Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AI/ML-Driven Cellular Monitoring in SD-WAN: Evolution and Implementation

Vijayakumar Venganti
Jawaharlal Nehru Technological University, Hyderabad, India

ARTICLE INFO

Received: 08 Aug 2025

Revised: 15 Sept 2025

Accepted: 24 Sept 2025

ABSTRACT

Cellular networks integration into Software-Defined Wide Area Networks (SD-WAN) has radically changed the paradigm of enterprise connectivity and has provided unprecedented flexibility and resiliency within the more distributed operational environments. The given scholarly article evaluates the evolutionary path of the monitoring approaches in this field and compares the traditional methods with the new artificial intelligence-based solutions. Conventional cellular monitoring of SD-WAN-based systems has traditionally been anchored on manual configurations, protocol-based polling processes, and reactive troubleshooting processes, which are not effective when facing the natural variability of wireless connections. Such traditional approaches are often limited by scalability constraints, latency sensitivities, and failure to proactively respond to performance degradations in cellular connections. On the contrary, newer-generation deployments take advantage of advanced AI and machine learning engines to provide predictive analytics features, behavioral anomaly detection engines, and autonomous optimization features, all of which collectively optimize network performance, security posture, and operational efficiency. Based on modern research and application examples, this article confirms that AI-based monitoring solutions will play a central role in future SD-WAN infrastructures, especially in latency-sensitive application environments like Internet of Things systems and edge computing systems. The article ends with extensive recommendations for the implementation of these transformational technologies in enterprise networking settings.

Keywords: Artificial Intelligence, Machine Learning, Software-Defined Networking, Cellular Monitoring, Reinforcement Learning

1. Introduction

Software-Defined Wide Area Networking (SD-WAN) represents a breakthrough in replacing traditional hardware-based WAN architectures with software overlays that dynamically control traffic of a heterogeneous underlay, including MPLS, broadband, and cellular connections. The global SD-WAN market has registered uncontrolled growth within the last couple of years, with market analysts predicting positive growth into the decade. This remarkable upward trend underscores how the technology has the potential to transform the enterprise networking infrastructure, most so as business firms are seeking more agile, robust, and lower-cost connectivity solutions for their long-distance operations.

The use of cellular has become an essential component of SD-WAN designs, and an extremely high percentage of organizations now deploy 4G/5G connectivity as either the first or second line of connection in remote offices. Growth is particularly noticeable in the distributed industries such as retail, manufacturing, health care, and financial services, where multi-location organizations have adopted cellular-enabled SD-WAN to facilitate business continuity and operational resilience. The combination of new network technologies and cellular connectivity will offer new edge computing apps and Internet of Things (IoT) implementations and mobility extensions to various industry segments [1]. Cellular monitoring in SD-WAN is important because of the variability inherent in wireless links, including signal variations, handover delays, and 4G/5G/6G bandwidth limitations.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

Field measurements have reported considerable signal strength variations in urban settings during times of peak usage, with attendant throughput variations that can significantly affect application performance. These variations pose significant challenges to mission-critical applications, where even transient connectivity problems can affect operations. Cellular connections within SD-WAN implementations generally see much greater variation in performance metrics than their wired counterparts, requiring advanced monitoring methods that can respond dynamically to such conditions [2].

With more organizations embracing hybrid models, the demand for strong monitoring rises to support seamless connectivity, particularly for mobile and remote users. Companies that have developed advanced cellular monitoring functionality in their SD-WAN deployments see fewer business-affecting network events and fix problems more quickly than those using legacy monitoring techniques. Furthermore, these companies report dramatic decreases in mean time to resolution (MTTR) for issues related to cellular connectivity, which equates to real business value and improved user experiences. These improvements are particularly necessary in such industries where the accessibility of the network has a direct impact on the generation of revenues, customer satisfaction, and the effectiveness of the operations [1].

