British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 32-47)
www.abjournals.org

NETWORK PERFORMANCE OPTIMIZATION WITH INTENT-BASED NETWORKING: A REVIEW

Kuyoro S. O.[1], Ayankoya F. Y.[2], Ikhioya Emmanuel[3], and Adeyemi John[4].

[1,2,3,4]Department of Computer Science, Babcock University, Ilishan-Remo, Ogun State, Nigeria.

Emails: [1]kuyoros@babcock.edu.ng, [2]ayankoyaf@babcock.edu.ng, [3]ikhioya0210@pg.babcock.edu.ng, [4]adeyemi0134@pg.babcock.edu.ng

Cite this article:

Kuyoro, S. O., Ayankoya, F. Y., Ikhioya, E., Adeyemi, J. O (2026), Network Performance Optimization with Intent-Based Networking: A Review. British Journal of Computer, Networking and Information Technology 9(1), 32-47. DOI: 10.52589/BJCNIT-ZDW0FQHA

Manuscript History

Received: 25 Nov 2025

Accepted: 29 Dec 2025

Published: 19 Jan 2026

ABSTRACT: *Intent-Based Networking (IBN) is transforming network management by shifting from manual, device-oriented configurations to high-level, intent-driven automation. In an IBN system, network operators express high-level objectives that are automatically translated into detailed network policies and configurations through artificial intelligence (AI), natural language processing (NLP), and closed-loop control mechanisms. This paper reviews recent advances in IBN, with a focus on its architecture, automation techniques, security frameworks, and AI-driven policy generation. Moreover, we discuss intent negotiation frameworks and voice-enabled interfaces for industrial automation. By integrating these technologies with Software-Defined Networking (SDN) and Network Function Virtualization (NFV), IBN optimizes network performance by enhancing resource utilization, reducing latency, and improving overall reliability. This paper also outlines the challenges and future research directions necessary for the deployment of IBN in next-generation networks.*

KEYWORDS: Intent-Based Networking, SDN, NFV, Artificial Intelligence, NLP, Policy Generation, Intent Negotiation, Voice-Enabled Networking, Security.

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

INTRODUCTION

The evolution of network infrastructures—with emerging technologies such as 5G, cloud computing, and the Internet of Things (IoT)—has resulted in increasingly complex, heterogeneous, and dynamic network environments. Traditional network management techniques, which rely heavily on manual configuration and static rules, are no longer sufficient to meet the requirements of modern networks. This is especially critical in scenarios where high availability, low latency, and dynamic resource allocation are necessary.

Intent-Based Networking (IBN) addresses these challenges by abstracting network control from low-level configurations to high-level business objectives. Instead of managing the intricacies of network protocols and device configurations, network operators express what they want the network to achieve. The IBN system then automatically translates these intents into detailed policies and continuously monitors the network to ensure that the desired state is maintained. This high-level abstraction not only reduces the cognitive burden on network administrators but also minimizes human error and improves overall network performance [1]–[4].

Recent research has demonstrated the potential of IBN to enhance network performance through various mechanisms such as dynamic traffic engineering, predictive analytics, and automated policy enforcement. Furthermore, advancements in AI, particularly in natural language processing and large language models (LLMs), have enabled IBN systems to automatically generate policies and resolve conflicts through intent negotiation [5]–[7], [11], [12]. In this review, we synthesize findings from multiple studies and discuss how IBN can optimize network performance while providing improved security and agility.

What is Intent-Based Networking?

Intent-Based Networking (IBN) is an advanced network management paradigm that enables operators to define high-level business or operational objectives, referred to as intents, which are then automatically translated into low-level configurations and enforced across the network. This approach shifts the focus from manual, device-specific configurations to an intent-driven model, where the network autonomously implements and maintains the desired state with minimal human intervention.

