*Proceedings of the International Conference on Industrial Engineering and Operations Management*

Publisher: IEOM Society International, USA DOI: 10.46254/GC03.20260309
Published: February 2, 2026

# Vulnerability-based Optimal Selection of Quantum-secured Links for Resilient and Energy-Efficient Smart Grids

**Norah Elkherayef, Rahaf Alharbi, Jori Albaqmi, Lubna Alsaeed and Yazan Allawi**
Department of Electrical Engineering, College of Engineering
Princess Nourah bint Abdulrahman University
P.O. Box 84428, Riyadh 11671, Saudi Arabia
NorahElkherayef@gmail.com, rahaf.abdulhadi.al@gmail.com, JoriAlbaqmi@gmail.com, Eng.lubnaalsaeed@gmail.com, ymallawi@pnu.edu.sa

**Alawi Alsaggaf**
Department of Information & Computer Science
IRC-Advanced Quantum Computing
King Fahd University of Petroleum and Minerals
Dhahran, Eastern Province 31261, Saudi Arabia
alawi@kfupm.edu.sa

## Abstract

The rapid evolution of Smart Grids (SGs) has improved efficiency, reliability, and sustainability, but also exposed critical infrastructures to sophisticated cyber threats, particularly from emerging quantum computing capabilities. Cryptography is a fundamental tool for securing communication networks, ensuring confidentiality, integrity, and authenticity of data transmission. Public Key Cryptography (PKC), a widely used conventional cryptographic scheme forming the backbone of SG security, facing risks from quantum attacks, necessitating Post-Quantum Cryptography (PQC) adoption. However, resource constraints in SG devices limit broad PQC deployment due to high computational and energy demands. This paper introduces a vulnerability-based optimization framework for selective deployment of quantum-secured links under budget and energy constraint. The proposed method prioritizes communications links based on novel composite vulnerability metrics, ensuring that cryptographic resources are allocated where they provide maximum security impact. By integrating security, cost-efficiency, and energy considerations into the selection strategy, the framework enhances resilience against both classical and quantum-enabled adversaries. The Most Vulnerable First (MVF) approach ranks and secures critical links, maximizing security impact while preserving energy efficiency. Simulation results demonstrate that the proposed approach achieves up to 97.8% security impact against coordinated group attacks, significantly outperforming conventional single-metric, random, or sequential augmentation approaches, while maintaining sustainable operational efficiency. This approach balances enhanced cyber resilience with sustainable operational costs, offering a practical, scalable path toward quantum-secured SG communications.

## Keywords
Cost efficiency, Energy preservation, Optimization, Quantum-safe cryptography, Vulnerability assessment

## 1. Introduction
The transition from conventional power systems to Smart Grids (SGs) represents a cornerstone of modern energy infrastructure. SGs integrate advanced communication networks, real-time monitoring, and automated control into traditional electricity generation and distribution systems, thereby enabling bi-directional power and data flows. These

capabilities enhance grid efficiency, reliability, and sustainability, while also supporting emerging technologies such as distributed renewable energy resources, electric vehicles, and demand response programs (Alonso et al. 2021), (Aloul et al. 2012). Consequently, SGs have become essential for optimizing energy management as well as achieving global sustainability and decarbonization goals.

However, this increasing reliance on digital connectivity also magnifies the cyber-physical attack threats to SGs (Gaspar et al. 2023). A SG comprises four interconnected subsystems: generation, transmission, distribution, and control centers. These subsystems are supported by multi-layered architecture, as shown in Fig. 1, which integrates:

- Physical layer: the traditional power system infrastructure responsible for electricity generation, transmission, and distribution.
- Cyber layer: communication and control mechanisms, including smart meters, control centers, and wired/wireless networks.
- Integration layer: the coordination interface that links cyber and physical domains, enabling real-time monitoring, automation, and decision-making (Figure 1).

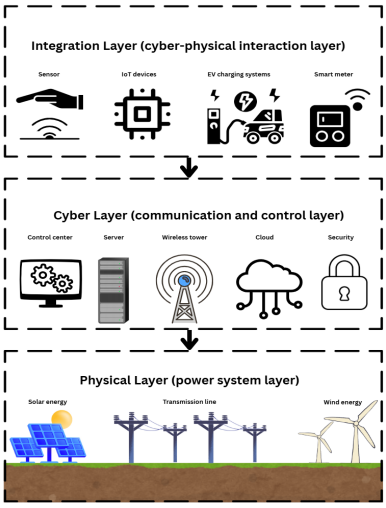


Figure 1. Smart Grid's layered communication architecture.

