SUBSCRIBER AWARENESS

SESSION AND SUBSCRIBER AWARENESS IN MOBILE CORE NETWORKS

GTP CORRELATION FOR REAL-TIME SUBSCRIBER INSIGHTS

ROHDE&SCHWARZ

Make ideas real

CONTENT

1. Introduction 3

2. GTP correlation for subscriber and session awareness 4

3. Intelligent load balancing 5
   - 3.1. Subscriber-aware traffic processing 5
   - 3.2. Partial vs full visibility 5
   - 3.3. Subscriber-aware aggregation, filtering and forwarding 5
   - 3.4. Deeper traffic awareness 6

4. Subscriber-aware traffic processing in mobile core networks 8
   - 4.1. Monitoring / analytics 8
   - 4.2. Traffic Management 9
   - 4.3. Policy control 9
   - 4.4. Network security 9

5. GTP subscriber resolving module - R&S®GSRM 10

6. Deployment models 11

7. Integrating R&S®GSRM with application awareness 13

8. The network impact 13

1. INTRODUCTION

By 2025, the number of mobile connections is expected to reach 8.8 billion, according to GSMA[1]. Mobile networks, running on 3G, 4G and 5G, will be processing unprecedented levels of traffic as the number and type of mobile applications continues to grow. It is expected that mobile networks will be processing over 12 billion gigabytes of data everyday by 2027[2].

Central to the management of today's mobile networks is the traffic processing capacity and capabilities in the mobile core, specifically the Evolved Packet Core (EPC) that is at the heart of LTE and 5G Non-Standalone (5G NSA) networks. This capacity and these capabilities are delivered by a number of network functions that route, process, manage and control all the traffic on the network on an end-to-end basis, from user devices through access and transport links all the way to the core.

An increasingly important feature, that improves the mobile core's traffic processing capability, is subscriber awareness. Also known as session awareness, subscriber awareness refers to the accurate identification of traffic at the packet level by a specific subscriber or session. Subscriber awareness enriches network functions with essential insights enabling them to increase their functionalities, improve processing efficiency and enhance output accuracy, thus improving the mobile core's capacity and capability of handling millions of subscriber sessions.

1) GSMA – The Mobile Economy
2) Ericsson Mobility Report – Mobile data traffic outlook

2. GTP CORRELATION FOR SUBSCRIBER AND SESSION AWARENESS

To deliver subscriber awareness, mobile networks leverage the correlation of GTP traffic in the mobile core. GTP refers to the GPRS tunnelling protocol, which is used by mobile operators to transport traffic across their mobile networks. It is an IP/UDP based protocol and is deployed in 2G, 3G, LTE and 5G networks. At any given time, a mobile network handles millions of GTP sessions at both the user and the control plane, forming the network's GTP user traffic (GTP-u) and the GTP control traffic (GTP-c).

The correlation of GTP traffic involves the real-time correlation of GTP-c attributes with GTP-u Tunnel Endpoint Identifiers (TEIDs). Among the key correlation attributes at the control plane are International Mobile Subscriber Identity (IMSI), Mobile Station International Subscriber Directory Number (MS-ISDN) and International Mobile Equipment Identity (IMEI). IMSI is a unique subscriber identifier used internally by mobile networks and is stored in the SIM, while MS-ISDN refers to the phone number associated with a SIM. IMEI refers to a unique number used to identify a mobile device. The GTP user plane traffic can also be correlated by type of interfaces such as Gn, S1-U, S11 and S5 across both GTPv1-C and GTPv2-C. These attributes are correlated with GTP-u's TEIDs, which are assigned to both GTP-c and GTP-u to identify the tunnel endpoints on the receiving nodes.

The correlation of the GTP-c subscriber specific attributes and the GTP-u TEIDs enables the identification of data packets by a specific subscriber or session for 4G and 5G NSA networks. This delivers complete mobile subscriber awareness in the mobile core.

GTP correlation-based subscriber resolution replaces the traditional subscriber session analysis, which has been rendered ineffective and inefficient due to bandwidth and throughput limitations, as the number of user sessions in the core continues to grow rapidly, especially in the EPC.