The advent of technologies, which are based on artificial intelligence and machine learning, has changed the SD-WAN environment radically and has provided unprecedented possibilities for optimizing the network, making it more secure and efficient. Today, SD-WAN technology is becoming more reliant on AI-based analytics to filter through big volumes of network telemetry data to find trends and anomalies that would otherwise be unknown to traditional monitoring and analysis tools. This move to a proactive and not reactive management of the network is one of the most advantageous developments in enterprise networking in the past couple of years that has allowed organizations to detect and prevent potential problems before they can disrupt business operations [2]. This piece explores the methodological dimension of AI deployment in network monitoring, extending from recent research with a focus on the inefficiencies of traditional systems and the potential of smart automation. Classic monitoring solutions are unsuitable for present-day hybrid networks, with network operators constantly complaining that traditional tools do not give sufficient insight into cellular performance. The conversation covers conventional methodologies, the developing function of AI/ML, and novel frameworks for SD-WAN next-generation applications, focusing especially on how these technologies can solve the cellular connectivity problems common in enterprise settings.

Monitoring Aspect	Traditional Monitoring	AI-Driven Monitoring
Issue Detection	Reactive (post-occurrence)	Proactive (predictive)
Signal Variation Response	Static thresholds	Dynamic adaptation
Traffic Management	Manual configuration	Autonomous optimization
Alert Handling	Alert storms, manual triage	Correlated root cause analysis
Mean Time to Resolution	Baseline	Significantly reduced
Security Approach	Signature-based	Behavioral analysis
Path Selection	Static policies	Reinforcement learning-based
Maintenance Model	Break-fix	Predictive maintenance
Configuration Management	Manual templates	Zero-touch automation
Service Continuity	Failover-based	Self-healing capabilities

Table 1: Performance Gap: Traditional vs. AI-Driven SD-WAN Cellular Monitoring [1, 2]

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

2. Legacy Methods of Cellular Monitoring within SD-WAN

2.1 An Overview of Legacy SD-WAN Architectures

Premeditive WANs that preceded SD-WAN were largely reliant on hardware routers and used manual settings, often in the form of Multiprotocol Label Switching (MPLS) to provide dedicated, predictable connections. Traditional architectures have been characterized by high initial investment, a high level of network engineering skills, and long provisioning time, which presented colossal challenges to organizations that desire to react swiftly to changing business requirements. Before SD-WAN adoption, enterprise WAN architectures often had hub-and-spoke topologies with corporate data centers as the center of the hub and branch offices backhauling all traffic, including clock traffic, via centralized security infrastructure. This resulted in high latency penalties and wasteful resource usage, especially as cloud usage sped up within industries [3].

Contrary to this, initial SD-WAN deployments created software overlays but kept much of the traditional monitoring aspects. These early SD-WAN solutions separated network control from hardware, allowing for more policy-driven management of traffic across a variety of transport mediums. Even with these improvements, the monitoring aspects of these systems were still rooted in traditional networking concepts and relied mainly on simple connectivity state and primitive performance data. This constraint became more and more problematic as deployments grew to include more sophisticated, hybrid environments with both wired and wireless transport components [3].

Cellular integration in these configurations is usually the monitoring of LTE or 5G connections as backup or failover links, where simple protocols such as Simple Network Management Protocol (SNMP) are used to poll device status and performance statistics. Embedding of cellular/network technologies in SD-WAN systems was also a significant development in branch connectivity backup, particularly where wired backup options were not possible or too expensive at the location. Yet, the intrinsic nature of cellular networks—variable signal quality, shared medium contention, and carrier-specific implementation variations—posed significant monitoring challenges for traditional tools. In most deployments, cellular links were set up largely for use in failover situations, with little visibility into performance characteristics until actively in use during primary link failures [4].

In this case, the parameters of interest, such as signal strength (Received Signal Strength Indicator or RSSI), packet loss, jitter, and throughput, are being monitored. These metrics are usually configured with fixed thresholds by the network administrators, and when the measurements exceed the thresholds, alerts are raised. Software such as NetFlow or sFlow gathers flow information from edge devices, making it possible to gain visibility into traffic patterns throughout the network fabric. This telemetry gives insight into application performance and resource utilization, albeit generally at a fairly coarse granularity in comparison to more sophisticated monitoring methods. Numerous companies enhance these capabilities with vendor-provided management software that gives additional visibility into proprietary device properties and connection status [3].

