Title	Author	Problem Domain	proposed solution	proposed work	algorithm used	advantages	disadvantages	metrics
A Multi-Protocol Software-Defined Networking Solution for the Internet of Things	Tryfon Theodorou George Violettas Polychronis Valsamas Sophia Petridou Lefteris Mamatas	Integration and scalability challenges of IoT devices using various communication protocols with traditional network infrastructures.	A multi-protocol SDN solution that centralizes control and manages diverse IoT communication protocols effectively.	Architecture design for integrating SDN in IoT networks, with implementation focusing on flexible, software-based control and protocol management.	SDN-based routing algorithms for dynamic protocol handling and network optimization.	Enhanced scalability Protocol interoperability Centralized control Improved network efficiency	Increased overhead Potential latency Security concerns Higher energy consumption	Throughput Latency Packet Loss Scalability Energy Efficiency Interoperability
AI-Assisted Framework for Green-Routing and Load Balancing in Hybrid Software-Defined Networking: Proposal, Challenges and Future Perspective	Richard Etengu Saw Chin Tan Lee Ching Kwang Fouad Mohammed Abbou Teong Chee Chuah	Challenges in achieving energy efficiency, load balancing, and high performance in hybrid SDN/OSPF networks amid increasing data traffic demands.	An AI-assisted framework leveraging Deep Reinforcement Learning (DRL) for predictive and adaptive energy-efficient routing and load balancing in hybrid SDN/OSPF networks.	Develop and implement an AI-assisted framework using DRL for optimized energy-efficient routing and load balancing in hybrid SDN/OSPF networks.	Deep Reinforcement Learning (DRL) for dynamic, adaptive routing and load balancing.	Predictive Adaptive Efficient Scalable	Complex Overhead Challenging	Throughput Latency Packet Loss Energy Efficiency Quality of Service (QoS)
An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security	Waseem Iqbal Haider Abbas Mahmoud Daneshmand Bilal Rauf Yawar Abbas Bangash	IoT security challenges due to the rapid adoption and diverse threats.	Integration of SDN with IoT for enhanced security through network-based deployment models and SDSec technology.	Review of IoT security requirements, SDN integration, and SDSec-based models.	Not focused on specific algorithms; discusses SDN integration	Confidentiality Integrity Non-repudiation Privacy Authentication	Complexity Overhead Standardization	Confidentiality Integrity Non-repudiation Privacy Authentication
DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges Problem	Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks targeting Software Defined Networks (SDNs).	The paper reviews and categorizes existing solutions to mitigate DoS and DDoS attacks in SDNs, focusing on intrinsic and extrinsic approaches.	The paper reviews and categorizes existing solutions to mitigate DoS and DDoS attacks in SDNs, focusing on intrinsic and extrinsic approaches.	Comprehensive survey of state-of-the-art solutions addressing DoS and DDoS attacks in SDNs. Categorization of solutions based on detection, mitigation, prevention, or graceful degradatio	Not specified as the paper focuses on surveying existing solutions rather than proposing a specific algorithm.	Comprehensive	Variable	Bandwidth Memory CPU Utilization
Toward an optimal solution against Denial of Service attacks in Software Defined Networks	Muhammad Imran Muhammad Hanif Durad Farrukh Aslam Khan Abdelouahid Derhab	Vulnerability of Software Defined Networks (SDN) to Denial of Service (DoS) attacks due to centralized control.	Review and classification of DoS mitigation approaches in SDN and identification of their limitations to propose features for an optimal solution.	Classification of DoS mitigation strategies into three categories based on their methodology and analysis of limitations in these strategies.	Various DoS miti	Comprehensive Categorized Innovative	Complex Static Limited	performance Resource Utilization Scalability Attack Resilience

Emerging DDoS Attack Detection and Mitigation Strategies in Software-Defined Networks: Taxonomy, Challenges, and Future Directions	Ismael Amezcua Valdovinos Jesús Arturo Pérez-Díaz Kim-Kwang Raymond Choo Juan Felipe Botero	DDoS attack detection and mitigation in Software-Defined Networks (SDN).	A systematic review of DDoS detection strategies and a new taxonomy for mitigation, incorporating emerging technologies like NFV, blockchain, honeynet, network slicing, and MTD.	providing a taxonomy of detection methods, discussing SDN security challenges, and identifying future research directions.	Statistical mechanisms, machine learning, Network Function Virtualization (NFV), honeynet, Moving Target Defense (MTD), network slicing.	Flexibility Scalability Efficiency Innovation	Complexity Vulnerability Bottlenecks Latency	Detection accuracy Entropy comparison Flow management Network performance
Secure Software-Defined Networking Communication Systems for Smart Cities	Mohamed Rahouti Kaiqi Xiong Yufeng Xin	Security challenges in Software-Defined Networking (SDN) for smart cities	including emerging technologies like NFV, blockchain, honeynet, network slicing, and MTD.	taxonomy of detection methods, discussing security challenges in SDN, and identifying future research directions.	algorithms for DDoS detection and mitigation strategies.	Efficient Scalable Flexible	Complexity Costly Vulnerability	Throughput Latency Packet Loss Security Breach Rate
Software Defined Networking Architecture, Security and Energy Efficiency: A Survey	Danda B. Rawat Swetha R. Reddy	Exploring SDN architecture, security threats, and energy efficiency solutions.	Categorization of security threats and energy efficiency strategies in SDN.	Survey of recent techniques and challenges in SDN security and energy efficiency.	Not explicitly stated; focuses on SDN architecture and management techniques	Flexibility Efficiency Programmability	Vulnerability Complexity Cost	Performance Security Energy Consumption
Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)	Aayush Pradhan Rejo Mathew	Addressing security vulnerabilities and threats in SDN architecture.	Overview of vulnerabilities, threats, and proposed security solutions for SDN.	Discusses the architecture of SDN and offers solutions to enhance its security.	Entropy Analysis SSL Encryption ARP Authentication Bot Management Password Protection	Programmability Efficiency Scalability	Vulnerability Complexity Resource Intensive	Security Posture Network Performance Response Time
Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects	Shahbaz Siddiqui Sufian Hameed Syed Attique Shah Ijaz Ahmad Adel Aneiba Dirk Draheim Schahram Dustdar	Challenges in managing IoT networks due to resource limitations and complexity.	Utilization of Software-Defined Networking (SDN) for effective IoT management.	Systematic Literature Review of SDN-based IoT frameworks from 2010 to 2022.	Open Flow slection algorithm	Scalability Flexibility Efficiency Programmability Security	Complexity Cost Interoperability Latency Reliability	Fault Tolerance Energy Management Load Balancing Security Service Provisioning Scalability

Towards Security Automation in Software Defined Networks	Noe M. Yungaicela-Naula Cesar Vargas-Rosales Jesús Arturo Pérez-Díaz Mahdi Zareei		complex networks manual intervention	Implement automated security solutions with classifications based on automation levels and use AI for reactive and proactive defenses.	Conduct a comprehensive analysis of SDN security solutions and identify challenges in security automation.	Machine Learning (Decision Trees, SVM, Random Forests), Deep Learning (CNN, RNN, Autoencoders), Reinforcement Learning (Q-Learning, DQN, Policy Gradient), Adversarial Learning (GANs), NFV Techniques (Service Function Chaining), MTD Strategies (Dynamic Reconfiguration), and Cyber Deception (Honeypot Deployment).	Efficiency Speed Scalability Consistency	Complexity Cost Reliability Adaptability	Automation Level Processing Resources Storage Requirements Implementation Time