



ARTICLE

Secure Multi-Zone Optimization of Demand Response in 5G-Enabled Smart Grids with Trust-Aware Communication

Sajjad Rabbani¹, Rao Muhammad Asif¹, Mai Alduailij², Adnan Yousaf^{1,*}, Upinder Kaur³,
Salil Bharany⁴ and Ateeq Ur Rehman^{5,*}

¹Department of Electrical Engineering, Superior University, Lahore, Pakistan

²Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, Saudi Arabia

³Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India

⁴Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, India

⁵School of Computing, Gachon University, Seongnam-si, Republic of Korea

*Corresponding Authors: Adnan Yousaf. Email: adnan.yousaf@superior.edu.pk; Ateeq Ur Rehman. Email: 202411144@gachon.ac.kr

Received: 01 June 2026; Accepted: 03 August 2026; Published: 22 October 2026

ABSTRACT: The implementation of 5G communication in smart grids facilitates real-time demand response (DR) management, but at the same time creates several problems concerning cyber security and communication reliability, as well as user trust. Currently, DR methods mainly aim at energy optimization and neglect the combined effect of communication performance, cyber threats, and trust-aware participation. In this work, a secure multi-zone optimization model for a 5G-enabled smart grid is proposed that jointly optimizes communication efficiency, cybersecurity mechanisms and DR control within a single framework. The system is divided into five operational zones: Utility layer, Secure 5G core and edge, Access and gateway layer, Local control layer, Consumer layer. The communication- and security-aware optimization formulation is defined to optimize the latency, packet error rate, security overhead and DR shortfall, while maximizing reliability, fairness, resilience and secure user participation. Besides, a trust-aware iterative optimization algorithm is proposed to adaptively align the authentication, intrusion detection, clustering, secure communication and DR activation under different network conditions and attacks. The simulation results illustrate that the proposed approach significantly enhances the performance of the system, with low latency (≈ 8 ms), a low packet error rate (≈ 0.03), high signal quality, and high DR participation in comparison with the benchmark approaches. The framework is also capable of supporting effective operation under cyberattack scenarios and in the presence of different levels of trust, making it a very effective framework for secure, reliable and scalable DR management in next-generation smart grids.

KEYWORDS: Demand response optimization; cybersecurity-aware optimization; trust-aware communication; cyber-physical energy systems

1 Introduction

Smart grids increasingly integrate intelligent communication, demand response (DR), cybersecurity, and consumer participation within a cyber-physical energy system. This integration improves resilience, sustainability, and efficient power use, while distributed and coordinated DR supports reliable operation under uncertain demand and consumer information [1]. However, developing a unified framework that simultaneously addresses communication performance, cybersecurity, and DR optimization remains a

major challenge [2]. Real-time DR depends on reliable data exchange among utilities, aggregators, smart meters, distributed energy resources, and consumers. Communication delay, packet loss, cyberattacks, and unreliable control signals can therefore directly affect DR execution. 5G is a promising enabling technology because it provides low latency, high data rates, dense device connectivity, and improved reliability for real-time monitoring and control [3]. Beyond-5G power management, energy-spectral efficiency optimization, and graph-neural-network-based intrusion detection further demonstrate the potential of intelligent communication and security mechanisms in connected cyber-physical systems [4,5]. Existing DR studies have used contract theory, stochastic optimization, and game-theoretic methods to improve user participation, manage uncertainty, balance demand, and reduce peak load [6]. Nevertheless, many models emphasize energy management while assuming ideal communication conditions. DR may be congested, lose packets, suffer a delay, or fail to verify in a 5G smart grid. False-data injection, denial-of-service, spoofing, replay, and control-signal manipulation are examples of cyber threats that can also adversely affect operational reliability, consumer trust, and energy-management decision-making [7–9]. Machine-learning-based intrusion detection has the ability to detect unusual activity, but in most cases, it is not integrated with DR optimization. More recently, advanced data-driven attacks were studied. Wang et al. [10] proposed a particle-swarm-optimization-based attention temporal graph convolutional network to detect dummy data injection attacks by modelling the spatial and temporal relationships in measurements of power systems. These methods help detect attacks, but they aren't directly linked to detecting the severity of an attack, evolving trust, communication delay and activation of secure DR. This leaves a cybersecurity monitoring gap in the energy control environment. Communication issues like packet loss, jamming and transmission delay and unstable connectivity can cause the DR commands not to reach the consumer and control devices on time [11,12]. Because of this, the load reduction that is expected may not be realized. Blockchain, federated learning, and privacy preserving technologies can be used to enhance data integrity, user trust, secure participation, and transparency of transactions [13,14]. However, these mechanisms can also introduce extra processing (processing overhead), authentication, storage and signalling overhead. In addition, a survey of residential DR studies reveals that smart meters, local controllers, communication infrastructure, consumer willingness and reliable ICT systems are all required to enable effective participation [15]. Likewise, in terms of resource-allocation, the QoS- and fairness-aware methods enhance the bandwidth allocation, throughput, service quality and fairness among users, particularly under the heavy network load [16,17]. More recent research also shows that cyberattacks can directly impact DR decisions, consumer involvement, and provided load reduction [18,19]. Accordingly, smart-grid resilience must be considered in the context of the joint consideration of communication performance, cyber security, trust, fairness, and physical energy response, not as individual factors.

To address these limitations, this study proposes a 5G-enabled, multi-zone, cybersecurity- and trust-aware DR optimization framework. Although its five-zone structure follows the general cloud-edge-gateway-end-user paradigm, its contribution is not the naming or division of the layers. The novelty lies in the cross-zone coupling of authentication delay, intrusion-detection delay, secure-signalling overhead, SINR, packet error rate, local verification, dynamic trust, cyberattack impact, and realized secure DR. The framework differs from conventional layered models in three ways. First, it accumulates communication and security delays across the secure 5G core/edge, access/gateway, and local-control zones and links them to DR effectiveness. Second, it makes user eligibility dependent on authentication, anomaly status, trust, communication reliability, and attack severity. Third, it connects cyberattack impact directly with physical DR realization, so that unreliable communication, low trust, or failed verification can reduce or prevent load activation. The proposed architecture should therefore be understood as a cross-layer optimization

framework rather than a renamed layered communication model. The key contributions of this work are listed as follows:

- Proposes a cross-layer, multi-zone optimization framework for a 5G-enabled smart grid that jointly optimizes communication efficiency, cybersecurity mechanisms, trust management, and DR control within a unified framework
- Enables communication-security-aware clustering, dynamic trust updating and attack-aware DR activation for enhanced secure participation and system resilience as load and threats mount.
- Analyzes the framework from communication, security, and DR perspectives, such as latency, PER, SINR, user rate, reliability, fairness, trust, DR response, shortfall, and resilience.
- Validates performance by 100 independent Monte Carlo runs, with the same simulation conditions for all the competing methods.
- Uses ablation-based benchmarks to measure the contribution of the dominant modules, and accepts some extra overhead in computing and coordination.
- Shows better integrated performance and practical scalability in different scenarios of network size, user density, cluster number, and attack situations.

The rest of this paper is organized as follows: [Section 2](#) introduces the system model of the proposed model. [Section 3](#) investigates iterative multi-zone cybersecurity-aware DR optimization under 5G. [Section 4](#) discusses the results and validates the model. [Section 5](#) presents the conclusions and suggests the future scope of the work.

2 Mathematical Model of the Proposed Multi-Zone Cybersecurity-Aware DR Framework

The framework proposed is a multi-zone cyber-physical DR framework where information, control, security verification and load response propagate through five zones: the utility control layer, the secure 5G core and edge layer, the 5G access and gateway layers, the local control layer, and the consumer/load layer. The model is developed as a communication-security-energy optimization problem.

2.1 Sets, Indices, and System Entities

Let $\mathcal{N} = \{1, 2, \dots, N\}$, denote the set of DR-enabled consumers or controllable load nodes, and $\mathcal{K} = \{1, 2, \dots, K\}$ denotes the set of communication clusters or service regions. The set of 5G base stations or small cells is taken as $\mathcal{B} = \{1, 2, \dots, B\}$, whereas $\mathcal{M} = \{1, 2, \dots, M\}$ is used for the set of directional antenna pairs. Meanwhile, $\mathcal{T} = \{1, 2, \dots, T\}$ denotes the set of discrete decision periods. Representation of the five system zones is considered by $\mathcal{Z} = \{1, 2, 3, 4, 5\}$, where $z = 1$ is the Utility Control Center, $z = 2$ is the Secure 5G Core and Edge Layer, $z = 3$ is the 5G Access and Gateway Layer, $z = 4$ is the Local Control Layer, and $z = 5$ is Consumers and Flexible Loads. In the end, $\mathcal{A} = \{1, 2, \dots, A\}$ denotes the set of cyberattack types, such as replay attacks, false data injection, delay attacks, spoofing, or denial-of-service.

