SUBSCRIBER AWARENESS

R&S®GSRM FOR ENHANCED FILTERING AND FORWARDING IN THE MOBILE CORE

DELIVERING SUBSCRIBER AWARENESS FOR TRAFFIC MANAGEMENT, POLICY CONTROL AND NETWORK SECURITY VIA GTP CORRELATION ANALYSIS

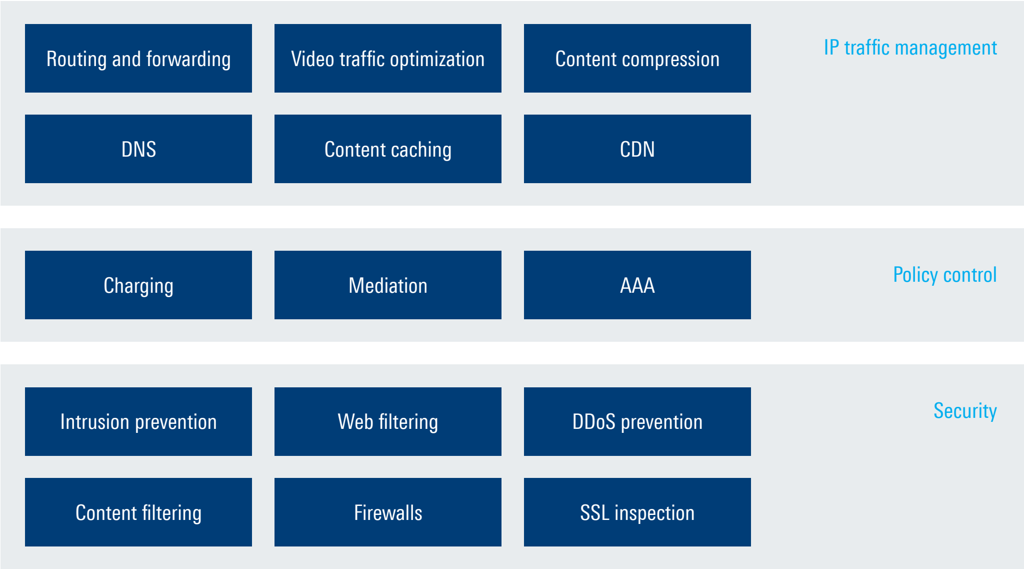
ROHDE&SCHWARZ
Make ideas real

INTRODUCTION

The mobile core network, namely the evolved packet core (EPC), hosts a number of key traffic processing functionalities. They ensure that packets are processed and delivered in a timely and secure manner. These functionalities are programmed based on a wide range of network and traffic attributes.

With the growth in operator service and plan types, attributes relating to subscribers — at the individual and aggregate level — have become increasingly important in meting out the appropriate traffic management, policy control and security responses. Key attributes include subcriber IDs such as international mobile subscriber identity (IMSI), mobile station international subscriber directory number (MSISDN) and international mobile equipment identity (IMEI). This information, along with bearer and location data, enables devices such as routers, firewalls, network address translation, charging and content compression engines to make real-time decisions for any traffic flow and the corresponding subscriber or network endpoint.

At the same time, load balancing was implemented to satisfy the rapid rise in traffic volumes in the core network. Load balancing supports network subsystems which deploy more than a single device per functionality. It involves the use of intermediaries such as network packet brokers (NPB) which identify, filter and distribute packets to multiple devices in a subsystem to ensure equal allocation of the processing load.