Unlike traditional networking, which requires administrators to manually configure individual network devices using command-line interfaces (CLI) or static rule sets, IBN leverages automation, artificial intelligence (AI), and machine learning (ML) to dynamically adjust network settings based on real-time conditions. By continuously analyzing network telemetry data, IBN ensures that policies remain aligned with the specified intent, allowing networks to proactively optimize performance, enhance security, and improve reliability. This self-adaptive capability makes IBN particularly well-suited for complex, large-scale environments such as 5G/6G networks, cloud data centers, enterprise networks, and industrial IoT infrastructures [4], [5].

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

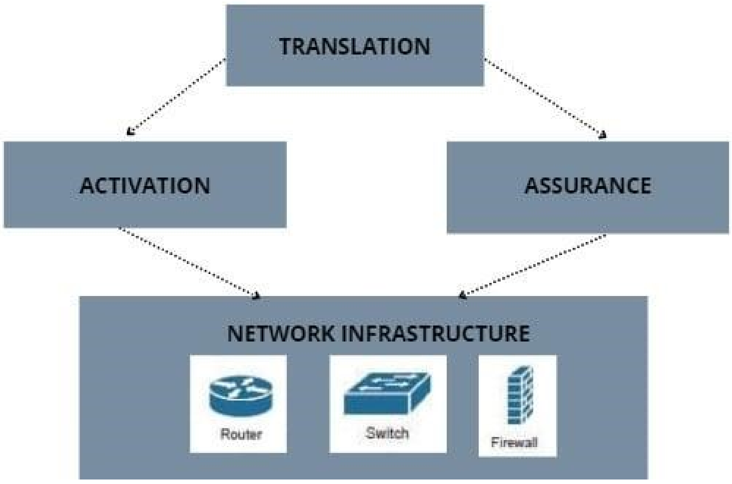
British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 32-47)

IBN Architecture and Components

IBN systems are designed using a layered architecture that supports the entire lifecycle of an intent—from its initial specification to final enforcement and assurance. This architecture is built upon several key components, each of which contributes to the overall performance and adaptability of the network.

Intent Lifecycle and Translation

The intent lifecycle in an IBN system comprises several stages:



- **Profiling:** In this stage, network operators or automated applications specify their service requirements using natural language or predefined templates. The profiling process captures both functional attributes (what service is required) and non-functional attributes (quality of service, cost, latency, etc.) [4], [7]. For instance, an operator might specify, "I want to ensure low latency for video conferencing traffic between data centers." Such intents are abstract and do not provide details on implementation.

- **Translation:** The Intent Processor (IP) uses Natural Language Processing (NLP) techniques to convert high-level intents into structured, machine-readable formats (such as JSON or RDF) without losing the original abstraction. This translation preserves the essential details while rendering them actionable by the underlying network management system [4], [7]. **Example:** An intent such as "Optimize video streaming performance" might be translated into policies that prioritize certain traffic flows, allocate additional bandwidth, or select low-latency routing paths.

- **Resolution:** Once an intent is translated, the system evaluates its feasibility by checking against current network conditions and resource availability. This may involve conflict detection, resource mapping, and the use of optimization algorithms to resolve potential ambiguities [7]. If a conflict is detected, the system may trigger an intent negotiation process (discussed later) to generate alternate solutions.

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

- **Activation:** The resolved policies are then deployed into the network. This involves configuring network devices, instantiating Virtualized Network Functions (VNFs), and initiating service function chains (SFCs) as required [10].
- **Assurance:** In the final stage, continuous monitoring and feedback mechanisms ensure that the deployed configuration remains aligned with the original intent. If deviations occur due to network dynamics, corrective actions are automatically initiated through closed-loop control [8], [11].

B. Closed-Loop Control and Automation

A central element of IBN is its closed-loop automation framework, which enables networks to operate with minimal human intervention. Using the Monitor-Analyze-Plan-Execute (MAPE) model, the system continuously collects network telemetry data, analyzes current performance, and dynamically adjusts configurations to maintain the intended network state [11], [15]. This feedback loop is critical for self-optimizing, self-healing, and intent-driven networks, ensuring that network operations remain efficient, resilient, and adaptive to changing demands [8], [14].

