White Paper

Digitalization with connectivity & AI

Building the Dynamic Private Wireless Network of the Future

Private 5G networks provide new tools and services for digital enterprises to utilize complementary technologies for multi-modal operation, security, sustainability, and management.

Authors

Valerie Parker
Network & Edge Senior Principal Engineer
Intel Corporation

Krishma S Hegde
Network & Edge Global Market Lead-Product Manager
Intel Corporation

Wireless network technologies have undergone significant evolution and improvement. Connectivity is becoming more software-based, enabling compute and communications to merge. This provides new innovations that allow enterprises to utilize multi-modal intelligent fabric networks that take advantage of any spectrum across multiple network types without isolation.

The private 5G network is a multi-access, data driven, intelligent network fabric utilizing data from multiple spectrums enabling network automation and the deployment of new applications. This network is the foundation of a range of future applications that will deliver highly immersive experiences. It leverages deeper levels of human-computer interaction, including innovative sensing, immersive extended reality (XR), distributed inferencing, management, and intelligent computing, among others.

5G networks offer multi spectrum access, enabling slicing, steering, switching, and aggregation of spectrum frequencies. Using network slicing, networks can be created with differing combinations of 5G network features for different use cases. For example, a slice with performance and low latency for streaming, and another slice with connectivity and reliability to support thousands of internet-of-things (IoT) sensors.

Similarly, Wi-Fi 7 brings multi-Gigabit data rates, deterministic latency, added privacy and security features. It provides reliability and more efficient operation through features like multi-link operation for simultaneous connection to two frequency bands, and multi resource units for sharing of data channels. This enables aggregation and slicing of spectrums.

What used to be clearly defined application use cases – 5G for wireless wide area networking and Wi-Fi for wireless local area networking – are blurring as the technologies grow more synergetic.

Enterprises are combining these wireless networks to create an Intelligent Fabric that optimizes data center and edge network connectivity through enhanced intelligence, performance, visibility, and control. Organizations can leverage the Intelligent Fabric for virtualization, containerization, workload optimization and bandwidth expansion. It serves the data center and the edge network. Applications can be placed anywhere within the scope of the fabric and have on-demand connectivity.

Now the fabric becomes a data driven network utilizing metrics and data analytics that automate the network behavior through AI, improving the quality of service, ensuring service level agreements (SLAs) are met and applications are placed based on policies and network capability.

Table of Contents

Networking Reimagined

While 5G, Wi-Fi, and other wireless technologies, provide the foundation for futuristic network services, there are other capabilities that are important in making private networks more dynamic and flexible. These technologies are embedded in data driven networks inclusive of traffic management, AI/ML, RAN intelligent controllers, confidential computing, security, and sustainability.

Multi Spectrum Traffic Management

The growth in data traffic globally combined with capacity constraints on 5G networks due to spectrum considerations, mean that 5G and Wi-Fi must work synergistically. Creating a multi-modal intelligent fabric is facilitated with Access Traffic Steering, Switching and Splitting (ATSSS) which is defined in 3GPP Rel16, and/or Generic Multi-Access (GMA). These technologies provide the ability to switch and steer data from 3GPP and non-3GPP networks.

As can be seen in Fig. 1, ATSSS provides the user equipment (UE) with Multipath TCP and ATSSS lower level (ATSSS-LL) functionality to steer data packets to either the 5G access point or the Wi-Fi access point (or other non-3GPP access point). The ATSSS functionality in the UE has a direct connection to the 5G Access and Mobility Management Function (AMF).

Generic Multi-Access[1] is an Intel innovation providing multi-access intelligent management control that can work with ATSSS or alternative methodologies at the IP Edge layer. GMA enables AI/analytics to perform on parameters like Quality of Service, bandwidth, noise and others from different connectivity infrastructures.

Data-Driven Networks (DDN)

In legacy networks, network management data is collected using agents and probes that are placed at key locations in the network. Samples of data packets are collected, analyzed and, based on that analysis, changes are made to network systems to improve performance.

DDN systems capture real-time data from every network node providing a complete view of network performance and environment such as temperature and security to isolate network problems so the right decision can be made automatically.

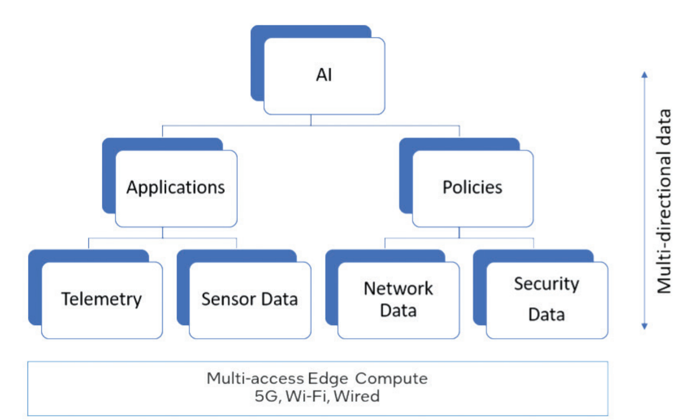

Figure 2. Information and analysis layers of an AI-based DDN.

