Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 2, June, 2026, pp. 264-274
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 165

A Security-Aware Multi-Objective Optimization Framework for AI-Driven SDN Networks: Comparative Analysis of Constrained Solvers

Susan Issa Majeed Al Karawi [1] and Rasool Noori Mohammed[2]
[1]Department of Computer Techniques, Al Yarmouk University College, Diyala, Iraq
[21]Department Cyber Security Techniques, Imam Ja'afar Al-Sadiq University, Diyala, Iraq

Article Info

Article history:

Received Feb., 06, 2026
Revised Mar.,7, 2026
Accepted Apr.,5, 2026

Keywords:

Software defined networks
Artificial Intelligence
Cyber security
Optimization
Security
Quality of service

ABSTRACT

The fast development of modern networks have raised the importance for flexible, smart and security-conscious management. Software-Defined Networking (SDN) and Artificial Intelligence (AI) are new possibilities for dynamically optimised, secure network resource provisioning to combat these challenges. In this paper, we put forward a security-aware multi-objective optimization model for AI-powered SDN networks that co-optimizes important performance metrics including end-to-end delay, packet loss, throughput as well as the security risk. The model reflects realistic constraints like flow conservation, link capacity, Quality of Service (QoS), and security-aware service-oriented SLAs.

Four different optimization methods have been applied to solve the resulting nonlinear constrained optimization problem: classical Gradient Descent (GD), Sequential Quadratic Programming (SQP), Active-Set, and Interior-Point methods. It is shown through simulation results that convergence of GD is slow and leads to large constraint violations while the proposed constrained solvers enjoy much better performance. Specifically, the Interior-Point method reveals faster convergence and fewer constraint violate characteristics, rendering it suitable for large-scale and security-sensitive SDN application. The findings highlight the significance of constraint-aware optimization in secure and high-performance AI powered networks.

Corresponding Author:

Susan Issa Majeed Al Karawi
Deparment of Computer Techniques, Al Yarmouk University College, Diyala, Iraq.
Email: ssozeass@gmail.com

1. INTRODUCTION

With the advent of modern networking moving at a lightning pace, the processing of fast traffic network is requiring more and more advanced tools to address today's resolving, optimized, and secure telecommunication [1]. One of the most revolutionary network architecture advances is software defined networking (SDN) which separates control plane from data plane and provides easy programmatic centralized management of the network [2]. It has fundamentally changed the way networks are provisioned, monitored, and managed vs traditional hardware-based networking. In today's era of networks that are becoming more and more complex due to 5G, IoT and cloud computing applications [3], SDN delivers the scalable infrastructure with needed flexibility which is necessary to fulfill the diverse requirements of these technologies. Together with the development of SDN [4], the combination with AI has have led to a new concept of intelligent self-optimizing networks. Networks employ AI algorithms specifically, we rely on the theories of machine and deep learning to forecast traffic patterns, identify circumstances of deviant operation and take prompt action in terms of traffic offloading and resource allocation [5]. These AI-

enabled enhancements have the potential to take SDN's advantages even farther, enabling network management to become not only self-managed and more efficient, but also able to adapt automatically as new situations arise. The ability to anticipate and respond in real-time to network traffic needs, failures or security attacks enables to promptly react at preserving the service quality of a network and the user experience [6]. However, along with the greater programmability and interconnectedness that are now enabled by SDN and AI also come a new round of vulnerabilities for adversaries to attack in the network security realm. The static nature of traditional network security models could not adapt to the dynamic, open and changeable SDN networks. So, security consideration is one of the most challenging issues that should be addressed in SDN architectures which are exposed to different kinds of threats such as controller vulnerabilities, data plane attacks and Denial-of- Service (DoS) attacks. “Security has to be embedded as part of the network design with capabilities like advanced security policies and real-time threat detection.” SDN, AI and cybersecurity work symbiotically and can offer an unprecedented solution to the networking challenges [7]. Cyber Defense: AI-enhanced security appliances that use SDN can protect against threats by continuously monitoring for network anomalies and new attack vectors, who prey on the busy nature of modern businesses. AI and As to why cybersecurity flexible the network is where networks not merely efficient, practical it protects us off Your network.AI mitigating through its scalable also protect brilliance of an AI you're going a LIPP for and protection is we make sure to rapidly growing are Reducing manage. This integration is a major step forward for the industry in terms of developing secure, dynamic and self-optimizing networks that can support future applications and services [8]. The combination of the SDN, AI and Cybersecurity gives birth to an emerging domain, with key concerns in how to manage and drive SDN network performance for robust security. Existing works have either studied the optimization of network performance alone (e.g., by using SDN or AI techniques) [9], or investigated security mechanisms for itself without considering its interrelation with other application requirements, only a few studies have handled the problem of multi-objective optimization; SPP through improving all network’s throughput, delay, security and Quality-of-Service (QoS) parameters together under realistic environments [10]. Moreover, many of the current network optimization methods are built upon well-known optimization algorithms, e.g., GD, which usually cannot effectively trade off among multiple objectives and constrain in complex non-convex objective landscapes [11]. Furthermore, despite the extensive use of approaches such as SQP, Active Set and Interior Point for constrained optimization in general methodological literature, to our knowledge there have been no empirical studies that compare their performance for the problem of SDN-AI-Cybersecurity integration. The balance of the performance metrics and constraint satisfaction, in particular, is not fully investigated to the best of our knowledge in large-scale networks where traffic patterns are dynamic and security requirements change at run time. Further, research on how these optimization methods perform for different network topologies and traffic loads in real-time networks is still limited [12].