2.2 Decision Variables

The binary variable $x_{ik}(t) \in \{0, 1\}$ equals 1 if user i is assigned to cluster k , and 0 otherwise. Similarly, $y_{ibm}(t) \in \{0, 1\}$ equals 1 if user i is served by base station b through antenna pair m , while $u_i(t) \in \{0, 1\}$ indicates DR activation. The variables $q_i(t) \in [0, 1]$, $s_i(t) \in [0, 1]$, and $\eta_i(t) \in \{0, 1\}$ denote participation probability, trust score, and security-verification success, respectively. Finally, $\psi_i(t) \in [0, 1]$ represents aggregate attack impact, and $\mu_k(t)$ denotes the centroid of cluster k .

2.3 Zone-Wise Mathematical Modelling

The proposed framework classifies the coverage area into five operational zones, representing the functional and architectural layers of the 5G-enabled smart grid, thereby enabling coordinated communication, cybersecurity, local control, and demand response management.

2.3.1 Zone I: Utility Control Centre Model

Zone I includes the system operator, DR aggregator, DR optimization engine, and cybersecurity dashboard. Let the required DR reduction at time t be $P^{req}(t)$ and let the realized secure DR be $\Delta P_{DR}(t)$. Then the DR shortfall is computed in Eq. (1). Therefore, the control centre computes a dispatch signal intensity ($\pi(t)$) which plays the role of DR incentive or dispatch weight. The control centre may enforce a dispatch consistency constraint, which is $0 \leq \pi(t) \leq \pi^{\max}$. The cybersecurity dashboard in Zone I aggregates global risk information. The system-wide cyber risk index is given in Eq. (2). Then the control center may restrict dispatch aggressiveness under high risk computed in Eq. (3).

$$\Delta P^{short}(t) = \max \{0, P^{req}(t) - \Delta P_{DR}(t)\} \quad (1)$$

$$\Gamma^{risk}(t) = \frac{1}{N} \sum_{i \in \mathcal{N}} \psi_i(t) \quad (2)$$

$$\pi(t) \leq \pi^{\max} (1 - \Gamma^{risk}(t)) \quad (3)$$

2.3.2 Zone II: Secure 5G Core and Edge Layer Model

Zone II contains the authentication server, MEC server, intrusion detection engine, and security orchestrator. The authentication delay for each user i , authentication overhead is modeled in Eq. (4), where τ_0^{auth} is the base authentication delay, $n_i^{cred}(t)$ is the number of credentials or tokens verified, $\ell_i^{sec}(t)$ is the security level. Intrusion detection latency is computed in Eq. (5), where $\chi_i^{traf}(t)$ is the traffic inspection complexity, $a_i(t)$ is the number of active attack signatures under evaluation, and the trust-score update. This zone continuously updates the trust score computed in Eq. (6), where ρ is the memory factor, $\mathbb{I}_i^{anom}(t) \in \{0, 1\}$ and indicates whether the security verification successfully detects anomalous behaviour.

$$\tau_i^{auth}(t) = \tau_0^{auth} + v_1 n_i^{cred}(t) + v_2 \ell_i^{sec}(t) \quad (4)$$

$$\tau_i^{det}(t) = \tau_0^{det} + v_3 \chi_i^{traf}(t) + v_4 a_i(t) \quad (5)$$

$$s_i(t+1) = \rho s_i(t) + (1-\rho) [\omega_1 \eta_i(t) + \omega_2 \mathcal{R}_i(t) - \omega_3 \psi_i(t) - \omega_4 \mathbb{I}_i^{anom}(t)] \quad (6)$$

In Eq. (6), ρ is the trust-memory factor, while ω_1 – ω_4 weight successful verification, communication reliability, attack impact, and anomaly detection, respectively. They lie in $[0, 1]$, sum to one, and are set to 0.40, 0.30, 0.20, and 0.10. The initial trust is $s_i(0) = 0.85$, and users remain eligible for secure DR when $s_i(t) \geq s^{\min} = 0.60$. A node is considered valid only if its trust exceeds a threshold given in Eq. (7). Finally, the secure signalling overhead of Zone II for the node i is the term that later enters the optimization objective, computed in Eq. (8).

$$e_i(t) = \begin{cases} 1, & s_i(t) \geq s^{\min} \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

$$\Omega_i^{(2)}(t) = c_1 \tau_i^{auth}(t) + c_2 \tau_i^{det}(t) + c_3 \mathbb{I}_i^{anom}(t) \quad (8)$$

2.3.3 Zone III: 5G Access and Gateway Layer Model

Zone III contains the gNodeB/small cells, the secure gateway, and the encrypted DR signalling module. Cluster assignment for each consumer must belong to exactly one cluster formulated in Eq. (9). Then the cluster cost function is not purely spatial. It is defined in Eq. (10), where d_{ik} is the user-centroid distance, $\tau_{ik}^{comm}(t)$ is communication latency, $\mathcal{R}_{ik}(t)$ is communication reliability, $\Omega_{ik}^{sec}(t)$ is security overhead, and $\psi_{ik}(t)$ is attack impact. Thus, cluster assignment becomes Eq. (11). Centroid update: each user is assigned to one base-station-antenna pair, and the received power at user i is computed in Eqs. (12)–(14), respectively, where $PL_{ib}(t) = C_0 d_{ib}^\beta 10^{\xi_{ib}/10}$ and interference can be written as in Eq. (15). SINR, rate, and communication delay in Zone III are computed in Eqs. (16)–(18), respectively. Gateway encryption delay is considered in Eq. (19). Thus, the total Zone III overhead is formulated in Eq. (20).

$$\sum_{k \in \mathcal{K}} x_{ik} = 1, \forall i \in \mathcal{N} \quad (9)$$

$$C_{ik}(t) = \alpha_1 d_{ik} + \alpha_2 \tau_{ik}^{comm}(t) + \alpha_3 (1 - \mathcal{R}_{ik}(t)) + \alpha_4 \Omega_{ik}^{sec}(t) + \alpha_5 \psi_{ik}(t) \quad (10)$$

$$k_i^*(t) = \arg \min_{k \in \mathcal{K}} C_{ik}(t) \quad (11)$$

$$\mu_k(t) = \frac{\sum_{i \in \mathcal{N}} x_{ik}(t) p_i}{\sum_{i \in \mathcal{N}} x_{ik}(t)} \quad (12)$$

$$\sum_{b \in \mathcal{B}} \sum_{m \in \mathcal{M}} y_{ibm}(t) = 1, \forall i \quad (13)$$

$$P_i^{rx}(t) = \sum_{b \in \mathcal{B}} \sum_{m \in \mathcal{M}} y_{ibm}(t) P_b^{tx}(t) G_{bm} H_{ib}(t) PL_{ib}^{-1}(t) \quad (14)$$

$$I_i(t) = \sum_{j \neq i} \sum_{b \in \mathcal{B}} \sum_{m \in \mathcal{M}} y_{jbm}(t) P_b^{tx}(t) G_{bm} H_{ib}(t) PL_{ib}^{-1}(t) \quad (15)$$

$$\gamma_i(t) = \frac{P_i^{rx}(t)}{I_i(t) + N_0} \quad (16)$$

$$r_i(t) = B_i(t) \log_2(1 + \gamma_i(t)) \quad (17)$$

$$\tau_i^{(3)}(t) = \tau_i^{tx}(t) + \tau_i^{queue}(t) + \tau_i^{prop}(t): \text{where } \tau_i^{tx}(t) = \frac{L_i^{pkt}}{r_i(t)} \quad (18)$$

$$\tau_i^{enc}(t) = \tau_0^{enc} + v_5 L_i^{pkt} + v_6 \ell_i^{sec}(t) \quad (19)$$

$$\Omega_i^{(3)}(t) = c_4 \tau_i^{enc}(t) + c_5 \tau_i^{queue}(t) \quad (20)$$

To model dynamic bandwidth allocation, the bandwidth assigned to user i at time t is computed in Eq. (21), where B_b is the total bandwidth available at base station b , $N_b(t)$ is the number of users scheduled by that base station, and $\mathcal{U}_b$ denotes its associated user set. The projection operator $\Pi_{[B_{\min}, B_{\max}]}$ limits each user's allocation to the permitted range, with $B_{\min} = 0.2$ MHz and $B_{\max} = 1.0$ MHz.

