Performance analysis of subscriber sessions on Mobile-IP networks

Benefits

- Integrates with nGenius® InfiniStream™, allowing users to capture and analyze days of packet-level data for key mobile metrics.
- Advanced mobile filtering enables both Mobile Control filtering and subscriber-specific filtering. This advanced filtering eases the identification of mobile sessions based on NAI, IMSI, MSISDN, and APN. Also provides wildcard support for filtering.
- Subscriber session mining presents individual subscriber data sessions. Details include time and duration, IMSI, NAI, MSISDN, and APN and important network addresses: SGSN, GGSN, PCF, PDSN, home address, care of address, and home agent.
- Includes WAP Dynamic Port Detection to decode Wireless Transaction Protocol (WTP) and Wireless Session Protocol (WSP) messages when dynamic port assignment occurs.
- Call trace visualization capabilities present data sessions in a ladder diagram as a graphical depiction of specific communications.

Business Challenge

The future of mobile communications is converging upon feature-rich, IP-based voice, video and data (a.k.a. “triple play”) services. In the highly competitive mobile services market, providers urgently need to protect and enhance customers’ experience in order to reduce churn and grow the provider’s average revenue per user (ARPU). Although early mobile networks were designed primarily for telephony service, they have since evolved to support a wide number of IP-based data applications and services – including streaming of the latest music and video downloads as well as location-based services for mapping and navigation.

Such new services help retain subscribers and drive incremental revenue from consumer market segments. At the same time, mobile operators need to capture and retain the growing number of business customers who require email/calendar, VPN, Push-to-Talk and other applications in order to gain a competitive edge through an always-connected mobile field workforce. To successfully acquire and retain both consumer and business customers, mobile service providers need tools that help them optimize performance, and when problems do occur, to quickly and efficiently identify them and reduce the time required to resolve service-impacting issues.
With an eye towards the bottom line, operators are focused not only on subscriber acquisition and retention and increased ARPU but also on minimizing operating expense (OPEX). This has driven key infrastructure and technology investments including a migration of both voice and data traffic onto converged IP links. In support of this migration, mobile operators require a means of efficiently analyzing this packet-based traffic with an eye toward improved performance and problem resolution.

Mobile service providers require a solution for IP-based service assurance to help them monitor service quality and improve performance. Ultimately this solution minimizes operational expenditures while improving subscriber experience.

The Solution

NetScout’s Sniffer® Mobile Intelligence enables mobile wireless carriers to test, deploy, and operate 2.5G, 3G and emerging 4G mobile wireless data networks by providing protocol analysis and reporting tools for the wired/core side of General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), Code Division Multiple Access (CDMA) 2000, WiMAX, and Wideband Code Division Multiple Access (W-CDMA) networks. Using Sniffer Mobile Intelligence, mobile operators can resolve issues related to subscriber registration, network latency, dropped packets, and application response times, as well as Mobile IP and GPRS Tunneling Protocols (GTP). As operators deploy and manage the day-to-day operations of mobile data networks they need tools that support a wide variety of technologies and network protocols in order to help them more efficiently improve performance, quickly resolve service issues, and ultimately reduce OPEX.

Sniffer Mobile Intelligence leverages the functionality, performance, and reliability of nGenius InfiniStream®, combining its carrier-class performance and multi-terabyte storage capacity as well as proven TCP/IP troubleshooting and analysis capabilities with the advanced mobile expertise of Sniffer Mobile Intelligence. Users are able to decode critical mobile operator protocols and take advantage of a comprehensive troubleshooting and analysis solution for 2.5G, 3G, and emerging 4G mobile wireless data networks. Coupled with nGenius InfiniStream and its extremely reliable high performance stream-to-disk architecture – providing visibility into wide time windows of retained packets, Sniffer Mobile Intelligence provides a means to examine mobile subscriber sessions. The module includes panels for analysis and data mining of individual subscriber sessions which are identified through correlation of traffic over key mobile core network interfaces such as the Gn, Gp, and, Gi interfaces in UMTS environments and the AAA(A12), R-P(A10/A11), and PI interface in CDMA2000 networks. Mobile-specific objects and metrics provide insight into the performance, duration, traversed elements, and success/failures of specific subscriber sessions. Using Sniffer Mobile Intelligence on nGenius InfiniStream, network engineers can rapidly perform fault and performance analysis on specific corporate subscriber services and next-generation multimedia and location-based retail subscriber services.
Key Features
Robust features speed analysis and accelerate problem resolution on mobile networks.

Mobile Environment Protocol Decodes
Sniffer Mobile Intelligence leverages the decode functionality of the nGenius InfiniStream appliance to provide insight into the following Mobile protocols:
- 2.5G Mobile Wireless Networks
- 3G and 4G Mobile Wireless Networks
- Tunneling and Routing Encapsulation Protocols – GRE, IP-IP, GTP-U, Radius, and Diameter
- CDMA Accounting and Control Protocols – Mobile IP, RADIUS, and Diameter
- GSM/UMTS Accounting and Control Protocols – GTP-C, Radius, Diameter, and DNS
- SIGTRAN – SCTP, M3UA, ISUP, etc.
- IMS, SIP and SIP-T
- IPv4 and IPv6
- Broadcast and Multicast Services (BCMCS)
- Wireless Application Protocols (WAP)
- Short Message Peer-to-Peer Protocol (SMPP)
- Point-to-Point Protocol (PPP)
- Wireless Session Protocol (WSP)

Expert Analysis
Expert symptoms and diagnoses make it possible to discover network inefficiencies before they lead to more substantial deterioration in network performance. Sniffer Mobile Intelligence integrates with nGenius InfiniStream to leverage Expert Analysis for GTP, Mobile IP, and RADIUS.