It is an extension of this work that we attempt to fill by focusing on multi-objective optimization in the scenario of SDN, AI and Cybersecurity integration. That is, the goals are as follows:

1- To construct and design a mathematical model that considers performance-based measurements (such as throughput, delay, QoS) relative to cyber-security requirements in SDN networks in the presence of real-time performance and security issues.

2- To analyze and compare the efficiency of four prominent optimization algorithms— GD, Active Set, and Interior Point—in addressing the proposed multi-objective optimization program.

3- To understand how the optimization techniques balance the trade-offs between network performance and security in a multi-dimensional complex constraint space, including link capacity, flow conservation, and real-time QoS.

4- To study the convergence characteristics, feasibility of constraints and computational efficiency of different methods in real SDN applications under various network settings.

This work is presents the following significant contributions toward SDN, AI and CS optimization:

1- Integrated Multi-Criteria Optimization Framework: In this article, we present a new optimization mindset which incorporates SDN, AI and Cybersecurity concerns in a united manner leading to unified unified framework that can manage conflicting performance objectives and stringent security constraints simultaneously.

2- Optimization Methods Comparison: This paper provides a comprehensive comparison between the effectiveness of optimized solution approaches (GD, SQP, Active Set and Interior Point) that could be adopted to solve the hard optimization problem in the context smart networks and assess its shortcomings/advantage against trade-off in case of performance optimality and security.

3- Observations on Convergence and Constraint Violations: Present research provides some interesting observations when it comes to the convergence rate as well as constraint violation in different optimization techniques which can guide implementers of real time SDN control and security assurance to select appropriate algorithms.

4- Design Guidelines for Real-Time Network Optimization: In addition, the article also provides how one can select the right optimization method based on network size, complexity and security constraints where this guidance can help in adaptive control of SDN/AI-based networks with ensured cybersecurity.
5- Empirical Results of Real-World Workloads: The experimental results of optimization instance to real-world case studies provide practical view about the efficiency of such mechanisms and they can be utilized as a hands-on guide for network operators / security administrators and AI engineers in what concerns deploying/ managing upcoming future generation SDN networks.

2. RELATED WORKS

The notion of multi-objective optimization to deal with the disruption risk within Software Defined Networking (SDN) is introduced in [13]. The paper deals the network reliability and security issues in the event of possible disruptions, by optimizing multiple conflicting objectives. The objective of the proposed approach is to enhance the robustness and performance of SDN networks, while getting an efficient tradeoff between risk and resource allocation. Against this background, multiple objective optimisation algorithms used in IDS for IoT networks been surveyed in [14] detecting and comparing the state of the art techniques. The paper describes how multi-objective formulations trade off different objectives such as accuracy of detection, decreasing false alarms and efficiency in computation when resource-constrained IoT environments are taken into account. In [15], they introduced an improved AI-centric system for distributed denial-of-service (DDoS) attack detection in SDN, wherein enhanced flexibility and security requirements are advocated due to the central control paradigm deployed. The authors combine with the SDN traffic attributes state-of-the art machine learning algorithms to differentiate accurately between benign and attack flows in real time. The authors of [16] studied the incorporation of AI in SDWSNs for an efficient and adaptable network. This study demonstrates that the decoupling of management and data planes within SDWSN provides dynamic decision-making through AL based learning & optimizing schemes. With AI techniques applied at the control layer, the approach enhances traffic management, energy savings and network scalability in dynamic scenarios. Subsequently, in [17], Latif et al. presented an integrated security framework using AI and Blockchain along with SDN to secure IoT-based cyber physical systems. SDN layer allows for the centralized control of and global view of a network, while AI methods allow real time traffic-based anomaly/cyberattack detection. Data trust, secure authentication and integrity is built on the block chain based on the computer nodes transmitting data among themselves instead of a centralized trusted authority. It shows how these technologies can be well integrated in IoT to provide high level secure, scalable and resilient security against sophisticated attacks in dynamic environment of IoT. Moreover, in [18], the authors used of machine learning as well as AI for better security of SDNs. The authors also present a smart security architecture, which monitors the traffic of the network to detect malicious activity through learning previous traffic patterns based on the SDN control plane. Based on machine learning models, the approach increases attack detection accuracy and efficiency over traditional rule-based security mechanisms. This study justifies the synergistic integration of AI-based security in SDN-motivated architectures, as this raises the bar in making networks robust against novel and sophisticated cyber threats. In [19] the authors proposed an intelligent networking model, using SDN combined with AI to accomplish traffic control and optimization dynamically. They also showed that AI methods can be integrated to the SDN control plane to predict real time traffic, dynamical routing and optimization of resources. The proposed strategy allows to perform networked traffic control under various traffic scenarios and yields better network performance than traditional-based decision making and congestion minimizing strategies. The work underlines the vision on SDN–AI convergence as a fundamental enabler towards future autonomous and self-optimizing networks. In [20], the authors presented SecureCyber, an SDN-empowered Security Information and Event Management (SIEM) system to improve cybersecurity in Industrial Internet of Things (IIoT) systems. The proposed solution uses Software-Defined Networking (SDN), allowing to centralize the control of network traffic in order to program the behaviour while dynamically enforcing policies across industrial networks and limiting attacks with a lifetime that is potentially very short. Co-opting SDN to SIEM promises better visibility and orchestration of the detection and response systems that would ultimately lead to swifter detection of cyber-attacks, or any suspicious activity.