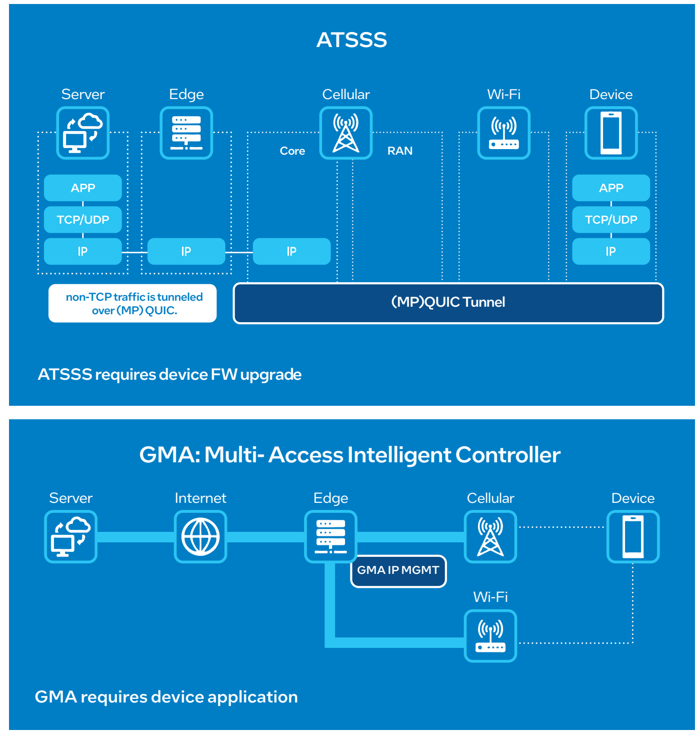

Figure 1. Multi-modal networks enabled through ATSSS and GMA.

The real time data is processed by artificial intelligence / machine language (AI/ML) systems to make instantaneous network changes to ensure that service level agreements (SLAs) and QoS requirements are enforced including those involving network latency which is very sensitive to network congestion/ degradation. The combination of information processing and AI/ML has led to data-driven networks (DDN) In DDN, the analysis of large volumes of real-time network data can help optimize network forwarding mechanisms. Stated another way, DDN is the application of big data analysis to raw network data, with the results then used to optimize network performance as seen in Figure 2.

Data Security at All Levels

To reduce cybersecurity risks in future networks, data security must be built into all levels of the solution including the CPU, the server, the application, and the network. Intel is innovating in this space with its Intel® Software Guard Extensions (Intel® SGX),which offers hardware-based memory encryption that isolates specific application code and data in memory.

Blockchain is already being used to secure vital management, billing, and other data transactions. But there's great potential in having it secure network data such as low latency transactional data or the authentication tokens for network slices.

Open RAN Intelligent Controller (RIC) Brings New Functionality

Open RAN (ORAN) has revolutionized cellular networking by virtualizing and disaggregating the baseband controller into standalone distributed units (DUs) and centralized units (CUs) which enables greater customization, flexible deployment options, including cloud deployment, and a larger RAN ecosystem for innovation with the potential for reduced cost.

The RAN intelligent controller (RIC) builds on this by adding software-defined functionality to control and optimize the CU and DU. The RIC can onboard two types of third-party applications that customize the network for specific use cases or automate and optimize RAN operations. These are:

- xApps are software programs that manage the near-real time aspects of the network. xApps can utilize metrics and data from the RAN to respond to network events in real time. With this capability, xApps can enable dynamic slicing, location services, quality of service (QoS) and other management and control applications.
- rApps are for non-real time (>1 second) applications that are a part of the Service Management and Orchestration (SMO) Framework and provide policy-based control of the xApps.

Figure 3 shows the overall RIC architecture and how it is a critical piece of ORAN, providing intelligence and policy to improve network performance and to enable new functionality.

