of unconditionally secure keys using SQKD was studied in this paper. In this paper, full quantum upgrade of cyber nodes and fiber links upgrade are specified only for a subset of cyber nodes and links, respectively, while the remaining cyber nodes have limited quantum capabilities. This paper formulated the upgrading of the cyber layer problem as a binary program and proposed a genetic algorithm as a solution to reduce the computational complexity. In the IEEE 14-bus test system, the proposed algorithm requires 47.8%, 36.8%, and 42.9% less upgrades compared with the source rate of 10^7 pps, 10^8 pps, and 10^{10} pps solutions in the benchmark in [12], respectively. Also, for the IEEE 14-bus test system, the proposed algorithm requires 52.17% less upgrades compared with the QKD solutions. In the IEEE 39-bus test system, the proposed algorithm requires 19.6%, 22.6%, and 19.6% less upgrades compared with the source rate of 10^7 pps, 10^8 pps, and 10^{10} pps solutions in the benchmark in [12], respectively. Also, for the IEEE 39-bus test system, the proposed algorithm requires 52.3% less upgrades compared with the QKD solutions.

References

[1] M. Alshowkan, P. G. Evans, M. Starke, D. Earl, and N. A. Peters, "Authentication of smart grid communications using quantum key distribution," *Scientific Reports*, vol. 12, 12 2022.

[2] R. A. Mollin, *RSA and Public-Key Cryptography*. USA: CRC Press, Inc., 2002.

[3] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-hellman key distribution extended to group communication," in *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, 1996, pp. 31–37.

[4] J. Suo, L. Wang, S. Yang, W. Zheng, and J. Zhang, "Quantum algorithms for typical hard problems: a perspective of cryptanalysis," *Quantum Information Processing*, vol. 19, pp. 1–26, 2020.

[5] C. Easttom, "Quantum computing and cryptography," in *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. Springer, 2022, pp. 397–407.

[6] Z. Tang, P. Zhang, and W. O. Krawec, "A quantum leap in microgrids security: The prospects of quantum-secure microgrids," *IEEE Electrification Magazine*, vol. 9, no. 1, pp. 66–73, 2021.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557*, 2020.

[8] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical review letters*, vol. 68, no. 21, p. 3121, 1992.

[9] S. Mutreja and W. O. Krawec, "Improved semi-quantum key distribution with two almost-classical users," *Quantum Information Processing*, vol. 21, no. 9, p. 319, 2022.

[10] M. Boyer, M. Katz, R. Liss, and T. Mor, "Experimentally feasible protocol for semiquantum key distribution," *Physical Review A*, vol. 96, 12 2017.

[11] W. O. Krawec, T. Mor *et al.*, "Security proof against collective attacks for an experimentally feasible semiquantum key distribution protocol," *IEEE Transactions on Quantum Engineering*, 2023.

[12] M. Gado, M. Ismail, and W. O. Krawec, "Upgrading the cyber layer of power systems to support semi-quantum key distribution," in *2024 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2024, pp. 1–5.

[13] AZO Quantum. How the 'Mozi' Satellite Grants Quantum Security From Space. [Online]. Available: www.azoquantum.com/Article.aspx?ArticleID=308

[14] M. Soetan, Z. Mao, and K. Davis, "Statistics for building synthetic power system cyber models." Institute of Electrical and Electronics Engineers Inc., 4 2021.

[15] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, 2015.

[16] S. Katoch, S. S. Chauhan, and V. Kumar, "A review on genetic algorithm: past, present, and future," *Multimedia Tools and Applications*, vol. 80, pp. 8091–8126, 2 2021.

[17] C. Qian, C. Bian, W. Jiang, and K. Tang, "Running time analysis of the (1 + 1)-ea for onemax and leadingones under bit-wise noise," *Algorithmica*, vol. 81, pp. 749–795, 2 2019.

[18] Manitoba Hydro International. (2018) PSCAD TM IEEE 39 Bus System. [Online]. Available: https://www.pscad.com/knowledge-base/article/28

[19] Manitoba Hydro International. IEEE 14 Bus System. [Online]. Available: https://www.pscad.com/knowledge-base/article/26

[20] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure microgrid," *IEEE Transactions on Power Systems*, vol. 36, pp. 1250–1263, 3 2021.