How AI is transforming networks

Capacity's Ben Wodecki explores AI's impact on improving and securing communication networks

Artificial intelligence (AI) has had an impact across every business and every industry, no matter how big or how small. Even before that fateful November day when OpenAI captured the public's imagination with ChatGPT, AI was already transforming various sectors.

Communication networks are no different, with AI-powered tools and algorithms helping to transform communication networks to become faster and more secure.

Statistics from Veritis, the Texas-based technology consulting company, suggest that using AI to help with network optimisation can result in a 20% reduction in latency and AI-based cybersecurity measures can reduce fraud-related losses by 30%.

A 2024 Forrester study found that technology from AI translation company DeepL reduced translation workloads by 50%, generating a 345% return on investment (ROI).

Telcos are already looking to augment their operations with AI, with figures from Research and Markets suggesting that the global AI in telecommunication market size will reach $11.29 billion by 2030.

Capacity takes a look at AI's impact on communication networks, showcasing what's to come in this space.

AI-DRIVEN NETWORK AUTOMATION

While still an emerging technology, AI is already being leveraged to automate tasks that once required manual human effort. Communication network operators are increasingly turning to AI-driven solutions to streamline a wide range of processes, enhancing both operational efficiency and service quality.

From productivity tools like chatbots trained on company data to customer service automation, AI is reshaping how networks function. It's also being deployed for more complex tasks, such as traffic management, predictive maintenance,

and even network optimisation, where algorithms analyse vast amounts of data to anticipate and resolve issues before they affect performance.

This shift not only reduces the need for constant human oversight but also allows for faster, more accurate decision-making. By automating routine tasks, AI frees up skilled operators to focus on more strategic initiatives, driving innovation and competitive advantage within the industry.

For example, Hewlett Packard Enterprise (HPE) launched an AI-powered tool that monitors IoT devices, looking for signs of unusual activity.

"AI-driven network automation, particularly around enhancing operational efficiency and responsiveness, ensures providers can achieve greater efficiencies across all levels of their networks, leading to improved profitability," said Stuart Strickland, wireless chief technology officer and fellow at HPE Aruba Networking at HPE.

"By making it easier for telcos and others to leverage AIOps in network orchestration, they can virtualise and scale their infrastructure to provide new services and lower their operational costs."

Other such applications are the Infosys-Nvidia co-developed suite of microservices that provide network operators with generative AI tools to build their own custom customer-facing chatbots or solutions that help network engineers and operations personnel troubleshoot issues faster.

> "By embracing AI we can better handle future network demands and craft a more efficient world"

"AI extends beyond merely boosting efficiency – it's being used to revolutionise how networks handle the growing complexity of devices and data flow," said Ulises Olvera-Hernandez, senior principal engineer at InterDigital.

"AI-driven innovations are designed to foster more dynamic network environments, reduce energy consumption, enhance user experiences, and fortify security protocols. By embracing AI, we can better handle future network demands and actively craft a more interconnected and efficient world."

OPTIMISING BANDWIDTH & REDUCING COMPLEXITY

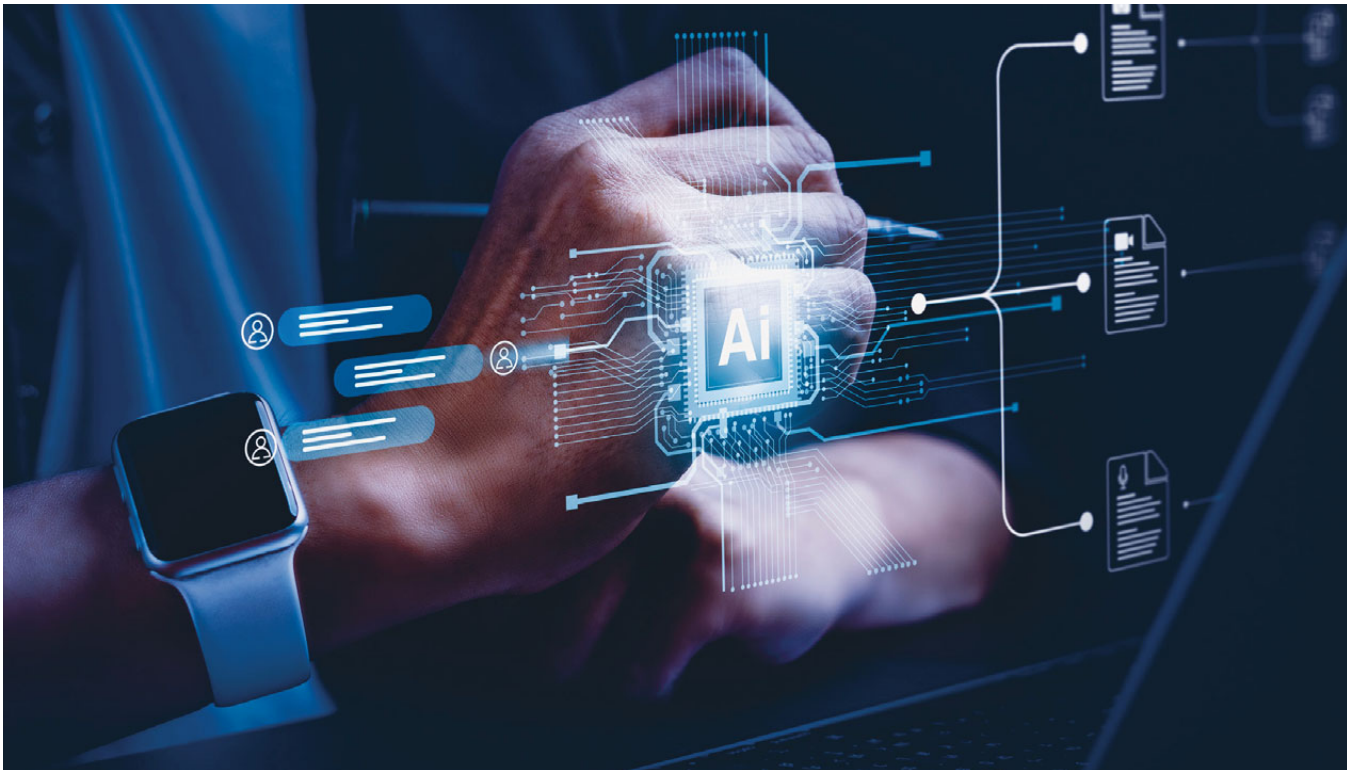
In line with automating network operations, AI is also helping improve bandwidth optimisation.