Key benefits of closed-loop automation include:

- **Dynamic Reconfiguration:** The closed-loop automation system automatically reroutes traffic, reallocates resources, and adjusts Quality of Service (QoS) parameters based on real-time network conditions [4], [6]. This capability ensures optimal bandwidth utilization while minimizing network congestion, particularly in multi-domain and SDN-integrated environments [7].
- **Fault Tolerance and Resilience:** The feedback loop enables rapid anomaly detection and mitigation by using AI-powered predictive analytics to anticipate link failures, security threats, and network degradations before they impact service quality [10]. By integrating real-time monitoring and machine learning (ML) models, IBN can autonomously apply corrective actions and restore network stability [12].
- **Real-Time Policy Enforcement:** Closed-loop automation ensures continuous enforcement of network policies and security rules by dynamically adapting to changing traffic patterns and intent modifications [5]. This enhances compliance, security, and service consistency across different infrastructure domains [13].
- **Adaptive Intent Optimization:** The IBN controller continuously learns from historical traffic data, user-defined intents, and real-time network analytics to refine intent translation and execution [3], [9]. This iterative learning process makes network adjustments more intelligent and efficient over time [16].
- **Energy Efficiency:** By dynamically optimizing resource allocation, closed-loop automation contributes to energy-efficient networking, particularly in cloud data centers and virtualized environments [2]. This approach aligns with sustainability goals by minimizing unnecessary resource consumption while maintaining high network performance [1].

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

C. Integration with SDN and NFV

The success of IBN is largely enabled by its seamless integration with Software-Defined Networking (SDN) and Network Function Virtualization (NFV). These technologies provide the flexibility, scalability, and automation necessary to implement intent-driven networking effectively.

- **SDN Centralized Control and Abstraction:** SDN introduces a centralized control plane that abstracts network hardware, enabling global visibility, policy enforcement, and intelligent traffic management. By decoupling the control and data planes, SDN allows IBN systems to dynamically reconfigure traffic flows, prioritize critical applications, and optimize bandwidth allocation [10].

- **NFV-Driven Virtualization and Scalability:** NFV virtualizes network functions, enabling them to run as Virtualized Network Functions (VNFs) on standard servers instead of dedicated hardware. This allows dynamic instantiation, scaling, and migration of network functions based on real-time demand, network congestion, or security threats [10], [12].

- **End-to-End Orchestration and Service Agility:** IBN, combined with SDN and NFV, enables end-to-end service orchestration across heterogeneous infrastructures—ensuring that performance optimization can be achieved in diverse environments such as data centers, enterprise networks, cloud environments, and wide-area networks (WANs). This facilitates faster service deployment, automated scaling, and intelligent workload distribution [11], [13].

- **Multi-Domain and Multi-Vendor Interoperability:** SDN and NFV allow IBN to function across multi-domain and multi-vendor ecosystems, eliminating traditional vendor lock-in and promoting programmability through open standards such as OpenFlow, NETCONF/YANG, and REST APIs [14].

- **Network Slicing and Resource Optimization:** With NFV-enabled network slicing, IBN can dynamically provision, configure, and allocate network slices to support differentiated services such as 5G, IoT, and ultra-low latency applications. This improves resource utilization and energy efficiency [15], [16].

- **Security and Compliance Management:** By integrating SDN's centralized monitoring with NFV's flexible service chaining, IBN enhances security posture by automating real-time threat detection, compliance enforcement, and anomaly mitigation—ensuring secure intent execution across the network [10], [14].

Network Performance Optimization through IBN

IBN's ability to dynamically adapt network configurations and allocate resources is fundamental to optimizing network performance. By leveraging AI-driven automation, telemetry data, and real-time analytics, IBN ensures networks are resilient, efficient, and adaptive to fluctuating traffic demands. This section discusses key mechanisms by which IBN enhances performance and service reliability.

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

A. Traffic Engineering and Load Balancing

IBN utilizes real-time telemetry and AI-driven analytics to monitor network traffic patterns, predict congestion, and optimize routing paths dynamically. These capabilities help distribute loads efficiently across network resources, improving overall network performance and preventing bottlenecks.