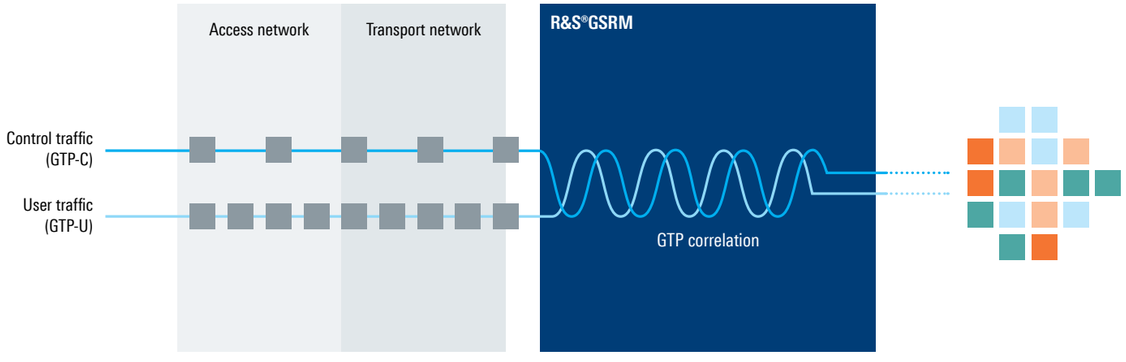

Figure 1: Illustrative diagram showing how user and control traffic correlation delivers identification of IP packets by sessions and subscribers

3. INTELLIGENT LOAD BALANCING

3.1. Subscriber-aware traffic processing

Subscriber awareness is required in the core across a large number of traffic processing functions that rely on the identification of subscribers and subscriber sessions. For example, a policy control engine in the core requires subscriber identification to authorize user access to mobile plans and content offerings.

Identification of all the subscriber sessions allows charging and rating engines to determine a subscriber's cumulative usage and assign the correct billing rates, respectively. Similarly, in managing network security, a firewall in the core requires identification of infected packets originating from subscribers to enable timely flagging of all incoming traffic originating from the same terminal device.

3.2. Partial vs full visibility

Subscriber identification powers a host of subscriber-aware processing functions. However, a large part of processing hinges on full traffic visibility, which means the reception of all packets from a subscriber's active session. Full visibility is often a challenge when network function workloads are distributed among multiple servers or virtual machines. Distribution of workloads across multiple servers enables concurrent traffic processing, increasing the total processing capacity in the core. It also helps operators minimize traffic disruptions from congestion, hardware or software issues and cyberattacks in an environment where multiple functions are service-chained and poor performance in one functionality can affect the entire core.

Splitting incoming traffic into multiple flows that are subsequently forwarded to different servers or devices requires load balancing, a process which ensures optimization of the available capacity and resources. This process is implemented via intermediary tools such as a network packet broker or a load balancer. These tools sit between the unfiltered traffic and the subsystems that run the network functions and implement forwarding with rules such as packet rate, total traffic, bandwidth, number of connections or a logical sequence such as round-robin or a more complex distribution such as stateless hashing.

While load balancing improves network capacity and reduces latencies and delays caused by the extensive processing in the core, the use of traditional forwarding rules causes packets from a single subscriber session to be split into separate flows, resulting in the processing server receiving only part of the traffic. This leads to both loss of information and inconsistent treatment of traffic as packets are processed out of sequence and at random, based on the forwarding queue. As a result, network operators are forced to rely on extensive post-processing reconciliation before they gain full visibility into a single subscriber session.

Partial visibility has various other implications for the network. For example, network subsystems, where multiple devices are deployed, show a high degree of redundancy arising from each of these devices communicating information on the same session to other subsystems. This results in network inefficiencies and can lead to conflicting information on a session given that different parts of a session typically display different traffic attributes.

3.3. Subscriber-aware aggregation, filtering and forwarding

To circumvent the limitations of traditional load balancing, tools such as network packet brokers are integrating subscriber awareness into their equipment to enable real-time identification of subscriber traffic. These tools can then aggregate and filter the identified packets according to the onward processing requirements and may include further manipulation such as replication and deduplication as well as the addition of new metadata for a more detailed identification. The subscriber-filtered traffic is then forwarded to output ports in such a way that traffic from an entire session is delivered to the same server, enabling full visibility into a subscriber's session.

3.4. Deeper traffic awareness

Subscriber awareness also plays an important role in delivering deeper traffic visibility that extends to insights on the application and network level. Without subscriber awareness, processing servers only see a portion of the communication. This makes the real-time and accurate identification of applications and security threats as well as the monitoring of traffic performance complex and time-consuming, even with the deployment of advanced traffic inspection tools. By enabling session-aware traffic aggregation, filtering and forwarding, subscriber awareness empowers various functions in the core with greater traffic visibility, specifically:

