defense solutions for the modern SMS ecosystem

SMS messaging problem overview

SMS is a ubiquitous communication method for person-to-person (P2P) text messaging, which has been in use globally for nearly 20 years. While consumers have grown ever more dependent on text messaging as a preferred method of communication, service providers continue to suffer major financial losses due to rampant misuse within the Short Message Service (SMS) environment The telecommunications industry organization GSMA states that an average-sized mobile network of 16 million subscribers could easily experience revenue leakage in excess of $4 million per year from SMS-related fraud alone.

Today, SMS platforms are increasingly being used for illicit application-to-person (A2P) communication purposes, especially grey route messaging. Within the telecommunications industry, grey route messaging refers to A2P messages that originate outside of authorized networks, and illicitly infiltrate service provider networks by exploiting traffic channels designated specifically for P2P messages. For the average service provider, grey route messaging is extremely hard to identify and intercept, leading to immense revenue leakage.

did you know?

Unauthorized SMS traffic on a network is an immediate loss of billing revenue for service providers, as is it circumvents legitimate commercial channels and cheats service providers out of termination charges they would otherwise receive.

Historically, mutually beneficial agreements between service providers have facilitated simple SMS billing policies when terminating inbound messaging. To reduce costs and save time, customer messaging between different service providers has been mostly settled by mutual forgiveness, which is also known as GSMA AA.13 “bill and keep” policy.

Third-party content providers and aggregators, however, have begun exploiting these flexible policies for illicit A2P messaging, resulting in unauthorized A2P messaging flooding routes designed specifically for P2P messaging. This abuse has resulted in a tremendous strain on P2P routes and exposed subscribers to countless instances of spam and consumer fraud.

Spam traffic overwhelms P2P links and reduces the ability for legitimate messaging traffic to enter the respective network and reach appropriate end users on schedule.

defense solutions for the modern SMS ecosystem

a tough choice for service providers

Standard service provider network capabilities do not have the ability to identify and segregate A2P spam from P2P traffic, without compromising and interrupting legitimate traffic. This technical limitation creates an all-or-nothing scenario for service providers and allows A2P traffic to enter the service provider's network unhindered. The vast amount of unregulated A2P traffic leads to a lower quality of service on the networks, and inundates subscribers with unwanted and harmful messages, which leads to increased customer dissatisfaction and higher levels of user account cancelations.

To prevent the disruption of legitimate messaging traffic, A2P messages are usually allowed to circulate unchecked within the network, creating additional risks and challenges for service providers and their customers. Among them:

- Spam traffic overwhelms networks causing the reliability of legitimate P2P messages to drop.
- Emergency services may get halted, as important SMS alerts/communications are unable to reach the respective emergency service providers.
- Customer complaints rise as end users receive delayed P2P messages or lose messages outright.
- Transactional notifications are negatively impacted and require banks/ institutions to send duplicate notifications, causing additional financial burden.
- Service providers suffer a tarnished brand reputation, leading to reductions in market growth.
- Storage limits in end user devices can be quickly filled to capacity by spam, further hindering legitimate P2P message delivery.
- End users can become easily confused by excessive spam messages, and accidently delete legitimate P2P messages.

> The difficulty in anticipating the frequency, duration, and origin of A2P attacks creates a complicated technical and financial challenge for the service providers.