- **Dynamic Rerouting:** When high traffic congestion is detected on a primary path, the IBN system can automatically redirect flows to alternate routes with lower congestion. This minimizes packet loss, latency, and jitter, ensuring a smooth user experience for time-sensitive applications such as video conferencing and cloud gaming [10].

- **Load Balancing Across Multiple Links:** IBN ensures optimal utilization of network links by distributing traffic intelligently. Instead of overloading specific links, IBN proactively balances traffic to maximize throughput and prevent excessive latency [4], [5].

- **Network Slicing:** IBN supports fine-grained resource allocation by creating dedicated network slices for different types of traffic. This ensures that latency-sensitive applications (e.g., real-time gaming, industrial automation, and telemedicine) receive priority treatment, while less critical traffic is processed with lower priority [2], [5].

B. Latency and Bandwidth Optimization

IBN enhances service quality by dynamically optimizing bandwidth allocation and reducing latency through intelligent routing.

- **Intent-Based Bandwidth Allocation:** IBN dynamically prioritizes critical applications, ensuring that mission-critical workloads, such as financial transactions and emergency communications, receive sufficient bandwidth at all times [2], [6].

- **Latency Reduction via Edge Computing:** By integrating with edge computing, IBN processes data closer to end-users, minimizing the distance data must travel and significantly reducing round-trip latency. This is particularly beneficial for applications requiring ultra-low latency, such as autonomous vehicles, AR/VR, and industrial IoT [5], [9].

- **Adaptive QoS Policies:** AI-driven models continuously refine QoS policies based on network conditions, ensuring dynamic resource allocation that adapts to traffic fluctuations and real-time application demands [7], [8].

- **Predictive Bandwidth Optimization**: Using historical traffic data and predictive analytics, IBN anticipates bandwidth surges and preemptively scales resources to prevent service degradation [3], [4].

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 32-47)
www.abjournals.org

C. Self-Optimizing and Self-Healing Networks

The combination of AI-based predictive analytics and closed-loop automation enables IBN to create self-optimizing and self-healing networks, capable of detecting, mitigating, and recovering from failures without human intervention.

- **Anomaly Detection with AI**: Machine learning models continuously monitor performance metrics (e.g., latency, packet loss, throughput) to detect irregularities or network degradation before they affect end users [8], [12].
- **Automated Recovery & Fault Mitigation:** When anomalies or failures occur, IBN can automatically trigger corrective actions such as rerouting traffic, reallocating bandwidth, and adjusting routing paths to restore optimal performance without human intervention [11], [14].
- **Proactive Failure Prevention:** Predictive analytics identifies potential failures before they happen, allowing IBN to preemptively adjust configurations and prevent service disruptions [6], [13].
- **Continuous Learning & Improvement:** Feedback loops enable the system to learn from past network failures, refining decision-making processes to prevent future incidents and enhance long-term network resilience [15], [16].

Intent Negotiation and AI-Driven Policy Generation

While IBN systems excel in translating high-level intents into actionable policies, conflicts may arise when user requirements exceed the current network capacity or when multiple intents compete for the same resources. This section reviews the mechanisms used to resolve such conflicts.

A. Intent Negotiation Frameworks

Intent negotiation frameworks are designed to reconcile differences between user demands and network capabilities. When a conflict is detected, these frameworks:

- **Generate Alternate Intents:** By adjusting non-functional parameters (e.g., relaxing latency or reducing bandwidth requirements), the system produces alternate solutions that may be more feasible given current resources [9].
- **Iterative Negotiation:** The system presents these alternatives to the user or automatically selects the most optimal solution based on predefined criteria, thereby maximizing the acceptance rate of service requests and ensuring efficient resource utilization [9].

B. AI-Based Policy Generation Using LLMs

Recent research has demonstrated the effectiveness of Large Language Models (LLMs) in generating network policies from high-level intents. LLM-based policy generation:

- **Decomposes Complex Intents:** By using few-shot learning, LLMs can break down complex user intents into a sequence of actionable steps that are mapped to network APIs [12].