$$B_i(t) = \Pi_{[B_{\min}, B_{\max}]} \left(\frac{B_b}{N_b(t)} \right), \sum_{i \in \mathcal{U}_b} B_i(t) \leq B_b \quad (21)$$

2.3.4 Zone IV: Local Control Layer Model

Zone IV includes the smart meter, HEMS/BEMS, secure control terminal, and encryption chip. In this regard, local processing delay is formulated in Eq. (22), where $n_i^{dev}(t)$ is the number of devices under local management, $\ell_i^{ctrl}(t)$ is the control complexity, and Local control is executed only if it passes local secure

verification by the given formula in Eq. (23). Local telemetry feedback delay is given in Eq. (24), where $n_i^{sens}(t)$ is the number of telemetry channels, and Zone IV overhead is calculated in Eq. (25).

$$\tau_i^{proc}(t) = \tau_0^{proc} + v_7 n_i^{dev}(t) + v_8 \ell_i^{ctrl}(t) \quad (22)$$

$$\zeta_i(t) = \begin{cases} 1, & \eta_i(t) = 1 \text{ and } e_i(t) = 1 \\ 0, & \text{otherwise.} \end{cases} \quad (23)$$

$$\tau_i^{fb}(t) = \tau_0^{fb} + v_9 n_i^{sens}(t) \quad (24)$$

$$\Omega_i^{(4)}(t) = c_6 \tau_i^{proc}(t) + c_7 \tau_i^{fb}(t) \quad (25)$$

2.3.5 Zone V: Consumers and Flexible Loads Model

Zone V includes consumers and flexible loads, such as HVAC systems, electric-vehicle chargers, smart appliances, and storage. This is where the actual DR response is realized and $P_i^{base}(t)$ is the baseline demand, and $P_i^{red}(t)$ is the maximum reducible load. Then, the participation probability depends on incentive, communication quality, and security trust in Eq. (26). The user-specific participation probability depends on time-varying incentive, communication quality, control delay, dynamically accumulated trust history, and heterogeneous discomfort sensitivity, as formulated in Eq. (26).

$$q_i(t) = \frac{1}{1 + \exp[-(\beta_0 + \beta_1 \pi_i(t) + \beta_2 \gamma_i(t) - \beta_3 \tau_i(t) + \beta_4 s_i(t) - \beta_5 \delta_i)]} \quad (26)$$

Although Eq. (26) uses a logistic form, it is tailored to secure DR participation through incentive $\pi_i(t)$, communication quality $\gamma_i(t)$, delay $\tau_i(t)$, dynamic trust $s_i(t)$, and user-specific discomfort δ_i . Trust captures prior verification and abnormal behaviour, while δ_i represents behavioural heterogeneity. The model keeps participation within $[0, 1]$; social learning, demographics, and explicit long-term participation records are left for future work. The attack-aware DR realization, which secures the DR response of the node i , as is computed in Eq. (27).

$$\Delta P_i(t) = u_i(t) q_i(t) P_i^{red}(t) \mathcal{R}_i(t) s_i(t) (1 - \psi_i(t)) \zeta_i(t) \quad (27)$$

DR realization depends jointly on the activation decision. $u_i(t)$, willingness to participate $q_i(t)$, reducible load $P_i^{red}(t)$, communication reliability $\mathcal{R}_i(t)$, trust score $s_i(t)$, attack impact $\psi_i(t)$, and successful local secure verification $\zeta_i(t)$. Then, the aggregate DR response and post-DR net load are modelled in Eqs. (28) and (29) as:

$$\Delta P_{DR}(t) = \sum_{i \in \mathcal{N}} \Delta P_i(t) \quad (28)$$

$$P^{net}(t) = \sum_{i \in \mathcal{N}} P_i^{base}(t) - \Delta P_{DR}(t) \quad (29)$$

2.4 Cross-Zone Delay, Security, and Reliability Coupling

The complete cross-zone delay (end-to-end delay) is the sum of delays across Zones II–IV, and is given in Eq. (30) as: Thus, the total secure signalling overhead and the aggregate cyberattack impact are calculated in Eqs. (31) and (32).

$$\tau_i(t) = \tau_i^{auth}(t) + \tau_i^{det}(t) + \tau_i^{enc}(t) + \tau_i^{tx}(t) + \tau_i^{queue}(t) + \tau_i^{prop}(t) + \tau_i^{proc}(t) + \tau_i^{fb}(t) \quad (30)$$

$$\Omega_i^{sec}(t) = \Omega_i^{(2)}(t) + \Omega_i^{(3)}(t) + \Omega_i^{(4)}(t) \quad (31)$$

$$\psi_i(t) = \sum_{a \in \mathcal{A}} \chi_a \delta_{ia}(t) \quad (32)$$

In Eq. (32), χ_a is the severity coefficient for attack type a , and $\delta_{ia}(t) \in [0, 1]$ is the time-varying attack intensity experienced by user i . The attack set includes replay, false data injection, delay, and DoS/jamming, with $\chi_a = \{0.15, 0.30, 0.20, 0.35\}$, respectively. Attack intensity is sampled from $[0, 0.2]$, $[0.2, 0.6]$, and $[0.6, 0.9]$ for low, moderate, and severe conditions, and is varied from 0 to 0.9 in sensitivity analysis. The aggregate attack impact combines χ_a and $\delta_{ia}(t)$, capturing heterogeneous and time-varying cyber threats. Then, the packet error rate and cybersecurity-aware reliability are calculated in Eqs. (33) and (34) as:

$$PER_i(t) = e^{-\kappa \gamma_i(t)} \quad (33)$$

$$\mathcal{R}_i(t) = \eta_i(t) (1 - PER_i(t)) \exp(-\lambda_1 \tau_i(t) - \lambda_2 \Omega_i^{sec}(t)) (1 - \psi_i(t)) \quad (34)$$

Eq. (34) combines verification success, packet-delivery probability, exponential delay and security penalties, and attack impact. The exponential component decreases monotonically with delay and security overhead, while $\eta_i(t)$, $1 - PER_i(t)$, and $1 - \psi_i(t)$ account for verification, packet errors, and attacks. The sensitivity coefficients are consistently applied across all methods and require empirical calibration for practical deployment.

2.5 Fairness and Resilience Metrics

Fairness and Resilience Metrics are computed in Table 1, where $\varepsilon > 0$ avoids division by zero. This resilience metric increases when DR, reliability, and fairness are high and delay and security burden are low.

Table 1: Fairness and resilience metrics.

Metrics	Expression
Fairness of secure DR allocation	$F(t) = \frac{(\sum_{i \in \mathcal{N}} \Delta P_i(t))^2}{N \sum_{i \in \mathcal{N}} \Delta P_i^2(t)}$
Average system reliability	$\overline{\mathcal{R}}(t) = \frac{1}{N} \sum_{i \in \mathcal{N}} \mathcal{R}_i(t)$
Average end-to-end delay	$\overline{\tau}(t) = \frac{1}{N} \sum_{i \in \mathcal{N}} \tau_i(t)$
Average security overhead	$\overline{\Omega}^{sec}(t) = \frac{1}{N} \sum_{i \in \mathcal{N}} \Omega_i^{sec}(t)$
Cyber-resilient DR efficiency	$\Xi(t) = \frac{\Delta P_{DR}(t) \overline{\mathcal{R}}(t) F(t)}{\overline{\tau}(t) + \overline{\Omega}^{sec}(t) + \varepsilon}$

2.6 Objective Function

The proposed framework minimizes a joint cost comprising latency, packet error rate, unreliability, security overhead, DR shortfall, fairness and resilience, and cyber risk. Thus, the overall optimization problem is written in Eq. (35), where $\theta_1, \dots, \theta_8$ are weighting coefficients.

$$\begin{aligned} \min J = \sum_{t \in \mathcal{T}} & [\theta_1 \overline{\tau}(t) + \theta_2 \overline{PER}(t) + \theta_3 (1 - \overline{\mathcal{R}}(t)) + \theta_4 \overline{\Omega}^{sec}(t) + \theta_5 (\Delta P^{short}(t))^2 + \theta_6 (1 - F(t)) \\ & + \theta_7 (1 - \Xi(t)) + \theta_8 \Gamma^{risk}(t)] \end{aligned} \quad (35)$$