This layered structure enhances operational efficiency but also exposes SGs to a wide spectrum of cyber threats. Malicious actors may exploit vulnerabilities in communication channels, control centers, or end-user devices to launch attacks such as false data injection, Denial-of-Service (DoS), or Man-in-the-Middle (MITM) (Paul et al. 2024). These attacks can manipulate power flows, cause large-scale outages, compromise sensitive operational data, and inflict severe financial losses. The interconnected and distributed nature of SG infrastructures amplifies the risks, as disruptions in one subsystem can propagate rapidly across others, potentially resulting in cascading failures (Islam et al. 2023).

Adding to this complexity is the looming threat of quantum computing. Breakthroughs in quantum algorithms, particularly Shor's algorithm (Ugwuishiwu et Al. 2020) pose a direct challenge to Public-Key Cryptography (PKC) schemes that currently underpin secure communications. As a result, today's widely used PKC algorithms, including RSA and ECC (Mahto and Yadav 2017), may become vulnerable to efficient decryption by quantum adversaries. To address these risks, two major security paradigms have emerged; Post-Quantum Cryptography (PQC) focuses on creating encryption schemes by building cryptographic solutions resilient against both classical and quantum attacks, and Quantum Key Distribution (QKD), which leverages the physical principles of quantum mechanics to provide information-theoretic security. While both approaches offer promising defenses, their adoption in SGs is constrained by implementation costs, computational overhead, and significant energy demands. These limitations are particularly critical in resource-constrained devices such as smart meters, sensors, and embedded controllers, which form the backbone of SG communications.

Recent studies have explored the vulnerabilities of SGs from various perspectives, including multilayer network

analysis (Hossain and Peng 2020), (Ullah et al. 2022), cryptographic innovations (Li et al. 2023), and resilience modeling (Allawi et al. 2015). While these works contribute valuable insights, they often neglect the interplay between link-level vulnerability, cost constraints, and energy efficiency in determining where and how Quantum-Safe Cryptography (QSC), such as PQC or QKD, should be applied. Furthermore, most existing models assume single-attack scenarios, whereas real-world adversaries may act in coordinated groups targeting multiple subsystems simultaneously, amplifying the risks of widespread disruption.

In such real scenarios, deploying quantum protections indiscriminately may waste resources on low-impact links while leaving high-risk ones exposed. To ensure resilient and sustainable operations, a selective, vulnerability-based approach is required.

Figure 2 illustrates such scenario of normally operating COST239 SG topology (Jin et al. 2018), (a) gets under a group attack in (b), simultaneously targeting multiple critical nodes and links in the grid. The attackers coordinate their efforts within a defined geographical radius to maximize disruption. Within the highlighted circle are the links that are most affected. This example shows how serious and complicated cyberattacks can be when they strike the SG infrastructure and it points out the need for quantum modules that support vulnerable links.

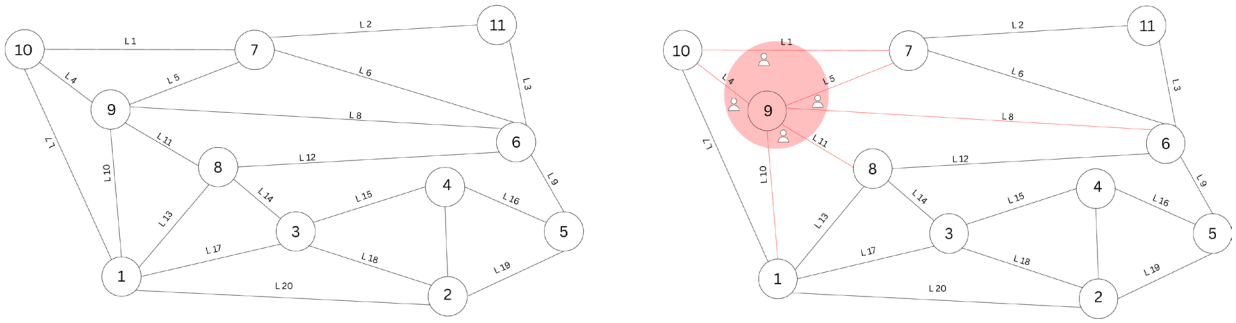


Figure 2. COST239 SG topology under: (a) normal operation, (b) coordinated group attack (red circle), simultaneously targeting several links (red lines).