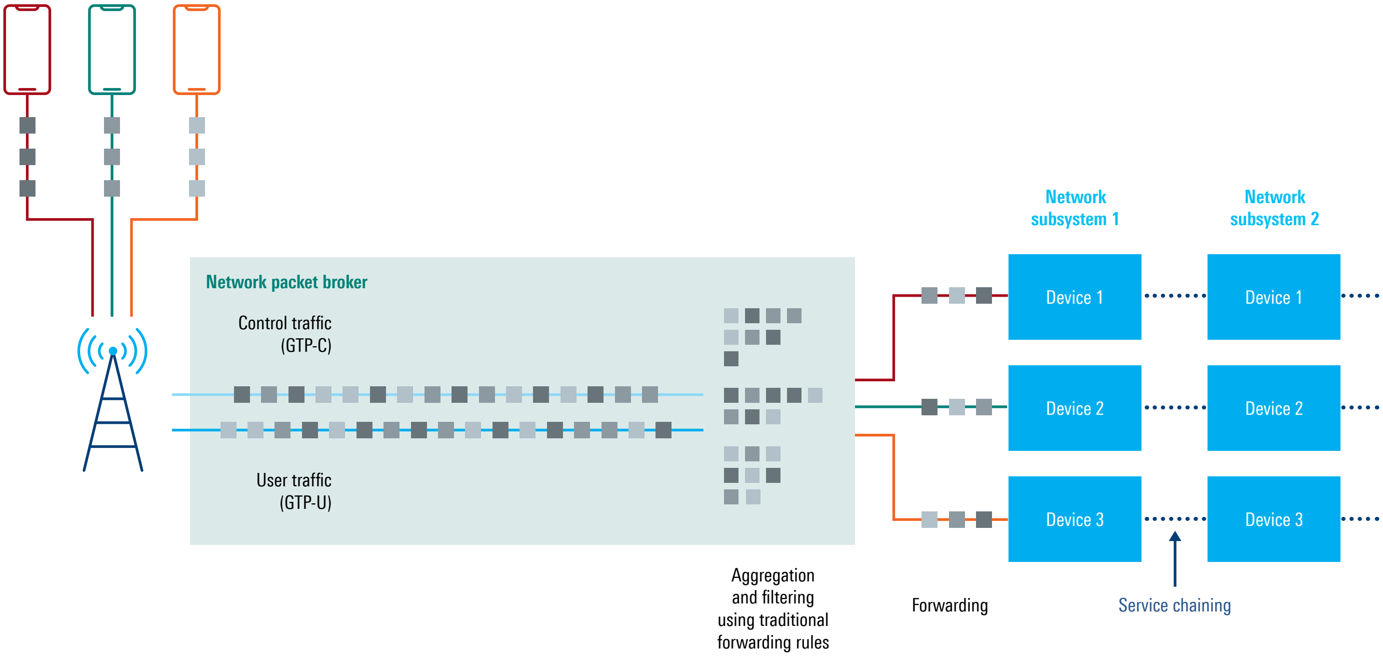


Traffic management, policy control and security functions/subsystems in mobile core networks

GTP CORRELATION FOR INTELLIGENT LOAD BALANCING

The use of load balancing introduces a new challenge for subscriber-based traffic processing due to the use of traditional methods for distribution that do not take into account subscriber session information. These include rules such as packet rate, total traffic and bandwidth, logical sequences such as round robin or complex distributions such as stateless hashing.

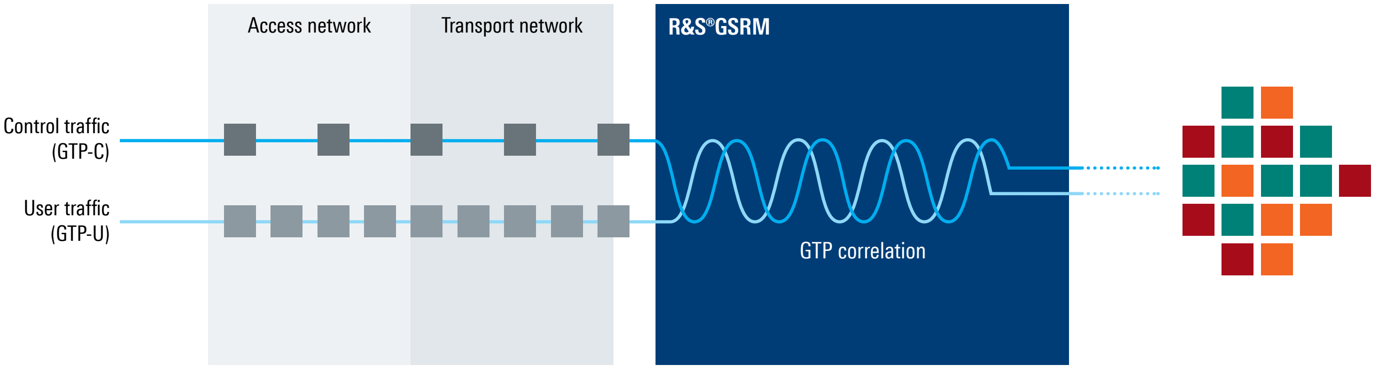
Consequently, packets from a single session are split and forwarded to different devices in a subsystem, resulting in partial visibility across any onward processing function. This leads to inconsistent analysis of traffic, eventuating in processing disparities between devices of a subsystem and inconsistencies in network responses across various subsystems.