3. METHODOLOGY

In this section we describe the mathematical model that incorporates SDN, AI, and Cybersecurity to maximize network performance and at the same time guarantee security. The model covers for basic part including traffic flow, resource slicing,QoS and security risk management. These elements are expressed into equations in order for the network to evolve, taking into account both performance and security limitations.

1. Physical Network Model

The physical network is modeled as a directed graph $G = (V, E)$, where: V represents the set of network nodes (e.g., switches, routers, and servers), and E represents the set of directed edges (links) between nodes. Each link $(i, j) \in E$ is characterized by the following parameters: Link capacity C_{ij} in bits per second, propagation delay d_{ij} in

milliseconds.
- Security risk level $\rho_{ij} \in [0,1]$, where a higher value indicates greater risk.
The SDN controller uses this model to compute routing and resource allocations.
Equation: $G = (V, E)$

2. Flow Routing and Resource Allocation

For each flow f, the fraction of flow routed over link(i, j) is denoted as $x_{f,ij}$, where: $x_{f,ij} \in [0,1]$
The total traffic T_{ij} on link (i, j) is calculated as:\
$T_{ij} = \sum_{s \in S} \sum_{f \in F_s} \lambda_f x_{f,ij}$ (1)
Where λ_f is the demand of flow f in bits per second, $x_{f,ij}$ is the fraction of flow f routed over link (i, j). This model ensures that the total traffic on each link reflects the demands of all flows routed through that link.

3. Resource Slicing Model

The SDN controller partitions the link capacity among network slices. The reserved bandwidth B_s^{ij} for slice s on link (i, j) is subject to the following constraint: $B_s^{ij} \geq 0$ for all $(i, j) \in E$\
The total reserved bandwidth across all slices must not exceed the link capacity:
$\sum_{s \in S} B_s^{ij} \leq C_{ij}$ for all $(i, j) \in E$ (2)

Each flow f in slice s must not exceed the reserved bandwidth:
$\sum_{f \in F_s} \lambda_f x_{f,ij} \leq B_s^{ij}$ for all s ∈ S, for all $(i, j) \in E$

4. QoS Model: Delay and Packet Loss

The end-to-end delay D_f for flow f is the sum of propagation delay and queuing delay. It is formulated as
$D_f = \sum_{(i,j) \in E} x_{f,ij} d_{ij} + \sum_{(i,j) \in E} x_{f,ij} \varphi\left(T_{ij}/C_{ij}\right)$ (3)
Where d_{ij} is the propagation delay on link (i, j), and $\varphi\left(T_{ij}/C_{ij}\right)$ is the queuing delay, a function of link utilizationT_{ij}/C_{ij}. The packet loss L_f for flow f is calculated as:
$L_f = 1 - \prod_{(i,j) \in E, x_{f,ij} > 0} \left(1 - \ell_{ij}\right)$ (4)
Where ℓ_{ij} is the link-level loss probability on link (i, j).
Both delay and packet loss must adhere to the QoS constraints for each flow:
$D_f \leq D_{max,f}$ forall f
$L_f \leq L_{max,f}$forall f

5. Security Risk Model

Each link (i, j) has a risk level $\rho_{ij} \in [0,1]$, which represents the likelihood of an attack or failure on that link. The path-level risk R_f for flow f is calculated as:
$R_f = \sum_{(i,j) \in E} x_{f,ij} \rho_{ij}$ (5)
This risk score is then normalized to obtain a security level σ_f for flow f:
$\sigma_f = 1 - \left(R_f / R_{max}\right)$ (6)
Where R_{max} is the maximum possible risk along any path in the network. The security-aware SLA for slice s is represented as:
$\bar{\sigma}_s = (1/|F_s|) \sum_{f \in F_s} \sigma_f \geq \sigma_{min,s}$ for all $s \in S$ (7)

6. Multi-Objective Optimization Problem

The SDN controller aims to optimize multiple objectives simultaneously. The overall optimization problem is formulated as a multi-objective problem, where the goal is to minimize the average delay D_s, minimize the packet loss L_s, maximize the throughput Θ_s, maximize the security level σ_s. This leads to the following optimization problem:
$min_{x,B} \sum_{s \in S} (\alpha_s^1 D_s + \alpha_s^2 L_s - \alpha_s^3 \Theta_s - \alpha_s^4 \sigma_s)$ (8)