In response to these challenges, this paper proposes a vulnerability-based optimization framework for selective deployment of quantum-secured links within SG communications networks. The framework introduces a composite vulnerability metric based on traffic, link length, and vertex connectivity to rank communication links according to their susceptibility and potential impact.

Building on this metric, an optimization strategy selectively deploys PQC modules under strict budgetary, which consequently preserves energy consumption via prioritizing links that yield the greatest resilience gains. By integrating security, cost-efficiency, and energy-awareness, the proposed approach provides a scalable pathway to safeguard SGs against both classical and quantum-enabled threats.

### 1.1 Objectives

The deployment of PQC is growing rapidly in smart grid security. However, there have been relatively few works on the selection of quantum-secured links in the network, which plays an important role in reducing energy consumption and adhering to budget constraints. This paper aims to propose a vulnerability-based matrix for the optimal selection of quantum-secured SG communication links and compare the results with other commonly used frameworks, such as sequential and random selection, which sometimes tend to be neither energy efficient nor cost-effective. The results will validate the constructive method via software simulation over different selection scenarios.

## 2. Literature Review

Research on SG security has evolved significantly over the past decade, addressing both the cyber and physical dimensions of this critical infrastructure. Early studies primarily investigated vulnerabilities through multilayer network models, showing how interdependencies between physical and cyber subsystems can propagate failures across the grid (Alonso et al. 2021), (Islam et al. 2023). These works highlight the structural fragility of SGs but stop

short of proposing operational countermeasures or cryptographic safeguards against advanced adversaries. Other research efforts have focused on cataloging attack vectors, which can degrade reliability, disrupt operations, and compromise sensitive data (Paul et al. 2024), (Nguyen et al. 2025). Surveys, such as the work in (Hossain and Peng 2020) and (Bi et al. 2025), stress the importance of integrated security frameworks, yet they tend to emphasize physical protection mechanisms while providing limited insights into cryptographic enhancements tailored for SG communication networks.

With the emergence of quantum computing, attention has shifted toward cryptographic resilience. Quantum algorithms such as Shor's have been shown to undermine widely deployed PKC systems, raising concerns about the long-term confidentiality of SG communications (Ugwuishiwu et al. 2020), (Xiong et al. 2025). In response, two key directions have been pursued; namely, PQC and QKD. PQC introduces a new mathematical structure robust schemes designed to resist quantum adversaries, while QKD leverages quantum mechanical principles to achieve unconditional security. Notably, the authors in (Ullah et al. 2022) investigated quantum computing applications in SGs, highlighting both the potential benefits and the inadequacy of conventional cryptography. Similarly, the work in (Li et al. 2023) emphasized PQC as a promising alternative but acknowledged challenges in computational overhead, latency, and energy use.

Despite these advances, several research gaps remain. First, existing studies rarely account for the energy efficiency and resource constraints of SG devices, which are critical for sustainable large-scale deployment (Jabłoński and Dylewski 2025). Second, most frameworks consider uniform or system-wide cryptographic upgrades, neglecting the fact that not all links contribute equally to resilience. Finally, many models assume single adversaries, overlooking coordinated attacks by multiple actors targeting diverse parts of the grid simultaneously.

To address these shortcomings, our work introduces a vulnerability-based optimization framework that integrates structural vulnerability metrics with cost and energy considerations. By selectively deploying quantum-secured protections on the most critical links, the proposed approach bridges the gap between theoretical quantum security and practical SG operation, offering a scalable and resilient solution tailored to real-world constraints.

## 3. Methodology

To address the evolving security demands of SGs under quantum-era threats, we propose a vulnerability-based optimization framework that strategically deploys PQC modules across communication links. The model integrates three key components: (*i*) a novel vulnerability metric to quantify the risk associated with each link, (*ii*) a link-selection strategy that prioritizes quantum-augmentation of high-risk links for a given budget constraint, and (*iii*) a comprehensive performance analysis capturing both cost and energy efficiency. By focusing on these elements, the proposed approach aims to maximize Packet Delivery Ratio (PDR) that will provide an overall grid resilience while ensuring highly secure, energy-efficient, and cost-effective framework.

