Spam threat

Table of Contents

Table of Tables

1 Introduction

The purpose of this document is to provide details regarding growing SMS relatedspam threats in India.

1.1 TRAI Guideline.

To control growing problem on SMS Spam and phishing attack TRAI came up with guideline to CSP. This would require CSP toin placeinfrastructure with following mandatory features.

- All international SMS containing alphabet header or alphanumeric header or +91 as originating country code should not be delivered through the network"
- "If any source or number from outside the country generates more than two hundred SMS per hour with similar 'signature', the same should not be delivered through the network. However, such restriction shall not be applicable on blackout days."
- Only valid codes associated with the network of those entities with which agreements have been signed by the Access Providers shall be allowed in the network.

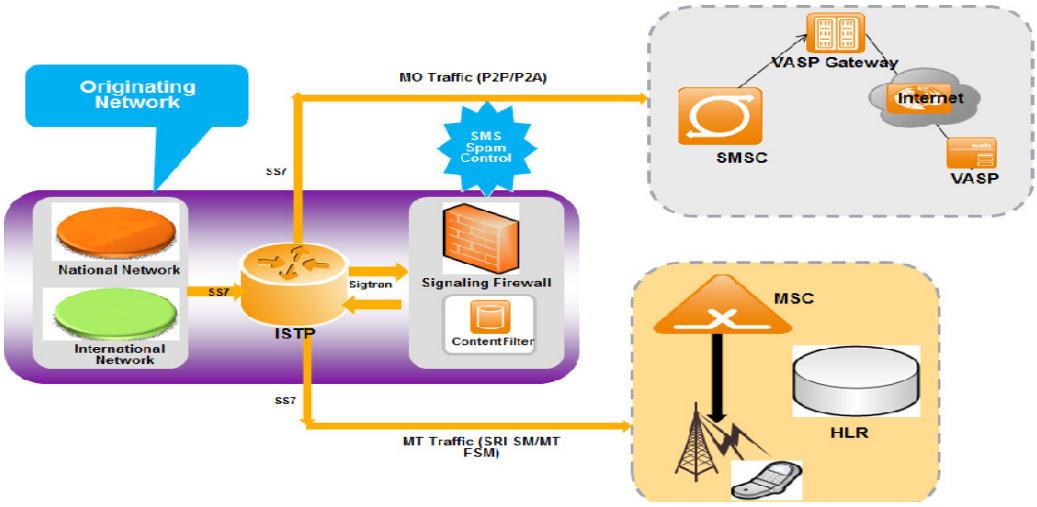
1.2 Current Status

- Compliance to TRAI guidelines. In absence of appropriate filtering capability spam attack from international and national network growing. Especially from alphanumeric CLI and similar signature.
- Most of the mobile service provided does not have infrastructure to control spam as they have passed responsibility to implement TRAI guideline to there ILD service provider with assumption origination of spam is only international network .
- Some ILD CSP has deployed very basic spam control capability.Platform does not support advance signalling level like correlation between SRI and MT FSM parametrs ,Spam via long message etc .Platform does support message level filtering like signature handling, fingerprinting, volume traffic, traffic/message analysis, user traffic analysis, URL categorization etc. Also capability is required these signatures ones detected should be added automatically into permanenet signature database without manual intervention.
- It has been observedglobally services providers are able to control spam attack close to 100% by deploying advance Spam filter platform in there network .These platform primarlyperform filtering at both signalling and message level .

