allot
See. Control. Secure.

Whitepaper

AI-Powered DPI: Top 10 Use Cases for 5G Networks Optimization, Monetization, and Protection.

August 2025

Executive Summary

The deployment of 5G networks promises transformative performance improvements in speed, latency, and connectivity. However, realizing these benefits requires overcoming significant network availability, complexity, security, and monetization challenges.

Deep Packet Inspection (DPI), enhanced with AI/ML, is evolving into Deep Network Intelligence (DNI) and plays a pivotal role in addressing these challenges by enabling granular traffic management, improving security, and supporting monetization strategies. This paper explores the top 25 use cases for DNI in 5G networks and their role in maximizing network efficiency and revenue potential while protecting the network and securing customers.

Use Cases

1. Network Analytics and Insights
    A. **Real-Time Network Visibility**

    DNI provides granular insights into network usage, enabling operators to understand user behavior, device trends, and application performance for data-driven decision-making.

    B. **Predictive Maintenance**

    DNI helps predict network failures by analyzing traffic patterns and subscriber QoE, enabling proactive maintenance and minimizing service disruptions.

2. Quality of Experience (QoE) Assurance and Traffic Optimization (where 5G availability is still low)
    A. **Dynamic Traffic Prioritization for sensitive applications.**

    DNI facilitates real-time network traffic analysis, enabling operators to prioritize latency-sensitive services such as VoIP, cloud gaming, AR/VR, and V2X communications. This ensures optimal performance even during network congestion. By identifying and managing latency-sensitive applications, DNI ensures that 5G's ultra-low latency capabilities are effectively utilized, delivering superior user experiences.

    B. **Congestion Management**

    DNI detects congested network elements and dynamically allocates bandwidth, balancing network load and maintaining high performance, especially where 5G availability is still low and networks rely on congested 4G infrastructure.

    C. **Video QoE**

    Video now accounts for over 80% of total network traffic, a dominance driven by the sheer volume of viewers and the increasing quality of the content they consume. As resolutions rise, so does bandwidth demand. DNI's QoE analytics for encrypted video gives operators deep visibility into user experience, even when content is encrypted. By capturing each video session as a distinct event, such as a Netflix movie, it delivers detailed QoE metrics such as resolution, duration, and a new Encrypted Video QoE score.

This matters because video traffic is massive, error-prone, and highly sensitive to quality disruptions. Further more, with DNI, operators can proactively improve customer satisfaction, reduce churn, and plan smarter network upgrades.

3. Network Slicing and Customization
   A. **Slice-Specific Traffic Management**

      5G networks employ slicing to dedicate virtual network segments for specific use cases. DNI enables detailed analysis and policy enforcement within each slice, ensuring performance consistency across diverse services.

   B. SLA Monitoring and Assurance

      i. SLA Monitoring:

         DNI monitor compliance with Service-Level Agreements (SLAs) by continuously monitoring key slice performance metrics such as latency, jitter, and throughput—essential for enterprise services and industrial IoT.

      ii. SLA assurance:

         In parallel, DNI provides QoE assurance by tracking the actual user experience within each slice. This enables operators to validate not only that the network is performing to spec, but also that end-users are receiving the quality they expect.

         Together, SLA and QoE assurance empower operators to deliver reliable, high-performance services with full transparency and control.

4. Security and Threat Detection
   A. **Advanced Threat Detection & Mitigation**

      5G is built to support high-performance applications including autonomous vehicles, AR/VR, eHealth, and more. But its distributed architecture and massive scale also expand the network's attack surface, increasing vulnerability to sophisticated cyber threats. To protect their networks, 5G service providers need more than traditional security. The scale of connected devices, thousands of MEC nodes, and gigabit-level throughput per device demand a smarter, more adaptive approach.