### 3.1 Vulnerability Metric

The first step in the proposed framework is the evaluation of link-level vulnerabilities across the SG communication topology. Rather than assessing devices and links in isolation, the grid is modeled as a multilayer cyber-physical network, and a scanning method is used to evaluate PDR and highlight the links whose failure would cause significant degradation (Allawi et al. 2015). To capture the risk of compromising a link $l$ connecting nodes $i$ and $j$, a composite vulnerability score is defined based on the following four parameters:

- Traffic load ($T_l$): the volume of data traffic transmitted across link $l$, indicating its operational significance.
- Link length ($L_l$): the physical distance of link $l$, which influences both susceptibility to interception and latency.
- Vertex connectivity ($\Delta\kappa_l$): the structural importance of link $l$ in maintaining network connectivity, which is calculated as the average number of links connected to both nodes $i$ and $j$, such that $\Delta\kappa_l = \frac{(\kappa_i + \kappa_j)}{2}$.
- Hit link ($h_l$): A Boolean parameter for the probability of the group attack $A(r)$ of radius $r$ to intersect with a link $l$, such that

$$h_l = \begin{cases} 1, & l \cap A(r) \\ 0, & otherwise \end{cases} \quad (1)$$

Accordingly, the vulnerability metric of each link $l$ is expressed as:

$$V_l = h_l(\ \alpha\, T_l + \beta\, L_l + \ \delta\, \Delta\kappa_l) \qquad (2)$$

where $\alpha$, $\beta$ and $\delta$ are weighting factors that balance the contributions of the three parameters $T_l$, $L_l$, and $\Delta\kappa_l$ respectively, after being normalized. Links with higher $V_l$ values represent critical points of failure whose compromise would cause the most severe operational degradation.

### 3.2 Quantum-secured Links Selection

Once vulnerability scores are computed based on (2), the second stage determines which links should be augmented with PQC modules. Deploying PQC uniformly across all links is infeasible due to high computational and energy demands. Instead, the proposed approach selects a subset of links that optimally balances security benefits against deployment constraints. Thus, links are ranked in descending order of $V_l$. Then, a fixed budget constraint is introduced, allowing only a proportion total links to be upgraded (e.g., 40% in baseline simulations). The top-ranked links are sequentially augmented until the budget is exhausted. We refer to our proposed approach as the Most Vulnerable First (MVF) approach, which contrasts with sequential or random selection strategies. By focusing augmentation on the most critical communication paths, it strengthens grid resilience while conserving resources.

### 3.3 Cost and Energy Efficiency Model

Deploying PQC within SG communications networks offers a promising path to securing infrastructure against future quantum adversaries. However, PQC algorithms typically incur greater computational complexity and larger key sizes compared to classical cryptographic methods, resulting in increased energy consumption and processing delays, significant considerations for SG devices that often operate under strict resource constraints.

To address this challenge, our framework emphasizes selective deployment of PQC protections on communications links evaluated as most vulnerable and critical. By focusing cryptographic enhancements where they provide the greatest security return, the overall energy consumption and computational burden on the grid are minimized. This strategy allows devices with limited processing power and battery life to maintain operational efficiency without sacrificing security. Accordingly, we model the total energy consumption $E_{\text{total}}$ after PQC deployment as:

$$E_{\text{total}} = \sum_{l \in Q}(E_{\text{base}} + \Delta E_l) \qquad (3)$$

where $Q$ is the set of quantum-secured links, $E_{\text{base}}$ is the baseline communication energy per link (e.g., $E_{\text{base}} = 1$ ), and $\Delta E_l$ is the incremental energy overhead from PQC processing on both ends of augmented link $l$.

Similarly, cost factors influence deployment decisions. The integration of PQC may require hardware upgrades or software optimizations, thus incurring capital and operational expenditures. However, compared to system-wide deployment, our vulnerability-based selection optimizes budget allocation by limiting PQC deployment to critical links, thereby improving cost-effectiveness. we model the deployment cost $C_{\text{total}}$ as:

$$C_{\text{total}} = \sum_{l \in Q}(C_{\text{base}} + \Delta C_l) \qquad (4)$$

This balanced approach leverages recent advances in lightweight PQC algorithms tailored for constrained environments, ensuring that SG operators can achieve quantum-based security while managing energy consumption and economic impact, which are essential for sustainable and scalable grid protection in the quantum era.

## 4. Results and Discussion

### 4.1 Graphical Results

A set of comparative simulations were performed to evaluate the effectiveness of different PQC augmentation strategies in an SG topology under various coordinated group attack scenarios. Four representative augmentation strategies were examined: Most Vulnerable First (MVF), Sequential (SEQ), Random (RND), and Least Vulnerable First (LVF). The test network consists of 9 nodes and 11 links, with link properties and traffic loads set as described in earlier sections. Attacks were simulated by the group attack's radius $r$ and augmentation budget $\gamma$ parameters, focusing on the effect on PDR as a measure of security as well as $E_{\text{total}}$ for the energy efficiency.