Mobile Filters
Advanced mobile filtering, efficiently mines wide timeframes or windows of nGenius InfiniStream packet history and discovers mobile sessions for specific subscribers.
- An embedded Mobile Control filter can be quickly selected to optimize mining operation on appropriate Mobile Core Network control protocols.
- Subscriber-specific filtering provides a means for mobile sessions to be identified based on a Mobile Station ISDN (MSISDN), APN (Access Point Name), International Mobile Subscriber Identifier (IMSI), and Network Access Identifier (NAI) value.
- Wildcard support provides flexibility to search for MSISDNs, IMSIs and NAIs with multiple prefixes, suffixes or other variable fields.

Subscriber Summary
This Intelligence panel yields insight into the packet data sessions that match the subscriber and time-based filters selected in the mining console.
- Presents each unique session connection over time, including when and how the mobile subscriber connected to and used mobile data services.
- Session summary rows identify the subscriber by MSISDN, APN, IMSI, and NAI, with details of the other key encapsulation and tunneled network elements that provide mobility across each core network interface.
- Individual sessions can be expanded to reveal the mobile core network control protocols that have been correlated through the Sniffer Mobile Intelligence mining operation.
- Mobile signaling protocols are analyzed and presented at an interface detail level so mobile support staff can quickly determine which particular control message exchanges resulted in success or failure conditions.
- Individual or groups of Subscriber Sessions can be quickly filtered for detailed protocol decode analysis.
- CDMA2000 Environments – Correlates traffic traversing key interfaces and provides visibility into the registration process of each subscriber’s mobile IP session:
  - R-P (A10/A11) interface detail reveals the GRE keys and airlink state transitions throughout the entire data session.
  - AAA(A12) details present Radius Access messages and their success or failure status.
  - Pi interface detail reveals Mobile IP messages and their success or failure status.
- UMTS/GPRS Environments – Correlates and presents metrics and analysis of GTP-C, DNS, and DHCP providing users with visibility into the setup and teardown of the PDP context:
  - GTP presents information on GTP-C messages on the Gn interface.
  - DNS displays key messages between the GSN and the DNS server.
  - DHCP details reflect the relevant messages for the allocation of an address for the mobile node.
Call Trace Visualization
Subscriber data sessions can be presented in a ladder diagram as a graphical depiction of specific communications. For each subscriber session total elapsed time is presented along with individual delays associated with individual messages/commands. This view of traffic provides users with an understanding of latency associated with different network components and messages and ultimately their effect on subscriber experience.

Mobile IP, GTP, and Radius Expert Systems
Upon session-based filtering to a packet-level of operation, Expert systems further analyze Mobile subscriber activity and provide advanced protocol analysis and filtering. The user can choose whether packet mining and Expert analysis shall be performed for either session control alone or session control and data packets together.

- Individual Mobile IP gRE and IP-IP tunnels are identified and processed – even revealing the tunneled applications and their performance characteristics.
- Radius Access and Accounting messages are examined to ensure successful responses and low response time.

- Expert Alarms provide automated detection of session-related events and can be customized to assess impacts on the subscribers’ experience. Example Alarms include:
  - Mobile IP Registration Failures
  - Mobile IP Registration Slow Response Times
  - Radius Access Rejections
  - Radius Accounting Timeouts
  - Radius Access and Accounting Retransmissions
  - GTP PDP Cause Error
  - GTP PDP Context Request Timeout
  - GTP Slow PDP Context Response

About NetScout Systems
NetScout Systems provides advanced network and application service assurance solutions that deliver complete visibility into real-time, packet/flow-based operational intelligence. IT operators at the world’s largest enterprises, government agencies, and service providers use the Sniffer and nGenius solutions to troubleshoot service degradations faster and more efficiently in order to reduce MTTR.

Our world-renowned Sniffer and nGenius solutions include:
- Intelligent Data Sources for high capacity, deep-packet recording and monitoring
- Analysis Software for real-time and historical network and application performance management, troubleshooting, capacity planning, and reporting
- Advanced Intelligence for early detection and in-depth analysis of complex or specialized application services
- Comprehensive, global support, consulting and training services

Corporate Headquarters
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 888-999-5946
www.netscout.com

European Headquarters
NetScout Systems (UK) Ltd.
100 Pall Mall
London SW1Y 5HP
United Kingdom
Phone: +44 (0)20 7321 5660

Asia/Pacific Headquarters
Room 105, 17F/B, No. 167 TunHwa N. Road
Taipei, Taiwan
Phone: +886 2 2717 1999
www.netscout.cn