- **Application awareness**
  With all packets from a session aggregated and processed in succession, processing tools are able to not just identify in real-time the protocols and applications that are in use, but also determine the usage tenure and the devices these applications are accessed from. Operators are also able to identify multiple concurrent sessions (for example, the use of Instagram and Facebook) and single out packets that involve different application attributes such as video and audio communications (for example, video calls on WhatsApp and audio calls on Skype) and capture all in-app activities such as gaming (for example, Facebook Gaming) or purchasing (for example, on Amazon.com and Walmart.com).
- **Identification of threats and anomalies**
  With an entire session processed in a single instance, patterns of cyberattacks and network abuses can be detected as they happen. This includes attacks such as malware, mobile network mapping, IMSI impersonation and SIM-jacking as well as fraud and unauthorized tethering. DDoS attacks, for example, become visible in real-time as the rate of requests from a single subscriber surpasses a specified threshold.
- **Identification of network attributes**
  With all packets from a single session or subscriber assembled in a single processing sequence, attributes of the network, such as its speeds, jitter, latency and throughput, can be calculated accurately. For example, operators can easily determine the speed of a session by measuring throughput over the length of that session without having to reconcile throughput figures across multiple servers in a separate reconciliation process.

The enhanced traffic visibility enabled by subscriber awareness can also be used to deliver a more granular traffic analysis on a per subscriber basis. This could include application usage by a subscriber or a subscriber class, frequency of cyberattacks by end points or speeds experienced on a specific application by a specific subscriber during a specific session.

Operators are also able to identify multiple concurrent sessions (e.g., the use of Instagram and Facebook) and single out packets that involve different application attributes such as video and audio communications (e.g., video calls on WhatsApp and audio calls on Skype) and capture all in-app activities such as gaming (e.g., Facebook Gaming) or purchasing (e.g., Amazon.com and Walmart.com).