Figure 3(a) visualizes the MVF strategy where links are ranked and augmented based on our proposed composite vulnerability metric integrating link length, traffic, and connectivity. Here, the most critical links are protected first, creating a strong, optimal backbone for data flow even under group attacks. Notably, augmented links are distributed to intercept the most likely attack paths, ensuring that even if attackers compromise peripheral links, communications remain robust for essential routes.

The SEQ augmentation strategy in Fig. 3(b) applies PQC to links in a fixed, topological order without regard for vulnerability or criticality. The Figure 3 shows less strategic distribution of secured links, with some key attack-prone paths left less protected. This can result in network partitions or bottlenecks if the attack was coordinated against unsecured, central links.

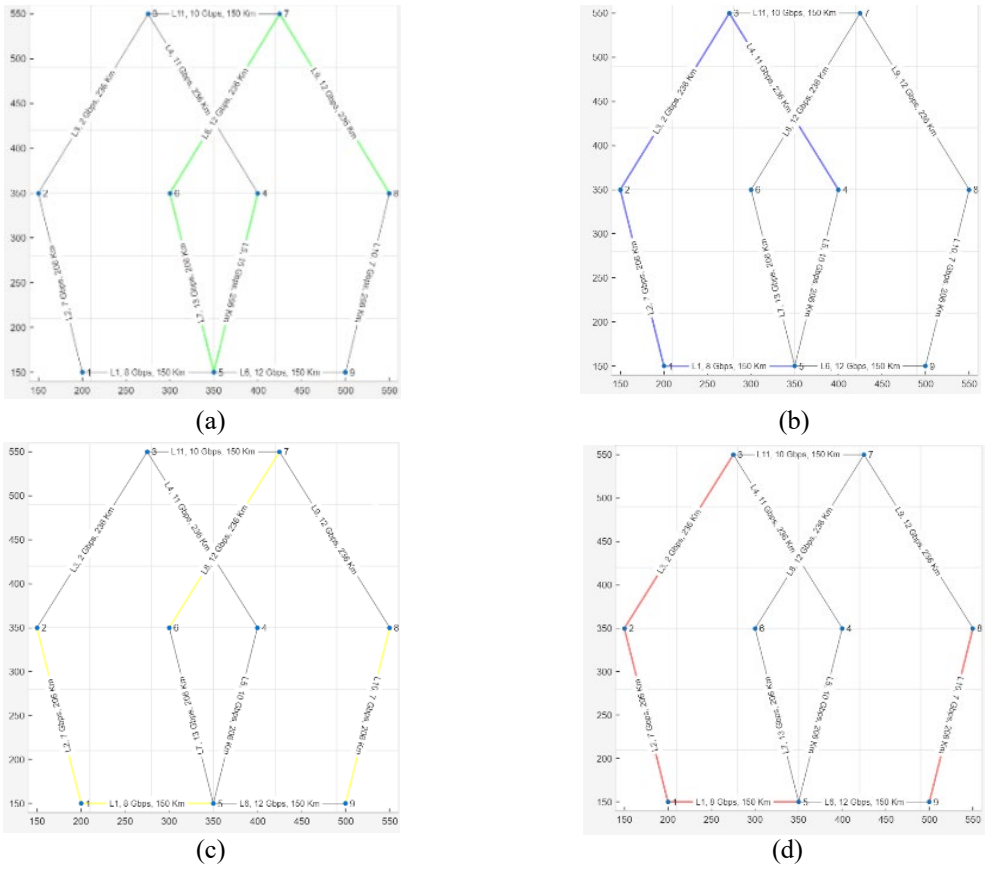


Figure 3. Simulation topology of 9 nodes and 11 links, with results of quantum-secured links for a budget $\gamma = 40\%$, utilizing: (a) the proposed MVF scenario, (b) SEQ, (c) RND, and (d) LVF scenario.

RND augmentation selects links to secure in an ad hoc manner. The corresponding Fig. 3(c) demonstrates the unpredictability of coverage, where some central and high-risk links may remain unprotected, and less important links gain security upgrades unnecessarily. This yields inconsistent grid resilience, and, on average, lower PDR compared to targeted approaches.

The LVF strategy, illustrated in Fig. 3(d), prioritizes augmenting links viewed as least vulnerable according to the composite metric. This approach results in securing peripheral or less critical links first while leaving key backbone links exposed for longer durations. The figure shows this distribution, where augmented links fail to effectively intercept probable attack paths, leading to faster network degradation and significantly lower PDR under coordinated multi-link attacks compared to MVF and even some random strategies.

