

SGA-SMSFD

SMS Fraud Detection System

Securing Your Network and Subscribers

Mobile phone operators and users are all threatened nowadays by malicious usage of SMS systems. There are various methods for sending "free" SMS to any locations around the world by people who are not the actual subscribers of the operator's network, although they use valid (stolen) SIM information of existing subscribers. Someone has to pay for this traffic, and it will ultimately be the operator, since the subscribers will either complain and ask for refund, or become dissatisfied, which may lead to gossip or churn. SGA-SMSFD, AITIA's latest SMS Fraud Detection system, allows the operators to filter this non-authentic traffic and helps avoid its unpleasant consequences.



Alerting, Logging and Blocking Fraud

SGA-SMSFD can be considered as a firewall protecting the SMS Center (SMSC) in the SS7 world. The operator can assign various treatments to handle suspicious messages - from merely logging the event to the extreme case of blocking the SMS and warning the operating staff by an alarm.

Operating Principles

SGA-SMSFD receives several types of SMS-related messages that were sent towards the SMSC. Upon receiving a ForwardSM message, SGA-SMSFD analyzes the signaling message structure, and checks if all fields are filled out according to the expectations; incorrectly given message fields (such as variables related to encoding schemes, network node identification or user identification) yield for suspicion. Then it checks whether the sender of the SMS *really* resides in the MSC/VLR area that is suggested by the message header - this is done by a HLR interrogation procedure. This analysis has an end-result for each message.



AITIA International, Inc.

Czetz J. utca 48-50., H-1039 Budapest, Hungary

Tel.: +36 30 397-8303, +36 1 453-8080 Fax: +36 1 453-8081

E-mail: info@aitia.ai

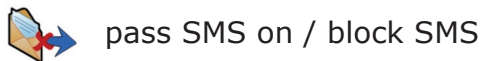
www.aitia.ai

SGA-SMSFD

SMS Fraud Detection System

How Threats Are Treated

The operator can define various rule-sets for the messages and assign actions to these rule-sets. SGA-SMSFD treats a message depending on the rule that fits the analysis result and the actions that are assigned to the rule. The operator can assign any combinations of the following basic actions to the rule-sets:



pass SMS on / block SMS



log event / no logging



send alarm / no alarm

A more sophisticated rule can be the forwarding of a certain amount of SMS first, then blocking the rest.

Examples

Example rules and actions could be the following:

- MSC address of the message is in the home network
"good, pass SMS on, no log, no alarm";
- MSC address in the message does not match the HLR interrogation result
"suspicious, block SMS, log event, alarm";
- HLR returned an error code or its query timed out
"pass SMS on, log event, no alarm"; etc.

Additional Features

- Threshold-based alarming
 - number of messages sent from the same subscriber (MSISDN) within a certain interval
 - number of messages sent towards a country (prefix) over a threshold
 - number of messages sent from a country (prefix) over a threshold
- Comparison of number ranges, masked numbers
- Statistics on messages classified, HLR requests and its answer types, etc.
- Easy configuration of rule-sets and actions

Hardware and Software Configuration

The system hardware consists of a single industrial grade PC with an SGA-47 interface card. Its software is also well optimized, hence computationally not intensive. These hardware and software requirements allow the operators to use various other SGA products on the same PC. Application availability can be increased by system duplication, which is highly cost-effective for SGA-SMSFD, due to its minimized hardware requirements.

AITIA Telecommunications References



AITIA International, Inc.

Czetz J. utca 48-50., H-1039 Budapest, Hungary

Tel.: +36 30 397-8303, +36 1 453-8080 Fax: +36 1 453-8081

E-mail: info@aitia.ai

www.aitia.ai