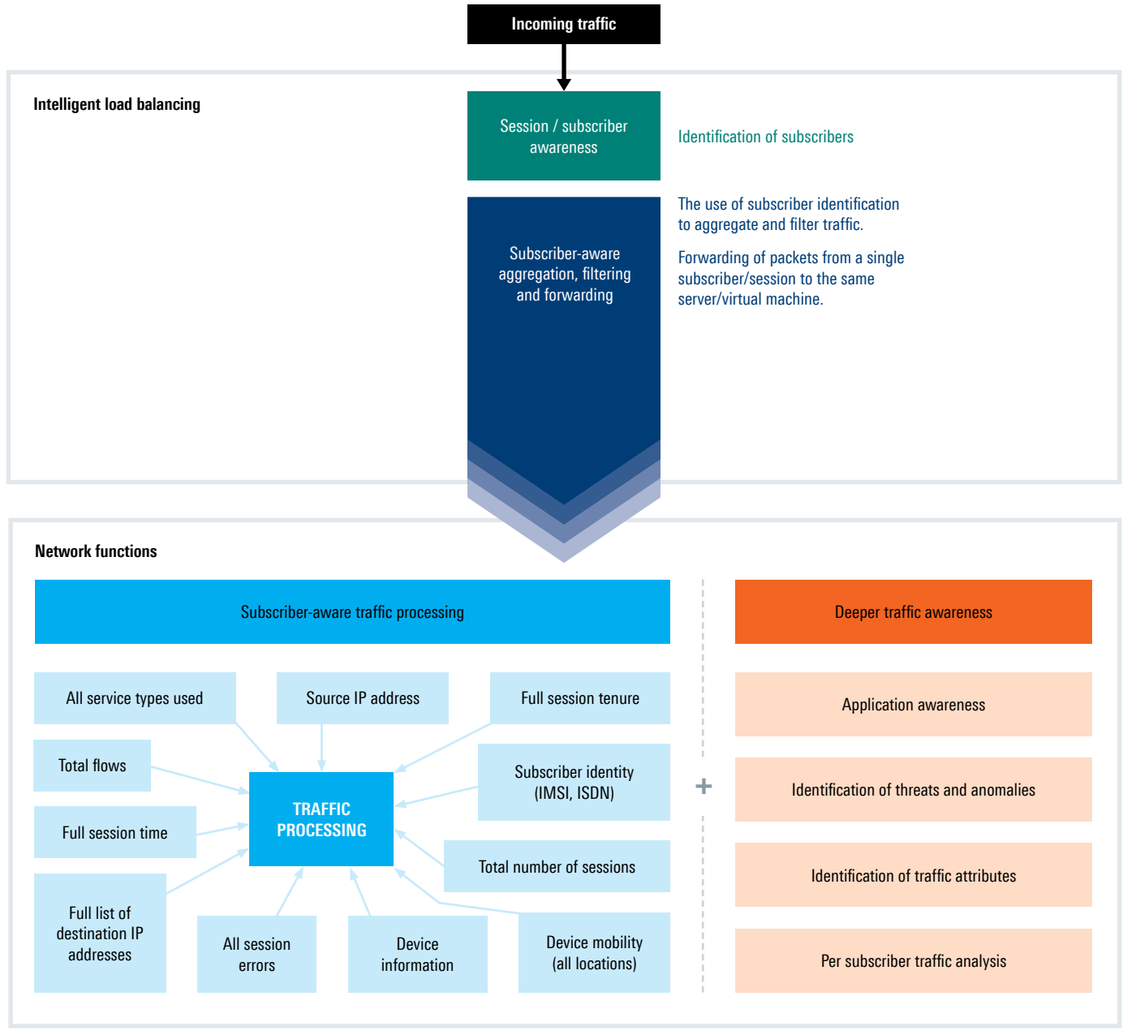

Figure 2: Delivering full visibility with subscriber awareness

4. SUBSCRIBER-AWARE TRAFFIC PROCESSING IN MOBILE CORE NETWORKS

Subscriber awareness is becoming increasingly important for the management of mobile networks. From identifying subscribers to aggregating and filtering traffic, this capability is incorporated across a number of key traffic processing areas within the Packet Switched Core and the EPC, namely for:

4.1. Monitoring / analytics

Network monitoring tools such as IP probes rely on subscriber awareness to log subscriber information in the network. This includes the information on a subscriber's connection requests, source and destination IPs, connection timing and duration, device identity, device type and location.

With full visibility: By capturing and processing all the packets belonging to a subscriber in the same processing sequence, mobile operators are able to measure and monitor various metrics relating to a subscriber's mobile usage. Network operators can establish the average duration of subscriber sessions at any given time and distinguish them by type of subscriber class.

By aggregating session data, mobile operators are able to accurately and timely determine if they are meeting the requirements in their SLAs in terms of speeds and latency and establish subscriber experience with every session. They are also able to extract subscriber mobility patterns and learn about data offloading between 3G-LTE-5G networks in a heterogeneous network setting.

Using application and general traffic awareness, operators can derive a specific subscriber's application usage and determine their experience on each. This enriches mobile network analytics with subscriber behavioral insights, allowing mobile network operators to better understand their subscribers' preferences.

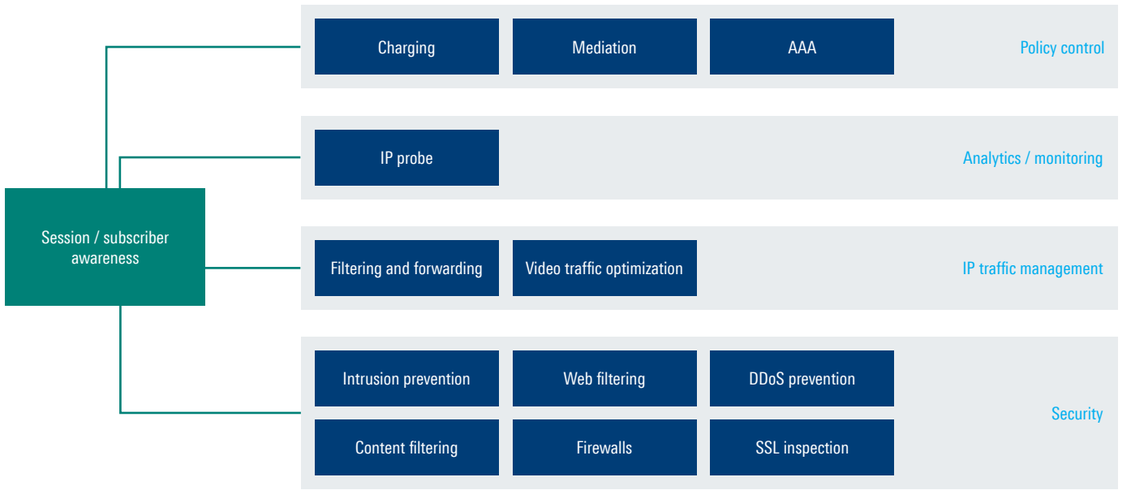

Figure 3: Subscriber awareness for network functions in mobile core networks

4.2. Traffic management

Traffic management functions such as routing, video traffic optimization, filtering and forwarding are greatly improved with subscriber identification information as it speeds up the implementation of subscriber-based traffic policies. These include the routing, forwarding, content caching and content filtering that are implemented based on subscriber classes, plan types and location.

