Alqalam Journal of Medical and Applied Sciences. 2026;9(6):1736-1741
https://doi.org/10.54361/ajmas.269639

Review article

Control Management and Configuration Plans in Network Devices: A Comparative Analysis of Traditional and Emerging Paradigms

Wafa Souysi[1]*, Nuredin Ahmed[2]

[1]*Department of Information Engineering, Libyan Academy for Postgraduate Studies, Tripoli, Libya*
[2]*Department of Computer Engineering, University of Tripoli, Tripoli, Libya*
Corresponding email. *flowerconction@gmail.com*

Abstract
Modern computer networks are undergoing a fast paradigm shift toward software-defined architectures to conquer the complexities and restrictions associated with traditional network management. This paper aims to provide a comprehensive analytical and comparative study of prominent prior literature focusing on configuration management and control plans in network devices. By reviewing and classifying some selected recent academic papers, this study highlights the fundamental differences between traditional hardware-centric approaches and emerging software-based paradigms, evaluated against criteria such as operational efficiency, flexibility, and security. The analytical findings reveal that the shifting toward centralized and programmable control mechanisms significantly reduces human configuration errors and enhances network agility, despite ongoing challenges regarding security and system stability. This paper contributes a structured reference framework that assists researchers and network engineers in understanding current gaps and identifying future directions for developing more efficient and reliable networking environments.
Keywords. Configuration Management, Control Planes, Network Devices, SDN.

Introduction

The rapid expansion of emerging technologies like IoT, 5G, and AI has caused a major paradigm shift in network management from traditional manual systems to intelligent, automated solutions, which are capable of real-time analysis and proactive decision-making [1]. The implementation of the aforementioned advanced tools and modern infrastructures showed critical benefits such as predictive AI-driven monitoring, customized 5G network slicing for specific performance needs, minimized human configuration errors, and significantly improved operational efficiency that can reduce costs by up to 40% [2].

Within the context of this paradigm shift, it is of crucial importance to reexamine the core architectural levels of network devices, such as the Control Plane, Management Plane, and Configuration mechanisms[3]. Additionally, the traditional networking models rely heavily on embedding these planes vertically within each proprietary device, leading to rigid, static, and complex manual management [4]. In contrast, emerging trends—such as Software-Defined Networking (SDN) and Intent-Based Networking (IBN)—introduce a fundamental separation of these layers, decoupling the control logic from the underlying forwarding hardware to permit centralized, programmable, and vendor-agnostic orchestration[5]. Consequently, the core motivations driving current research and the adoption of these modern architectures include reduction of operational costs, intent extraction, enhancement of security, network programmability, and energy optimization [6].

The primary motivations underpinning this study arise from the need to transition away from manual, low-level command-line configuration toward human-friendly interfaces that abstract technical barriers, thereby accelerating deployment speeds and reducing the likelihood of misconfigurations [6]. Central to this vision is the utilization of Large Language Models (LLMs) and advanced prompting techniques to automatically translate high-level natural language requirements into functional configurations, specific Python scripts, or 3GPP-standardized intent types [7]. A further motivation is the mitigation of severe control plane threats, including Distributed Denial of Service (DDoS) attacks and IP spoofing, through the integration of distributed blockchain ledgers, smart contracts, and dedicated middleware layers. Such mechanisms eliminate single points of failure and establish immutable audit trails [8]. In parallel, the adoption of microservice-based containerized architectures and standardized models, such as OpenConfig YANG and NETCONF, enables vendor-agnostic programmability, real-time state collection, and comprehensive configuration verification, thereby minimizing network downtime prior to the deployment of changes [9].

Equally important is the development of automated, machine learning-driven knowledge bases and multi-tier energy management layers designed to calculate cost-effective routing paths, alleviate traffic congestion, and dynamically optimize node power consumption in resource-constrained environments such as Industrial Wireless Sensor Networks [10]. Ultimately, this paper presents a comprehensive comparative analysis between traditional device-centric models and emerging cloud-native, programmable paradigms, examining how these distinct control, management, and configuration layers interact to meet the demands of next-generation infrastructures.

Received*: 20-04-2026 -* ***Accepted****: 19-06-2026 -* ***Published****: 25-06-2026*

Related Work

The research [1] proposes, a novel four-layer architectural framework of IS2N, which enhances traditional software-defined networks by integrating a specialized middle layer powered by blockchain and intent-driven technologies. This architecture enables automated network security management by utilizing an intent-driven mechanism that translates high-level user requirements into actionable security policies through a continuous closed-loop process. By deploying blockchain within the middleware, the system establishes a decentralized authority for device registration and identity verification while maintaining immutable snapshots of network states and flow messages for superior traceability. The introduction of the middle layer effectively decouples the static relationships between controllers and switches, providing the unique capability to dynamically cut off hijacked or malicious control links without corrupting the overall network performance.