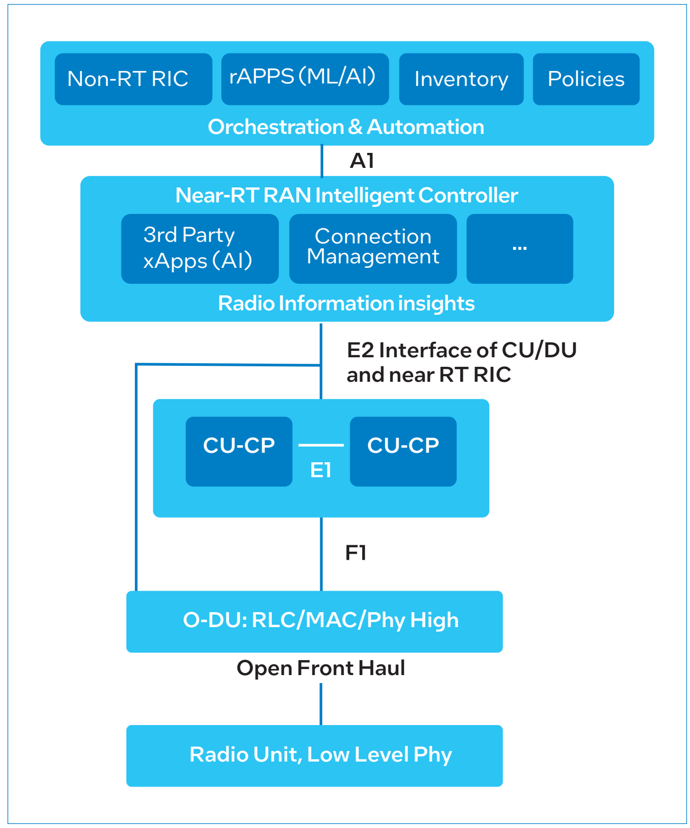

Figure 3. RIC architecture showing both the near-RT RIC and the non-RT RIC.

Protecting Data in Use with Confidential Computing

When moving workloads to the cloud, enterprises give up the physical control of their data which raises questions about privacy and data security. Cloud companies offer data privacy guarantees, but company events such as bankruptcy or government seizure of data are examples of the limits of these protections.

Its best practice to encrypt data while in transit and while being stored (at rest), and confidential computing enables data to remain encrypted while in use (being processed).

To accomplish this, confidential computing platforms utilize a hardware-based trusted execution environment (TEE). This enables a more secure cloud and hybrid computing environments that involve sensitive data.

Project Amber is an Intel Software as a Service (SaaS) project, leveraging the company's confidential computing architecture. It is a SaaS-based implementation of a zero-trust authority that provides remote verification of the trustworthiness of a compute asset based on attestation and policy.

Project Amber will verify the trustworthiness of Intel TEEs and the vision extends to much broader device verification, like IPUs, GPUs, platform roots of trust, and beyond. Project Amber is architected as a cloud-native microservice platform running on a managed Kubernetes service, with appropriate abstractions on different cloud infrastructure platforms, on-prem private networks, and edge locations.

DDN Use Cases

RF noise mitigation:

To protect the low latency levels offered by 5G it is important to reduce the RF noise. This can be done using AI to spot patterns in the layer 1 RAN. Wi-Fi metrics are proprietary, but there are projects underway with several standards bodies to further open metrics.

Quality of Service (QoS):

QoS is handled differently for 3GPP and non-3GPP networks. QoS is evolving to a multi-spectrum world to support very low latency wireless networks where networks must trigger a response. For example: The network now has the possibility to increase bandwidth to maintain network quality parameters, or to hand off a data flow to another network (from 5G to Wi-Fi, for example) in order to maintain QoS set by SLAs. Examples that could take advantage of DDN-based QoS include robotic surgeries, metaverse and financial applications.

Increasing Edge Network Sustainability

Increasing sustainability for intelligent fabric networks will be beneficial to the planet and help to make these remote networks cost effective. Governments and enterprises are headed towards more sustainable systems with low to zero emissions.

Intel is working on ways for servers in private networks, data centers, edge, and cloud to save energy via power consumption and providing processor SKUs fabricated utilizing green energy. Plus, Intel® Xeon® Scalable processors can minimize power consumption by configuring voltage levels (P-states) or by changing the sleep mode (C-state) status.

At first thought adding private networks might not seem helpful for sustainability but in reality, it helps move toward power management and distribution of power to go green. The private network and edge systems themselves, are moving towards a lower power consumption to reduce emissions. In private networks, Intel is using data transport traffic efficiencies to consume fewer resources. In addition, Intel has developed different ways to reduce power when networks are idle or at non-peak.

Conclusion

Wireless networks are becoming more critical to enterprises which has lead to the creation of an intelligent fabric that can be used to deliver new services with increased observability, bandwidth, and reduced latency. Advances in 5G and Wi-Fi 7 will enable these new network services and use cases. In addition, DDN, AI/ML, RICs, security, confidential computing, traffic management, and sustainability technologies deliver required functionality to ensure the security, manageability, and control of these networks.

Learn More

Intel's Project Amber

Solution Brief: Multi-access Traffic Management at the Edge

Intel Software Guard Extensions (Intel SGX)

UDP-based Generic Multi-Access (GMA) Control Protocol

Details of 'RGS/MEC-0015v211TrafMngtAPIs' Work Item

Multi-access Edge Computing (MEC); Radio Network Information API

Multi-access Edge Computing (MEC); WLAN Information API

Endnote

[1] https://www.ietf.org/archive/id/draft-zhu-intarea-gma-control-02.txt.

Notices & Disclaimers

Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.