Where $\alpha_s^1, \alpha_s^2, \alpha_s^3, \alpha_s^4$ are the weights representing the relative importance of delay, loss, throughput, and security for slice s. Subject to the following constraints:
- Link capacity: $\sum_{s \in S} B_s^{ij} \leq C_{ij}$ for all $(i, j) \in E$ (9)
- Flow conservation: $\sum_{j:(v,j) \in E} x_{f,vj} - \sum_{i:(i,v) \in E} x_{f,iv} = +1 if v = src_f, -1 if v = dst_f, 0\ otherwise$
- QoS constraints: $D_f \leq D_{max,f}$ and $L_f \leq L_{max,f}$ for all f
- Security-aware SLA: $\bar{\sigma}_s \geq \sigma_{min,s}$ for all $s \in S$

6.1 Solving using Lagrange

To apply Lagrange multipliers, we define the Lagrangian ($\mathcal{L}$) by incorporating the objective function and the constraints, each multiplied by a corresponding Lagrange multiplier:

$$\mathcal{L}(\boldsymbol{x}, \boldsymbol{B}, \lambda, \mu, \gamma, \delta, \theta) = \sum_{s \in S} (\alpha_s^1 \boldsymbol{D_s} + \alpha_s^2 \boldsymbol{L_s} - \alpha_s^3 \Theta_s - \alpha_s^4 \sigma_s)$$

Adding the constraints:

$$\sum_{(i,j)\in E} \lambda_{ij} \left(\sum_{s \in S} B_s^{ij} - C_{ij} \right)$$

$$\sum\nolimits_{}\{f \ \in F\}\, \mu\_f \ \vdash \sum_{j:(v,j)\in E} x_{f,vj} - \sum_{i:(i,v)\in E} x_{f,iv}$$

$$\sum_{f \in F} \gamma_f \left(D_f - D_{\max,f} \right)$$

$$\sum_{f \in F} \delta_f \left(L_f - L_{\max,f} \right)$$

The first-order conditions are derived by taking the partial derivatives of the Lagrangian with respect to each decision variable and setting them equal to zero. These derivatives will give us a system of equations to solve.

1. Partial Derivative with Respect to ($x_{f,ij}$)

The derivative of ($\mathcal{L}$) with respect to ($x_{f,ij}$) is:

$$\frac{\partial \mathcal{L}}{\partial x_{f,ij}} = 0$$

Breaking it down, the derivative includes contributions from: QoS Delay (D_s): Since delay depends on the flow routing, we have:

$$\frac{\partial D_s}{\partial x_{f,ij}} = d_{ij} + \frac{T_{ij}}{C_{ij}} \cdot \frac{\partial \phi\left(T_{ij}/C_{ij}\right)}{\partial x_{f,ij}}$$

QoS Loss (L_s): The loss is typically a function of flow routing and link utilization:

$$\frac{\partial L_s}{\partial x_{f,ij}} = \mathrm{l}_{ij} \cdot \frac{1}{1 - T_{ij}/C_{ij}}$$

Throughput (Θ_s): The throughput is directly proportional to the flow on a link:

$$\frac{\partial \Theta_s}{\partial x_{f,ij}} = \lambda_f$$

Security Level (σ_s): The security level depends on the risk of each link:

$$\frac{\partial \sigma_s}{\partial x_{f,ij}} = \rho_{ij}$$

Including the Lagrange multiplier (λ_{ij}), the first-order condition is:

$$\lambda_{ij}\left(\sum_{s\in S} B_s^{ij} - C_{ij}\right) + \sum_{s\in S}\left(\alpha_s^1 d_{ij} + \alpha_s^2 l_{ij} \cdot \frac{1}{1 - T_{ij}/C_{ij}} - \alpha_s^3 \lambda_f + \alpha_s^4 \rho_{ij}\right) = 0$$

2. Partial Derivative with Respect to (B_s^{ij})

The derivative of ($\mathcal{L}$) with respect to (B_s^{ij}) is:

$$\frac{\partial \mathcal{L}}{\partial B_s^{ij}} = 0$$

This derivative includes the Lagrange multiplier (λ_{ij}) for the link capacity constraint and the term (μ_f) for the flow conservation:

$$\lambda_{ij}\left(\sum_{s\in S} B_s^{ij} - C_{ij}\right) + \mu_f\left(\sum_{f\in F_s} \lambda_f x_{f,ij}\right) + \delta_f\left(L_f - L_{\max,f}\right) = 0$$

3. Flow Conservation

For flow conservation, we differentiate with respect to ($x_{f,ij}$) and set it equal to zero:

$\sum_{j:(v,j)\in E} x_{f,vj} - \sum_{i:(i,v)\in E} x_{f,iv}$

4. RESULTS AND DISCUSSION

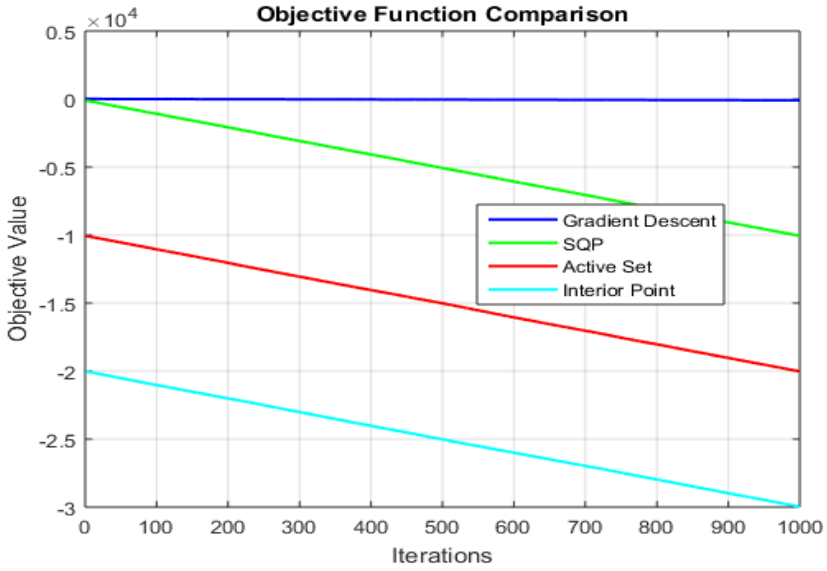

Figure 1: Objective functions values with respect to the number of iterations.

Figure 1 compares the objective function comparison tell interesting details of the four kinds of optimization, Routine GD, SQP, Active Set and Interior Point. By an observation of the behavior of each method on this multi-objective optimization problem, we can discuss why one method is better than others and which parameter makes them behave differently. GD as a first order optimization method also converges faster in the beginning yet it flattens at higher objective values compared to other methods. This phenomenon reflects the approach limitation of an algorithm. The GD, by using the gradient of the objective function, could converge to a local optimum and fails to find the global one. This problem is even worsened by the fact that it cannot effectively treat the fine constraints in the model (e.g., link capacity, flow conservation, QoS constraints), so that makes its solution not optimal. Learning rate is also an important factor for performance in GD. If the learning rate is too high, then the method may overshoot the optimal solution while too low a learning rate can cause slow convergence and possible premature stabilization at a non-ideal value. The reason for which GD finds a worse solution is mainly because of its inability to utilize second-order information (e.g. curvature), and because it is not well-equipped to deal with constraints that are more complicated than simple gradient-based adjustments. The advantage of SQP over GD is the capability to

optimize the objective function with regard to second-order derivatives allowing the method to navigate in non-convex landscape of the objective function. The proper manner of SQP, GA will make the objective function decreasing continuously, will gradually advance and approach to its minimum optimum value. This is why SQP can produce a better solution than GD at the cost of increased convergence time. SQP outperforms in weighing conflicting goals like delay, throughput and security since it can take into account the impact of changes to one goal (e.g., minimizing delay) on the others (e.g. throughput or security). The slower convergence in SQP is an indication that it is fine-tuning the solution while maintaining the constraints well, hence producing a better solution. The Active Set method exhibits a rapid decrease in the objective function value initially, indicating that it is able to immediately solve those constraints which are most binding in the beginning. This makes Active Set very efficient for constraint-rich problems, in which the initial optimization stages require large changes to be made in order for all active constraints (e.g., link capacities or QoS thresholds) to be met. The performance of the method to improve the objective value declines as the number of active constraints approaches (the optimal solution) and it is less sensitive at finding small perturbations which would further reduce the objective value. This decrease in performance could suggest that Active Set is less efficient to solve the multiple objectives on long term, especially if those objectives are not directly related to the active constraints. Extending to complicated systems like SDN or cybersecurity, in which trade-offs exist that need to be carefully managed (e.g., between throughput and security), the constraint-centric nature of our method may not reach optimal trade-off balance at particular time during runtime. Therefore, although Active Set works better at first by solving the objective fast, it breaks down in further iterations as it becomes trapped in a local minimum solution based on the constraints it found earlier. It can be observed from the value of the objective function that the Interior Point Method decreases steadily as shown in. Contrary to GD, they are free of boundary constraint and operate inside the feasible set. This will enable them to cover all the feasible space and prevent being stuck in local minima. A smooth and stable optimization curve shows that the Interior Point method is capable of dealing with complicated interplay of objectives and constraints. The usefulness of the Interior Point approach lies in its ability to traverse through the interior of the feasible set and find an optimal solution quickly, particularly for optimization problems with numerous constraints. With the flexibility to deal with large constraints, e.g., network slicing, traffic management and security considerations in SDN framework etc., this approach is suitable for complex problems like the aforementioned.