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

- **Automates Policy Mapping:** This method reduces the need for manual intervention by automatically creating a hierarchy of policies that can be executed by the network management system.
- **Enhances Adaptability:** As network conditions evolve, LLM-driven systems can rapidly regenerate policies to adapt to new requirements, ensuring that network performance remains optimal [12].

Security and Policy Management

The autonomous nature of IBN necessitates robust security measures to protect network integrity and ensure compliance with regulatory requirements.

A. Adaptive Security Policies

IBN systems implement adaptive security mechanisms that dynamically adjust to the network environment:

- **Intent-Based Firewall Automation:** Security policies can be automatically updated based on real-time threat detection, ensuring that only authorized traffic is permitted [6].
- **Zero-Trust Architecture:** IBN enforces a zero-trust model where every access request is continuously verified, reducing the risk of unauthorized access [6].

B. Compliance and Continuous Assurance: Continuous monitoring is critical to ensure that network configurations remain aligned with regulatory and operational standards:

- **Automated Auditing:** IBN systems maintain detailed logs and audit trails of all configuration changes, providing transparency and traceability [5].
- **Real-Time Policy Enforcement:** Through closed-loop control, the system verifies that deployed policies comply with Service Level Agreements (SLAs) and industry standards such as GDPR and HIPAA [11].

RELATED LITERATURE

S/N	Author & Year	Paper Title	Summary	Research Gap
1	Kristina Dzeparoska, Ali Tizghadam & A. Leon-Garcia (2024)	Emergence: An Intent Fulfillment System	Proposes Emergence, an intent-based management system that abstracts network infrastructure and refines intents into policy trees. It uses Finite State Machines (FSM) and closed-loop	Further automation is needed in intent decomposition, particularly leveraging LLMs for scalable intent-to-policy translation and broader applicability

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

			automation to execute network policies. The system integrates with Metro Ethernet Forum (MEF) Policy-Driven Orchestration (PDO) and explores the potential role of Large Language Models (LLMs) in intent decomposition.	across diverse network environments.
2	B. Martini, M. Gharbaoui & P. Castoldi (2022)	Intent-Based Zero-Touch Service Chaining Layer for Software-Defined Edge Cloud Networks	Introduces an intent-based zero-touch service chaining layer for edge cloud networks. It automates dynamic service chain deployment via SDN and NFV, enabling real-time adaptation to congestion and improved service reliability.	Needs formalized intent templates, sophisticated assurance parameters (e.g., per-flow monitoring), and validation across diverse topologies and traffic patterns.
3	Lei Pang, Chungang Yang, Danyang Chen, Yanbo Song & Mohsen Guizani (2020)	A Survey on Intent-Driven Networks	Provides a comprehensive survey on Intent-Driven Networks (IDN), covering definitions, architectures, and key features. It highlights IDN as a self-driving network that automates intent deployment via decoupled control logic and closed-loop orchestration.	The lack of a unified IDN definition and unclear research background remain gaps. Standardization and further exploration of continuous closed-loop verification and fully automated deployment mechanisms are needed.