The weighting coefficients of Eq. (35) are the relative engineering priorities of the secure DR objectives. The objective terms are normalized prior to their aggregation to ensure that none of the terms dominates entirely due to the magnitude of the objective term. The baseline values are $\theta_1 = 0.18$, $\theta_2 = 0.12$, $\theta_3 = 0.15$, $\theta_4 = 0.12$, $\theta_5 = 0.20$, $\theta_6 = 0.08$, $\theta_7 = 0.10$, and $\theta_8 = 0.05$, which sum to one. DR shortfall takes precedence over latency and unreliability, since the DR target must be met in a timely and reliable manner by delivering the commands. The rest of the weights do the job of balancing packet error rate, security overhead, fairness, resilience and cyber-risk. A sensitivity analysis is used to assess the effect of the primary weights by changing the weights around from the base weight and keeping the total weight normalized. The overall performance trends are the same, meaning that they are not sensitive to the way the weights are chosen. Increasing θ_5 improves DR target satisfaction, whereas increasing θ_1 , θ_3 , or θ_7 places greater emphasis on latency reduction, reliability, or resilience, respectively. Thus, the selected coefficients provide a reproducible trade-off among communication, cybersecurity, fairness, resilience, and DR performance. The weighted-sum form in Eq. (35) provides a computationally tractable scalar representation of the multi-objective problem by assigning normalized weighting coefficients to the individual objective components. The success of the verification and the packet error rate, delay, and security overhead are all factors in reliability, while the reliability of communication, trust, attack severity, and activation and participation probability are all factors in realising DR; and local verification is a factor of both. This means that, although they are linked together in a weighted objective, they are not independent of one another. Due to the presence of binary clustering, base-station and antenna assignment, DR activation, nonlinear SINR and rate expressions, dynamic trust, attack-aware reliability, fairness, and resilience, the overall formulation is a MINLP, which is not convex. Through normalized coefficients, the weighted formulation provides a practical method to balance these competing objectives and change engineering priorities. However, if non-convex Pareto-optimal solutions exist, weighted-sum scalarization does not guarantee to find all of them and needs prior preferences. Pareto-front, ε -constraint, robust and chance-constrained formulations in the future could be employed to handle uncertainty in communication, participation and attack intensity. It brings together communication, cybersecurity and energy response performance into a single model. The number of constraints is specified in Table 2.

Table 2: Constraints metrics.

Constraints	Metrics
User-cluster association	$\sum_{k \in \mathcal{K}} x_{ik} = 1, \forall i$
Base station/antenna assignment	$\sum_{b \in \mathcal{B}} \sum_{m \in \mathcal{M}} y_{ibm} = 1, \forall i$
Cluster capacity	$\sum_{i \in \mathcal{N}} x_{ik} \leq N_k^{\max}, \forall k$
SINR threshold	$\gamma_i(t) \geq \gamma^{\min}, \forall i, t$
Delay threshold	$\tau_i(t) \leq \tau^{\max}, \forall i, t$
Trust threshold	$s_i(t) \geq s^{\min}, \forall i, t$ for activated users
Reliability threshold	$\mathcal{R}_i(t) \geq \mathcal{R}^{\min}, \forall i, t$
DR activation feasibility	$\Delta P_i(t) \leq P_i^{\text{red}}(t), \forall i, t$
Required DR satisfaction	$\Delta P_{DR}(t) \geq P^{\text{req}}(t) - \varepsilon^{\text{tol}}, \forall t$
Binary constraints	$x_{ik}, y_{ibm}, u_i(t), \eta_i(t), \zeta_i(t) \in \{0, 1\}$

The study is a numerical proof-of-concept, not actual field measurements, in the context of controlled smart-grid conditions, enabled by 5G. The validation consists of comparisons to benchmarks, Monte Carlo

testing, and variations of the network load, the severity of the attack, the trust threshold, the time for authentication, the number of users, and the number of clusters, to determine the robustness and scalability. Per-user bandwidth is dynamically allocated within $B_i(t) \in [0.2, 1.0]$ MHz according to the number of users scheduled by each base station. An equal-share allocation $B_b/N_b(t)$ is projected onto the permitted range while satisfying $\sum_{i \in \mathcal{U}_b} B_i(t) \leq B_b$. When capacity is insufficient, scheduling prioritizes users meeting the trust, SINR, reliability, and DR conditions. The 5 dB SINR threshold determines secure DR eligibility, whereas 0 dB identifies cell-edge links. The 256-bit packet represents a compact 32-byte URLLC-type DR control or acknowledgement message as shown in Table 3. Queueing and propagation delays are fixed at 2 and 0.5 ms, respectively, and are applied consistently to all methods as controlled simulation assumptions rather than field measurements.

Table 3: Simulation parameters for the proposed cybersecurity-aware demand response optimization framework.

Parameter	Value	Parameter	Value
DR users N	500	Clusters K	9
5G base stations B	9	Antenna pairs/BS M	4
Simulation area	2 km $\times$ 2 km	Zones Z	5
Attack types	4	Time slots T	24
Time-slot duration	5 min	Carrier frequency	28 GHz
System bandwidth	100 MHz	Per-user bandwidth	0.2–1.0 MHz
BS transmit power	30 dBm	Shadowing deviation	6 dB
Path-loss exponent	3.2	Cell-edge SINR	0 dB
Minimum SINR	5 dB	Maximum latency	20 ms
Packet size	256 bits	Minimum trust	0.60
Initial trust	0.85	Minimum reliability	0.60
Replay/FDI/delay/DoS coefficients	0.15/0.30/0.20/0.35	Reducible load/user	0.5–3.0 kW
Baseline demand/user	1.5–5.0 kW	Discomfort sensitivity	0.1–0.8 p.u.
Incentive	0.1–0.9 p.u.	Required DR target	300–800 kW

3 Iterative Multi-Zone Cybersecurity-Aware Demand Response Optimization under 5G

Input: User locations, baseline load, reducible load, 5G communication parameters, security parameters, attack scenarios, trust thresholds, objective weights, and maximum iterations.

Output: Optimal cluster assignment, secure communication assignment, trust scores, DR activation states, aggregate secure DR, and system-level performance metrics.

The simulation parameters are given in Table 3, while the proposed algorithm is presented as Algorithm 1 follows.

Algorithm 1: Decomposition-based iterative heuristic for multi-zone cybersecurity-aware demand response optimization

- 1: Input:** network parameters, $P^{req}(t)$, $L_{\max}$, ε_f , and ε_μ .
- 2: Initialize** user states, centroids, trust scores, attack intensities, assignments, DR activations, and $J^{(0)}$.
- 3: For each** $t \in \mathcal{T}$, compute $\psi_i(t)$, $\Gamma^{risk}(t)$, and risk-aware dispatch using Eqs. (2), (3) and (32).
- 4: Set** iteration index $\ell = 1$.
- 5: Repeat:** compute Zone II security delays, verification, trust eligibility, and overhead using Eqs. (4)–(8).

(Continued)

Algorithm 1 (continued)

-
- 6: Update** clustering, centroids, BS–antenna assignments, and bandwidth using Eqs. (9)–(13) and (21).
7: Compute SINR, rate, communication delay, encryption delay, and Zone III overhead using Eqs. (14)–(20).
8: Compute local processing, secure execution, feedback delay, and Zone IV overhead using Eqs. (22)–(25).
9: Compute end-to-end delay, total security overhead, PER, and reliability using Eqs. (30), (31), (33) and (34).
10: Update trust using Eq. (6) and re-evaluate user eligibility.
11: Compute participation probability using Eq. (26), update $u_i(t)$, and calculate DR response using Eqs. (27)–(29).
12: Evaluate Table 1 metrics and objective $J^{(\ell)}$ using Eq. (35).
13: Check all constraints in Table 2; reject infeasible or objective-worsening updates.
14: Stop if $|J^{(k)} - J^{(k-1)}| \leq \varepsilon_J$ and $\max_{c \in \mathcal{K}} \|\mu_c^{(k)} - \mu_c^{(k-1)}\| \leq \varepsilon_\mu$, or if $k = L_{\max}$.
15: Store the optimized solution for time slot t .
16: Output: optimized clustering, radio assignments, trust scores, DR activations, and performance metrics.
-

Algorithm 1 uses objective-function and centroid tolerances, together with a maximum iteration count, to ensure finite termination at a stable feasible solution. Since the problem is a non-convex MINLP and the algorithm initializes user states, centroids, trust scores, attack severity, DR activations, and the objective values before proceeding with the iterative optimization process. At each time slot, it determines the DR target, updates authentication, intrusion detection, anomaly risk, and trust, excludes insecure users, performs communication-security-aware clustering, allocates BS–antenna pairs and bandwidth, and evaluates SINR, rate, and delay. It then completes secure verification and feedback, estimates participation, activates eligible users, and calculates secure DR response. Finally, it evaluates reliability, security overhead, fairness, resilience, DR shortfall, and the global objective. The process repeats until the objective and centroid changes meet the prescribed tolerances or the maximum iteration limit is reached, thereby integrating communication, cybersecurity, trust, and DR decisions within a unified iterative framework.