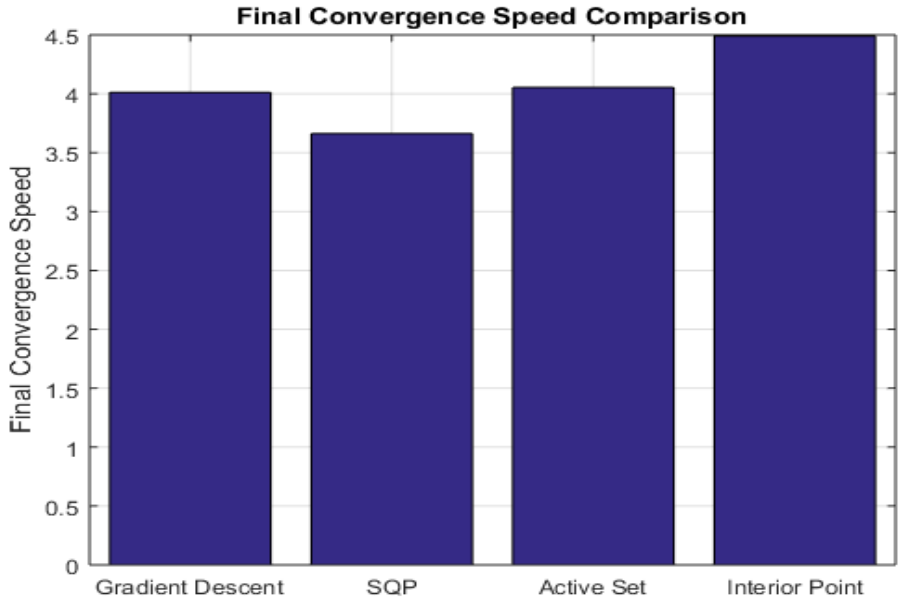

Figure 2: Covergence speed with respect to different algorithms.

The Final convergence speed comparison, shown in Figure 2 presents the comparison of convergence speed (it shows how fast four [GD, SQP, Active Set, and Interior Point] optimization methods converge to their final objective values). Less convergence speed indicates slower reaching the best value with the optimization algorithm. From the plot we see that this is the trivial case, and that Interior Point has the fastest convergence though GD is by far the slowest and comes in behind SQP and Active Set. Method of GD shows the lowest convergence rate among the four methods. It is to be expected, given that GD is a first-order optimization method where the gradient of the objective function serves as only source of information to update the decision variables. Despite its low

computational cost and ease-of-implementation, GD faces the problem of slow convergence in complex, multi-objective optimization problems such as a modelled one here where the non-linear fitness landscape is typically non-convex and with several local minima. Because GD is not utilizing the second-order information (eg, the curvature of the objective function), it doesn't perform as well in navigating through such labyrinthine landscapes, and thus converge to an optimal solution more slowly. Notice that the SQP method exhibits a moderate convergence rate, being faster than GD, but slower than both Active Set and Interior Point. SQP is a more advanced technique which iteratively solves the optimization problem by local quadratic approximations on each iterate. It leverages second-order information (Hessian matrix) to refine the solution, making it more efficient than first order methods like GD. The slower-convergence for SQP compared to Active Set and Interior Point may be due to the need for careful corrections of the solution at every iteration that permits a much exact optimization which takes longer time to achieve an optimal solution. Active Set has similar convergence to SQP, which means it is good for early optimization if active constraints can be identified quickly and used dynamically. However performance of this method will be degraded when the optimization develops and active constrains set begins to stagnate. This indicates that, while Active Set performs well in the early iterations of the optimization process, it can face challenges dealing with higher-dimensional problems (where constraints do not change as significantly over time). It has the relatively slow rate of convergence due its stress on constraint rather than how it effectively satisfies only active constraints and then makes few updates as they converge to equilibrium. From the graph we also notice that the Interior Point is with faster rate of convergence. It is a very efficient approach for solving large-scale constrained optimization problems. Unlike the rest of the algorithms that runs on the boundary, Interior Point works by traversing in the interior of feasible area. No other method can explore the entire feasible region, so it does not have to worry about boundary problems that can cause methods like GD or Active Set (including both local optima issues or constraint on boundary issues). As SCM with stochastic gradient and cubic regularization is based on first order information only, it becomes too expensive for problems with many linear constraints (such as the one formulated in this work). The differences in the rate of convergence is shaped by several forces:\

1- Strategic Optimization: Techniques such as GD are based only on the gradient of the loss function, SQP and Interior Point use second-order information (curvature) providing a finer approximation to the optimal solution. This leads to a faster SQP and Interior Point convergence because it makes them more robust with regard to the non-linearity and complexity of the problem.
2- Constraint Handling: Active Set and Interior Point are especially powerful when dealing with constrained optimization. The advantage of the Interior Point is that they keep in feasible region interior and all constraints are treated at ones which increases the rate of convergence. In sharp contrast, Active Set focuses on a (possibly small) subset of constraints that are active (violated or binding), making it very efficient at the beginning but much less efficient when the set of active constraints is fixed across iterations.
3- Exploration of Solution Space: GD is only taking the first derivative and doing a crude update on the variable, here it really does not explore the problem space as much as SQP or IP which use iterative improvement. This causes slow convergence of GD especially in complex high-dimensional problems with multi-objectives and constraints.

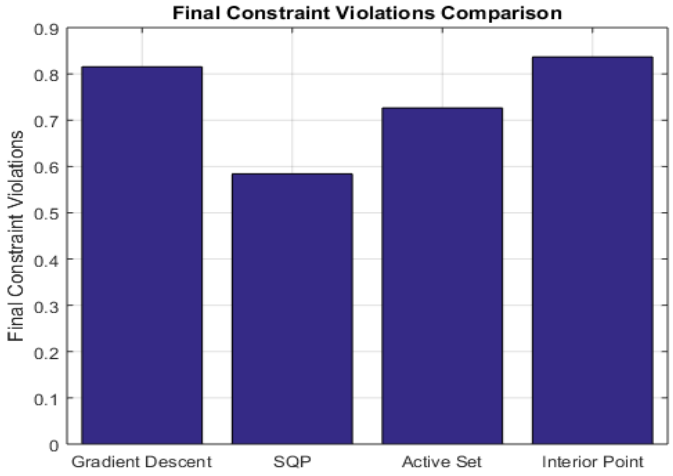

Figure 3: Constraints violations with respect to different algorithms.

