www.pipelinepub.com
Volume 21, Issue 1

What Will Shape the Future of Non-Terrestrial Networks and Global IoT?

By: Avnish Chauhan

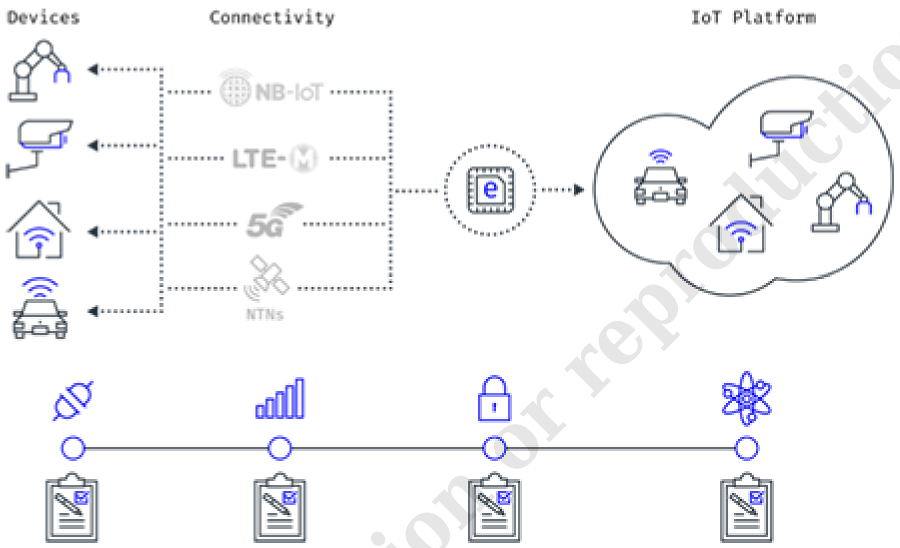
The rise of Non-Terrestrial Networks and the acceleration of IoT are a $58 billion opportunity that is knocking on CSPs' doorsteps. However, to seize this opportunity, operators need to understand the underlying trends molding these markets and to start addressing some critical questions.

Trend 1: The Rise of NTNs

Non-Terrestrial Networks (NTNs) will soon become an integral part of the future connectivity fabric. Juniper Research projects that the number of satellites is expected to grow 150 percent over the next five years, from 10,000 in 2024 to over 24,000 by 2029. While strategic partnerships are already underway to deliver the promise of seamless, borderless connectivity for consumers and enterprises, the global network ecosystem needs to start adapting today to the rise of NTNs – from a technical, commercial, and philosophical standpoint.

For example, operators will need to adapt their business model and infrastructure to integrate NTNs with their existing networks. This will involve technical changes, such as upgrading core networks to handle satellite communications and hybrid terrestrial-satellite architectures. It also includes investment in new systems for managing spectrum, handling latency issues, and ensuring service continuity as users move between terrestrial and non-terrestrial networks. Operators will need advanced real-time analytics and monitoring to ensure network performance and reliability across the diverse and geographically dispersed endpoints and to deliver a quality of experience (QoE) similar to the one that users have grown accustomed to in today's cellular networks. And they will require evolved service assurance capabilities to support emergency services that need reliable and stable connectivity in every corner of the world. Operators will also need to understand what fraud and security risks they need to prepare for with NTNs. Particularly as fraud and security threats will become more complex as traffic moves across the different types of networks and new vulnerabilities are exposed.

How operators approach roaming will also need to be redefined. Roaming agreements will involve terrestrial operators as well as satellite network operators and will become more complex as global and regional agreements take into account the unique nature of satellite communications, including longer latency times and the movement of satellites. New frameworks will also be needed to manage cross-network interoperability, spectrum allocation, and billing. To meet all of NTN's new demands, operators will need advanced roaming and interconnect solutions to enable seamless transitions and handover between terrestrial and non-terrestrial networks, ensuring transparent billing, quality of service, and regulatory compliance across borders.