3.1 Decomposition-Based Iterative Solution and Convergence Handling

The formulation in Section 2 is a non-convex MINLP due to binary assignment and activation variables, nonlinear SINR and rate expressions, and dynamic trust, reliability, fairness, and resilience terms. Because exact global optimization is impractical for large-scale real-time operation, a decomposition-based iterative heuristic is used. It sequentially updates security and trust, communication-aware clustering, radio-resource allocation, and DR-user activation. Discrete variables are handled through feasibility-based greedy assignment, while continuous variables are updated using the models in Section 2. After each iteration, the global objective is recalculated from latency, PER, unreliability, security overhead, DR shortfall, fairness, resilience, and cyber risk. Global optimality is not claimed. The algorithm terminates if $|J^{(k)} - J^{(k-1)}| \leq \varepsilon_J$ and $\max_{c \in \mathcal{K}} \|\mu_c^{(k)} - \mu_c^{(k-1)}\| \leq \varepsilon_\mu$, or if $k = L_{\max}$. Since the discrete space is finite and the continuous variables are bounded, the method converges in practice to a stable feasible solution.

3.2 Computational Complexity Analysis

The computational complexity of the proposed decomposition-based iterative algorithm depends on the main decision blocks executed in each iteration. Let N denote the number of DR users, K the

number of clusters, B the number of base stations, A_p the number of antenna pairs per base station, A_c the number of cyberattack types, T the number of time slots, I_c the number of clustering updates, and $I_{\max}$ the maximum number of optimization iterations. For each time slot, cyberattack-impact evaluation and trust updating require $O(NA_c)$. Communication-security clustering requires $O(I_cNK)$, including repeated assignment and centroid updates. Base-station and antenna-pair selection examines up to BA_p candidate links per user, giving $O(NBA_p)$. The calculations of received power, SINR, achievable rate, delay, security overhead, and reliability are mainly linear in N ; however, explicit interference evaluation among all users requires $O(N^2)$. DR eligibility, participation, activation, aggregate response, fairness, shortfall, and resilience calculations each require $O(N)$ where the dominant per-iteration complexity is $O(I_cNK + NBA_p + N^2 + NA_c)$. Considering T time slots and at most $I_{\max}$ iterations, the total worst-case complexity becomes $O(TI_{\max}[I_cNK + NBA_p + N^2 + NA_c])$. When interference and link-quality values are precomputed or vectorized, the N^2 term can be reduced in practical implementation, giving an approximate complexity of $O(TI_{\max}[I_cNK + NBA_p + NA_c])$. Since A_c , A_p , and B are small and fixed in the simulation, the computational cost is mainly determined by the numbers of users and clusters. The proposed method therefore avoids exhaustive enumeration of all MINLP assignments.

4 Results and Discussion

The proposed CCA-DR-Sec framework is evaluated against three controlled benchmark configurations: Comm-Aware DR, Secure Static DR, and Unicast Secure DR. These benchmarks are implemented as ablation-based variants of the proposed framework rather than exact reproductions of previously published algorithms. This design isolates the contribution of dynamic trust, attack-aware DR realization, cross-zone security coordination, communication-aware clustering, and fairness-resilience optimization. For every Monte Carlo run, all methods use identical user locations, baseline demands, reducible loads, channel realizations, cyberattack intensities, DR targets, bandwidth, transmission power, time slots, trust initialization, and random seeds. The feasibility thresholds, maximum iteration count, stopping criteria, and traffic conditions are also kept identical wherever applicable. Consequently, performance differences arise only from the mechanisms enabled or disabled in each configuration. Comm-Aware DR considers communication-based association and activation using SINR, latency, packet error rate, and reliability, but excludes dynamic trust, attack-aware response adjustment, local secure verification, and cross-zone security overhead. Secure Static DR includes authentication, encryption, intrusion-detection overhead, and fixed security eligibility, but does not update trust or attack impact across time slots. Unicast Secure DR applies authentication and encryption separately to each user without communication-security-aware clustering, joint base-station/antenna assignment, or fairness-aware resource coordination. Fig. 1 compares communication performance under increasing normalized cell load. In Fig. 1a, the proposed CCA-DR-Sec latency increases from approximately 4.9 to 8 ms, while Comm-Aware DR, Secure Static DR, and Unicast Secure DR reach about 11.5, 13.3, and 23.9 ms at load 0.7. Fig. 1b shows that the proposed packet error rate rises only from 0.006 to 0.03, compared with final values of 0.050, 0.073, and 0.230. In Fig. 1c, the proposed SINR decreases from approximately 32.4 to 24.0 dB but remains higher than the benchmark values of 17.9, 13.5, and 3.4 dB. These results show that the proposed method controls congestion and interference more effectively. The user rate and user demand response performance are shown in Fig. 2. As illustrated in Fig. 2a, the proposed average user rate drops from 2.65 to 1.60 Mbps, while the benchmark rates drop to around 1.00, 0.65 and 0.28 Mbps, respectively. For the proposed method, the DR response of the aggregates decreases from about 766 to 680 kW, while the other methods have DR responses of 607, 549, and 375 kW, as shown in Fig. 2b. The active DR user ratio is still high for all the schemes, dropping from 0.985 to 0.93 for the proposed framework, whereas 0.870, 0.810 and 0.515 for the benchmark schemes, as shown in Fig. 2c for

details.) This proves that the proposed structure keeps the quality of communication as well as secure DR participation when the load is high. Fig. 3 evaluates reliability, trust, and fairness. Fig. 3a shows that the proposed communication reliability decreases from approximately 0.875 to 0.685, compared with final values of about 0.580, 0.480, and 0.260 for the benchmark methods. Fig. 3b shows that the proposed average trust score remains approximately 0.80 at maximum load, while the benchmark values decline to about 0.75, 0.695, and 0.595. In Fig. 3c, Jain's fairness index decreases from around 0.905 to 0.790, but remains higher than the benchmark values of approximately 0.725, 0.655, and 0.455. Therefore, the proposed framework preserves reliable, trusted, and fair participation more effectively. Fig. 4 examines edge-user support, DR shortfall, and resilience. In Fig. 4a, the proposed cell-edge SINR remains around 11 dB at load 0.7, while Comm-Aware DR falls to approximately 4.2 dB, Secure Static DR approaches 0 dB, and Unicast Secure DR becomes negative. Fig. 4b shows that the proposed DR shortfall is only about 20 kW, compared with approximately 133, 221, and 475 kW. Fig. 4c shows that cyber-resilient DR efficiency decreases from about 68 to 48 for the proposed framework but reaches only around 32, 21, and 11 for the benchmarks at maximum load. These results demonstrate stronger edge protection, target fulfilment, and cyber resilience.

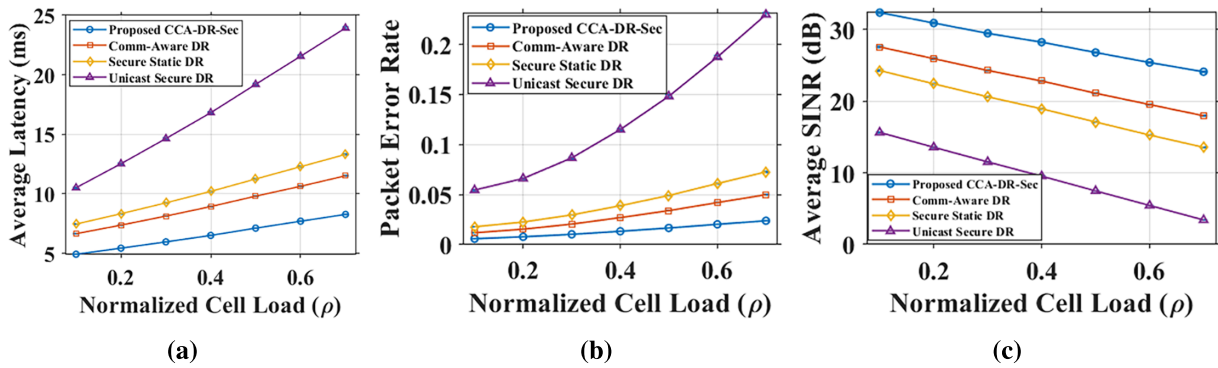


Figure 1: Communication performance comparison under increasing normalized cell load: (a) average end-to-end latency; (b) packet error rate; and (c) average SINR.