Figure 4 presents a comparative assessment of all four augmentation strategies under varying attack radii. The MVF consistently outperforms the benchmark approaches, achieving the highest PDR across all scenarios. By prioritizing critical backbone links, MVF prevents rapid network partitioning even as the attack radius grows, under which more links are simultaneously targeted. Even when only 40% of links are augmented, MVF achieves up to 97.8% PDR effectiveness, balancing resilience with cost and energy efficiency. On the other hand, both the SEQ and RND

approaches initially offer moderate resilience but fail to match the targeted efficiency of MVF under larger radii because critical links remain exposed. Their PDR curves decline more sharply than MVF's, resulting in a widening performance gap that becomes ten times larger at a radius of 80 km than at 20 km. Among all, the LVF augmentation approach consistently yields the poorest performance, rapidly driving down PDR as the attack radius increases, demonstrating the risks of misaligned security allocation, especially when considering the compounding effect of coordinated attacks under which securing the most vulnerable links becomes essential.

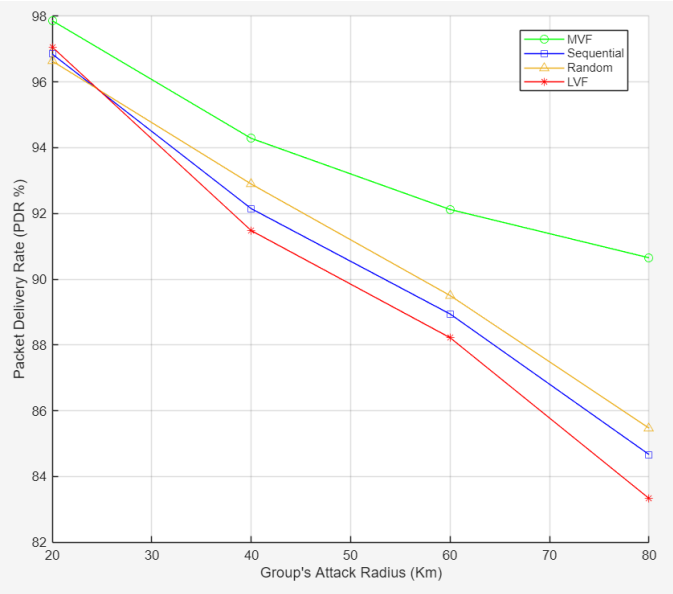


Figure 4. PDR results with $\gamma = 40\%$ of proposed MVF against sequential, random and LVF approaches, post a group attack of various radii.

## 4.2 Numerical Results

To quantify the energy efficiency ($E_e$) of selective PQC deployment as in (5), we first computed the total incremental PQC energy $E_{\text{total}}$ based on (3) for each augmentation strategy, where $\Delta E_l$ is modeled proportional to the normalized vulnerability score $\hat{V}_l$ based on (6) and as given in Table 1, such that $\Delta E_l = \eta\, \hat{V}_l$ with $\eta = 0.5\, J$.

$$E_e = \frac{\text{PDR}}{E_{\text{total}}} \tag{5}$$

$$\hat{V}_l = \frac{V_l - V_{min}}{V_{max} - V_{min}} \tag{6}$$

Table 1. Ranked links with vulnerability scores, normalized vulnerability, and corresponding PQC energy overheads

| $\boldsymbol{l}$ | $V_l$ | $\hat{V}_l$ | $\Delta \boldsymbol{E_l}$ | $\boldsymbol{E_{\text{base}} + \Delta E_l}$ |
|---|---|---|---|---|
| $l_7$ | 2.8741 | 1.0000 | 0.5000 | 1.5000 |
| $l_8$ | 2.6731 | 0.7928 | 0.3964 | 1.3964 |
| $l_9$ | 2.6731 | 0.7928 | 0.3964 | 1.3964 |
| $l_5$ | 2.6433 | 0.7621 | 0.3811 | 1.3811 |
| $l_4$ | 2.5962 | 0.7136 | 0.3568 | 1.3568 |
| $l_6$ | 2.5591 | 0.6754 | 0.3377 | 1.3377 |
| $l_{11}$ | 2.4052 | 0.5167 | 0.2584 | 1.2584 |
| $l_1$ | 2.2514 | 0.3582 | 0.1791 | 1.1791 |
| $l_2$ | 1.9126 | 0.0091 | 0.0045 | 1.0045 |
| $l_{10}$ | 1.9126 | 0.0091 | 0.0045 | 1.0045 |
| $l_3$ | 1.9038 | 0.0000 | 0.0000 | 1.0000 |