Traditional load balancing

R&S®GSRM

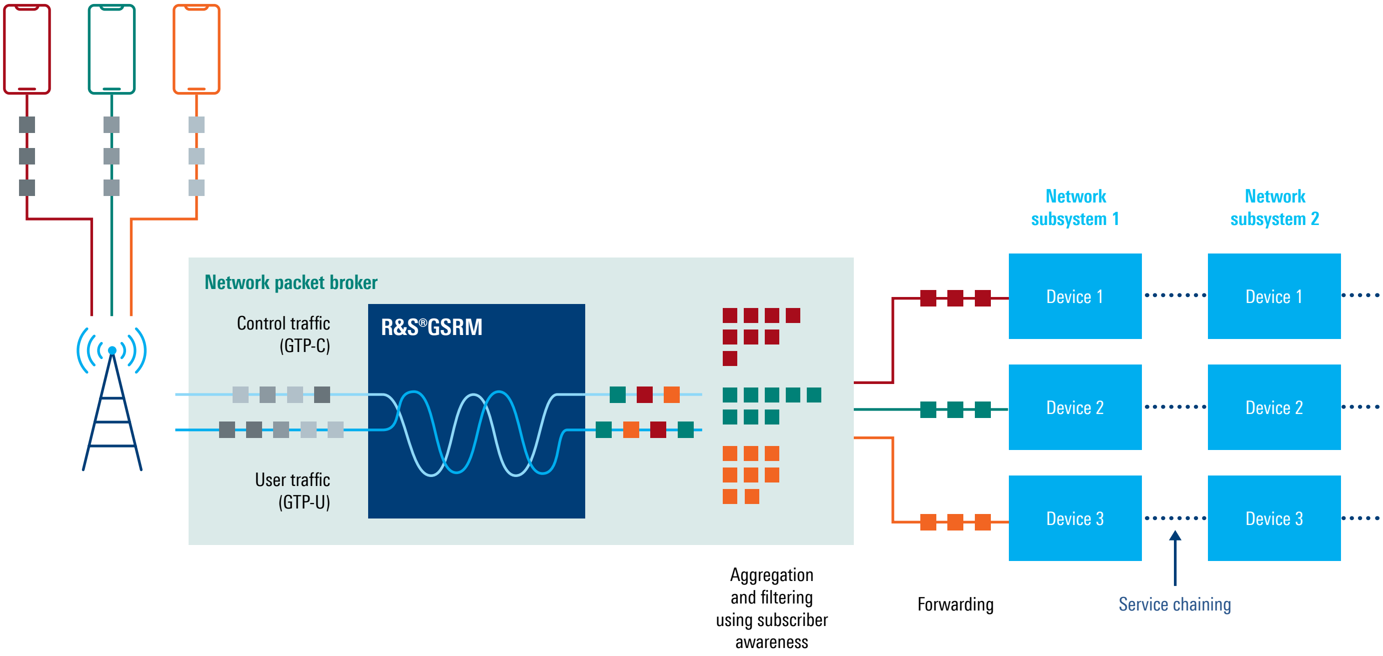
The GTP subscriber resolving module by Rohde&Schwarz (R&S®GSRM) provides subscriber and session awareness for mobile core networks, namely LTE and 5G NSA. It analyzes GTP user and control traffic by correlating GTP-C attributes such as IMSI, MSISDN and IMEI with GTP-U's tunnel endpoint identifiers (TEID). It also correlates user plane traffic by type of interfaces such as Gn, S1-U, S11 and S5 across both GTPv1-C and GTPv2-C. Correlation analysis by R&S®GSRM delivers accurate and reliable real-time identification of subscribers and sessions for GTP traffic in the mobile core network. It supports a wide range of functionalities that require subscriber awareness.



GTP correlation by R&S®GSRM

Real-time identification of subscribers and sessions by R&S®GSRM enables intelligent load balancing. It allows tools such as NPBs to identify, aggregate, filter and forward traffic by subscribers to the respective devices in a mobile core subsystem. This results in packets from a single session being directed to the same processing device through service-chained subsystems, delivering complete visibility into each session.