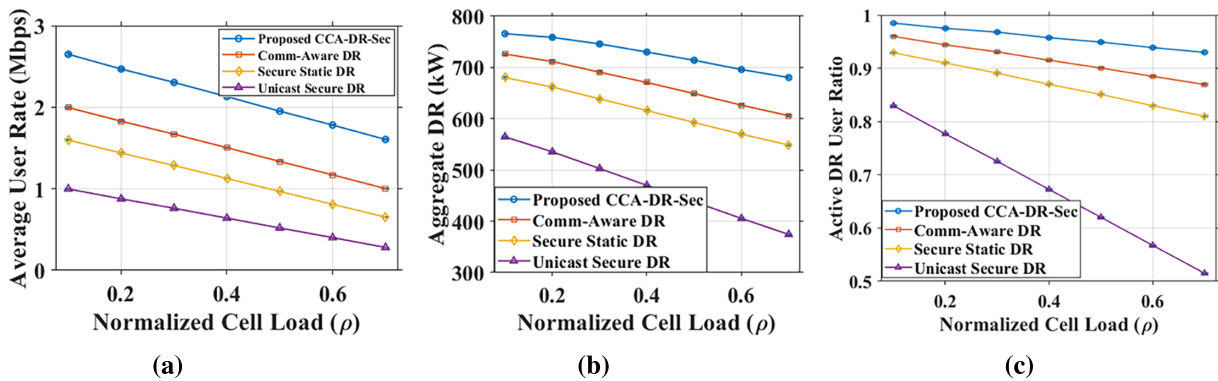


Figure 2: Communication and demand-response performance under increasing normalized cell load: (a) average user rate; (b) aggregate DR response; and (c) active DR user ratio.

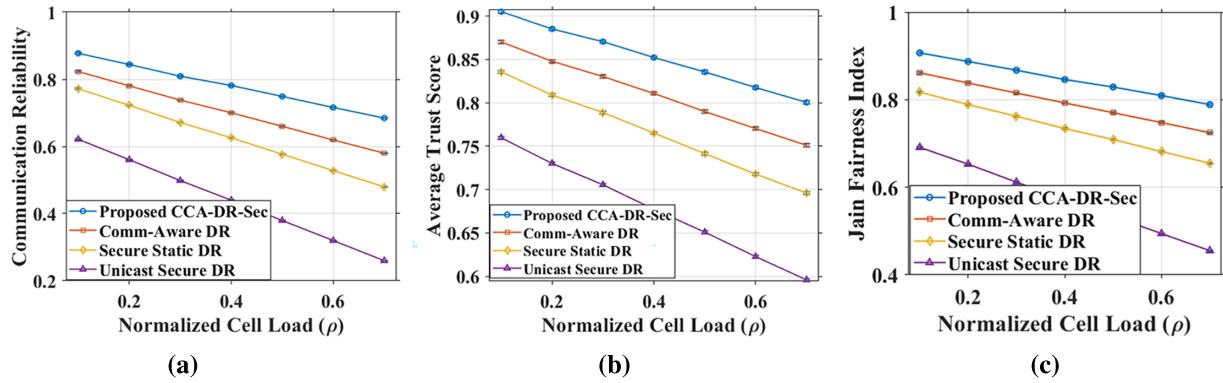


Figure 3: Secure participation and fairness performance under increasing normalized cell load: (a) communication reliability; (b) average trust score; and (c) Jain fairness index.

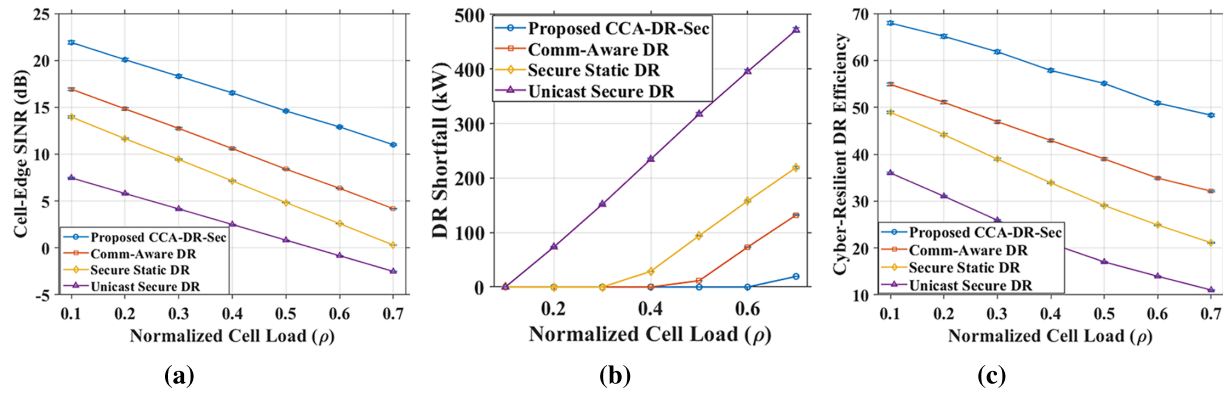


Figure 4: Edge robustness and secure demand-response performance under increasing normalized cell load: (a) cell-edge SINR; (b) DR shortfall; and (c) cyber-resilient DR efficiency.

Validation is based on the distribution in Fig. 5. The median latency of the proposed framework is approximately 8 ms, whereas for the benchmarks it is 11, 13 and 20–21 ms, respectively, as shown in Fig. 5a. Fig. 5b reports a median PER of 0.015–0.020, vs 0.035, 0.050, and 0.150, while Fig. 5c shows a median SINR of about 27 dB, compared with 22, 17, and 7 dB. The shifted CDF graphs illustrate the gains that occur for most of the users. The reliability and cybersecurity sensitivity are analyzed in Fig. 6. Fig. 6a shows a median reliability of about 0.74, compared with 0.66, 0.58, and 0.40. As attack severity increases from 0 to 0.9, the DR response for the proposed scenario decreases from about 765 to 575 kW and the DR responses for the three benchmarks decrease to about 490, 430 and 350 kW, respectively, in this scenario in Fig. 6b. The active DR user ratio dropped from 0.99 to 0.83 as the trust level increased, whereas the final benchmark values were 0.68, 0.59, and 0.30 Fig. 6c. Fig. 7 compares the authentication delay, the reliability of the attack type, and the runtime. Fig. 7a illustrates a latency increase from 6.8 to 10.2 ms but still lower than the benchmarks. Replay, FDI, delay and DoS/jamming reliability values are 0.80, 0.74, 0.70 and 0.62, respectively, as shown in Fig. 7b. As evident in Fig. 7c, the runtime grows slowly with increasing number of users from 3.3 ms at 100 users to 8.2 ms at 700 users. The cluster design, scalability and spatial deployment are presented in Fig. 8. The DR response is seen to increase from 4 clusters to 16 clusters with the value of 698 kW at 4 clusters to 724 kW at 16 clusters, and then decrease to 703 kW at 25 clusters and the SINR drops from 27.8 dB at 4 clusters to 25.0 dB at 16 clusters are shown in Fig. 8a. The reliability values for the students' answers in Fig. 8b decreased from 0.90 to 0.70, whereas the final benchmark values were 0.60,

0.51, and 0.34. Compact clusters, distributed centroids and base-station locations of 5G that can support the observed performance gains are shown in Fig. 8c. All major simulations were repeated over $N_{MC} = 100$ independent Monte Carlo trials. Each algorithm has been tested 100 times, and each normalized cell-load point has been tested for each algorithm, and the reported value is the mean of the samples. The statistical uncertainty was evaluated by computing the 95% confidence interval, $CI_{95} = 1.96 \frac{\sigma}{\sqrt{N_{MC}}}$ where σ is taken as the sample standard deviation over the Monte Carlo trials across Figs. 1–4 and 6–8, where applicable.