With full visibility: With traffic from a single subscriber processed on a single device, mobile operators are able to fine-tune subscriber-based traffic management decisions to match the real-time usage of network resources. High ARPU subscribers, typically routed over premium pathways, may be routed over standard pathways when session thresholds (timing/total bandwidth) are exceeded. Bandwidth-light sessions may be prioritized over bandwidth-heavy ones, depending on the subscriber classes.

Similarly, by combining subscriber awareness with application awareness, operators may cache frequently used content for users on specific plans and compress content for users on selected device types in order to free up network resources during peak traffic hours.

4.3. Policy control

Policy control engines, that apply charging, mediation and AAA, benefit from subscriber awareness as a subscriber session is identified in real-time and the appropriate authentication and controls can be put in place instantaneously, improving network response times and subscriber experience. This includes authorization for access to premium content libraries, roaming services and operator WiFi hotspots.

With full visibility: By processing all the packets belonging to a subscriber in the same sequence, operators can capture all concurrent sessions and establish cumulative consumption. This allows them to launch real-time controls on subscriber data usage, implement tiered charging, make contextual data offers and raise timely alerts or reminders to avoid overages.

Operators can also introduce differentiated policies for multiple subscribers under family plans with shared usage limits and manage data-exhausted accounts via the use of throttled speeds. Combined with traffic visibility at the application and network level, mobile operators are also able to introduce fine-grained policies that map subscribers and subscriber classes to application-specific and content-specific authorizations and differentiated charging based on content and applications used.

4.4. Network security

Network security functions in the core, e.g., intrusion prevention, web filtering, DDoS prevention, content filtering, firewalls and SSL inspection, can use subscriber awareness to pin down subscribers and terminal devices that are the source of network threats. These threats include cyberattacks and fraud. Real-time identification enables security tools to act promptly in blacklisting these sources and securing the network from further attacks.

With full visibility: Identification of threats by network security tools is made more accurate and timelier when all packets from a single security incident, such as a DDoS attack, a malware attack or IMSI fraud, are processed in a single device. It makes threat patterns immediately visible when matched against threat libraries and prompts network operators to quarantine or block packets from the flagged subscriber or terminal device in real-time.

Subscriber awareness also helps network security tools to identify new threat patterns whose signatures are not readily available. By capturing the full sequence of an incident, security vendors can quickly build a repository of information that can be used to identify new and emerging threats on the network.

By capturing the full sequence of an incident, security vendors can quickly build a repository of information that can be used to identify new and emerging threats on the network.

5. GTP SUBSCRIBER RESOLVING MODULE – R&S®GSRM

Subscriber awareness is easily integrated as part of the mobile core using the GTP Subscriber Resolving Module (R&S®GSRM) by Rohde&Schwarz.

R&S®GSRM is a cutting-edge OEM network intelligence software that performs GTP user and control plane correlation to deliver real-time traffic visibility on a subscriber and a session level in the mobile core for 4G and 5G NSA networks. It taps into a rich set of attributes at both GTP-c and GTP-u layers, identifying and correlating identifiers such as TEIDs, IMSIs, MS-ISDNs and IMEIs with support for all standard network interfaces such as Gn, S1-U, S11 and S5. It can be deployed across both GTPv1 and GTPv2.

R&S®GSRM is deployed by network monitoring, traffic management, policy control and network security vendors to deliver subscriber awareness across various IP traffic processing functionalities in the mobile core. Functions such as load balancing, content filtering, mediation and intrusion prevention benefit from session-aware traffic identification provided by R&S®GSRM, improving their processing capabilities and accuracy with session-aware aggregation, filtering and forwarding across any number of traffic sessions and flows.

As a lean OEM software module, R&S®GSRM can be seamlessly integrated across physical and virtual machines and be deployed without any vendor lock-in. Running on Intel architecture, it boasts no external dependencies and provides well-documented APIs and flexible SLAs for easy deployment, delivering an optimized total cost of ownership.

As a solution for the rapidly growing traffic across today's core networks, especially on LTE and 5G NSA, R&S®GSRM offers highly performant and cost-effective subscriber resolution via a multi-core architecture that offers linear scalability.

R&S®GSRM boasts extensive field testing and active deployments, enabling network operators and equipment vendors to tap into the expertise and experience required for integrating subscriber and session awareness into mobile core networks across different architectures and traffic processing needs.