Yet, these techniques are intrinsically reactive: problems are detected after the fact via threshold-based alarms, resulting in downtime in dynamic cellular settings in which mobility, interference, and congestion are common. This constraint becomes quite critical where one has mobile users, vehicles, or transient deployments, where the cellular connectivity behavior may rapidly change, depending on location, environmental conditions, and network load. Traditional monitoring mechanisms typically cannot manage this variation, typically resulting in an excessive number of false alarms (because they are sensitive enough) or missed service-quashing conditions (because they are permissive enough). Such a reactive approach often means prolonged resolution times, lowered user experience, and operational inefficiencies [4].

2.2 Most Important Conventional Monitoring Methods

Conventional cellular monitoring in SD-WAN environments involves some time-tested methods, each with certain capabilities and shortcomings. Protocol-Based Polling and Telemetry is one of the most prevalent methods, with SNMP still being a foundational technology for network management across various infrastructure components. This technique includes regular querying of equipment for statistics such as CPU usage, interface errors, memory consumption, and bandwidth use. In SD-WAN implementations involving cellular connectivity, this includes cellular modems, monitoring modem health, signal quality readings, connection statuses, and data transfer rates. SNMP implementations usually work on a fixed polling cadence, which introduces a trade-off between monitoring granularity and system overhead: shorter cycles yield more responsive detection but create higher management traffic and processing loads [3].

Another significant technique of testing cellular performance in an SD-WAN environment is Synthetic Monitoring and Probes. Such products as ThousandEyes, AppNeta, and vendor-specific software employ active probes to simulate traffic along cellular routes and measure the end-to-end performance properties that better represent the experience of actual users. Such synthetic transactions are able to test application-specific metrics such as DNS resolution time, HTTP response time, voice quality metrics, and video streaming quality. Through this method, bottlenecks and degradations in the communication path including carrier networks outside the enterprise perimeter can be detected. However, synthetic monitoring adds other complexities such as requiring probe placement to be done thoughtfully, determining test frequency correctly, and taking into account the impact of monitoring traffic itself on network usage. Manual setup is required for the approach and can utilize valuable bandwidth, especially on limited cellular links where monitoring traffic may contend with business-critical applications [4].

Log Analysis and Threshold Alerting is are core components in traditional cellular monitoring for SD-WAN. Centralized controllers collect SD-WAN edge logs, with rule-based systems triggering alerts when metrics surpass predetermined thresholds, including high cellular handover latency or prolonged bandwidth usage nearing link capacity. This method takes advantage of the large telemetry data created by contemporary SD-WAN deployments, including detailed cellular modem states, carrier network health, and application performance metrics. Log analysis generally uses filtering rules and correlation policies to detect patterns of potential service effects. Although useful for finding obvious threshold breaches, the technique has difficulty with subtle degradations that may not break defined thresholds but still affect user experiences. Furthermore, log data volume in large-scale deployments can grow too large, possibly hiding valuable insights amidst mundane operational information [3].

Hardware-Centric Security Monitoring is an important element of classical SD-WAN cellular integration, especially considering the increased attack surface brought about by wireless connectivity. Classic methods involve simple firewalls and VPNs for cellular traffic, threat monitoring through signature-based intrusion detection systems. These security controls normally aim to enforce perimeter-based policies, scan traffic for recognized attack patterns, and provide encrypted tunnels for the transmission of sensitive data. The security monitoring functions focus mainly on capturing unauthorized attempts at access, anomalous traffic behaviors, or recognized malicious signatures. Such methods tend to lack the complexity, though, of recognizing advanced threats or zero-day attacks, especially those that are directly aimed at cellular network vulnerabilities. The security monitoring features tend to run detached from performance monitoring systems, generating potential blind spots where performance and security issues converge [4].