Experimental simulations validate that this approach significantly improves resilience against control plane threats like DDoS attacks and offers flexible policy adjustments that outperform conventional security strategies in maintaining network stability. This paper [2] introduces a sophisticated framework that utilizes Large Language Models to transform natural language queries into workable, task-specific code for managing complex network topologies and communication graphs. By adopting a code-generation approach instead of direct data processing, the system effectively bypasses the inherent scalability limitations of these models, such as restricted token windows, which enable it to handle massive networks irrespective of their size. This proposed method significantly enhances data privacy and security because the sensitive network information remains within the local environment while only structural metadata and natural language instructions are shared with the model.

A major advantage of this system is its high degree of explainability and accuracy, as network operators can manually inspect the generated code to validate its logic, thereby curtailing the risks associated with AI hallucinations and black-box decision-making. Despite these clear strengths, the research identifies critical challenges such as the need for better domain-specific knowledge in language models and the difficulty of maintaining high accuracy when generating code for increasingly complex or multi-layered network management tasks. The authors in [3] present a paradigm-shifting approach to network management by utilizing Large Language Models (LLMs) to automate the extraction of user intents within 5G and next-generation core networks. The researchers developed a customized framework capable of interpreting unstructured natural language and categorizing requests into six standardized 3GPP intent types, which include deployment, modification, and performance assurance.

A significant contribution of the research lies in emphasizing explainability, where the model provides a sound justification for its intent classification to ensure transparency and trust in automated decision-making processes. While the results demonstrate a high level of accuracy in identifying multiple intents and filtering out unrelated conversational inputs, challenges such as model drift, potential hallucinations, and the ambiguity of specific user requests remain areas for further refinement. Moving forward, the study suggested transitioning to open-source models and integrating the system into live 5G testbeds to achieve a fully autonomous, end-to-end intelligent network architecture.

On the other hand, the research in [4] introduces the Open Software Defined Framework (OSDF), an intent-based networking system designed to allow network administrators to manage infrastructure through high-level abstractions and descriptive policies rather than complex, low-level flow rules. By providing a sophisticated Northbound Interface that hides hardware-specific details, the framework permits the expression of complex necessities such as routing, security, and quality of service through application-oriented vocabulary. One of its core features is the dedicated policy management module that automatically detects and resolves conflicts between different network rules, ensuring that the global network state remains reliable and functional. While the system offers significant advantages in terms of flexibility and automated rerouting for network resiliency, it faces challenges related to hardware dependencies and performance overhead when dealing with high-frequency configuration changes. Ultimately, OSDF demonstrates a shift toward more programmable and intuitive network management, although limitations in TCAM memory and rule installation latency highlight the ongoing need for optimization in large-scale enterprise environments.

Additionally, the research paper [5] examines the transformative potential of Large Language Models in streamlining network management by converting natural language requirements into functional network configurations and specialized Python code. The authors introduce a comprehensive evaluation framework designed to test the proficiency of various models in handling tasks such as formal specification generation, routing algorithm development, and low-level protocol configuration. The study further demonstrates that while advanced models can effectively automate repetitive configuration tasks and simplify complex technical documentation, they still exhibit significant restrictions when dealing with intricate logical reasoning and large-scale network topologies. Key findings underscore the integration of these models into networking workflows, which requires the implementation of structured design principles, including the use of specialized verifiers to ensure the accuracy and safety of the generated outputs. Finally, the paper concludes that while AI can significantly reduce the barrier to entry for network configuration, a human-

Received*: 20-04-2026 -* ***Accepted****: 19-06-2026 -* ***Published****: 25-06-2026*

in-the-loop approach remains essential to curtail the risks associated with model hallucinations and ensure the reliability of critical infrastructure.

The researchers in [6] present NETBUDDY, an innovative framework that controls the power of Large Language Models to automate the complex process of translating high-level natural language requirements into functional network configurations through a multistage pipeline involving formal specification, script generation, and vendor-specific command production. By decomposing the translation task into smaller steps and incorporating a self-healing verifier loop, the system significantly improves the ability of models like GPT-4 to produce accurate configurations for both P4 and BGP protocols while reducing the need for deep human expertise in domain-specific languages. One of the primary advantages of this approach is its human-friendly interface, which allows operators to describe network intents simply, potentially lowering operational costs and increasing the speed of network deployment compared to traditional manual coding methods. However, despite its capability, the system faces notable challenges regarding the absolute correctness of translations, as LLMs can frequently struggle with implicit logical contradictions and may lose accuracy when dealing with highly complex sets of requirements that exceed certain prompt limits. Ultimately, while the framework demonstrates great versatility in modern network emulation environments, further research is still needed to ensure stability, handle proprietary protocols, and eradicate the inherent ambiguities found in natural language descriptions.

