SMS Flood Protection

Protect against attacks, originating from both inside and outside your network

Advanced measures to protect against SMS Spam

SMS Flood | A high rate or large number of messages being sent to one or more destinations, regardless of the validity, purpose or content of the messages.

The GSM Association defines SMS Flood as:

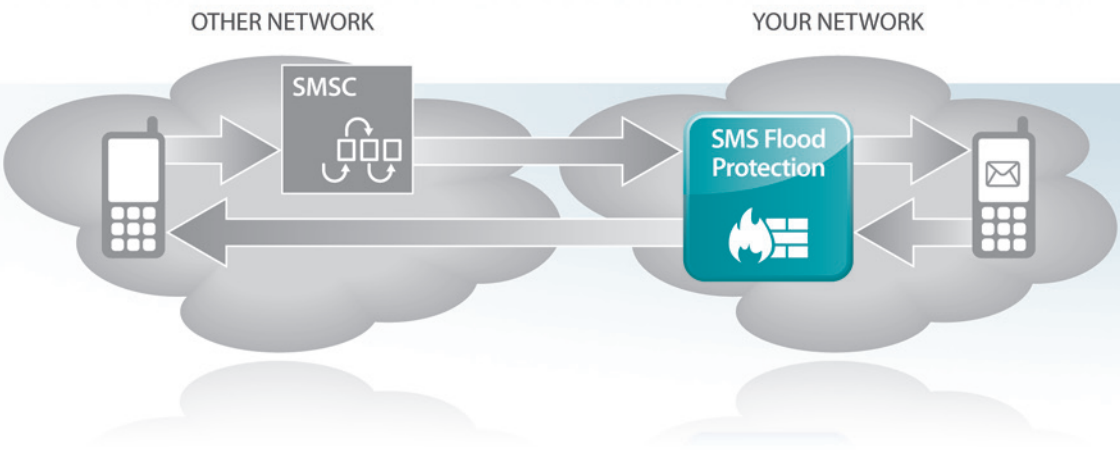
"A high rate or large number of messages being sent to one or more destinations, regardless of the validity, purpose or content of the messages.

SMS flooding is typically detected by comparing the rate or number of messages in a selected message flow to a pre-selected defined average or expected load. If the number or rate of messages exceeds the pre-defined rate with no other explanation (e.g. festival, social event) then this may be considered flooding. SMS flooding can often occur together with the other SMS fraud scenarios, for example SMS malware attacks through the network could generate SMS flooding events, SMS text spam is often enclosed within the flooding messages and large number of SMS faking/spoofing messages could also be considered a SMS flooding attack as well."

Mobile Terminated SMS Flood can be a nuisance to on-net subscribers and can also be a type of denial of service attack, designed to overload the signalling network.

Mobile Originated SMS Flood is typically caused by handsets that have been compromised, either by being cloned or by being infected with mobile malware. This can cause billing issues and damage to an operator's brand and reputation, both with its own customers and with other network operators.

Telsis SMS Flood Protection, together with Telsis SMS Spoof and SMS Fake Protection, can provide a safety net around the network, protecting both subscribers and your reputation.



SMS Flood Protection

Mobile Terminated Flood Protection

In order to protect against mobile terminated message floods, the Telsis SMS Flood Protection system first uses SMS Fake Protection in order to ensure that each message has not been sent using SMS Fake fraud (Please refer to the Telsis document 'SMS Fake Protection').

Providing that a message is not fraudulent, the Telsis SMS Flood Protection system increments the recorded number of messages originating from the off-net sending SMSC in the pre-determined period.

Providing that the number of messages from that SMSC has not exceeded a pre-configured maximum during the period, then message delivery is allowed. If the number of messages from a given SMSC exceeds a pre-defined limit, then the messages are treated as SMS Flood messages.

An SMSC address prefix whitelist is provided to allow selected SMSC or SMSC groups to be marked as trusted and bypass the rate limit check.

Mobile Originated Flood Protection

In order to protect against mobile originated message floods, the Telsis SMS Flood Protection system first uses SMS Spoof Protection to ensure that each message has not been sent using SMS Spoof fraud (Please refer to the Telsis document 'SMS Spoof Protection').

Providing that a message has not been Spoofed, the Telsis SMS Flood Protection system increments the recorded number of messages sent by that subscriber in the pre-determined period.

Providing that the subscriber has not sent more than a pre-configured maximum number of messages during the period, the message is allowed. If the subscriber has exceeded their limit, then the message is treated as an SMS Flood message.

An MSISDN address whitelist is provided to allow selected MSISDNs to be marked as being trusted and bypass the rate limit check.

Defaults

The precise SMS Flood configuration may be varied per operator, however the default configuration is:

Mobile Terminated Messages allowed:	
From other networks in the same country	1 million SMS per message period per SMSC
From other countries	100 thousand SMS per message period per SMSC
Mobile Originated Messages allowed:	
All mobile originated messages	100 SMS per message period per MSISDN
Periods:	
Message periods	1 hour 3 hours 6 hours 24 hours

Actions

When SMS Flood is detected, one of three actions may be carried out, as shown below:

Monitor

In Monitor Mode, messages are delivered as normal, however an alert is raised to indicate that an SMSC has exceeded the pre-defined maximum limit and that there is a potential SMS Flood attack. The operator cannot view these messages, but can decide whether to Groom or Block messages from this SMSC.

Groom

In Groom Mode, rather than being delivered, messages are groomed to a Service Provider account for further analysis and an alert is raised to indicate that there is a potential SMS Flood attack. The operator can then choose to discard or deliver these messages.

Block

In Block Mode, any potential SMS Flood message is silently discarded, and an alert is raised to indicate that there is a potential SMS Flood attack in progress.

The operator can switch between modes of operation, depending on the prevailing network conditions.

Telsis SMS Flood Protection, together with SMS Spoof Protection, SMS Malware Protection and SMS Fake Protection can provide a safety net around the network, protecting both subscribers and brand reputation.

Contact: sales@telsis.com

www.telsis.com

UK	Germany	España	Italia	Middle East	Singapore	Australia
T: +44 (0) 1489 76 00 00	T: +49 (0) 6151 827 850	T: +34 91 532 72 10	T: +39 02 655 1644	T: +971 4 361 6179	T: +65 6224 5585	T: +61 (0) 2 9978 5300
F: +44 (0) 1489 76 00 76	F: +49 (0) 6151 827 8521	F: +34 91 532 96 40	F: +39 02 657 5302	F: +971 4 439 3554	F: +65 6224 7356	F: +61 (0) 2 9978 5333

Telsis High Value Mobile Innovation