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

Monitoring Technique	Primary Function	Key Limitations	Resource Impact
Protocol-Based Polling (SNMP)	Device status metrics collection	Fixed polling intervals	Higher with shorter intervals
Synthetic Monitoring	End-to-end performance simulation	Manual configuration required	Consumes valuable bandwidth
Log Analysis	Threshold-based alerting	Misses subtle degradations	High storage requirements
Hardware-Centric Security	Signature-based threat detection	Limited zero-day protection	Separate from performance monitoring

Table 2: Limitations of Legacy SD-WAN Cellular Monitoring Techniques [3, 4]

3. The Role of AI/ML in SD-WAN Cellular Monitoring

The introduction of artificial intelligence and machine learning is a revolution to SD-WAN, particularly cellular monitoring. The core idea of AI-based solutions is that network management will shift to a more reactive than proactive state, using sophisticated data analytics to predict and prevent possible issues before they negatively influence the quality of services. This shift is a big leap from conventional threshold-based monitoring practices that have long been the norm for networking operations. Current AI-powered SD-WAN offerings mitigate long-standing issues through automation of intricate telemetry analysis, behavioral anomaly detection, fine-grained cellular traffic classification, predictive maintenance processes, and self-optimizing routing choices that update dynamically in response to evolving network conditions [5].

The embedding of AI/ML technology into cellular monitoring platforms has resulted in a number of pioneering innovations that together improve network resilience, performance, and security. Preemptive anomaly detection solutions use machine learning algorithms to scan large databases of historical performance data, providing the ability to predict cellular link failures and service degradations in advance of their effects on business operations. Such systems can identify fine-level trends that cause the loss of signal during peak times, and thus mitigation can be done before the problem occurs. What is more, AI-based traffic management systems are able to predict congestion events across the cellular network and re-steer application flows of mission-critical applications to alternative transport channels automatically, enabling continuity of services even when networks are poor. Sophisticated platforms offer conversational question functionality for network professionals, significantly lowering mean time to resolution for difficult cellular connectivity problems. AI-based monitoring regularly looks at wireless link statistics for preemptive signs of congestion, interference, or device failure, reducing any downtime through swift remediation processes [5].

Dynamic Quality of Service (QoS) and path optimization are other important features supported by AI/ML technologies in cellular SD-WAN deployments. Smart systems dynamically allocate traffic over hybrid cellular and wired networks based on demand that depends on applications on the basis of superior reinforcement learning policies that are updated in response to changing user behaviors and application patterns. These ML algorithms examine historic performance trends and network telemetry in real time to take routing decisions in milliseconds, such that high-priority application traffic is routed across the best available links. It is this capability that will be most useful in a cellular world, wherein conditions of linkages change rapidly depending on such factors as mobility, environmental conditions, and the changing rates of network congestion. The AI-optimized

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

optimization goes beyond basic failover to include sophisticated traffic engineering judgments that take into account application sensitivity to certain performance metrics such as latency, jitter, and packet loss [6].

Integrated security analytics are now key elements of SD-WAN deployments today, in which AI technologies are baked in to protect against increasingly evasive threat patterns that target distributed networks and wireless links specifically. The security platforms quickly detect potentially malicious traffic patterns, abnormal data flows, and anomalous activities that could signal attempts at compromise. The integration supports zero-trust-enabled automated response policies underpinning zero-trust security guidelines in which each connection request is stringently authenticated irrespective of origin. This is especially important for cellular-connected locations, which historically have exposed security monitoring difficulties as a result of their distributed location and carrier network dependencies [5].

Advanced SD-WAN implementations increasingly integrate self-healing functionality driven by machine learning algorithms. These autonomous systems continuously monitor the health of networks on cellular links and fixed links, and dynamically adjust the settings, rerouting traffic streams, and reducing inconveniences with minimal human intervention. Self-healing component makes use of predictive analysis capability to anticipate potential areas of failure and proactively implement mitigation measures, which greatly reduces the impact of services. This automated operation is particularly beneficial for cellular-connected remote facilities where technical support on-site may be sparse or nonexistent. These systems' ongoing learning components allow them to become increasingly proficient in the administration of complex network infrastructures, as they gain experience through operational data and improve their analytical models using supervised and unsupervised learning methodologies [6].