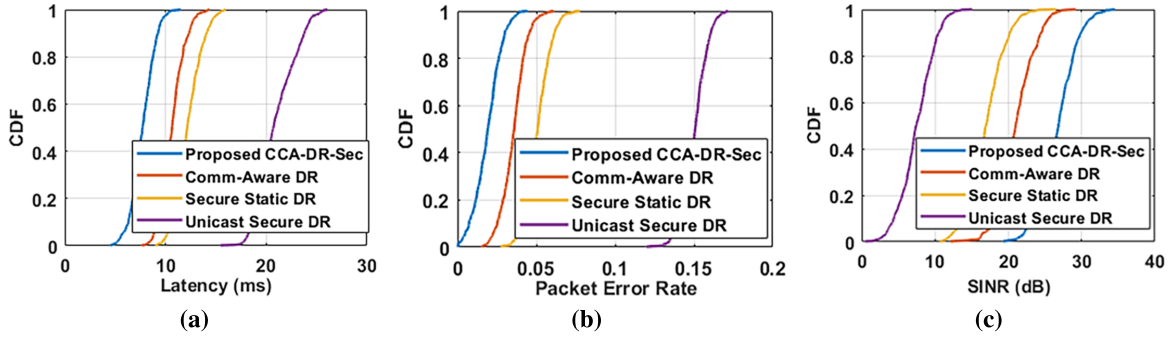


Figure 5: Distribution-based communication performance comparison: (a) empirical CDF of end-to-end latency; (b) empirical CDF of packet error rate; and (c) empirical CDF of SINR.

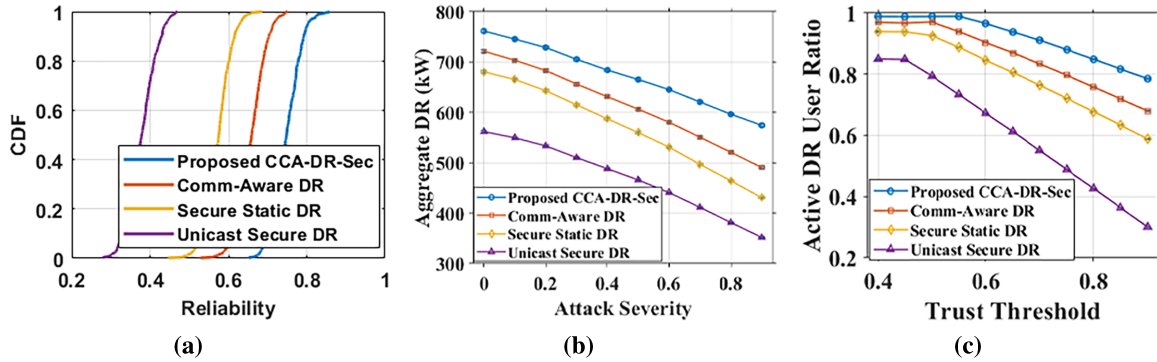


Figure 6: Reliability and cybersecurity sensitivity analysis: (a) empirical CDF of communication reliability; (b) aggregate DR response vs. attack severity; and (c) active DR user ratio vs. trust threshold.

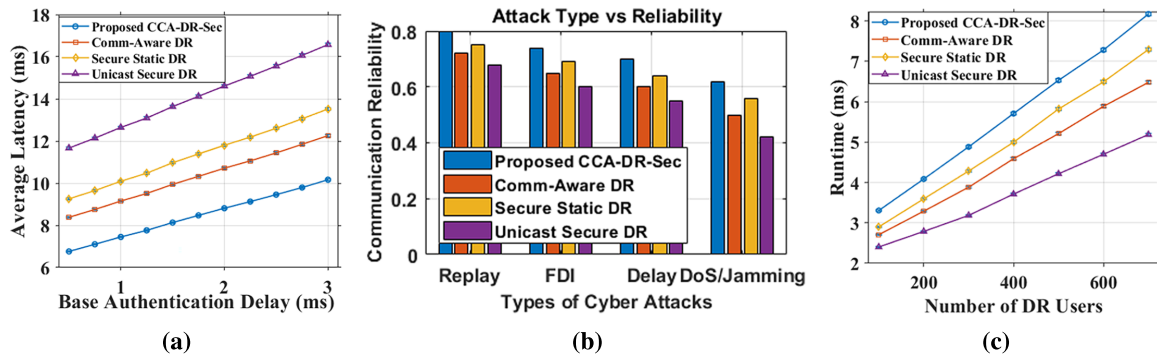


Figure 7: Security-processing, attack-resilience, and computational performance: (a) average end-to-end latency vs. base authentication delay; (b) communication reliability under replay, false-data-injection, delay, and DoS/jamming attacks; and (c) algorithm runtime vs. number of DR users.

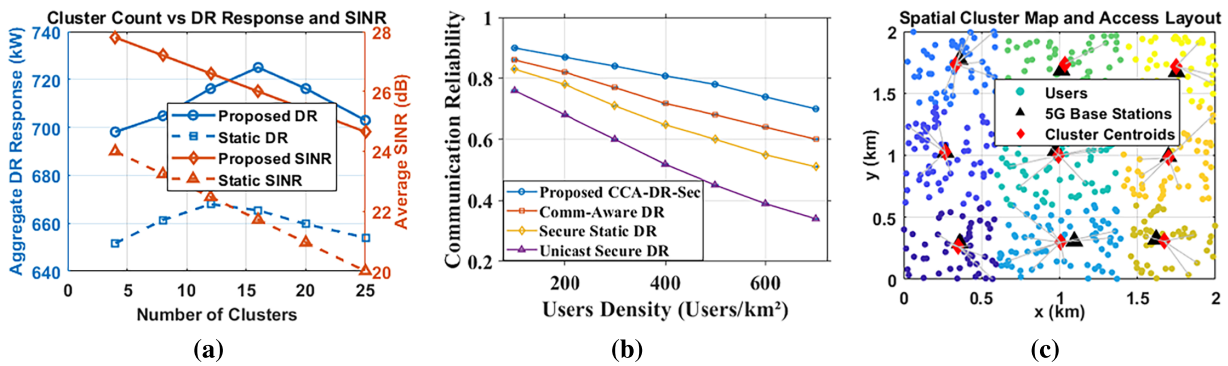


Figure 8: Cluster design, user-density scalability, and spatial deployment: (a) aggregate DR response and average SINR vs. number of clusters; (b) communication reliability vs. number of DR users; and (c) spatial distribution of DR users, cluster centroids, and 5G base stations.

Overall Discussion and Comparison

The study presented in [20] focused on the implementation of hybrid LPWAN smart-grid communication and reported over 97% packet delivery, an SNR of about 9 dB, a latency of less than 150 ms, and reliability of 0.98; it was not concerned with the controllability of DR under dense 5G load conditions. On the other hand, it is also found that the fairness is approximately 0.78 in QoS-sensitive 5G uplink scheduling, but their experiment focused on radio scheduling rather than the secure implementation of DR [21]. In [22], cybersecurity performance improves, but it is primarily security-oriented. Still, cybersecurity, trust, 5G communication delay, packet error rate, and attack-aware DR execution are not considered in this model. A blockchain-integrated secure authentication for smart grid IoT is presented in [23], but it is not directly linked with DR response, SINR, cell-edge reliability, or multi-zone DR control. However, they do not jointly assess DR response, reliability, trust, fairness, and attack-aware participation. As shown in Table 4, the proposed CCA-DR-Sec framework integrates these aspects and, at load 0.7, achieves about 8 ms latency, 0.03 PER, 24 dB SINR, 1.60 Mbps user rate, 0.93 active DR user ratio, 0.685 reliability, 0.79 fairness, 11 dB cell-edge SINR, 680 kW DR response, and 20 kW shortfall. The gains result from the combined effects of clustering, dynamic trust, security verification, resource allocation, and attack-aware DR activation, although this integration increases runtime from 3.3 ms at 100 users to 8.2 ms at 700 users. Thus, the results demonstrate the benefit of integrated coordination under a common simulation environment.

Table 4: Positioning of the proposed model against recent research.