Intelligent load balancing powered by R&S®GSRM also allows session-specific manipulation of traffic including replication, deduplication and additional tagging. It also addresses the visibility gaps inherent in traditional traffic distribution while replacing bandwidth-intensive methods for subscriber identification. Additionally, it removes conflicting analysis and redundant communications on any session in the core network, reducing traffic processing cycles and improving network efficiencies.

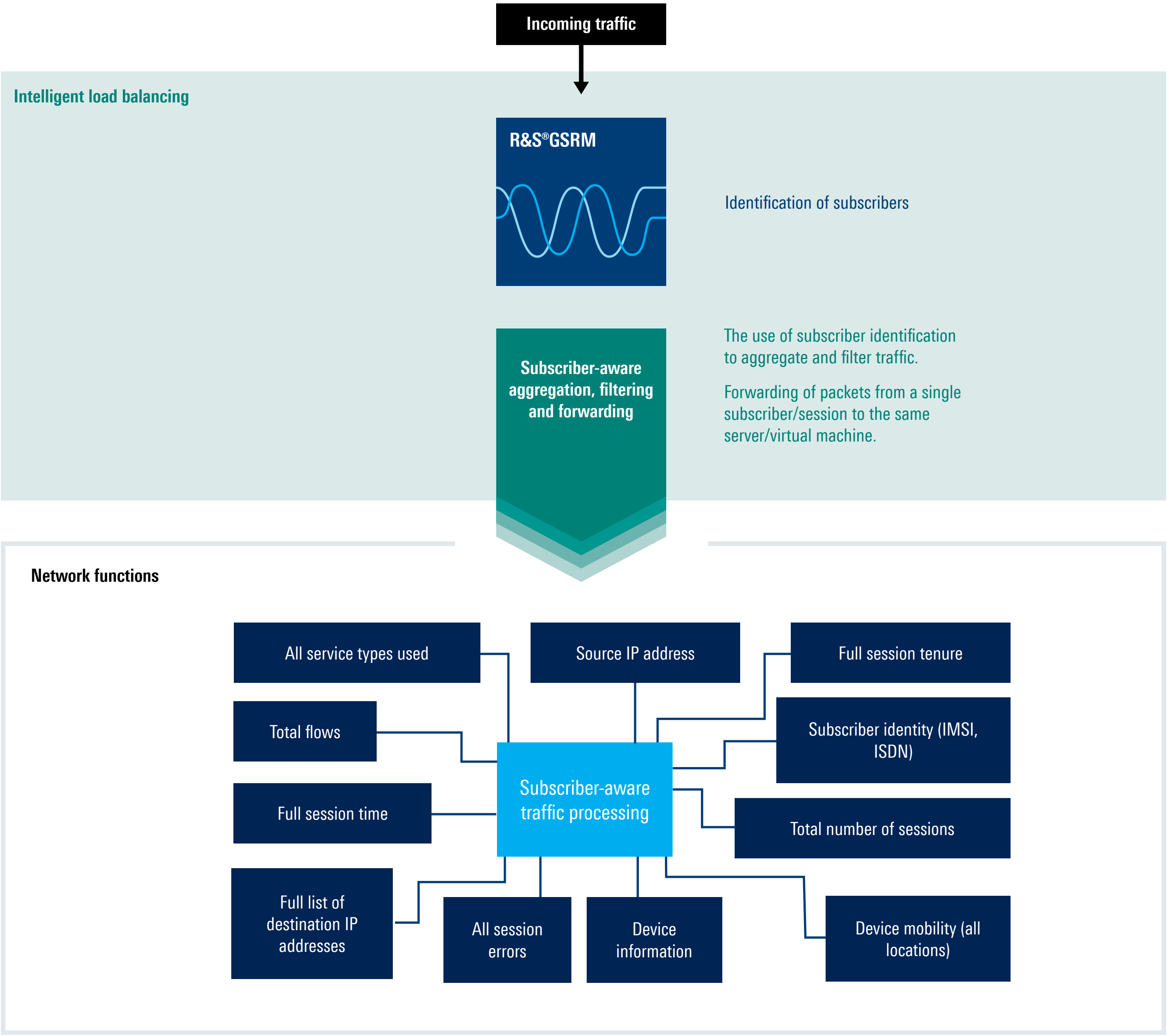


Intelligent load balancing

SUBSCRIBER AWARENESS FOR TRAFFIC MANAGEMENT, POLICY CONTROL AND NETWORK SECURITY

Intelligent load balancing via R&S®GSRM introduces two capabilities. Firstly, it provides real-time identification of the subscriber, allowing network functions to undertake subscriber-aware traffic processing based on a host of session parameters.