To address the critical issue of excessive power consumption in Industrial Wireless Sensor Networks, the study in [7] introduces an Enhanced Energy Optimization Model that leverages automated knowledge-based Machine Learning techniques within a dedicated energy management layer to dynamically optimize and forecast node energy levels during scheduled tasks. The proposed framework structures the network into a specialized three-tier architecture comprising a Perception Layer with embedded solar-powered nodes for energy harvesting, a Network Layer driven by Edge Routers, and an interactive Application Layer to streamline data flow across the system. By calculating the most cost-effective routing paths and analyzing network feedback, the model successfully avoids redundant data transmissions, alleviates localized traffic congestion, and significantly extends the overall operational lifetime of the sensor nodes. Extensive technical simulations demonstrate that this model achieves substantial power savings across transmission, reception, idle, and sleep modes, while maintaining exceptional mathematical accuracy and reliability across various performance evaluation metrics.

Despite these substantial benefits in productivity and predictive maintenance, the deployment of this architecture still faces shortcomings regarding high implementation costs, structural complexity, limited network bandwidth, and the need for robust security frameworks against potential industrial cyberattacks.

The research paper [8] presents a hybrid security framework that integrates Software-Defined Networking (SDN) with Blockchain technology to strongly protect the SDN Controller from Distributed Denial of Service (DDoS) attacks. To achieve this, the system replaces traditional flow tables with a distributed, immutable blockchain ledger and utilizes Smart Contracts to authenticate network switches and verify the validity of incoming data packets.

By establishing a decentralized database of trusted IP addresses, the framework effectively prevents IP spoofing while eliminating the "Single Point of Failure" to ensure overall data integrity. Furthermore, the proposed model provides strict device authentication and a transparent audit trail of all network operations, which is essential for conducting detailed post-attack forensics and analysis. However, the implementation faces significant flaws such as increased latency due to consensus mechanisms, substantial resource overhead for CPU and memory, and complex scalability issues as the network expands. The study in [9] introduces an innovative architecture centered around Large Language Models to manage the complete lifecycle of network intents by converting unstructured natural language into specific technical configurations for 5G and 6G environments. By integrating advanced prompting techniques and few-shot learning, the framework successfully automates the decomposition of high-level user requirements into standardized formats across multiple domains, such as the radio access network and core cloud infrastructure. This approach significantly lowers the technical barriers for operators by abstracting complex low-level configurations and providing an interactive interface for intent negotiation and automated structural validation before deployment.

The system ensures continuous consistency and intelligence through a specialized validation agent and a feedback loop that incorporates human input to refine the model's accuracy and handle the inherent ambiguities of human language. Practical experiments conducted within the EURECOM 5G facility demonstrate the feasibility of the approach while highlighting critical future challenges related to processing latency, resource feasibility, and the need for domain-specific datasets in telecommunications. This project in [10] proposes a highly resilient and scalable microservice-based architecture that utilizes standardized Open Config YANG models and the NETCONF protocol to achieve uniform, vendor-agnostic network programmability and management across diverse equipment. By decoupling tasks into independent, containerized services using Docker, the framework efficiently handles real-time notifications, state collection, and device configuration within a dynamic, event-driven interaction design. A major advantage of this approach is its ability to perform comprehensive configuration verification and network state analysis

Received*: 20-04-2026 -* ***Accepted****: 19-06-2026 -* ***Published****: 25-06-2026*

through an internal data model, which allows operators to prevent errors and minimize network downtime before changes are deployed. Performance evaluations conducted on a physical testbed successfully confirm the system's efficacy, demonstrating high processing throughput and compact message sizes perfectly capable of meeting the demands of large-scale infrastructures. However, implementing this architecture introduces notable challenges, particularly regarding the inherent complexity of modern networks, the maintenance of data consistency across independent services, and the management of intricate inter-service communication.