By integrating the GTP correlation module into their networks, network solution vendors and operators enjoy:

- Faster time to market and reduced R&D cost through quick integration
- Improved analytics accuracy through reliable correlation of subscriber sessions
- Optimized tool infrastructure as a result of a more efficient and effective processing throughput
- Flexible SLAs to meet end-customer's requirements

> Functions such as load balancing, content filtering, mediation and intrusion prevention benefit from session-aware traffic identification provided by R&S®GSRM, improving their processing capabilities and accuracy with session-aware aggregation, filtering and forwarding across any number of traffic sessions and flows.

6. DEPLOYMENT MODELS

The integration of subscriber awareness in the core can take one of many approaches suited to the requirements of the network.

Model 1

For core-wide subscriber awareness, operators can either deploy a network packet broker already equipped with R&S®GSRM for intelligent load balancing or collaborate with existing network packet broker vendors to integrate R&S®GSRM into their equipment. Incorporating R&S®GSRM into network packet brokers benefits mobile networks in terms of leaner post-processing as subscriber awareness is already built into the network and does not have to be replicated in each network function.

It also maintains the consistency in user and control plane correlation results across multiple network function subsystems. This is important in a mobile core with many network function subsystems that are interdependent. Consistent tagging of packets in terms of subscribers and sessions at a network-level avoids conflicting packet information at different subsystems. This enhances processing accuracies while also facilitating real-time network performance audits in the core.

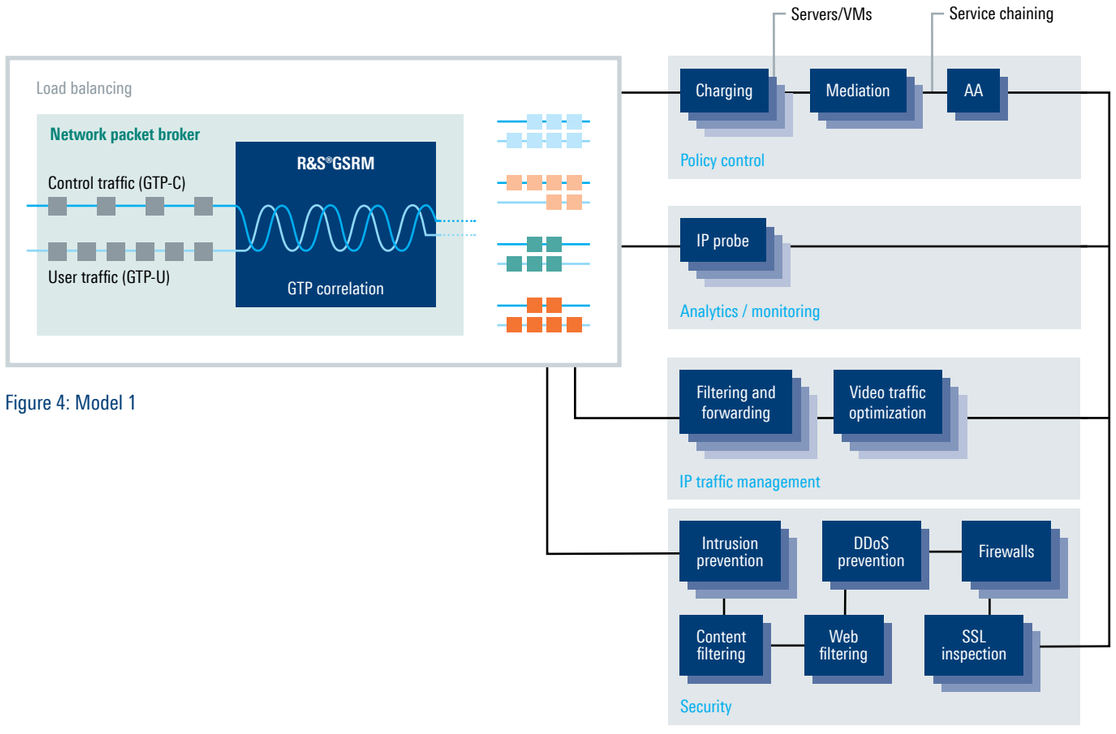

Figure 4: Model 1

Model 2
For subscriber awareness that is limited to a single subsystem, vendors can opt to pair their processing servers with their own network packet brokers which can be easily equipped with R&S®GSRM, specifically for larger deployments where traffic volumes and vendor budgets are sufficiently large to justify such investments. This allows only network function subsystems requiring subscriber awareness to receive subscriber-filtered traffic. However, this model requires localized load balancing at each network function subsystem, which results in processing duplication and may lead to different correlation outputs, especially if different subscriber resolution tools are deployed.