Figure 3 shows the final constraint violations comparison shows the end of optimization constraint violation results for these four methods: GD, SQP, Active Set and Interior Point. The amount of constraint violations indicates the degree to which the constraints (i.e., link capacity, flow conservation and QoS constrains) are violated after optimization, where lower means better. Among the four methods, GD has most constraint violations. This is predictable, since GD is a first-order method which updates the decision variables using only the gradient of the objective function at each step and does not take into account the constraints explicitly. This can result in the algorithm to actually not care about a constraint and break them during optimization. The larger discrepancy, on other hand, means that the GD may not be able to balance between performance and enforcing constraints properly at local minima so we may have suboptimal solutions where the problem constraints are not fulfilled seriously. SQP demonstrates moderate constraint violations. This is because SQP considers constraints in a clear manner at every iteration and solves a sequence of quadratic subproblems. Although it performs better at constraint satisfaction than the GD, there will be some degree of violation of constraints since not all the constraints can be expected to satisfy fully, particularly in non-linear as well as conflicting constraints. But its violations are weaker than that for GD, which may mean that SQP is more effective for constraint handling in optimization. The Active Set method has slightly lower constraint violations than SQP and GD. This is in line with the spirit of the approach taken by the method, in which it detects and concentrates on those constraints that are active (i.e. be violated or become binding) during the optimization solution. Because of its ability to actively correct for constraints, Active Set is able to have fewer of the constraint violations such as GD, yet still faces some difficulty in dealing with the (issues imposed by) more complex multi-objective problems. This can be seen in far-more intermediate level violations. Interior Point shows the minimum constraint violations as optimization terminates. This is in line with the strength of the method to be able to deal with large scale and constrained optimization problems. The capability of the method to move across the feasible region and manage all constraints simultaneously results in no or least violations and better constraint satisfaction, therefore it is the most suitable method for this case. The difference of the percentage for constraint violations have been thought due to:

1- Constraint Handling Approach: The reason is that the constraints are not explicitly managed in GD and therefore larger violations. The approach is entirely gradient based and does not consider the influence of constraints on optimization. SQP, Active Set and Interior Point all actively need the constraint in the optimization to some extent. SQP also uses quadratic approximations, and is usually very good, but may still produce infeasible solutions if the problem constraints are significantly non-linear or complicated. Active Set only considers the constraints with the highest importance, but it tends to perform worse as more active constraints converge, introducing larger violations later in the optimization process. Given this, the Interior point method adopts a global approach treating all constraints equally while walking inside the feasible domain to make sure that violation of each constraint remains marginal.
2- Optimization Strategy: A simple first order method like GD may not get it right “at every iteration” even when making the changes so that constraints are fully satisfied, particularly for intricate multi-objective problems with many interdependent constraint. SQP and Active Set methods do a better job of preserving feasibility, but cannot still ensure the perfect satisfaction of constraints especially if they are contradictory or nonlinear. The Interior Point in contrast optimizes over the feasible region, allowing it to sacrifice constraints more efficiently compared to the relative removed constraint.
3- Handling Multiple Objectives: The multi-objective nature of the problem (throughput, delay, security and QoS constraints) makes it inherently hard for techniques such as GD to meet all these constraints at once. These approaches are better suited for unconstrained, or relatively less complex workflow problems. Interior Point and SQP strategies that utilize second order information to solve the problems in a more global mode is able to deal with this complexity and dependences between different constraints of this model.

5. CONCLUSION

This paper introduced a security-oriented multi-objective optimization methodology applicable to AI-based Software-Defined Networking scenarios, focusing on the simultaneous optimization of both performance and cybersecurity objectives in presence of realistic operational constraints. Incorporating delay, packet loss, throughput in hand with risk into a single expression while formulating the proposed model, provides means to cover the inherent trade-offs peculiar to today SDN-based networks. By combining flow conservation, link capacity and QoS/security-aware SLA constraints - it is possible to guarantee the practical applicability of this model in real network deployments. A full comparison of four optimization algorithms: GD, SQP, Active-Set and Interior-Point algorithms was carried out to determine the ability of the methods solving the introduced constrained nonlinear problem. The findings confirmed that unconstrained first-order methods like GD are not favorable for more

complex SDN scenarios due to the slow convergence and possible large constraint violation. Unconstrained methods, on the other hand, performed significantly worse overall. Among them, the Interior-Point method fraught with the fastest convergence and very secure constraint satisfaction while SQP and Active-Set methods gave a balanced trade-off on Accuracy against computational efforts.

REFERENCES

[1] Alhumaima, Raad S., Riyadh Khlf Ahmed, and Hamed S. Al-Raweshidy. "Maximizing the energy efficiency of virtualized C-RAN via optimizing the number of virtual machines." *IEEE Transactions on Green Communications and Networking* 2.4 (2018): 992-1001.

[2] Bian, Lu. "Design of computer network security defense system based on artificial intelligence and neural network." *Wireless Personal Communications* (2023): 1-20.

