

To prevent mobile-to-mobile SMS spam and fraud

Mobile-to-mobile SMS spam and fraud comes in many forms and can cause substantial damage with respect to customer satisfaction, financial performance and network operations. The table below summarizes some of the more common types of mobile-to-mobile SMS spam and fraud in existence today:

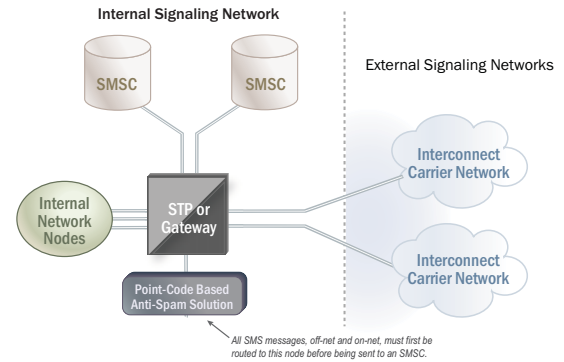
Type	What Happens	Risk to the Operator
Spamming	Unwanted messages are delivered to subscribers	Irritated subscribers, degraded performance, blamed for relay
Flooding	Remote system sends massive numbers of messages targeting subscribers and nodes	Overload in the signaling network, home operator incurs relay operator costs
Faking	Foreign system uses identity of legal SMSC	Home operator cannot collect termination fees
Spoofing	Messages sent illegally by simulating subscribers in a roaming situation	Subscribers wrongfully billed for unsent messages and perhaps unwanted content
Smishing	Messages that appear to be from a valid company attempt to acquire subscriber information	Subscriber annoyance, billing issues, potential to spread viruses and then more spam
Viruses	Hacker engine launches messages luring subscribers to a download site with viruses	Compromised handsets cause customer service problems and may send unwanted messages

Mobile-to-mobile SMS spam and fraud is a rapidly growing problem with the most prevalent provider concerns being that it:

- Irritates subscribers and in turn increases churn, raises support costs and casts a negative light on the carrier's brand. Subscribers find spam annoying and many regard it as an invasion of privacy. It also results in unwarranted charges leading to customer frustration, subscriber complaints and operator refunds.
- Results in lost revenue for inter-carrier messages. With SMS fraud, the sender assumes the identity of a valid subscriber or SMSC, so the operator receives no termination fee.

- Increases operational costs because of the large volumes of unauthorized messages. SMS spam and fraud can degrade network and SMSC performance and at times severely impact them.
- Damages the adoption of revenue-producing services. Spam can destroy trust in an operator, leading subscribers to opt-out of emerging mobile advertising and m-commerce opportunities.

One approach that is used to try and prevent mobile-to-mobile SMS spam and fraud is to deploy a Point Code Based anti-spam element(s) within a carrier's SS7 core network, as shown in the diagram below.



Point Code Based Anti-Spam Approach

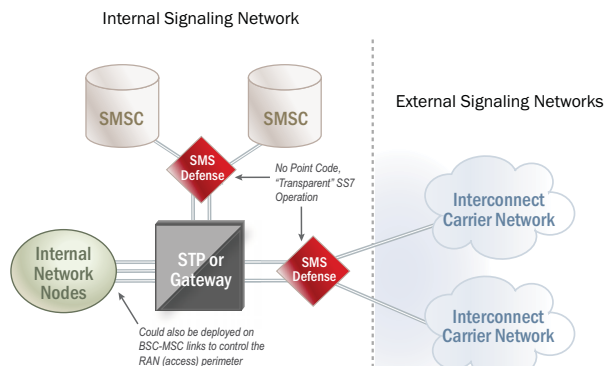
This approach has several disadvantages however, including that:

- All "off-net" (i.e. originating on another carrier's network) mobile-to-mobile SMS spam and fraud is allowed to enter a carrier's signaling network unchecked and consume STP/Gateway resources.
- Every off-net and "on-net" (i.e. originating on a carrier's own network) SMS message must first be routed to the Point Code Based node before being sent to an SMSC, increasing the amount of SMS traffic in a carrier's SS7 core and consuming more network resources.
- Because this approach requires an SS7 point code, carriers must reengineer their SS7 network and in some cases deploy intelligent routing mechanisms and additional STP resources.

Prevent mobile-to-mobile SMS spam and fraud transparently with SMS Defense

In contrast to taking a Point Code Based approach to preventing mobile-to-mobile SMS spam and fraud, **SMS Defense** resides transparently (i.e. it does not require a point code) on both carrier-to-carrier SS7 interconnect links and SMSC signaling links. With SMS Defense you can stop off-net spam and fraud before it can reach your external facing STPs/Gateways and not have to reroute every SMS message to a new network element before it can be sent to an SMSC, minimizing the amount of SMS traffic in your signaling core network.

SMS Defense is equipped with the core capabilities needed to manage SMS spamming, flooding, faking, etc. along with enhanced content filtering and advanced control features that include message thresholding, re-routing, modification and response. And because it utilizes Sevis' "transparent" Signaling ASE® Platform, SMS Defense does not require any network re-engineering to install it and it can be positioned anywhere within your signaling network, including the Radio Access Network perimeter or "Access Edge" (i.e. on BSC-MSC signaling links).