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

4	Khizar Abbas, Muhammad Afaq, Talha Ahmed Khan, Adeel Rafiq & Wang-Cheol Song (2020)	Slicing the Core Network and Radio Access Network Domains through Intent-Based Networking for 5G Networks	Presents an intent-based network slicing system for 5G, enabling automated core network and RAN slicing. It leverages IBN tools and a GAN-based deep learning model to optimize slice admission, improving bandwidth and latency.	Enhanced lifecycle management for network slicing is needed. Future research should expand automation features, refine slice admission strategies, and integrate advanced AI models for resource forecasting.
5	Md. Zahirul Islam, Syed Md. Galib & Md. Humaun Kabir (2024)	Automation of 5G Network Slicing Security Using Intent-Based Networking	Focuses on automating security for 5G network slicing using IBN. The framework integrates an IBN manager into the slicing architecture to automate security controls and mitigate DDoS and ARP spoofing attacks. Experimental results show improved availability, packet loss, and response times.	Large-scale real-world testing of IBN-based security automation is still limited. Future work should explore (1) scalability for commercial networks, (2) AI-driven anomaly detection, and (3) improved cross-domain security enforcement.
6	Mir Muhammad Suleman Sarwar, Afaq Muhammad & Wang-Cheol Song (2022)	IBN@Cloud: An Intent-Based Cloud and Overlay Network Orchestration System	Presents IBN@Cloud, an intent-based system for multi-cloud orchestration and overlay network management. It automates cloud-to-cloud connectivity using OpenStack-based	Suggests using Graph Neural Networks (GNNs) for better path selection and calls for real-time monitoring enhancements to improve intent-based orchestration in

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

			clouds and GENEVE tunnels, leveraging ML models (RNN, LSTM, GRU, SVR, Linear Regression) to predict RTT and optimize communication paths.	hybrid cloud environments.
7	Adeel Rafiq, Asif Mehmood, Talha Ahmed Khan, Khizar Abbas, Muhammad Afaq & Song Wang Cheol (2020)	Intent-Based End-to-End Network Service Orchestration System for Multi-Platforms	Proposes an Intent-Based Network Service Orchestration System for multi-platform virtualization in 5G networks. It automates VNF modeling and NS orchestration via M-CORD and OSM orchestrators, reducing manual errors and improving network slicing efficiency.	Advanced automation is needed for cross-domain network slicing, real-time monitoring for auto-scaling, and enhanced interoperability across virtualization platforms.
8	Kashif Mehmood, Katina Kralevska & David Palma (2021)	Intent-Driven Autonomous Network and Service Management in Future Networks: A Structured Literature Review	A structured literature review on IBN, examining intent description models, lifecycle management, and orchestration techniques within NFV/SDN-based infrastructures. Proposes a converged IBN management framework integrating closed-loop control, intent processing, and service orchestration.	Highlights the need for improved AI-driven intent translation and decision-making. Future work should refine intent abstraction models, integrate learning-based control loops, and standardize intent representation across domains.

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

9	Yogesh Sharma, Deval Bhamare & Andreas Kassler (2022)	Intent Negotiation Framework for Intent-Driven Service Management	Introduces an Intent Negotiation Framework (INF) for Intent-Driven Service Management (IDSM), addressing conflicts in intent fulfillment by negotiating alternative solutions based on real-time network conditions.	Existing intent negotiation solutions are platform-dependent. Future work should focus on multi-provider negotiations, conflict resolution, standardized negotiation protocols, and AI-driven conflict handling.
10	Barun Kumar Saha, Luca Haab & Łukasz Podleski (2021)	Intent-Based Industrial Network Management Using Natural Language Instructions	Explores Intent-Based Industrial Network Management using natural language instructions to simplify network configuration and automation. Uses machine learning classification to map natural language intents to network tasks, demonstrating automated execution of industrial networking operations.	Multilingual support is needed to increase accessibility. Additionally, future work should improve conflict detection between intents and develop a robust intent manager for industrial network automation.
11	Kristina Dzeparoska, Jieyu Lin, Ali Tizghadam & A. Leon-Garcia (2023)	LLM-Based Policy Generation for Intent-Based Management of Applications	Proposes leveraging LLMs for automated intent decomposition and policy execution. The system uses few-shot learning to progressively generate policies, creating a closed	Policy validation remains a key challenge, requiring techniques such as FSM-based validation, logic checks, and digital twin simulations. Future work