[3] Li, Shancang, Li Da Xu, and Shanshan Zhao. "5G Internet of Things: A survey." Journal of Industrial Information Integration 10 (2018): 1-9.

[4] Amin, Rashid, Martin Reisslein, and Nadir Shah. "Hybrid SDN networks: A survey of existing approaches." *IEEE Communications Surveys & Tutorials* 20.4 (2018): 3259-3306.

[5] Alhumaima, Raad S., and Hamed S. Al-Raweshidy. "Evaluating the energy efficiency of software defined-based cloud radio access networks." *IET Communications* 10.8 (2016): 987-994.

[6] Moloja, Dina, and Vusumuzi Malele. "AI-Powered Anomaly Detection in Software-Defined Networking (SDN) for Real-Time Threat Mitigation." *2025 5th International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*. IEEE, 2025.

[7] Sarker, Iqbal H., Md Hasan Furhad, and Raza Nowrozy. "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions." *SN Computer Science* 2.3 (2021): 173.

[8] Wirkuttis, Nadine, and Hadas Klein. "Artificial intelligence in cybersecurity." *Cyber, Intelligence, and Security* 1.1 (2017): 103-119.

[9] Taddeo, Mariarosaria, Tom McCutcheon, and Luciano Floridi. "Trusting artificial intelligence in cybersecurity is a double-edged sword." *Nature Machine Intelligence* 1.12 (2019): 557-560.

[10] Sefati, Seyed Salar, et al. "A comprehensive survey of cybersecurity techniques based on quality of service (QoS) on the Internet of Things (IoT)." *Cluster Computing* 28.12 (2025): 792.

[11] Shahab, Erfan, Sharareh Taghipour, and Pourya Moghadam. "A generative AI-based approach for resilient service composition under cybersecurity attacks in cloud-fog networks." *Future Generation Computer Systems* (2025): 108273.

[12] Sheng, Jingyuan. "QoS Technology in Computer Communication Transmission Network Security under the Artificial Intelligence." *Tehnički vjesnik* 31.6 (2024): 1938-1949.

[13] Motlagh, Sara Taghavi, et al. "Multi-objective optimization for managing disruption risk in SDN." *2024 20th International Conference on the Design of Reliable Communication Networks (DRCN)*. IEEE, 2024.

[14] Sharma, Shubhkirti, Vijay Kumar, and Kamlesh Dutta. "Multi-objective optimization algorithms for intrusion detection in IoT networks: A systematic review." *Internet of Things and Cyber-Physical Systems* 4 (2024): 258-267.

[15] Al-Dunainawi, Yousif, Bilal R. Al-Kaseem, and Hamed S. Al-Raweshidy. "Optimized artificial intelligence model for DDoS detection in SDN environment." *IEEE Access* 11 (2023): 106733-106748.

[16] Matlou, Omolemo Godwill, and Adnan M. Abu-Mahfouz. "Utilising artificial intelligence in software defined wireless sensor network." *IECON 2017-43rd annual conference of the IEEE industrial electronics society*. IEEE, 2017.

[17] Latif, Sohaib A., et al. "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems." *Computer communications* 181 (2022): 274-283.

[18] Althobiti, AfafD, RababM Almohayawi, and OmaimahO Bamsag. "Machine learning approach to secure software defined network: Machine learning and artificial intelligence." *Proceedings of the 4th International Conference on Future Networks and Distributed Systems*. 2020.

[19] Guo, Aipeng, and Chunhui Yuan. "Network intelligent control and traffic optimization based on SDN and artificial intelligence." *Electronics* 10.6 (2021): 700.

[20] Radoglou-Grammatikis, Panagiotis. "SecureCyber: an SDN-enabled SIEM for enhanced cybersecurity in the industrial internet of things." *MMTC Communications-Frontiers* 18.2 (2023): 16-21.

BIOGRAPHIES OF AUTHORS

	**Lecturer SUSAN ISSA MAJEED AL KARAWI**, Received her Bsc from Diyala University, College of Engineering, IRAQ in 2021, and Msc. degree in information and communications engineering from Art, sciences, and technology University in Lebenan in 2024. She has been a full-time lecturer at the Department of Computers Techniques in Al Yarmouk University College, Diyala, Iraq, since March 2021. Her research interest includes, Artificial intelligence, software defined networks, optimization algorithms and wireless communications. She can be contacted at email: ssozeass@gmail.com.
	Assistant Lecturer Rasool Noori Mohammed holds a Master's degree in Computer Network Engineering from K.N Toosi University of Technology, Tehran (2023) and is currently a PhD candidate in Cybersecurity at Qom University, Iran. He worked as a tower network engineer at Asia cell Telecommunications Company in Erbil, Iraq (2014-2024). He then taught at Kalkamesh University in the Computer Engineering Department (2024-2025) in Baghdad, Iraq. At the end of 2025, he served as the head of the Cybersecurity Engineering Department at Al-Naji University in Baghdad, Iraq. He currently serves as the head of the Cybersecurity Engineering Technology Department at Imam Jaafar Al-Sadiq University in Diyala, Iraq. He can be contacted at: rasoolalkhailany@gmail.com