These include parameters such as service types, total flows, session time, destination IP address, source IP address, session tenure, subscriber identity (IMSI, ISDN), number of sessions, device mobility (all locations), session errors and device information.


Incoming traffic
Intelligent load balancing
R&S®GSRM
Identification of subscribers
Subscriber-aware aggregation, filtering and forwarding
The use of subscriber identification to aggregate and filter traffic.
Forwarding of packets from a single subscriber/session to the same server/virtual machine.
Network functions
All service types used
Source IP address
Full session tenure
Total flows
Subscriber identity (IMSI, ISDN)
Subscriber-aware traffic processing
Full session time
Total number of sessions
Full list of destination IP addresses
All session errors
Device information
Device mobility (all locations)

Subscriber-aware traffic processing based on session parameters

Secondly, it enables aggregation and forwarding of an entire session to a single device, enabling full visibility into a subscriber session. Mobile operators and vendors of traffic management, policy control and network security solutions can leverage these capabilities to deliver a wide range of use cases covering the following areas:

Traffic management

Traffic management includes traffic processing functionalities such as routing, network address translation, content caching and content optimization. Session-aware traffic management enables these functions to be granularized based on subscriber-specific attributes such as plan types and location. Examples for these include the provisioning of premium routes for subscribers generating a high average revenue per user (ARPU) and the compression of content on 'all you can eat' plans.

Traffic management with intelligent load balancing

Via intelligent load balancing, R&S®GSRM enhances subscriber-aware traffic management with real-time, dynamic traffic decisions. A routing device such as a switch or a router can route a high ARPU customer to a standard routing path if the customer exceeds prespecified session thresholds in terms of timing or total bandwidth to avoid network congestion and the overuse of network resources. Similarly, the same customer may have more low-bandwidth sessions prioritized over high-bandwidth sessions because information on cumulative usage is readily available to the switch or the router forwarding the traffic.

R&S®GSRM also avails operators real-time information on session performance. As all packets from a single session are logged into a single device, traffic parameters such as speeds, latency and jitter are easily established for any single subscriber. Traffic management decisions such as re-routing or content compression that are triggered based on traffic performance attributes benefit from this implementation as it allows different sessions to be accorded different policies. This enables operators to optimize the network by fine-tuning each session to existing network conditions and customer plan SLAs. Traffic aggregation enabled by R&S®GSRM also accelerates traffic delivery. Given that most packet processing methodologies rely on the local memory cache, processing all packets from a session in a single device allows processing devices to leverage cached instructions based on a common set of traffic attributes (e.g. subscriber ID, device type, host IP address and location), reducing the use of the device's main memory cache. R&S®GSRM's session aggregation therefore greatly benefits batch processing of packets. Routers, for example, can leverage R&S®GSRM-based session tagging to implement session-based compression for higher compression rates and increased throughput.

Policy control

R&S®GSRM supports subscriber authentication and usage controls across LTE and 5G NSA networks. Where authentication and usage policies are drawn based on a subscriber's identity, R&S®GSRM readily identifies each packet and provides this information to devices such as policy control, charging and mediation engines. This fuels a range of use cases, from basic authentication for 4G or 5G services to approvals for accessing exclusive services such as premium content libraries, roaming and operator Wi-Fi hotspots as well as the implementation of content permissions and parental controls.

Support for subscriber-aware authentication and control policies is an important feature in 5G, in particular across IoT and M2M services. These services involve the authentication of millions of connected endpoints, dispersed in multiple geographies as in the case of smart meters and coupled with high mobility needs as in the case of a connected fleet. Similarly, subscriber awareness delivered via GTP correlation analysis can be used in private 5G networks to allow only authorized users and endpoints to connect to a campus or a corporate network. This provides network operators the ability to granularize access controls

> Traffic management decisions such as re-routing or content compression that are triggered based on traffic performance attributes benefit from this implementation as it allows different sessions to be accorded different policies.

based on a hierarchy of privileges which includes selective access to gated content such as critical applications and sensitive data files. The use of R&S®GSRM for private 5G can also improve a company's control of its network assets as part of its zero-trust access network (ZTNA) strategy which includes the management of remote access via the secure access service edge (SASE).