Table 2. Performance comparison of link augmentation strategies in SG security

| ***Method*** | ***Links Selected*** | ***PDR (%)*** | $E_{Total}$ ***(J)*** | $E_e$ ***(J)*** |
|---|---|---|---|---|
| ***MVF*** | $l_7, l_8, l_9, l_5$ | 97.8 | 5.67 | 0.172 |
| ***SEQ*** | $l_1, l_2, l_3, l_4$ | 96.8 | 4.54 | 0.213 |
| ***RND*** | $l_1, l_2, l_8, l_{10}$ | 96.6 | 4.58 | 0.210 |
| ***LVF*** | $l_3, l_{10}, l_2, l_1$ | 97.0 | 4.18 | 0.230 |

With an augmentation budget $\gamma$ of 40%, Table 2 shows the specific links selected by each deployment strategy. MVF upgrades the four links with the highest vulnerability ($l_7, l_8, l_9, l_5$), compared with the SEQ, which selects the links ($l_1, l_2, l_3, l_4$). RND upgrades a randomly chosen set of links ($l_1, l_2, l_8, l_{10}$), and the LVF focuses on upgrading links with the lowest vulnerability scores.

Thus, MVF delivers the highest absolute resilience with a PDR of 97.8% and an energy efficiency that is on par with SEQ and LVF. This means that MVF trades moderately higher PQC energy for substantially better resilience, which is a tradeoff that can be acceptable or even required in security-critical grid deployments.

## 6. Conclusion

This paper presented a vulnerability-based optimization framework for selective Post-Quantum Cryptography (PQC) deployment in Smart Grid (SG) communications. By combining traffic load, link length, and vertex connectivity into a composite vulnerability metric, the framework identifies and secures the most critical links under a given budget constraint. Simulation results showed that the proposed Most Vulnerable First (MVF) strategy significantly outperforms sequential (SEQ), random (RND), and Least Vulnerable First (LVF) approaches, achieving up to 97.8% resilience even with only 40% of quantum-secured links, and maintaining superior performance as coordinated attack radii increase, which demonstrates the framework's ability scale effectively for large network topologies. Although MVF incurs relatively higher energy costs by securing high-traffic links, the marginal energy per resilience gain remains favorable, making it a practical solution for sustainable SG security. Future work will focus on extending the model to large real-world dynamic traffic conditions, integrating heterogeneous PQC schemes, and validating performance on experimental testbeds under diverse attack scenarios.

## References

Allawi, Yazan M., Dujeong Lee, and June-Koo Kevin Rhee, A wireless link-up augmentation design for disaster-resilient optical networks, *Journal of Lightwave Technology*, vol. 33, no. 17, 2015.

Alonso, Monica, Jaime Turanzas, Hortensia Amaris, and Angel T. Ledo, Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks, *Sensors*, vol. 21, no. 17, 2021.

Aloul, Fadi, A. R. Al-Ali, Rami Al-Dalky, Mamoun Al-Mardini, and Wassim El-Hajj, Smart grid security: Threats, vulnerabilities and solutions, *International Journal of Smart Grid and Clean Energy*, vol. 1, no. 1, 2012.

Bi, S., Yuan, X., Hu, S., Li, K., Ni, W., Hossain, E., and Wang, X., Resilience and Failure Analysis in Next-Generation Communication Networks: A Contemporary Survey, *IEEE Transactions on Network Science and Engineering*, 2025.

Bibi, Hafsa, Mehran Abolhasan, Justin Lipman, Mahrokh Abdollahi, and Wei Ni, A comprehensive survey on privacy-preserving technologies for Smart Grids, *Computers and Electrical Engineering*, vol. 124, 2025.

Gaspar, José, Tiago Cruz, Chan-Tong Lam, and Paulo Simões, Smart substation communications and cybersecurity: A comprehensive survey, *IEEE communications surveys & tutorials*, vol. 25, no. 4, 2023.

Hossain, Md Musabbir, and Chen Peng, Cyber–physical security for on-going smart grid initiatives: a survey, *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 3, 2020.

Islam, Md Zahidul, Yuzhang Lin, Vinod M. Vokkarane, and Venkatesh Venkataramanan, Cyber-physical cascading failure and resilience of power grid: A comprehensive review, *Frontiers in Energy Research*, vol. 11, 2023.