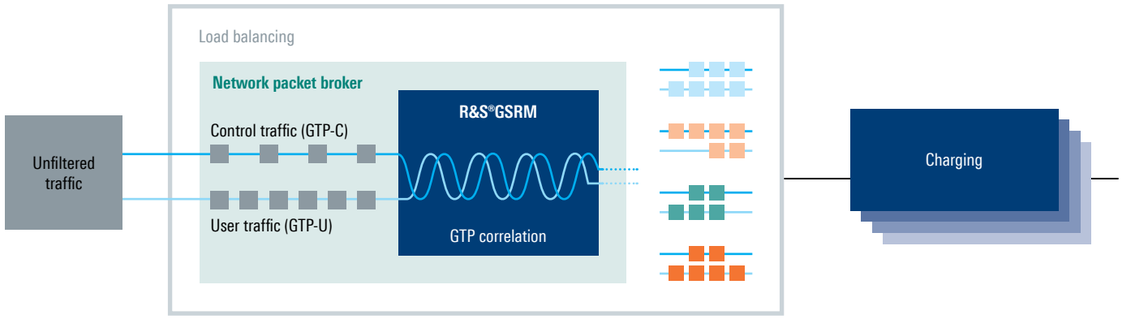

Figure 5: Model 2

Sampling for network analytics

For network analytics tools such as IP probes, R&S®GSRM enables the use of unique samples to represent selected traffic classes. Traffic from low ARPU subscribers, for example, can be forwarded using sampling to these tools, while traffic high ARPU subscribers are forwarded in whole. This reduces traffic processing in the core and improves overall network speeds and efficiencies.

Model 3
Equipment vendors with a more specific need for subscriber-aware traffic manipulation can incorporate R&S®GSRM directly into their own equipment and provide the capability as a built-in feature. This model is advantageous for vendors in network environments where intelligent load balancing is unavailable as a core-wide capability and where their traffic handling functions involve subscriber-aware traffic aggregating and filtering.

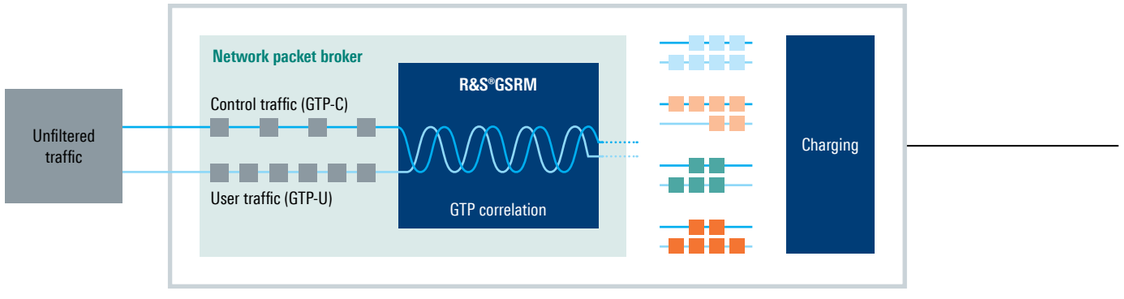

Figure 6: Model 3

7. INTEGRATING R&S®GSRM WITH APPLICATION AWARENESS

A large number of network functions leveraging subscriber awareness also rely on application awareness as well as insights on network performance and network security. Equipment vendors typically incorporate separate traffic detection and filtering engines to address these visibility needs. This often creates inconsistencies in processing speeds and traffic tagging, given that each engine deploys different inspection methods, analysis, algorithms and traffic signature libraries.

R&S®GSRM helps operators avoid these inconsistencies and enables equipment vendors, network packet brokers and mobile operators to deliver deeper traffic awareness by providing ready-to-use integration with R&S®PACE2, the deep packet inspection engine by Rohde&Schwarz. R&S®PACE2, an OEM software, performs real-time traffic classification by identifying protocols, applications and application attributes using statistical, behavioral and heuristical analysis as well as machine learning and deep learning. This enables operators to identify protocols (such as VPNs and BitTorrent) and applications (such as Netflix and Skype) in real-time. R&S®PACE2 also performs metadata extraction to deliver accurate and highly reliable information on various traffic attributes such as packet loss, latency and jitter.

R&S®GSRM combined with R&S®PACE2 provides mobile operators with deeper traffic awareness in a single integrated solution, even for encrypted, anonymized and obfuscated traffic, making the combination of R&S®GSRM and R&S®PACE2 the perfect solution for end-to-end visibility for mobile core networks.