Advances in IoT, 5G, and AI have accelerated the transition from manual network management to smart, automated solutions that support real-time analysis and proactive actions [10]. By implementing these advanced tools, modern infrastructures gain critical benefits such as predictive AI-driven monitoring, customized 5G network slicing for specific performance needs, minimized human configuration errors, and significantly improved operational efficiency that can reduce costs by up to 40%. However, organizations continue to face significant challenges, such as increased security and privacy concerns associated with decentralized networks, a heavy reliance on high-quality training datasets, complex integration with legacy systems, and limited transparency in AI decision-making. To ensure seamless functionality across multi-vendor platforms, the industry must overcome interoperability challenges through more robust global standardization. For future research areas, the study suggests more focus and priority on developing explainable AI to enhance administrator trust, utilizing federated learning for privacy-preserving machine learning, and integrating sustainability through power-conscious monitoring techniques.

Challenges

Despite the remarkable technological progress achieved in modern intelligent network management systems, several critical obstacles continue to hinder their efficiency and reliability. One of the most pressing challenges lies in the integration of blockchain with Software-Defined Networking (SDN). While blockchain offers immutability and decentralized control, its consensus mechanisms introduce significant latency, high CPU and memory consumption, and scalability limitations as networks expand. These issues are further compounded in decentralized IoT and multi-domain environments, where the attack surface is enlarged, and security and privacy risks become more pronounced. Large Language Model (LLM)-based frameworks also face substantial limitations.

Model drift, ambiguity in interpreting user intents, and restricted domain-specific knowledge reduce their accuracy when applied to highly complex or multi-layered network configurations. Moreover, LLMs struggle with implicit logical contradictions and prompt-length restrictions, making fully autonomous configuration generation unreliable without human oversight. Intent-Based Networking (IBN) and programmable networking frameworks encounter additional hardware-related constraints, including TCAM memory limitations, rule installation latency, and performance overhead during frequent configuration updates, all of which undermine their scalability and responsiveness. Microservice-based architectures, while offering modularity and flexibility, introduce challenges in maintaining data consistency across distributed services, managing complex inter-service communication, and handling the inherent intricacies of large-scale networks.

Organizations adopting AI-driven network management must also contend with the integration of modern technologies into legacy infrastructures, ensuring interoperability across multi-vendor platforms, and safeguarding transparency in AI decision-making processes. These difficulties are exacerbated by high implementation costs, limited network bandwidth, dependency on high-quality training datasets, and the urgent need for robust cybersecurity protections, particularly in industrial and IoT environments. Collectively, these obstacles underscore the necessity of advancing research into blockchain-SDN integration, refining LLM-based frameworks, optimizing IBN programmability, and strengthening microservice architectures to ensure that intelligent network management systems can meet the demands of next-generation infrastructures.

Research Gap

Although significant progress has been made in integrating AI, SDN, blockchain, microservices, and LLM-based automation into modern network management, several important research gaps remain that are not fully addressed by existing solutions. A key limitation is the lack of fully reliable end-to-end automation. Although Large Language Model (LLM)-based systems and intent-driven frameworks can translate natural language into configurations, they continue to require human supervision due to persistent issues such as hallucinations, ambiguous intent interpretation, and inconsistent reasoning across complex scenarios. These shortcomings prevent the realization of true zero-touch network management at scale. Another major gap lies in the absence of unified, standardized frameworks capable of seamlessly integrating emerging technologies. Current approaches often emphasize isolated solutions—such as combining SDN with blockchain, employing LLM-based intent extraction, or adopting microservice architectures—but there is still no comprehensive architecture that consistently merges AI reasoning, secure distributed ledgers, microservices orchestration, and real-time network programmability into a production-ready system.

Received*: 20-04-2026 -* ***Accepted****: 19-06-2026 -* ***Published****: 25-06-2026*

Scalability and performance also remain problematic in real-world deployments. While many frameworks demonstrate promising results in simulations or controlled testbeds, they frequently encounter operational constraints such as blockchain consensus latency, excessive resource overhead, and synchronization challenges when scaled to enterprise or telecom environments. Trust, explainability, and validation of AI-driven decisions represent further obstacles.

Although partial explainability has been achieved, formal verification of AI-generated configurations is still insufficient, limiting operator confidence in autonomous decision-making within mission-critical infrastructures. Finally, there is a pronounced data and domain specialization gap in LLM-based networking systems. Most existing models are trained on general datasets and lack deep knowledge of telecom-specific protocols, vendor-specific configurations, and low-level network semantics. This deficiency reduces their accuracy and reliability in practical applications, underscoring the need for domain-adapted training and specialized datasets. Together, these gaps highlight the necessity of advancing research into end-to-end automation, developing unified frameworks, addressing scalability and performance, and enhancing domain-specific LLMs to ensure that intelligent network management systems can evolve into trustworthy, scalable, and production-ready solutions. There is a deployment and integration gap with legacy systems. Most proposed architectures assume modern, cloud-native environments, while real networks still rely heavily on legacy hardware and protocols, creating significant challenges for migration, interoperability, and incremental adoption. Overall, these gaps highlight the need for more unified, scalable, verifiable, and domain-aware intelligent network management systems capable of operating reliably in real-world heterogeneous environments.