Jabłoński, Janusz, and Robert Dylewski, Quantum-Resistant Cryptography for Smart Metering in Smart Grid Systems, *Energies*, vol. 18, no. 5, 2025.

Jin, G. X., J. S. Li, J. Lu, W. W. Lin, and P. Cai, Two-layer QoS-guaranteed backbone communication network modeling for power protection services, *In IOP Conference Series: Earth and Environmental Science*, vol. 188, no. 1, 2018.

Li, Silong, Yuxiang Chen, Lin Chen, Jing Liao, Chanchan Kuang, Kuanching Li, Wei Liang, and Naixue Xiong, Post-quantum security: Opportunities and challenges, *Sensors*, vol. 23, no. 21, 2023.

Mahto, Dindayal, and Dilip Kumar Yadav, RSA and ECC: A comparative analysis, *International journal of applied engineering research*, vol. 12, no. 19, 2017.

Nguyen LH, Nguyen VL, Hwang RH, Kuo JJ, Chen YW, Huang CC, and Pan PI, Towards secured smart grid 2.0: exploring security threats, protection models, and challenges, *IEEE Communications Surveys & Tutorials*, vol. 27, no. 4, 2025.

Paul, Bishowjit, Auvizit Sarker, Sarafat Hussain Abhi, Sajal Kumar Das, Md Firoj Ali, Md Manirul Islam, Md Robiul Islam, Md Manirul Myeen, Sumaya Ishrat Badal, Md Faisal Rahman Ahamed, and Md Hafiz, Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies, *Heliyon*, vol. 10, no. 19, 2024.

Ugwuishiwu, C. H., U. E. Orji, C. I. Ugwu, and C. N. Asogwa, An overview of quantum cryptography and shor's algorithm, *Int. J. Adv. Trends Comput. Sci. Eng*, vol. 9, no. 5, 2020.

Ullah, Md Habib, Rozhin Eskandarpour, Honghao Zheng, and Amin Khodaei, Quantum computing for smart grid applications, *IET Generation, Transmission & Distribution*, vol. 16, no. 21, 2022.

Xiong, Jian, Lu Shen, Yan Liu, and Xiaofen Fang, Enhancing IoT security in smart grids with quantum-resistant hybrid encryption, *Scientific Reports*, vol. 15, no. 1, 2025.

## Biographies

**Norah Elkherayef** is an undergraduate student majoring in Electrical and Communications Engineering at Princess Nourah bint Abdulrahman University (PNU).

**Rahaf Alharbi** is an undergraduate student majoring in Electrical and Communications Engineering at Princess Nourah bint Abdulrahman University (PNU).

**Jori Albaqmi** is an undergraduate student majoring in Electrical and Communications Engineering at Princess Nourah bint Abdulrahman University (PNU).

**Lubna Alsaeed** is an undergraduate student majoring in Electrical and Communications Engineering at Princess Nourah bint Abdulrahman University (PNU).

**Yazan M. Allawi** is currently an Assistant Professor with the Electrical Engineering Department at Princess Nourah bint Abdulrahman University (PNU), Saudi Arabia. Prior to his current position, he served as the head of innovation and entrepreneurship department at the Scientific Research and Innovation Support Fund (SRISF), Ministry of Higher Education and Scientific Research, Jordan, and manager of the Innovative Technology R&D Center at HFR, Inc. for Mobile Internet, South. Early on his career, he made contributions in the area of integrated optical-wireless communications networks including the design and deployment of 5G-ready CWDM-based fronthaul solution for CPRI transport (Nokia's 1830 VWM), and the realization of the first commercially viable OFDMA-PON system. His current research interests include resource allocation and optimization techniques, vulnerability analysis, disaster-resiliency & preparedness, AI/ML algorithms, radio access networks, fronthaul/backhaul integration, 5G and beyond networks.

**Alawi Alsaggaf** holds a Ph.D. in Computer studies (Cryptography) and an M.Sc. in Mathematics. He is currently a faculty member in the Department of Information and Computer Science at King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia. His teaching and research focus on post-quantum cryptography, quantum computing, and information security. His work has advanced the fields of quantum-resistant authentication, biometric data protection, and secure IoT systems, resulting in a U.S. patent and several high-impact publications. He also leads research projects funded by KFUPM and external clients. At KFUPM, he has been recognized with multiple honors, including the Excellence in Teaching Awards (2020, 2025) and the Instructional Technology Award (2019).