      That’s where DNI with built-in AI comes in. It continuously inspects traffic in

real time to detect and mitigate threats such as DDoS attacks, botnets, and network intrusions—even before they impact service. By leveraging advanced machine learning, DNI identifies abnormal behaviors and adapts to evolving attack patterns, delivering intelligent, proactive protection for critical 5G infrastructure.

With solutions like Allot 5G Smart NetProtect powered by DNI, CSPs gain the layered, AI-enhanced defense they need to stay ahead of cyber threats in the 5G era.

B. IoT Device Protection

With billions of IoT devices connected to 5G networks, DNI is essential for detecting compromised devices and isolating threats to prevent network-wide disruptions.

5. Network Services Monetization

A. **Application Usage-Based Billing**

The ability to identify applications at Layer 7 allows operators to differentiate their offerings with a range of unique service plans based on popular applications, including gaming, social networking, video streaming, music streaming, and more. For example, operators may identify many customers as "Social minglers," meaning they are heavy users of social networks. This segment can be offered zero-rating on popular social networking apps so that usage is not counted against their data cap. Similarly, frequent gamers would be attracted to a plan that provides guaranteed quality of service for World of Warcraft, Call of Duty, and other interactive games.

B. OTT Premium Content

DNI enables differentiated pricing models by identifying premium services (e.g., UHD streaming, cloud gaming), allowing operators to offer tiered data plans that reflect consumption.

While most over-the-top content is free, many providers offer premium Internet content and services for a fee. Service providers can capitalize on this growing phenomenon by leveraging their unique ability to enable access, shape the user experience, and track and analyze OTT usage. For example, service providers can help popular music, video, or TV-on-demand providers expand their business by bundling the OTT service with smartphone

acquisition, high-speed access, guaranteed QoE, and unified billing in a premium package. The premium-content relationship may share revenue and offer options for targeted advertising based on subscriber behavior and application usage analysis.

C. **Differentiated Tiered Pricing**

Data service providers use service tiering to tailor competitive service plans to specific market segments and subscriber preferences. Service plans may be tiered according to different speeds (Mbps, Gbps), QoS, usage allowances, happy hours, application-based SLAs, etc. For example, a basic tier could offer high speed but low monthly data cap, while a premium tier provides high speed, unlimited data volume, and expedited forwarding for streaming video and gaming applications. Tiered plans can be rolled out for specific devices as well. In this way, operators can target each customer with the right service plan at the right price to grow revenue and upsell opportunities, service differentiation, and enhance customer satisfaction.

D. **Tethering management**

In many geographies, mobile broadband is the most accessible broadband option available, and some customers exploit tethering to enable secondary users to ride for free on their data plans. Tethering is challenging to detect, but if detected, it can be offered as an upsell and blocked when it has not been paid for.

E. **Roaming and network sharing cost reduction**

Operators gain granular visibility into subscriber behavior and application usage patterns control their bandwidth consumption while roaming or using shared network resources. DNI empowers operators to differentiate traffic accurately, prioritize critical services, reducing unnecessary roaming and interconnection costs. By closely analyzing usage in real-time, DNI-driven solutions enable operators to optimize partner agreements, minimize and enforcing application based policy on roaming traffic wholesale charges, and intelligently control network resource allocation, leading to significant operational savings and enhanced customer experience.

F. **Fair usage enforcement**

Whether it provides fixed or mobile connectivity, broadband service providers constantly struggle to deliver fair and consistent QoE to all network

subscribers. No single user is to be discriminated against, yet at the same time, no one is allowed to abuse shared network resources at the expense of others. Fair use management based on DNI ensures that no individual subscriber disrupts the service provided to others. It manages throughput and subscriber QoE based on congestion thresholds across the entire network based on each subscriber service plan. Furthermore, providers must refrain from making further investments in network resources.