Predictive maintenance is another example of AI/ML technologies used in cellular SD-WAN environments, with advanced algorithms predicting impending hardware failure or signal degradations from detailed device telemetry and historical trends of performance. These systems scan for faint symptoms that may signal equipment failures, allowing pre-emptive scheduling of maintenance prior to service-affecting failures. Predictive functions are not limited to cellular modems, antennas, and supporting infrastructure equipment, but also alert in advance of declining performance that may otherwise pass unnoticed until it produces serious service outages. This method converts maintenance activities from reactive to preventive, significantly enhancing service dependability while streamlining resource allocation for technical interventions [5].

3.1 New Age Approaches: The Underpinning Framework

The key to addressing the challenge of contemporary networking is in the holistic deployment of Artificial Intelligence for IT Operations, more popularly known as AIOps. This new field utilizes sophisticated machine learning algorithms and advanced big data analysis to drive automation of complex network management tasks, revolutionizing the operational model from a reactive, fire-fighting model to a proactive, intelligence-driven model that predicts and prevents impending problems. The powers of transformation in AIOps are built upon its unparalleled capacity to consume and systematically process vast amounts of operational data from a variety of sources across the network infrastructure, ranging from real-time performance measurements, granular event logs, system status signals, and application-level telemetry. Such end-to-end data integration facilitates the discovery of subtle patterns, detection of anomalous behavior, and execution of automated remediation workflows that are not feasible through traditional management paradigms [6].

A strong AIOps-powered SD-WAN solution that is appropriate for cellular integration can be well-architected by using a highly evolved layered structure that compartmentalizes functional tasks but continues to operate in coordination. The Data Layer constitutes the building block of such an

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

architecture, which includes distributed SD-WAN edge devices and purposeful routers strategically positioned at branch offices, data centers, cloud infrastructure, and remote sites. These edge pieces perform dual functions: directing network traffic based on predefined policies while, at the same time, gathering complete, high-resolution telemetry information in numerous dimensions, such as packet loss measurement, bandwidth usage patterns, latency, and jitter measurements for both fixed and mobile networks. The collected telemetry is a treasure trove of "data gold" whose size and intricacy are way beyond human analysis capability and require automatic processing via machine learning [5].

Learning Layer is the analytical core of the AIOps and accommodates sophisticated AI/ML models that are optimized to perform network optimization and management duties. The Learning Layer takes the enormous telemetry streams fed by the Data Layer in real time, and puts them through specialized algorithms, searching them to find patterns, establish performance baselines, detect anomalies, and provide predictive insights. The analytical potential enables autonomous control decisions and pushes predictive analytics that predict potential problems ahead of time, before affecting service quality. This layer uses varied machine learning techniques customized to particular analysis needs: supervised learning models for traffic classification and application detection; unsupervised techniques for anomaly detection and pattern recognition; and advanced deep reinforcement learning platforms for dynamic policy optimization and adaptive traffic management on cellular and wire transport options [6].

The Control Layer is the operational hub of the AIOps-powered SD-WAN ecosystem that is where the centralized or distributed SD-WAN controller infrastructure fortified with embedded AI models, resides. It is the key layer that converts the learned patterns and predictive information developed by the Learning Layer into actual, implementable network management actions, such as smart traffic steering, dynamic path choice, adaptive quality of service settings, and self-healing remediation processes. The Control Layer establishes a closed-loop system of management that optimizes network performance constantly without human intervention, vastly enhancing operational effectiveness while accelerating service quality. Autonomous operation becomes especially useful in managing cellular connectivity, where link behavior can shift quickly and instant adaptive action is needed to support desired levels of performance [5].

Layer	Primary Function	Key Components	Output
Data Layer	Collection	SD-WAN edge devices, distributed routers	Telemetry data (packet loss, bandwidth, latency, jitter)
Learning Layer	Analysis	AI/ML models (supervised, unsupervised, reinforcement learning)	Patterns, baselines, anomalies, predictions
Control Layer	Execution	SD-WAN controller with AI integration	Traffic steering, path selection, QoS adjustments, and remediation

Table 3: Closed-Loop Intelligence: The AIOps Framework for Cellular SD-WAN [5, 6]