Policy control with intelligent load balancing

Incorporating R&S®GSRM in an NPB that forwards traffic to policy control subsystems paves way for dynamic policy control where policies are meted out based on not only subscriber identity but also cumulative usage, traffic performance and applications accessed during a session. The implementation of a content pass governed by daily quotas, for example, relies on all packets from a session being aggregated and forwarded to the same policy control engine so that cumulative usage can be determined in real time.

Intelligent load balancing enabled by R&S®GSRM also allows packets from a subscriber to be processed in sequence, delivering full visibility into all concurrent application sessions. This supports the refinement of existing controls to include extended parameters such as network conditions and plan types. For example, within a shared family plan, all users may have their usage limits and speeds revised at the same time as a particular user hits the overall plan quota limits. Similarly, mobile operators can implement tiered charging and rating for different users in a shared plan in real time based on individual cumulative session thresholds. This can be extended to facilitate real-time convergent charging where usage across multiple data services is aggregated in the same engine to determine overall data consumption.

Traffic aggregation facilitated by R&S®GSRM also allows operators to identify users with immediate data needs. As a subscriber reaches their cumulative daily or monthly limits during an active session, a policy control engine can trigger contextual offers such as a data top-up or a plan upgrade. Contextual marketing can also be extended to cover content-specific offers based on applications accessed in the current session as this data becomes readily available through session-aware processing by a policy control engine.

> Incorporating R&S®GSRM in an NPB that forwards traffic to policy control subsystems paves way for dynamic policy control, where policies are meted out based on not only subscriber identity, but also cumulative usage, traffic performance and applications accessed during a session.

Throttling down user speeds, blocking and session termination are other control measures that rely on a subscriber's sessions being aggregated and forwarded to the same device in a network subsystem. This enables timely alerting for both the subscriber and the network operator which is key in avoiding overages and maintaining customer experience.

Network security

Mobile network security tools such as intrusion prevention, web filtering, DDoS prevention, content filtering, firewalls and SSL inspection benefit from real-time subscriber identification. It allows operators to pinpoint not only the source of traffic anomalies, fraud and cyberattacks but also other attributes relating to these events, including devices used, frequency, intensity and targeted resources. It is also useful in investigating inherent vulnerabilities in the network that have given rise to such incidents and the nefarious forces behind their orchestration.

Information provided by R&S®GSRM supports network security functions not only in identifying the forces behind malicious activity on the network but also in instituting, in real-time, mitigation measures that can include tightening of security filtering for traffic from certain IP addresses, devices and geographies as well as outright blocking of the infected sessions, quarantining of incoming traffic and blocklisting. The information can also be used to alert network administrators and users whose devices may have been compromised.

R&S®GSRM can also play a key role in endpoint security. This is especially so for 5G networks that have an expanded attack surface from the deployment of millions of IoT endpoints and the prevalence of multiple connected appliances and personal devices per subscriber. Managing network security requires susceptible endpoints such as security cameras and laptops used by network administrators to be secured with firewalls, anti-virus protection and URL filtering. The institution of granular rules based on subscriber security vulnerabilities and criticality can be carried out with a higher degree of accuracy and reliability when incoming packets are readily tagged with subscriber information.

Network security with intelligent load balancing

Intelligent load balancing via R&S®GSRM presents mobile operators an added advantage in managing the security of their mobile networks. With all infected packets inspected and processed by a single security tool, threats become easily and more accurately identifiable as traffic patterns from a single session are captured in a complete sequence. This helps detect cyber threats such as DDoS attacks, ransomware or IMSI fraud when incoming flows are matched against the tool's threat libraries, prompting operators to quarantine or block the infected packets while alerting the network of the attack sources.