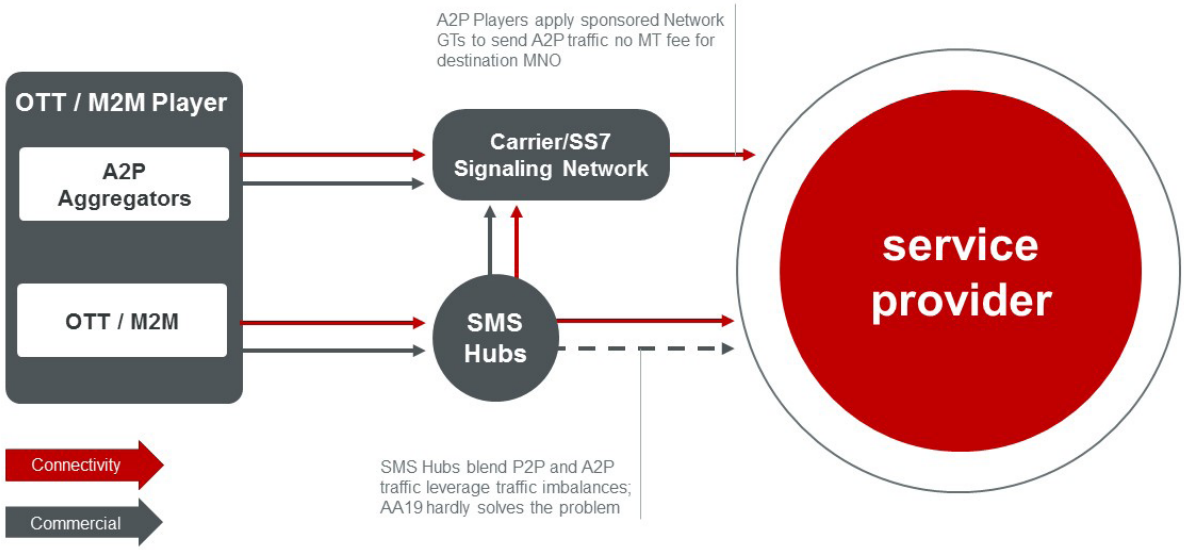


Figure 1: Depicts how unauthorized SMS traffic accesses and infiltrates service providers using unrestricted access via other service providers' networks. Any A2P provider can connect to a service provider network using an SMS hub and flood service provider platforms by blending undetected A2P messages with legitimate P2P traffic on the network.

defense solutions for the modern SMS ecosystem

common threats in the SMS ecosystem

SMS ecosystem threat	service provider impact
Fraudulent Messages Cause customer dissatisfaction and bog down service provider customer service departments with complaints and requests for refunds related to fraud-related messages. Example: Fraudsters may send an SMS message, asking subscribers to deposit money while pretending to be an official agent associated with the service provider.	• Financial losses associated with refunds for fraudulent charges. • Extended customer service resources to mitigate complaints. • Tarnished service provider brand reputation. • Lower account retention rates.
Grey Routes A2P messages that originate outside of authorized networks and illicitly exploit traffic channels designated specifically for P2P messages. For the average service provider, grey route traffic is extremely hard to identify and intercept, leading to immense revenue leakage.	• Revenue loss to service provider due to unmonetized traffic. • Increased infrastructure maintenance and costs to address increased network traffic due to illegitimate messaging. • Legitimate messaging interruption as service providers attempt to identify and shutdown potentially illegitimate traffic. • Increased subscriber dissatisfaction, as end users are being reached directly with unmonitored content.
Phishing Scams Messages containing links to malware, which when clicked install malicious programs that can access sensitive user information. These threats may also have the ability to take control of a smart device to send illicit text messages without the user's knowledge.	• Creates major end user dissatisfaction. • Phishing messages cause virus attacks, which may in-turn impact service provider network performance. • Illicit messages often go to premium rate destinations, causing service providers to absorb expensive termination charges.
Spoofing The ability to steal or misuse a user's identity to send and receive messages. Example: A legitimate service provider user account is targeted for international roaming access and incurs substantial fees, before being discovered by the legitimate subscriber at the end of a billing cycle.	• Subscriber dissatisfaction and possible legal litigation as subscribers receive inaccurate usage summaries, which can cause compound negative effects on credit scores. • Increased user account cancellations as unsatisfied customers look for more reliable service providers. • Loss of revenue as service providers have to settle incorrect billing.

impermeable defense solutions within the sms ecosystem

Deploying sophisticated anti-fraud technology and having it administered by an experienced and reputable organization can drastically curtail revenue leakage and improve service provider messaging operations in general.

The latest fraud solutions and services can provide a formidable multi-level defense by first digitally ring fencing a service provider network, to ensure complete SMS ecosystem isolation, and to obtain complete control on all messaging traffic flowing into the network.

Next, powerful filters and highly sensitive monitoring software is deployed, to curtail suspicious SMS activity and protect network infrastructure and resources. In addition to implementing filters and monitoring software, a detailed reporting system allows for efficient project management.

Once the necessary hardware and software is in place, all SMS traffic passes through a proprietary messaging solution, and is then cross-checked to identify any suspicious SMS activity, as well as eliminate any previously unnoticed revenue leakage.