3.2 Advanced AI-Driven Capabilities

3.2.1 Self-Healing SD-WANs

Autonomous SD-WAN networks that utilize sophisticated machine learning capabilities continuously monitor cellular and fixed links using advanced real-time analytics, process cloud-based telemetry using distributed computer frameworks, and apply remediation steps with low latency. These self-healing systems integrate multiple automated features that together improve network performance consistency and resilience. Smarter route failover techniques continuously monitor transport quality along accessible paths, automatically routing traffic over alternate connections when detected or anticipated performance degradations occur. The bandwidth optimization techniques are dynamically changing the resource allocation in real time according to the application demand and observed network conditions so that the effective throughput is optimized with the minimum impact of congestion. Fully embedded diagnostic methods constantly analyze performance telemetry to identify likely trouble spots ahead of time, before they can impact services and cause remediation processes with minimal or no human intervention. These abilities are especially useful for cell-connected locations, where link characteristics change widely depending on environmental conditions, network traffic, and mobility behaviors [6].

3.2.2 AI-defined Quality of Experience (QoE)

Legacy network management tends to concentrate on general Service Level Agreement (SLA) metrics that fail to capture real user experiences effectively. In contrast, contemporary ML-based systems utilize AI-defined frameworks for Quality of Experience that dynamically steer network policies and behaviors to optimize perceived user satisfaction and app performance. This advanced method goes beyond traditional monitoring with the addition of contextual awareness and application-specific needs to the management model. For cellular connections integrated into SD-WAN infrastructures, this translates to end-to-end performance monitoring that goes beyond simple availability monitoring and incorporates detailed control of throughput behavior, latency profiles, and jitter parameters optimized for mission-critical or latency-sensitive workloads. The AI-powered systems learn constantly from what is observed in terms of performance behavior and user activity, increasingly refining their intelligence about application needs and dynamically optimizing network behaviors accordingly. This method becomes especially useful for hybrid configurations that integrate both cellular and wired connections, where smart path choosing can significantly influence application performance and user experience [5].

3.2.3 AI-driven Threat Intelligence and Zero Trust

The shift towards direct branch-to-cloud models of connectivity enabled by SD-WAN has substantially redefined enterprise security models, calling for advanced protection mechanisms able to function efficiently in distributed configurations that include both wireless and wired links. AI-powered security engines constantly scan network traffic patterns, instantly detecting abnormal activity that could be a sign of attempted compromises or security policy infringement. The security systems can identify subtle signs such as aberrant lateral movement trends, suspicious DNS query habits, or unusual data transfer activities that human security software may fail to recognize. After they have identified possible threats, the AI-based security frameworks apply adaptive microsegmentation policies, impose contextual access controls, and orchestrate auto-response threat measures consistent with zero-trust security principles. This end-to-end strategy produces a strong, distributed security mesh that delivers uniform protection for every network segment, including cellular-connected remote offices that historically have posed security monitoring difficulties [6].

3.2.4 AI for Deployment and Lifecycle Automation

The sophistication of today's SD-WAN environments with multiple connectivity options, including cellular transport, poses important operational issues across the network lifecycle. AI-based automation greatly mitigates these efforts through functions such as zero-touch provisioning, which facilitates speedy deployment without intensive manual configuration; template-based configuration management that provides consistency across the distributed sites; and automated compliance monitoring that ensures policy compliance across the environment. In addition, new generative AI technologies are also being woven into operational processes to simplify site onboarding procedures, increase root cause analysis capabilities, and automate document generation. These technologies significantly lower Day 2 operational demands so that network teams can dedicate their time and energy to strategic initiatives instead of repetitive management processes. The automation advantages are especially useful for cellular-enabled SD-WAN rollouts, where site conditions, carrier partnerships, and connectivity settings can differ considerably within the organization [5].

3.2.5 Predictive Network Management using Predictive Analytics

Possibly the most important benefit of an AI-based methodology for managing SD-WAN is the underlying move away from reactive incident response and towards proactive problem avoidance using advanced predictive analytics. These higher-order abilities allow network management systems to predict impending issues before they affect business operations or user experience, significantly enhancing service dependability while decreasing operational downtime. Predictive operations constantly examine enormous stores of historical network information in addition to real-time telemetry streams, detecting faint trends and patterns that normally lead to particular categories of network problems. This predictive insight helps with automated mitigation and resolution processes that can avoid incidents altogether, as opposed to reacting after they have happened. The predictive features are most useful for cellular connectivity management, where the characteristics of a link may evolve quickly depending on environmental conditions, network congestion levels, and mobility patterns [6].