- Service providers doing basic filtering are indentfying alphanumeric CLI(One of the TRAIguideline)based on TON/NPI values which spammer fakes leading uncontrolled spam messages with dummy alphanumeric CLI.Spammer is sending traffic using nonstandard TON/NPIvalues which basic filtering platform is not able to detect and control.
- Platform should have capability to identify alphanumeric CLI by parsing the source CLI character by character. If at any location alphabet or special character comes platform should consider that as alphanumeric CLI.
- Phishing message attacks for example “CONGRAT:YOUR MOBILE NO HAVE WON YOU £500,000 IN ------- MOBILE DRAW UK, TO CLAIM PRIZE SEND BANK DETAIL, NAME, ADDRESS, MOBILE NO, SEX, AGE,TO ----------” **. These phishing attacks is not only coming from International network but coming from national network in a big way.**
- Customer complaints from these phishing attack as subscriber tends to lose money by calling the premium number.
- On National traffic promotional traffic(UCC) traffic was controlled due to capping SMS 200 sms/day/subscriber.Post removal of capping has led to increase in UCC message .This requires CSP to implement infrastructure which has capability of having automatic message level analysis(signature, traffic analysis etc.)on MO leg . Without SMS content analysis its difficult to segregate MO SMS and UCC traffic. This is standard practive globally to control spam traffic getting originated from onnet and ofnet.
- Today all service providers have allowed hundreds of Vas partner pushing millions of VAS messages to customer. In absence of any content , traffic analysis and control capably most of VAS partner are violating by pushing messages out of hours and malicious/phishing content inorder to earn high ARPU.CSP are able to work only on reactive mode.

1.3 What is required.

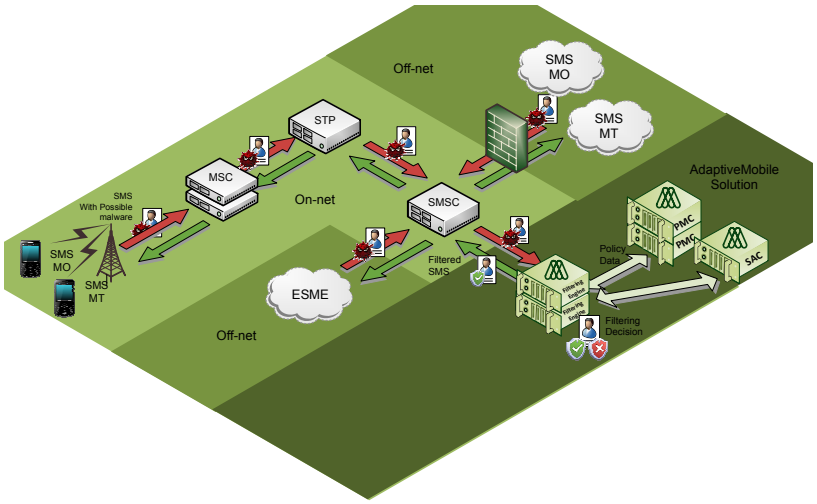
- Comprehensive advance SMS Filter platform having signalling and message level filtering across all interfaces(Onnet,Ofnet,Application originated)
- Platform to be deployed to intercept National/International SMS traffic .Today all CSP network node has capability on identifying/segregate SMS traffic at National/International level. Attach is the proposed architecture.