SMS Defense Example Network Deployment

Comparing a "Point Code Based" Approach to SMS Defense

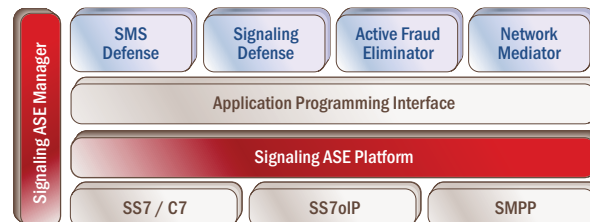
Benefit	Point-Code	SMS Defense
Spamming Protection	✓	✓
Flooding Protection	✓	✓
Faking Protection	✓	✓
Spoofing Protection	✓	✓
Smishing Protection	✓	✓
Virus Protection	✓	✓
Enhanced Content Filtering	Varies	✓
Stops spam at the network perimeter		✓
Does not increase SMS traffic in the SS7 core		✓
Advanced message control		✓
No SS7 network re-engineering required		✓

The Architecture:

One platform, no point code, many solutions

Each Sevis solution utilizes Sevis' patented **Signaling ASE[®] System**, a proven, carrier-grade system that enables both Sevis and partner-developed applications to be deployed without an SS7 point code, thus eliminating the need for operators to re-engineer their signaling network upon installation and allowing any ASE-enabled solution to operate independent of a carrier's existing vendor infrastructure.

The ASE System is comprised of the ASE Platform (the "transparent" SS7 network element) and the ASE Manager. The ASE System is the cornerstone of all of Sevis solutions, and once deployed it can be the foundation to help you address other needs in addition to controlling SMS spam to include improving SS7 network security and risk mitigation (*Signaling Defense*), enhancing your fraud control capabilities (*Active Fraud Eliminator*) and resolving network interoperability issues (*Network Mediator*).



The ASE platform and ASE architecture

Technical Specifications: Carrier-grade, high availability, flexible

Protocols

ANSI

- T1.111 MTP
- T1.113 ISUP
- T1.112 SCCP
- T1.114 TCAP
- AIN 0.1/0.2
- IN
- ANSI-41 D
- WIN

ITU/ETSI/3GPP

- Q.701 – Q.705, Q.707 MTP
- Q.761 – Q.764 ISUP
- Q.711 – Q.714 SCCP

Sigtran

- Q.771 – Q.774 TCAP
- Q.721 – Q.724 TUP
- INAP CS-1/CS-2
- GSM MAP
- CAMEL
- M3UA
- M2PA

Application

- SMPP
- SS7oIP

Platform Specifications

Chassis

- 2 U high, rack-mountable chassis
- 19" (482.6 mm) or 23" (584.2 mm) rack mount
- Packet switching backplane
- 3 trunk interface module slots
- Up to 12 T1/E1s per platform
- Up to 48 transparent low speed SS7 links per chassis
- Up to 3 transparent ATM high speed links per chassis
- Chassis clustering
- Alarm status display module
- Telco alarm interface (dry/wet contact relay)

- 5 10/100 Base-T Ethernet ports
- Hardware/software status reporting

Power Supplies and Fans

- N+1 redundancy
- Hot swappable
- DC (-48V)
- A and B DC power feed

Trunk Interface Module

- Up to four T1/E1s
- Up to 16 transparent low speed SS7 links
- Up to 1 transparent ATM high speed link
- A, B, C, D, E, F links
- Channel associated signaling
- T1/E1, RJ-48C
- Hot swappable
- 3 10/100 Base-T Ethernet ports
- Drop and insert grooming
- Automatic link protection
- LED status indicators
- Rear transition module

Regulatory Compliance

- NEBS Level III certified
- ETSI 300 019 2-1 to 2-4
- CE
- FCC Part 15, Class A (CSA)

Temperature Range

- Operating: -5°C to +55°C (23°F to 131°F)
- Storage: -40°C to +70°C (-40°F to +158°F)

Management Server

Architecture

- Centralized client/server
- Dual processor
- RAID 5
- Hot-plug hard drives
- Hot-plug redundant power supplies
- Java-based GUI client

Event Management

- Event filtering with audible event notification
- Hardware/software status reporting

Performance Management

- CPU and memory utilization monitoring
- Link status monitoring
- Detailed platform/server statistics

Security Management

- User-configurable multi-level security access
- User authentication and activity timeout
- Encrypted management interfaces

The Company: Helping carriers protect their revenue, subscribers and network

Sevis Systems helps communications service providers protect their revenue, subscribers and network through innovative signaling solutions. Founded in 1999, Sevis is an employee owned and operated company that is headquartered in Plano, Texas. Sevis' solutions have been purchased by some of the largest service providers in the world and are resold by globally-recognized equipment suppliers including Alcatel-Lucent. To find out more about Sevis and our unique solutions, please call us at **877.517.3847** or visit our website at www.sevis.com. We look forward to working with you.