A sophisticated messaging solution autonomously identifies suspicious SMS messages, and surgically eliminates them from the network before they reach end-user devices. The unauthorized traffic is then systematically categorized into different profiles i.e. Grey Routes, Spam/ Junk Traffic, Fraud Traffic, etc.

Once all SMS traffic has been successfully diverted to the filtering firewall, traffic patterns are then monitored by expert fraud and identity authentication analysts, based on the SMS content being passed, volume being sent at various intervals and frequency of traffic patterns being pushed through the network.

defense solutions for the modern SMS ecosystem

the SMS ecosystem under continuous protection

The service provider benefits from a stable and consistently secure SMS ecosystem are innumerable, both financially and as well as for brand integrity purposes. When fraudulent A2P traffic is effectively placed under the control and protection of a reputable anti-fraud organization, service providers focus on other operational and business development priorities.

Just some of the immediate benefits include:

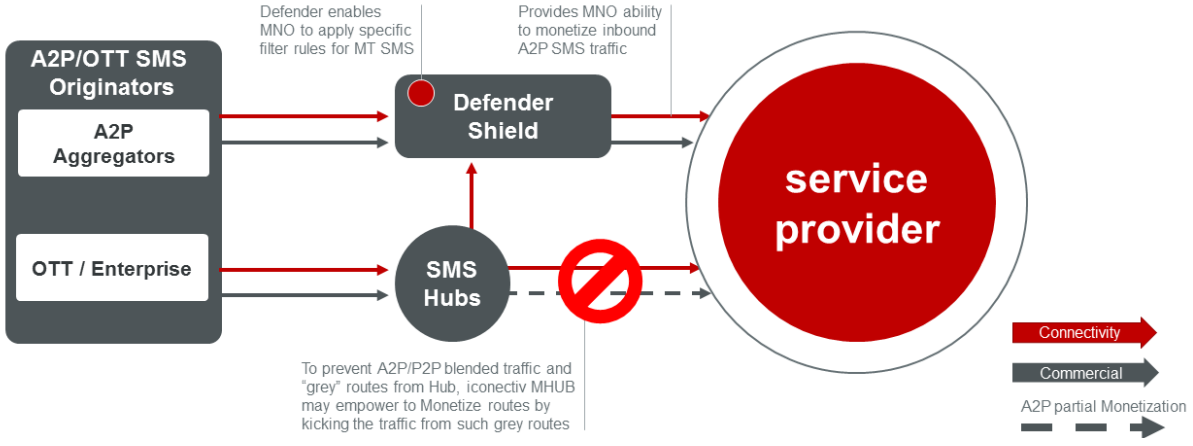
- Scanning all incoming SMS messaging via sophisticated filters, that allows service providers to identify and eliminate phishing threats before they reach end users.
- Closely monitoring SMS origins, and using powerful firewalls to block out unwanted threats and grey route traffic.
- Leveraging detailed SMS data to verify subscriber geographic location, and to cancel any questionable messaging traffic coming into the network that may be spoofed.

unprotected SMS ecosystems are under immediate threat

Without appropriate filters in place, service providers are currently highly vulnerable to fraud, spam and lost revenue. Most important of all, inadequate defenses in the SMS ecosystem can lead directly to customer dissatisfaction and may cause irreparable damage to a service provider's brand reputation.

With proper SMS defenses in place, service providers get the peace of mind knowing their network assets and infrastructure are well protected against misuse within their SMS ecosystem, as well as the multitude of existing SMS threats including spam, phishing activities, spoofing attacks and grey route messaging penetration.

SMS solution and service experts offer service providers network protection, extensive SMS reporting and monitoring; while their experienced support teams provide valuable insight into the complexity within the modern SMS ecosystem.



about iconectiv

As the authoritative partner of the communications industry for more than 30 years, iconectiv's market-leading solutions enable the interconnection of networks, devices, and applications for more than two billion people every day. Working closely with private, government and non-governmental organizations, iconectiv continues to protect and secure telecommunication infrastructures for service providers, governments and enterprises, while providing network and operations management, numbering, registry, messaging and fraud and identity solutions to more than 1,200 organizations globally. A US-based company, Telcordia Technologies, does business as iconectiv.

make the connection.

For more information about iconectiv, contact your local account executive, or you can reach us at:

+1 732.699.6800

info@iconectiv.com

www.iconectiv.com

iCOL-MB-DS-E-LT-002, Jan2017