Future Research Directions

Future research aims to enhance intelligent network management systems by improving Explainable Artificial Intelligence (XAI) techniques to increase administrator trust, transparency, and interpretability in automated decision-making processes. Researchers also recommend adopting Federated Learning approaches to enable privacy-preserving ML while reducing the need to share sensitive network data. Several studies propose transitioning toward open-source and domain-specific LLMs trained specifically for networking tasks to improve accuracy and enhance intent extraction capabilities. Integrating advanced validation agents, verifier loops, and human-in-the-loop mechanisms is also considered essential to ensure the correctness and safety of automatically generated configurations.

To overcome scalability and latency problems, future architectures are expected to optimize blockchain consensus algorithms, reduce computational overhead, and improve distributed resource management within SDN and microservice-based systems. Additionally, researchers highlight the importance of developing intelligent power-aware monitoring systems and sustainable energy optimization techniques, especially for Industrial IoT and Wireless Sensor Networks. Future network infrastructures are expected to incorporate proactive AI-driven predictive maintenance, automated configuration verification, adaptive security mechanisms, and fully autonomous intent-driven orchestration for 5G, 6G, and next-generation cloud-native environments.

Conclusion

In summary, this research presented a detailed comparative evaluation of traditional and emerging paradigms in network configuration and control management. The study successfully highlights the architectural transformation between these models, focusing on the core concept of separating the control plane from the data plane. The findings demonstrate that while traditional device-by-device configuration offers localized resilience and proven stability, emerging centralized paradigms provide superior scalability, greater programmability through automation, and a significant reduction in human-induced operational errors. Consequently, transitioning to centralized control frameworks optimizes network performance and simplifies management. Future work should focus on addressing the scalability and security challenges associated with centralized controllers to ensure robust and resilient network infrastructures.

References

1. Song Y, Feng T, Yang C, Mi X, Jiang S, Guizani M. IS2N: Intent-driven security software-defined network with blockchain. IEEE Netw. 2023;38(3):118–127.
2. Kumaran Mani S, Zhou Y, Hsieh K, Segarra S, Chandra R, Kandula S. Enhancing Network Management Using Code Generated by Large Language Models. arXiv e-prints. 2023;arXiv-2308.
3. Manias DM, Chouman A, Shami A. Towards intent-based network management: Large language models for intent extraction in 5g core networks. In: 2024 20th International Conference on the Design of Reliable Communication Networks (DRCN). 2024; p. 1–6.
4. Comer D, Rastegatnia A. Osdf: An intent-based software defined network programming framework. In: 2018 IEEE 43rd Conference on Local Computer Networks (LCN). 2018; p. 527–535.
5. Wang C, Scazzariello M, Farshin A, Ferlin S, Kostić D, Chiesa M. Netconfeval: Can llms facilitate network configuration? Proc ACM Netw. 2024;2(CoNEXT2):1–25.

Received*: 20-04-2026 -* ***Accepted****: 19-06-2026 -* ***Published****: 25-06-2026*

6. Wang C, Scazzariello M, Farshin A, Kostic D, Chiesa M. Making network configuration human friendly. arXiv Prepr arXiv2309.06342. 2023.
7. Bagwari A, et al. An enhanced energy optimization model for industrial wireless sensor networks using machine learning. IEEE Access. 2023;11:96343–96362.
8. Belkhadim A, Chahid A, Hilmani A, Ettaoufik A, Maizate A, Mansouri K. Enhancing SDN Security and Availability with Blockchain and Dual-Layer Isolation Forest–Driven DDoS Detection. Eng Technol Appl Sci Res. 2026;16(3):36393–36400.
9. Mekrache A, Ksentini A, Verikoukis C. Intent-based management of next-generation networks: An LLM-centric approach. IEEE Netw. 2024;38(5):29–36.
10. Amlou A, Abane A, Merzouki M, Ait Oucheggou L, Maasaoui Z, Battou A. Automated network programmability using OpenConfig YANG models and NETCONF protocol. In: 2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA). 2023; p. 1–5.

Received*: 20-04-2026 -* ***Accepted****: 19-06-2026 -* ***Published****: 25-06-2026*