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 32-47)

			control loop that maps policies to APIs for network and service orchestration.	should explore handling transformer model limitations, improving intent structuring, and avoiding unintended LLM-generated policy deviations.
12	L. Velasco et al. (2021)	End-to-End Intent-Based Networking	Proposes an E2E Machine Learning-powered Intent-Based Networking (IBN) framework for 5G networks. The system enables zero-touch control and orchestration by integrating ML-based predictions for service assurance, anomaly detection, and intent execution across RAN, cloud, and forwarding planes.	Future work should refine real-time decision-making models, intent coordination mechanisms, and elastic function placement strategies to optimize service automation and network efficiency.
13	Martins Mihaeljans, Andris Skrastins & Jurgis Porins (2024)	Paramounts of Intent-Based Networking: Overview	Studies IBN's structure and lifecycle, proposing two sub-models: one for autonomous networks and another for supervised networks. The paper highlights IBN's reliance on AI and ML, suggesting that full implementation remains unfeasible due to insufficient	Proposes the use of digital twins for network modeling to enhance intent tracking and network assurance. Future work should refine intent drift tracing, conflict prediction, and scalability solutions for full IBN automation.

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

			network knowledge bases.	
14	Ijaz Ahmad, Jere Malinen, Filippos Christou, Pawani Porambage, Andreas Kirstädter, Jani Suomalainen (2023).	Security in Intent-Based Networking: Challenges and Solutions	Analyzes security challenges in IBN, including trust, sovereignty, interoperability, and AI-based attack vectors. Proposes solutions such as policy validation, zero-trust architectures, and AI-enhanced anomaly detection.	Highlights the need for multi-domain security mechanisms, standardization efforts for IBN security, and further research on AI-driven attack mitigation.
15	Raul Barbosa, João Fonseca, Marco Araújo, & Daniel Corujo (2024).	VINIA: Voice-Enabled Intent-Based Networking for Industrial Automation	Proposes VINIA, an architecture integrating Voice-enabled Virtual Assistants (VVAs) with IBN and SDN to automate industrial network operations. It enhances network orchestration via OSM and ONAP, improving E2E network automation.	Future work includes expanding VVA capabilities for multi-language support, integrating AI-driven monitoring, and refining closed-loop automation for improved real-time network reconfiguration.
16	Yiming Wei, Mugen Peng & Yaqiong Liu (2020)	Intent-Based Networks for 6G: Insights and Challenges	Surveys IBN architectures and techniques for AI-enabled 6G networks, focusing on core network automation, RAN integration, and real-time adaptability. Highlights existing platforms like Apstra OS and Forward Networks.	More research is needed on AI-enabled IBNs tailored for 6G, improving flexibility, intelligence, and autonomous network operations. Challenges include handling open data platforms and improving automated fault diagnosis.

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

CHALLENGES AND FUTURE DIRECTIONS

Despite significant advancements, several challenges remain in the deployment of IBN systems:

- **Intent Ambiguity:** Translating abstract, high-level intents into precise, low-level configurations can be inherently ambiguous and requires advanced AI techniques [7].
- **Scalability:** Efficiently managing intents across large, multi-domain networks demands scalable orchestration frameworks that can operate in real time [3].
- **Interoperability:** The lack of standardized interfaces hinders seamless integration between IBN systems and legacy network infrastructures [10].
- **Resource Constraints:** In scenarios with limited network resources, intent negotiation becomes critical to resolving conflicts without compromising overall performance [9].

Future research should focus on enhancing AI-driven intent translation, developing cross-domain orchestration frameworks, and establishing standardized protocols to facilitate widespread IBN adoption in next-generation networks such as 6G and beyond.

CONCLUSION

Intent-Based Networking offers a transformative approach to managing complex network environments by abstracting low-level configuration details into high-level, declarative intents. By integrating AI-driven policy generation, closed-loop control, and intent negotiation frameworks, IBN systems can dynamically optimize network performance while ensuring security and compliance. Although challenges such as intent ambiguity and scalability remain, ongoing research and standardization efforts are paving the way for fully autonomous networks. As IBN continues to evolve, its ability to improve resource utilization, reduce operational costs, and enhance service quality will be critical for the future of network management.