AI can automatically adjust bandwidth allocation to ensure demands are met in real-time. With AI tools monitoring performance, such tools can be used to create a more dynamic and adaptable network to ensure demands are met and then scaled down during off-peak times.

Aside from helping meet demands, AI is also a leading cause for increased demand on network operations.

Training models and running inference require intense computing levels running continuously at high speeds.

Mattias Fridstrom, chief evangelist at Arelion, told Capacity that increased demands from AI workloads are essentially "forcing" operators to transform their networks to be faster, better and more flexible.



"This requires innovation of the optical networking layer through 400G coherent pluggables, open line systems and other technologies that can provide the immense bandwidth necessary for transporting AI's high data capacities between data centres," Fridstrom said.

Despite placing increased demands, Fridstrom suggested that network automation is key to optimising bandwidth to meet AI's immense real-time requirements, reducing the need for manual intervention when allocating resources to help increase network uptime.

AI is also being used to reduce network complexity by more easily spotting issues in legacy systems as well as newer systems.

"Due to mounting complexity, network operators face a growing number of service issues such as poor quality of experience and frequent 'alarm storms' which lead to extended outages, reduced network performance and inefficiencies," said Joe Krystofik, head of AI software product planning, network automation at Fujitsu Network Communications.

"Tracing the root cause of an alarm storm can take hundreds of staff hours, potentially costing millions of dollars in direct costs and customer churn. Static network management configurations are no longer sufficient to handle these complicated networks.

"The development of AI-powered models like neural networks, large language models and generative AI enables an intelligent network capable of autonomously making appropriate decisions on events that are difficult to handle manually to consistently maintain optimised service quality."

ENHANCING SECURITY

AI's automation extends to security, with such technologies providing operators a way to keep pace with incidents at speed.

"AI enables network operators to detect cyber threats in real-time," said Luis Fiallo, VP at China Telecom Americas. "AI systems can constantly monitor network traffic, identifying risks much faster than manual monitoring. This allows for a much faster response time to implement mitigation tactics that will fend off an attack altogether or limit the overall impact of a potential breach."

Tools like Aryaka and CheckPoint Software's ThreatCloud AI provide network operators with 24/7 observability of their network attack surface, routinely scanning environments for anomalies to notify operators of potential threats.

By automating threat detection with AI-driven security and monitoring solutions, network operators can reduce costs and allow staff to focus on system upgrades and improvements rather than continuous security monitoring.

"AI can identify weak points in the structure and identify solutions in a fraction of the time," said Edward Tian, CEO of AI-detection platform GPTZero. "That way, companies don't have to just respond to cyberattacks that are currently being attempted - they can better prevent them in the first place.

Security isn't a one-way street — it also involves embedding security practices directly into AI workflows to safeguard emerging systems.

This approach, known as MLSecOps, integrates "secure by design" principles into the development and deployment of AI and machine learning systems.

Although MLSecOps isn't exclusively tied to network operations, it can offer network operators a critical security baseline, ensuring that AI workloads are securely configured from the outset.

Imagine you're implementing an anomaly detection model to identify unusual signals or unauthorised access to the network. By addressing potential risks like denial of service (DoS) attacks or data poisoning early in the design phase, operators can quickly deploy safeguards, enhancing the system's overall resilience.

Fiallo added: "Not only can AI help detect potential breaches, but also help with automating responses to threats, like applying security patches."