Where devices are hacked by threat actors or deployed for illegal tethering, R&S®GSRM facilitates security tools in identifying anomalies via cumulative analysis of a subscriber's session data which includes bandwidth consumed, speed and number of concurrent sessions. Unnatural spikes in data consumption, previously not visible in a security subsystem, become immediately visible when the entire flow is processed by a single tool.

Additionally, with subscriber awareness, R&S®GSRM is able to support security tools with insights on new and emerging threats. As these tools now capture the full sequence of a security incident, security vendors are able to quickly develop new repositories of threat libraries that can future-proof the network against similar attacks.

Network automation

Another emerging use case for R&S®GSRM in the area of traffic filtering and forwarding is network automation. Network automation uses AI, namely machine learning (ML) and deep learning (DL) techniques to develop dynamic rules for traffic management, policy control and network security. This requires coherent session data provided by R&S®GSRM's reliable session tagging alongside data on corresponding network actions from various mobile core subsystems. The provided data enables ML and DL techniques to automate the right traffic management, policy control and security responses on future traffic flows.

WHY R&S®GSRM

LTE and 5G NSA networks benefit not only from R&S®GSRM's accurate and reliable identification of subscribers and sessions in real time but also from its rich features and range of expanded capabilities which include:

- An OEM software module that can be implemented in any network environment and integrated into any end solution without vendor lock-in
- A multicore architecture with linear scalability to satisfy high bandwidth demands
- Configurable input buffer and filter
- Session metadata including cell location and bearer IDs
- Support of all standard network interfaces such as Gn, S1-U, S11 and S5
- Easy-to-use REST APIs for seamless and fast integration
- Efficient total cost of ownership (TCO) from predictable costs and flexible SLAs
- Extension to 5G SA networks via R&S®5GSRM

Advantages of R&S®PACE 2

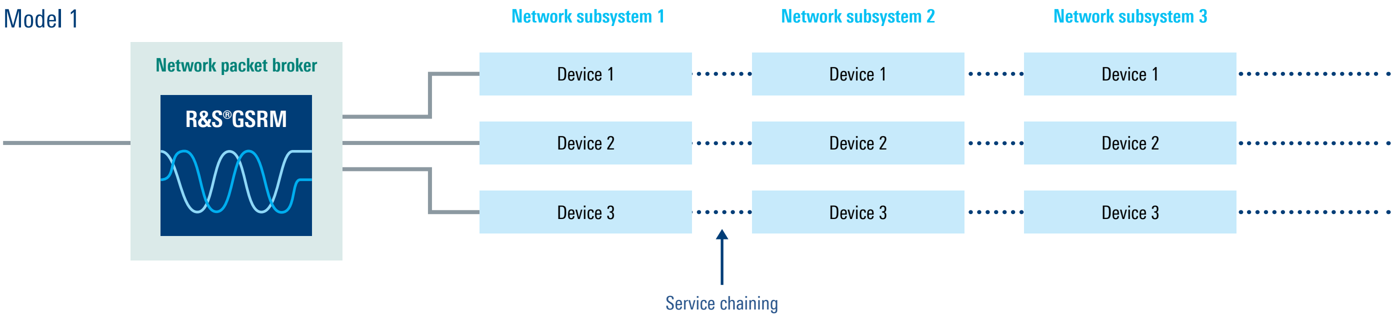
In addition to these, R&S®GSRM offers ready pairing with R&S®PACE 2, the high-performant deep-packet-inspection (DPI) engine by Rohde&Schwarz which delivers real-time classification of applications, protocols and services. R&S®PACE 2 includes a comprehensive weekly updated traffic signature library. R&S®PACE 2 uses advanced AI techniques such as ML and DL which enables accurate and highly reliable detection of applications even for traffic that is encrypted, anonymized or obfuscated. This enriches the current use cases in the following ways:

- **Traffic management** — expands subscriber and session rules to include attributes associated with specific application types. For example, traffic from high ARPU subscribers is routed via premium routes except for heavy file transfers and content downloads which are delivered via standard routes to optimize network resources while ensuring subscriber satisfaction.
- **Policy control** — enables authentication and controls to be specified by type of application. For example, special video plans can be programmed to grant subscribers unlimited usage on Netflix and YouTube but limited or throttled usage on all other web content such as social media applications and general browsing.
- **Network security** — enables security filtering and inspection to be customized based on application risk profiles. For example, requests to banking and other gated company applications are filtered through a threat detection engine while requests to access public internet sites such as news portals are forwarded without additional security filtering.