Predictive analytics capabilities provide great business value through a number of the most important applications in cellular SD-WAN setups. Predictive maintenance systems review past telemetry data to predict possible hardware failure or connectivity slowdowns prior to affecting services. For instance, a sophisticated machine learning algorithm may recognize subtle performance behaviors that point towards a cellular link's reliability weakening invariably after certain environmental factors remain in effect for a long duration, allowing the system to initiate automated failover procedures or send technical personnel in advance of affecting end-user experiences. In the same way, AI-based capacity planning features predict bandwidth demands based on past usage patterns, seasonal usage, and business growth metrics to enable organizations to make informed decisions regarding investments in the network and resource deployment. Through this foresight, organizations can prevent both expensive overprovisioning situations and potentially disruptive performance bottlenecks that could otherwise degrade user experiences during peak usage periods [5].

3.2.6 Autonomous Anomaly Detection and Root Cause Analysis

AI-based SD-WAN products exhibit outstanding proficiency in detecting unusual network activities that diverge from defined performance baselines, typically sensing faint signals that would most probably go unnoticed through traditional monitoring mechanisms. Advanced unsupervised learning algorithms, such as innovative autoencoders, k-means clustering algorithms, and density-based spatial analysis, analyze network telemetry data in real-time to automatically detect outliers without the need for pre-defined detection rules or thresholds. This feature facilitates the recognition of upcoming issues such as imminent cellular link degradations, router misconfiguration effects, or possible security attacks prior to significantly impacting service quality. The anomaly detection capabilities run on both cellular and wired connectivity platforms, gaining full visibility into hybrid network infrastructures typical of contemporary enterprise networks [6].

In advanced SD-WAN implementations with multiple transport types, such as cellular links, a single root problem often causes a cascade of effects that initiate multiple associated alerts across multiple monitoring platforms. This "alert storm" problem develops into major network operations challenges in pinpointing root causes amidst massive symptom indications. Next-generation AIOps solutions solve this problem by gathering and correlating telemetry across multiple domains—system logs, API transaction data, performance metrics, and application-level signals—to build an end-to-end, unified understanding of the situation. By subjecting this combined dataset to advanced machine learning algorithms, the systems are able to automatically detect causal relationships and identify root cause sources, slashing the time to manual investigation by orders of magnitude while speeding up the

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

resolution process. This ability is most useful in the context of cellular network connectivity troubleshooting, where issues may be located in carrier networks outside of the enterprise boundary but be experienced as performance degradations within the organizational infrastructure [5].

3.2.7 Intelligent Traffic Steering through Reinforcement Learning

While predictive analytics capabilities deliver useful insight into possible future network conditions, reinforcement learning (RL) technologies deliver the key mechanism for autonomous real-time optimization of traffic flows through available transportation options, such as cellular connections. Within this advanced deployment environment, expert RL agents serve as critical building blocks within the Learning Layer, constantly evaluating performance traits across every transport link available and calculating best routes for particular application streams in response to both immediate conditions and acquired patterns. Compared with traditional static policies with rigid, predefined decision trees, RL-based mechanisms learn from real-time dynamic network conditions continually, refining their decision models iteratively to respond effectively to abrupt changes in traffic patterns, link performance degradations, or connectivity disruptions without the need for administrative intervention or policy updates [6].

The SD-WAN controller platform, acting as a part of the Control Layer, utilizes these RL specialist agents to make highly advanced traffic steering decisions within each evaluation interval, implementing intelligent application flow distribution across available transports to guarantee balanced resource usage and performance delivery consistency. This ability is especially important in dealing with cellular connectivity over hybrid environments, since such wireless connections usually have higher performance variations than wired ones based on parameters such as environmental issues, network overloading, and movement patterns. An advanced RL agent can detect subtle indicators suggesting that a cellular link's latency characteristics are beginning to deteriorate and, without human intervention, automatically reroute latency-sensitive applications like video conferencing or VoIP communications to more stable transport alternatives, maintaining business continuity during challenging network conditions. This smart method guarantees that mission-critical applications get the right prioritization based on ongoing examination of real-time contextual elements and application behavior patterns instead of using static, preconfigured rules that are unable to change in response to shifting conditions [5].

