teleSys
SOFTWARE

MACH7- iMCP

“Intelligent Message Control Platform”

Overview

The MACH7 Intelligent Message Control Platform (MACH7-*i*MCP) is an efficient, cost-effective and scalable **SMS Gateway and Firewall** solution that facilitates advanced routing and secure home network & its subscribers from unwanted short message threats.

It can be also used as SMS Hub solution for clearing and settlement through the processing and reporting of SMS traffic on behalf of mobile operators. The MACH7-*i*MCP provides the ability to negotiate wholesale compensation agreements based on actual usage of the service.

Solution Advantages

- ❑ **Seamless Interoperability**: Uniquely positions service providers to effectively manage network and business issues associated with successful SMS delivery
- ❑ **Service Reliability and Security**: High-performance solution providing single connection point for SMS traffic to the connected operators. Screens SMS traffic to prevent any unauthorized and fraudulent traffic to the end-users.
- ❑ **Cost Savings**: Latest technology reach for service delivery without major capital expenses by significantly reducing transport costs using IP transport and associated protocols.
- ❑ **Revenue Generation**: Increases profitability of SMS service offerings, by enhancing subscriber satisfaction to drive up usages.

Offered Services

SMS Flood Prevention

SMS flood condition is triggered when a large number of messages being sent to one or more destinations, regardless of the validity, purpose or content of the messages.

It can be either,

- **Mobile Terminated SMS Flood**, which is act of denial of service attack to overload the signaling network, OR
- **Mobile Originated SMS Flood**, which may have caused by a handset(s) or device(s) that have been compromised

In either of the cases, it can cause billing issues, impacts quality of service and can damage operator’s brand and reputation to its subscribers and inter-connect operators.

MACH7-iMCP Flood Prevention service constantly monitors number of valid messages from / to configured sources / destinations to ensure that count remains within a pre-defined limit. Once that exceeds threshold criteria on pre-defined limits within a message period, flood prevention procedures get triggered.

Procedures can be,

- **Monitor** : when messages are not blocked, but alert is raised indicating the condition so that operator can decide on next steps.
- **Block**: when messages are discarded and alert is raised till it comes down to allowed limits.

SMS A-number Screening

SMS A-number screening is used to confirm usage of home SMSC(s) by legitimate home subscribers only. In order to ensure that, smart screening of MO-SMS traffic from foreign network(s), destined towards home SMSCs should be performed at the edge of the network.

SMS GW application hosted on MACH7-iMCP intercepts moFSM messages and screens received A-number (calling MSISDN), to deny MO-SMS services to ported-out subscribers (with MSISDN from home network range) and also to the ones which are not ported-in (with MSISDN from foreign network range).

SMS Spoof Prevention

The spoofing case is related to an illegal use of the home SMS-C by an external fraudulent party. In this case, a MO-SMS with a manipulated A-number arrives at home network from a foreign VLR (real or wrong SCCP Address). SMS Firewall application intercepts MO-SMS message, to validate:

- Legitimacy of received calling MSISDN , and
- Location of the subscriber by comparing source network address received against the current location stored in HLR

Based on validation result, service can be rejected for any spoofed MO-SMS

Fake SMS Protection

In Fake SMS scenario, source address of MT-SMS message is manipulated with some valid operator information. This faking causes inter-PLMN accounting error, affecting both operator whose address has been misused in the source address and also the subscriber receiving the message. Inconsistencies in interconnect billing records as well as unhappy subscribers can adversely impacts mobile operators business.

teleSys SMS Fake Protection prevents SMS Fake attacks, safeguarding the network from potential loss of subscriber confidence, by altering MT-SMS delivery path from external networks via SMS Firewall application following SMS Home Routing capability as specified in 3GPP Technical Report.

SMS First Attempt Delivery

SMS GW routing feature for First Attempt Delivery (FDA) increases revenue potentials by optimizing network resources related to SMS delivery. With this routing method, SMS GW first attempts to deliver all MO-SMS messages directly to the recipient instead of handing over the functionality to respective SMSC. Since most mobile subscribers are always-on and reachable via inter-operator connections, there are high chances of message delivery in very first attempt. In case first attempt fails, message will be handed over to the SMSC as specified by standards.

Using this model, store-and-forward procedures at SMSC is optimized considerably by operating only on those SMSes which are not delivered by first attempt methods.

Advanced SMS Routing

teleSys' advanced SMS Routing facilitates cost-effective delivery of SMS traffic for:

- SMS Offload, and
- SMS variant interworking

SMS Offload feature allows cost-effective message delivery using IP network off-loading these data traffic from expensive SS7 TDM based networks. Offloading to IP network is performed by conversion of SS7 based SMS signaling to operators SMSC capabilities which can be SIGTRAN based SS7-over-IP, SMPP (Short Message Peer to Peer) or any other protocols of choice. This frees up and optimizes SS7 network to process additional mobile traffic and other value-added services to end-users.

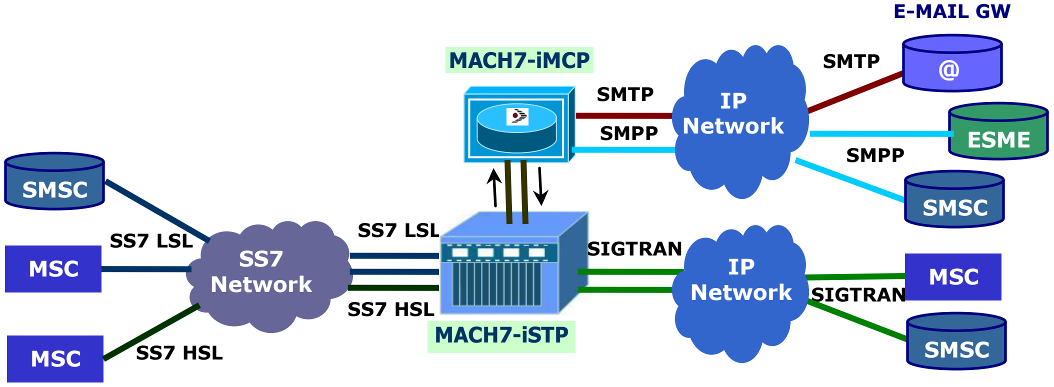
SMS variant inter-working feature can facilitate inter-carrier SMS service to increase messaging revenues with access to global mobile operators. Conversion of SMS traffic to SMPP protocol, allows seamless termination of SMS traffic from one network variant to any other network in a cost-effective way. This extends network reach-ability of mobile operators globally to other network variants.

Platform Capabilities

MACH7-iMCP platform features includes:

- Fully redundant carrier-grade solution
- Detailed message tracing functionality
- Real time debugging capabilities
- Real time Status and Statistic information
- Any-to-Any Signaling Interface
  - ❑ SS7-TDM Low/High Speed Links
  - ❑ SIGTRAN based SS7 over IP protocol
  - ❑ IP based SMPP protocol
  - ❑ SMTP interface to Email Gateways

The MACH7-*i*MCP solution can be deployed in two modes: a ***Standalone Deployment*** or an ***Integrated solution with the MACH7-iSTP***.



MACH7-iMCP integrated to MACH7-iSTP

teleSys Software, Inc.

teleSys is the premier provider of advanced Telecommunications solutions for the next generation LTE Signaling Networks, providing open systems hardware and software.