REFERENCES

[1] Y. Wei, M. Peng, and Y. Liu, "Intent-Based Networks for 6G: Insights and Challenges," IEEE Communications Surveys & Tutorials, vol. XX, no. XX, pp. 1–16, 2020.
[2] K. Dzeparoska, A. Tizghadam, and A. Leon-Garcia, "Emergence: An Intent Fulfillment System," in Proc. IEEE Conf. on Network Softwarization (NetSoft), 2024, pp. 1–8.
[3] B. Martini, M. Gharbaoui, and P. Castoldi, "Intent-Based Zero-Touch Service Chaining Layer for Software-Defined Edge Cloud Networks," IEEE Trans. on Network and Service Management, vol. XX, no. XX, pp. 1–12, 2022.
[4] L. Pang, C. Yang, D. Chen, Y. Song, and M. Guizani, "A Survey on Intent-Driven Networks," IEEE Access, vol. 8, pp. 1–20, 2020.
[5] K. Abbas, M. Afaq, T. A. Khan, A. Rafiq, and W.-C. Song, "Slicing the Core Network and Radio Access Network Domains through Intent-Based Networking for 5G Networks," IEEE Open Journal of the Communications Society, vol. XX, no. XX, pp. 1–14, 2020.

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA

[6] M. Z. Islam, S. M. Galib, and M. H. Kabir, "Automation of 5G Network Slicing Security Using Intent-Based Networking," IEEE Access, vol. XX, no. XX, pp. 1–10, 2024.
[7] M. M. S. Sarwar, A. Muhammad, and W.-C. Song, "IBN@Cloud: An Intent-Based Cloud and Overlay Network Orchestration System," in Proc. IEEE Int. Conf. on Cloud Engineering (IC2E), 2022, pp. 1–9.
[8] A. Rafiq, A. Mehmood, T. A. Khan, K. Abbas, M. Afaq, and W.-C. Song, "Intent-Based End-to-End Network Service Orchestration System for Multi-Platforms," IEEE Trans. on Network and Service Management, vol. XX, no. XX, pp. 1–12, 2020.
[9] R. Barbosa, J. Fonseca, M. Araújo, and D. Corujo, "VINIA: Voice-Enabled Intent-Based Networking for Industrial Automation," in Proc. IEEE Conf. on Industrial Informatics (INDIN), 2024, pp. 1–6.
[10] I. Ahmad, J. Malinen, F. Christou, P. Porambage, A. Kirstädter, and J. Suomalainen, "Security in Intent-Based Networking: Challenges and Solutions," IEEE Communications Standards Magazine, vol. XX, no. XX, pp. 1–14, 2023.
[11] K. Mehmood, K. Kralevska, and D. Palma, "Intent-Driven Autonomous Network and Service Management in Future Networks: A Structured Literature Review," IEEE Communications Surveys & Tutorials, vol. XX, no. XX, pp. 1–22, 2021.
[12] Y. Sharma, D. Bhamare, and A. Kassler, "Intent Negotiation Framework for Intent-Driven Service Management," in Proc. IEEE Conf. on Network Softwarization (NetSoft), 2022, pp. 1–10.
[13] B. K. Saha, L. Haab, and Ł. Podleski, "Intent-Based Industrial Network Management Using Natural Language Instructions," in Proc. IEEE Conf. on Artificial Intelligence for Industries (AI4I), 2021, pp. 1–7.
[14] K. Dzeparoska, J. Lin, A. Tizghadam, and A. Leon-Garcia, "LLM-Based Policy Generation for Intent-Based Management of Applications," IEEE Trans. on Artificial Intelligence, vol. XX, no. XX, pp. 1–9, 2023.
[15] L. Velasco et al., "End-to-End Intent-Based Networking," IEEE Trans. on Network and Service Management, vol. XX, no. XX, pp. 1–11, 2021.
[16] M. Mihaeljans, A. Skrastins, and J. Porins, "Paramounts of Intent-Based Networking: Overview," IEEE Access, vol. XX, no. XX, pp. 1–8, 2024.

Article DOI: 10.52589/BJCNIT-ZDW0FQHA
DOI URL: https://doi.org/10.52589/BJCNIT-ZDW0FQHA