DEPLOYMENT OPTIONS

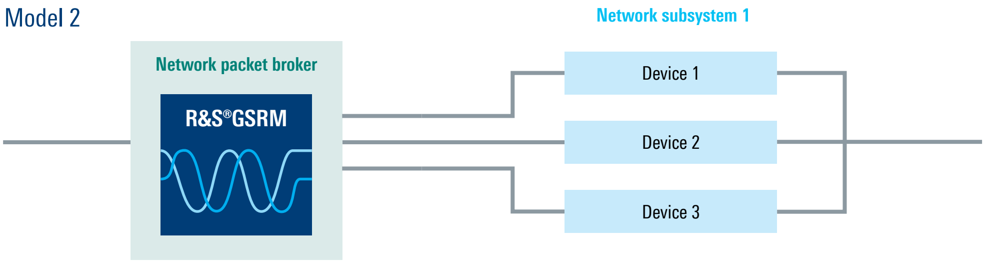
There are multiple models by which subscriber awareness powered by R&S®GSRM can be delivered for traffic management, policy control and security functionalities in the mobile core network. For network-wide intelligent load balancing, R&S®GSRM can be embedded into the main NPB. This allows one-time subscriber tagging that can be used by any onward subsystem in the core network. In this model, subsystems benefit from leaner setups, shared costs and consistency in traffic processing and analysis across all devices and subsystems (see Model 1).

Model 1



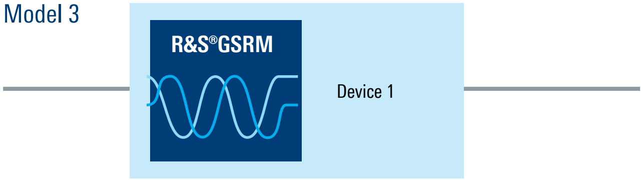
For traffic management, policy control and security deployments that are sufficiently large with a higher budget allocation, vendors can commission their own R&S®GSRM-embedded NPBs. This enables subsystem vendors to tap directly into subscriber and session tagging provided by R&S®GSRM and align packet manipulation at the NPB level to suit their subsystem requirements (see Model 2).

Model 2



In subsystems with only a single device or in a mobile core network with legacy load balancers, traffic management, policy control and security vendors can build R&S®GSRM directly into their devices. This enables deeper customization of GTP correlation analysis to meet specific session and subscriber identification needs at the device level (see Model 3).

Model 3



CONCLUSION

With the rapid growth in subscriber numbers and traffic across LTE and 5G NSA networks, real-time session and subscriber awareness provided by R&S®GSRM equips mobile operators and vendors in the traffic management, policy control and network security space with complete visibility into user sessions in the core network. This enables operators and vendors to enhance their traffic management, policy control and network security functions with granular policies that correspond to subscriber attributes while also taking into account session-specific parameters.

The full visibility into session data accorded by R&S®GSRM will also play a key role in the transitioning of today's networks into AI-driven automated networks capable of eliciting the right network response in real time. By integrating subscriber awareness, mobile operators are able to create networks that are truly responsive, dynamic and intelligent, paving way for greater performance and improved customer experience.

ipoque

ipoque, a Rohde & Schwarz company, is a global leader in the world of network analytics software. We leverage our deep domain expertise to create customized software solutions that empower our customers to transform data into intelligence. As a subsidiary of Rohde & Schwarz, we take advantage of potential synergies.

Rohde & Schwarz

The Rohde & Schwarz technology group develops, produces and markets innovative information and communications technology products for professional users. Rohde & Schwarz focuses on test and measurement, broadcast and media, cybersecurity, secure communications and monitoring and network testing, areas that address many different industry and government-sector market segments. Founded more than 80 years ago, the independent company has an extensive sales and service network in more than 70 countries.

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

ipoque GmbH
Augustusplatz 9 | 04109 Leipzig, Germany
Info: + 49 (0)341 59403 0
Email: info.ipoque@rohde-schwarz.com
www.ipoque.com

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG
Trade names are trademarks of the owners
PD 5216.2376.32 | Version 01.00 | May 2022
Use case | R&S®GSRM for enhanced filtering and forwarding in the mobile core
Data without tolerance limits is not binding | Subject to change