Trend 2: Ubiquitous Connectivity Sets up IoT for the Big League

One of NTN's key drivers is its ability to extend the reach of IoT devices globally, allowing for real-time data collection, monitoring, and control from any location, at any time. And while industries such as connected cars, eHealth, payments, logistics and travel are already making huge strides and gaining momentum, agriculture, mining, and maritime will soon join the fold with the rise of NTNs. (See diagram above.)

But connectivity is just part of the equation for IoT. CSPs also need critical IoT service assurance capabilities in place to truly deliver on the IoT promise. To unleash IoT's full potential, IoT service assurance needs to go beyond monitoring for connectivity. It needs to be global, and it needs to be hyper granular and application aware. This includes operators providing ubiquitous roaming capabilities, including IoT device management, visibility and monitoring, as well as global and targeted eSIM testing and detection.

It needs to assure the entire IoT Value chain, and it needs to link SLA monitoring to service-level objectives. Those service-level objectives must be relevant for each individual IoT service, application and device rather than general network-wide KPIs. For mobile operators to maximize their revenues, operators must have full control over which devices and subscribers can access certain services and at the right quality of service, and ensure that each chargeable event is billed correctly, fraud is detected and prevented, and revenue leakages are eliminated. With IoT service assurance, CSPs can perfectly balance QoE and business profitability. Juniper Research projects that by 2028, IoT connectivity revenue will be worth $28 billion per year. For operators to maximize their share of the revenue opportunities, AI is critical to ensure these requirements are addressed.

Trend 3: AI is Being Used for Good and Evil

AI will be essential to maximizing IoT and NTN revenues. AI is needed to provide CSPs with the ability to detect low-power devices and deliver real-time visibility into IoT KPIs, such as connectivity reliability and performance, power-saving features, and platform connectivity. Also, when satellite communications are involved, managing latency becomes critical and edge computing powered by AI will help minimize delays for time-sensitive applications.

Thankfully, when talking about the benefits of AI in the telecom industry, we are preaching to the converted. According to a study by Coleman Parkes Research, 70 percent of telcos are already using Generative AI (GenAI), with many fully implementing or testing the technology across departments such as marketing, sales, and IT. However, an important area where GenAI investment is critical is in the fraud and security arena. Generative AI and deepfakes have become a powerful new tool for fraudsters to scam consumers and businesses. Long gone are the days when we would easily spot a scam email from a Nigerian prince. Deepfake scams are now trying to deceive us via voice, SMS, and video. To demonstrate how real they are, consider this example: earlier this year a businessman was duped into transferring $25 million to fraudsters after having a video conference call with his deepfake “colleagues.” If humans are vulnerable, how can mobile networks protect themselves, consumers, and businesses from the new generation of fraud and security threats? It’s now time to fight fire with fire – or AI with AI.

Rules-based fraud and security detection provides a base level of protection that is not enough in today’s world. Machine learning helps to evolve rules-based detection by capturing information from each transaction it processes, learning the practices of traditional fraudsters and enriching the repository of historical data. But the next advancement will be critical for CSPs to minimize the prevalence of fraud and security threats. Generative AI empowers CSPs with greater precision and predictions to discover unknown threats and detect new and emerging fraud methods. With this information at hand, CSPs have actionable insights to respond quickly and block them.

As operators advance on their strategies to maximize their NTN and IoT revenues while eliminating fraud losses, they will have to upgrade their capabilities in terms of real-time network visibility, analytics, security and fraud management, and service assurance tailored to the complexities of NTNs and global IoT. The rise of NTNs and the rapid expansion of IoT will present a $58 billion per year opportunity for CSPs by 2035. But for communication service providers to capture this opportunity, they must answer these key questions: Are we ready for NTNs and making the required changes and investments to seize this opportunity? Do we have the IoT assurance systems and processes in place to ensure that each chargeable event is billed correctly, fraud is detected and prevented, and revenue leakages are eliminated? Do we have an AI roadmap prioritized and clearly defined to take advantage of emerging market opportunities? Are we making investments in the right areas?