AI Capability	Primary Function	Business Impact	Implementation Challenge
Self-Healing Networks	Autonomous remediation	Minimal downtime	Integration complexity
AI-defined QoE	Context-aware optimization	Enhanced user experience	Metric definition
Security Intelligence	Zero-trust enforcement	Reduced threat surface	Cross-domain visibility
Lifecycle Automation	Zero-touch provisioning	Operational efficiency	Multi-vendor support
Predictive Analytics	Proactive issue prevention	Business continuity	Data quality requirements
Anomaly Detection	Pattern deviation identification	Reduced alert storms	Baseline establishment
Reinforcement Learning	Intelligent traffic steering	Application performance	Model training needs

Table 4: Evolution of Intelligence: AI Capabilities in SD-WAN Cellular Monitoring [5, 6]

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Conclusion

The use of AI and machine learning technologies has truly changed the face of cellular monitoring in SD-WAN settings, and this shift is a paradigm shift from reactive to proactive network management. This development remedies the inherent shortcomings of traditional monitoring methods that were not suitable to dynamically cellular connections that are defined by variability of signals, difficulties in mobility, and carrier dependencies. Through the introduction of intelligence into the network infrastructure, organizations are now able to attain resilience levels, performance optimization and security improvements never before achievable using traditional means. The three-level AIOps system that encompasses information collection, machine learning data analysis, and automated control features constitutes a closed-loop system that can be continuously self-improved and take independent decisions. More sophisticated applications like predictive analytics, anomaly detection, intelligent control over traffic steering with reinforcement learning, and self-healing remediation, all enable networks to anticipate issues before they can impact the services, automatically optimize application delivery, and keep going even in challenging conditions. The AI-friendly functions will be essential rather than optional, particularly to support mission-critical operations in multiple locations, as additional companies will change their operational paradigm to distributed operations and create more solid hybrid connectivity requirements.Companies that manage to deploy these advanced monitoring systems achieve significant competitive advantages due to improved user experiences, improvements in operational efficiency, and complexity in management of their distributed networks. Further developmental solutions must be oriented towards further refinement of the algorithm, a wider range of machine learning applications, a holistic approach to security integration, and the development of new regulatory issues concerning automated decision-making in enterprise infrastructure.

References

[1] Eric Olinger, "How AI Will Shape the Future of SD-WAN," Equinix Blog, 2024. [Online]. Available: https://blog.equinix.com/blog/2024/04/10/how-ai-will-shape-the-future-of-sd-wan/

[2] Palo Alto Networks, "Why Machine Learning (ML) and Artificial Intelligence (AI) Are Key Technologies for SD-WAN,". [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/why-ml-and-ai-are-key-technologies-for-sd-wan

[3] Doug Bundgaard, "Best Practices for Operating and Monitoring an SD-WAN Network," Broadcom Academy, 2024. [Online]. Available: https://academy.broadcom.com/blog/network-observability/appneta/best-practices-for-operating-and-monitoring-an-sd-wan-network

[4] Juniper Networks, "AI-Driven SD-WAN Accelerates Digital Transformation with an Agile, Efficient and Resilient Network,". [Online]. Available: https://www.juniper.net/content/dam/www/assets/solution-briefs/us/en/routers/ai-driven-sd-wan-accelerates-digital-transformation-with-an-agile-efficient-and-resilient-network.pdf

[5] Lightpath, "How SD-WAN Can Optimize Networks for AI and Cloud Applications," 2025. [Online]. Available: https://lightpathfiber.com/articles/how-sd-wan-can-optimize-networks-ai-and-cloud-applications

[6] Pham Tran Anh Quang et al., "Routing and QoS Policy Optimization in SD-WAN," arXiv:2209.12515, 2022. [Online]. Available: https://arxiv.org/abs/2209.12515