Subscriber awareness for 5G SA networks

The coming years will see the rapid deployments of Standalone (5G SA) networks. Unlike 5G NSA and its predecessors, 5G SA will involve the use of new protocols including the Packet Forwarding Control Function and HTTP/2 to replace GTP. To deliver subscriber awareness for these protocols, Rohde&Schwarz is introducing the 5G Subscriber Revolving Module (R&S®5GSRM), which will be deployed in the 5G Core Network (5GC). The introduction of R&S®5GSRM will further enhance the suite of visibility tools provided by Rohde&Schwarz, specifically for subscriber awareness. This becomes increasingly critical as 5G service classes such as Massive Machine-Type Communications (mMTC) introduce millions of new sessions into the network.

8. THE NETWORK IMPACT

While general traffic awareness grants IP network operators an overview of the network, subscriber awareness goes a step further by unearthing deeper insights at the subscriber level. Subscriber awareness plays a key role in the management of networks. This is especially true for mobile networks where limited bandwidth and expensive network resources require networks to be continuously optimized and where minor hiccups can result in major implications for subscribers' quality of experience. It helps operators fine-tune their networks to improve not just basic metrics such as speeds and latency but also other parameters such as responsiveness, cost-efficiencies and monetization. GTP correlation, which involves the correlation of GTP user and control planes, provides operators with a highly effective technique to deliver subscriber awareness for mobile networks by analyzing parameters at both traffic layers for all incoming sessions. It replaces legacy methods for subscriber analysis, which are typically resource-intensive and time-consuming.

By providing seamless and real-time identification of subscribers, GTP correlation supports a wide range of network functionalities with real-time subscriber insights. Key among these functionalities is load balancing where the identification of subscribers in real-time enables subscriber-aware traffic aggregation, filtering and forwarding. This capability is particularly important for network packet brokers as it enables them to deliver intelligent load balancing, which addresses the shortcomings of traditional forwarding, especially the loss of crucial information that arises from involuntary session disaggregation.

Subscriber awareness enables network packet brokers to forward all the packets from a single subscriber in a single sequence to the same receiving device, delivering complete visibility for each subscriber session. This benefits network equipment vendors and mobile operators across a wide range of network subsystems and traffic processing functionalities, such as:

- **Monitoring / analytics** - enriching IP probes and other network monitoring tools with detailed data on subscriber behavior and data usage, including granular analysis by applications. This helps operators to keep a close eye on network performance, costs as well as user behavior and experience and better manage their assets and operations.

- **Traffic management** - providing traffic management functions such as routing, forwarding, content caching and content filtering with complete information on subscriber sessions. This allows operators to optimize network capacity by putting in place policies at the network and subscriber level. These policies are aligned with subscriber usage and network conditions. As a result, operators can deliver the expected SLAs across different subscribers and plans while maintaining network performance goals.

- **Policy control** - equipping policy control functions such as charging, mediation and AAA with information on subscriber sessions in order to implement appropriate authentication and controls. This improves overall service responsiveness, enhances subscriber experience and reduces fraud while driving monetization via contextual marketing.

- **Network security** - furnishing network security functions such as intrusion prevention, web filtering, DDoS prevention, content filtering and firewalls with accurate identification of sessions. As a result, these tools can detect suspicious and anomalous traffic in real-time. This secures mobile networks from cyberattacks, abuse and fraud.

To introduce subscriber awareness across these functionalities, network packet brokers, equipment vendors and mobile operators can depend on R&S®GSRM. As an OEM software module, R&S®GSRM delivers subscriber awareness seamlessly in any network environment and leverages its fast processing capabilities to ensure smooth network performance.

Coupled with R&S®PACE2, R&S®GSRM can be used to deliver granular insights into applications and threats for a more comprehensive analysis of subscriber preferences, usage trends and risks.

Conclusion

By incorporating R&S®GSRM, network packet brokers, equipment vendors and mobile operators are able to enhance the performance of their network functions. More importantly, it allows them to focus on subscribers and traffic that really matter based on significance, criticality and impact on revenue.

While the number of sessions in the core continues to grow and the complexities of managing different subscribers and plans increase, the ability to distinguish traffic by subscribers in real-time paves the way for intelligent traffic management, delivering improved customer experience and enhanced monetization for mobile operators.

By incorporating R&S®GSRM, network packet brokers, equipment vendors and mobile operators are able to enhance the performance of their network functions.

More importantly, it allows them to focus on subscribers and traffic that really matter based on significance, criticality and impact on revenue.

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

PD 3683.6441.52 | Version 01.00 | February 2022
White paper | Session and subscriber awareness in mobile core networks
Data without tolerance limits is not binding | Subject to change

3683644152
3683.6441.52 01.00 PDP 1 en