6. Regulatory Compliance and National Cyber Protection
    A. **Data Privacy Compliance**

    DNI ensures operators comply with data sovereignty regulations by controlling cross-border data flows and implementing robust privacy measures.
    B. **National Cyber Shield**

    Safeguarding national cyberspace, ensuring digital sovereignty, and returning some measure of network control to the country is critical for governments worldwide. Allot Solutions for Government Agencies enable governmental organizations to gain visibility into their national network traffic and control it with digital enforcement to uphold national laws and policies.

7. Content Filtering and Parental Controls
    A. **Customizable Content Filtering Services**

    DNI enables operators to offer content filtering services for enterprises and families, blocking harmful or inappropriate content and enhancing user safety.
    B. **Security Policy Enforcement for Enterprise**

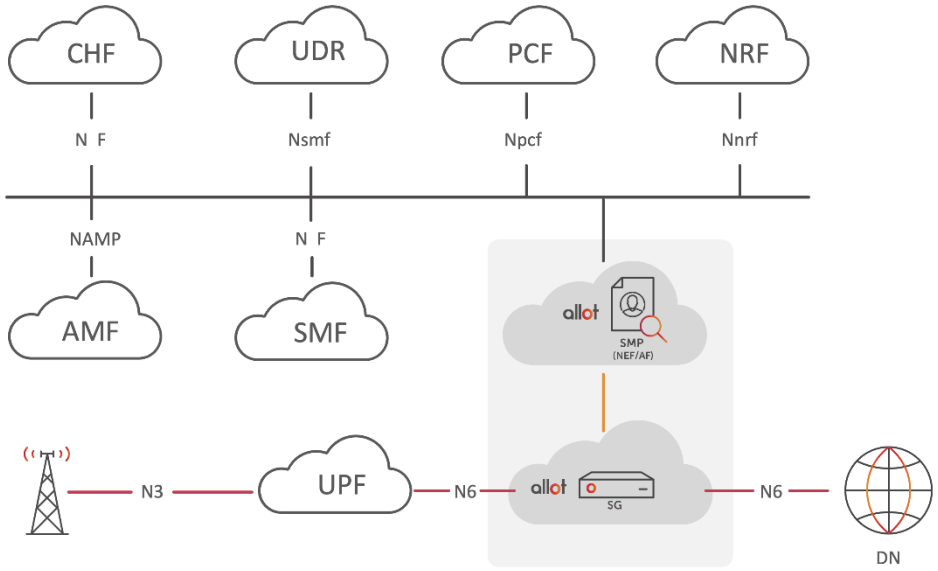
    Businesses can enforce security policies using DNI by restricting access to unauthorized and malicious applications or websites, reducing the risk of data breaches.

8. Edge Computing Enablement
    A. **Intelligent Traffic Steering**

    DNI detects applications that benefit from edge processing and directs data to Multi-access Edge Computing (MEC) nodes, minimizing latency and improving performance.

    B. Local Breakout Optimization

    By recognizing content types, DNI ensures that latency-sensitive applications are processed locally, while other traffic is routed efficiently to centralized clouds.



Allot Smart 5G deployment blueprint example

9. Application-Aware Routing
    A. **Cloud Access Optimization**

    DNI detects specific SaaS applications and ensures optimal routing, improving performance for enterprise cloud services.

10. Private 5G Networks Sensitive App Prioritization
    A. **Industrial IoT Traffic Management**

    In private 5G networks, DNI prioritizes and protects mission-critical IoT traffic, supporting industrial automation and smart manufacturing.

    B. **Custom Enterprise Policies**

    DNI facilitates custom traffic policies tailored to enterprise needs, enabling advanced use cases like autonomous robotics and predictive maintenance.

Conclusion

Deep Packet Inspection (DPI) is indispensable in the 5G era, evolving into Deep Network Intelligence (DNI) to address next-generation networks' complexity and performance demands. DNI empowers operators with tools to optimize network performance, enhance security, and create new monetization opportunities. By leveraging DNI across these diverse use cases, telecom operators can unlock the full potential of 5G, delivering unparalleled value to consumers and businesses alike.

———