Ref.	Main Focus	Key Reported Results
[20]	Hybrid LPWAN communication and energy management for smart grids	Packet delivery rate >97%, SNR $\approx$ 9 dB, end-to-end latency <150 ms, reliability = 0.98, peak reduction = 1.83%
[21]	QoS-aware 5G uplink scheduling for MTC	Fairness $\approx$ 0.78 at high load, delay violations capped at 8.3, throughput $\sim$ 15% lower
[22]	Hybrid AI-blockchain security framework for smart grids	Only focuses on AI and blockchain-based detection and defence against communication-layer

(Continued)

Table 4 (continued)

Ref.	Main Focus	Key Reported Results
[23]	Blockchain-integrated secure authentication for smart grid IoT	35% throughput improvement, 25% latency reduction, 25% energy-efficiency improvement, 98.69% authentication accuracy
Proposed model	5G-enabled DR management with clustered communication-aware optimization	Latency = 8 ms, packet loss = 0.03, SINR = 24 dB, user rate = 1.6 Mbps, active DR ratio = 0.95, reliability = 0.66, fairness = 0.79, cell-edge SINR = 11 dB at load 0.5

5 Conclusion and Future Work

In this paper, a cybersecurity-aware DR optimization framework for 5G-enabled smart grid is proposed, which integrates communication management, cybersecurity protection, trust assessment and DR control into a single system. The proposed solution considers both latency and PER, SINR, user rates, active DR user ratio, reliability, fairness, resilience and aggregate DR response. It has a multi-zone architecture that helps manage communication security-aware clustering, resource allocation security, trust creation and updating and activation of DR in response to attacks. The framework acquires a latency of about 8 ms, a PER of 0.03, a SINR of 24 dB, a user rate of 2 Mbps, an active DR user ratio of 0.93 and a reliability of 0.685 under high load, outperforming the ablation-based baseline configurations for the considered scenario. It also performs better with different levels of attacks and trust. The study is restricted, however, to several controlled numerical simulations, to a set of parameters, to the use of weighted-sum scalarization, and to a heuristic method based on a decomposition approach, which is not guaranteed to reach a global optimum. The extra security and coordination mechanisms also result in tolerable computational cost. As such, they need to be integrated with the platforms of the utilities, 5G infrastructure, smart meters, edge servers, and local energy-management systems for the deployment to be implemented. Future work will comprise an NS-3 and power-system co-simulation, real-world datasets, hardware-in-the-loop testing, empirically informed trust and attack models, lightweight cryptography, Pareto optimization, and extension to AI-powered 6G smart grids.

Acknowledgement: This research has been supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2026R232), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Statement: This research has been funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2026R232), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Sajjad Rabbani; methodology, Sajjad Rabbani, Salil Bharany; validation, Upinder Kaur, Adnan Yousaf, Rao Muhammad Asif; formal analysis, Upinder Kaur, Adnan Yousaf, Ateeq Ur Rehman; investigation, Sajjad Rabbani, Rao Muhammad Asif; resources, Salil Bharany, Mai Alduailij, Ateeq Ur Rehman; data curation, Sajjad Rabbani; writing—original draft preparation, Sajjad Rabbani, Mai Alduailij; writing—review and editing, Upinder Kaur, Salil Bharany, Adnan Yousaf, Ateeq Ur Rehman; supervision, Rao Muhammad Asif, Adnan Yousaf; funding acquisition, Mai Alduailij. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Cao Y, Xu Y. Robust coordination of preventive and corrective security control for a multi-energy microgrid with multiple demand response participation. *IEEE Trans Smart Grid*. 2026;17(4):3017–31. doi:10.1109/TSG.2026.3653574.
2. Saleem MU, Usman MR, Yaqub MA, Liotta A, Asim A. Smarter grid in the 5G era: integrating the Internet of Things with a cyber-physical system. *IEEE Access*. 2024;12(3):34002–18. doi:10.1109/ACCESS.2024.3372379.
3. Goswami P, Naseem H, Abbas K, Choi K. An agent-based network power management scheme in WSN for enhanced edge communication in beyond 5G networks. *Comput Mater Contin*. 2026;87(3):42. doi:10.32604/cmc.2026.077012.
4. Muhammad Asif R, Shakir M, Nebhen J, Ur Rehman A, Shafiq M, Choi JG. Energy efficiency trade-off with spectral efficiency in MIMO systems. *Comput Mater Contin*. 2022;70(3):5889–905. doi:10.32604/cmc.2022.020777.
5. Azeez SD, Ilyas M, Ahmed SR. Graph neural networks with multi-head attention and SHAP-based explainability for robust, interpretable, and high-throughput intrusion detection in 5G-enabled software defined networks. *Comput Mater Contin*. 2026;87(3):66. doi:10.32604/cmc.2026.074930.
6. Xu X, Shao Z, Chen F, Cheng G. Stochastic robust optimization scheduling for integrated energy system cluster based on data-driven method. *Appl Energy*. 2025;400(2):126512. doi:10.1016/j.apenergy.2025.126512.
7. Gunduz MZ, Das R. Cyber-security on smart grid: threats and potential solutions. *Comput Netw*. 2020;169(11):107094. doi:10.1016/j.comnet.2019.107094.
8. Jørgensen BN, Ma ZG. Cybersecurity and resilience of smart grids: a review of threat landscape, incidents, and emerging solutions. *Appl Sci*. 2026;16(2):981. doi:10.3390/app16020981.
9. Sahani N, Zhu R, Cho JH, Liu CC. Machine learning-based intrusion detection for smart grid computing: a survey. *ACM Trans Cyber Phys Syst*. 2023;7(2):1–31. doi:10.1145/3578366.
10. Wang X, Geng Y, Luo X, Guan X. Detection of dummy data injection attacks by using particle swarm optimization-attention temporal graph convolutional network model in power system. *Eng Appl Artif Intell*. 2026;171(5):114259. doi:10.1016/j.engappai.2026.114259.
11. Chai B, Yang Z. Impacts of unreliable communication and modified regret matching based anti-jamming approach in smart microgrid. *Ad Hoc Netw*. 2014;22(1):69–82. doi:10.1016/j.adhoc.2014.05.011.
12. Reka SS, Dragičević T, Siano P, Prabakaran SRS. Future generation 5G wireless networks for smart grid: a comprehensive review. *Energies*. 2019;12(11):2140. doi:10.3390/en12112140.
13. Antal M, Mihailescu V, Cioara T, Anghel I. Blockchain-based distributed federated learning in smart grid. *Mathematics*. 2022;10(23):4499. doi:10.3390/math10234499.
14. Koukaras P, Afentoulis KD, Gkaidatzis PA, Mystakidis A, Ioannidis D, Vagropoulos SI, et al. Integrating blockchain in smart grids for enhanced demand response: challenges, strategies, and future directions. *Energies*. 2024;17(5):1007. doi:10.3390/en17051007.
15. Haider HT, See OH, Elmenreich W. A review of residential demand response of smart grid. *Renew Sustain Energy Rev*. 2016;59:166–78. doi:10.1016/j.rser.2016.01.016.
16. Kamal MA, Raza HW, Alam MM, Su'ud MM, Abu Bakar Sajak AB. Resource allocation schemes for 5G network: a systematic review. *Sensors*. 2021;21(19):6588. doi:10.3390/s21196588.
17. Abuajwa O, Roslee M, Yusoff ZB, Chuan LL, Leong PW. Resource allocation for throughput versus fairness trade-offs under user data rate fairness in NOMA systems in 5G networks. *Appl Sci*. 2022;12(7):3226. doi:10.3390/app12073226.
18. Tang D, Guerrero JM, Zio E. Securing demand–response in smart grids against false pricing attacks. *Energy Rep*. 2024;12(4):892–905. doi:10.1016/j.egy.2024.06.068.
19. Nikoobakht A, Aghaei J. Robust inter-reliant resilience of cyber-physical smart grids. *Sustain Energy Technol Assess*. 2023;60(7291):103449. doi:10.1016/j.seta.2023.103449.
20. Veloso AFS, Reis JV Jr, Rabelo RAL. A microservices-based solution with hybrid communication for energy management in smart grid environments. *Sensors*. 2026;26(5):1714. doi:10.3390/s26051714.
21. Khunteta A, Baheti PK. QoS-aware resource scheduling for machine type communication in 5G networks. *J King Saud Univ-Eng Sci*. 2026;38(4):33. doi:10.1007/s44444-026-00107-0.

22. Ghadi YY, Mazhar T, Shahzad T, Jaghdam IH, Khan S, Khan MA, et al. A hybrid AI-blockchain security framework for smart grids. *Sci Rep.* 2025;15(1):20882. doi:10.1038/s41598-025-05257-w.
23. Saleh OA, Cevik M. Blockchain-integrated secure authentication framework for smart grid IoT using energy-aware consensus mechanisms. *Sensors.* 2025;25(21):6622. doi:10.3390/s25216622.