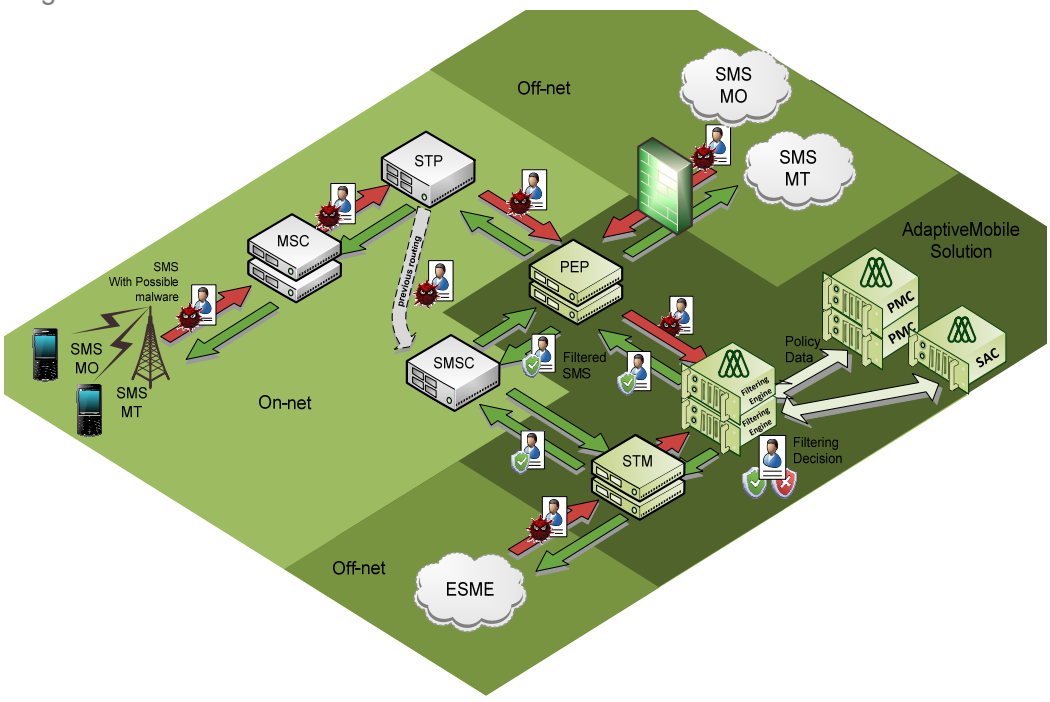
- Platform should do signalling level filtering and control
  - Capability to correlate MAP and SCCP level addressing in SRI/FMS
  - Capability to correlate addressing Between SRI and FSM and also to ensure them below to same message set.
  - Capability to correlated considerable delay between an SRI-SM and the associated MT-FSM,
  - Spoof check on IMSI/Originating SCCP address
  - Capability to correlate IMSI in SRI-SM and MT FSM and take action accordingly.
  - Capability to handle Long message
  - Capability to correlate Copa addresses of TC-Begin and TC-Continue in long message case.
  - Flooding for SRI/FSM.
  - Capability to detect and control fake SC .
  - Capability to handle long message filtering(Concatenated message)
- Platform should message level filtering and control for example
  - Signature handling(Used to match known threats (spam, fraud, virus) Fuzzy matching (token/ normalisation/ similarity)
  - Advance signature database, capability to add new signatures automatically by system.
  - Global signature updates
  - Fingerprinting
  - Network-local fingerprint creation
  - Signature creation
  - Traffic analysis(Sender, Recipient and message level)
  - User traffic analysis
  - Sender and destination traffic volume/type analysis

- Trusted source analysis to avoid binary/text messages like OTA,MCA,VMS,WAP messages pushed across network.Used to match approved content when from specific sources
- **SMS Spam Analysis Engine**
  - Heuristic-based spam scoring
  - Multi-language SMS specific
- Spam/signature database
- URL categorization/filtering
- **Cartridge Update** Automatic signature update
- **Source Usage Controls**
  - Volumetric limits
  - Time of Day/ Week /Date
  - Rate controls
  - Sender/recipient limits
- **Throttling**
  - Control / contain abuse or suspicious senders.
  - Enforcement of volumes/ rate limits
- **Recipient Controls**
  - Time of day
  - Blacklist / whitelist
  - Premium service restrictions
  - "STOP" handling
- **Behavioural Reputation**
  - Behaviour based subscriber attributes
  - Flexible definition of reputation scores
- **VASP Management**
  - Automated restrictions for parental or corporate control
- **Malware Revocation**
  - Real-time blocking of access to known malware domains, or bad signature apps.

- Platform should have capability to integrate with existing messaging nodes to filter mo traffic in the cost effective way . for example platform can integrate with SMSC on diameter or cops interface.



- Platform to be deployed to intercept VAS application (A2P) . In order to ensure message delivery by VAS players is done as per the time window guideline and filter content to avoid malicious/phishing message.
- Platform should support single deployment multiple interface integration like core network for MT national/International, diameter/SMPP/Cops for MO message and SMPP to intercept A2P. Please have a look at below diagram.



1.4 SMS Filter globalReference.

Project Need	OpCo	Network Size (Subs)	Traffic Covered
Content Analysis Spoofing	Bharti Airtel	180 Million	MT (International & National)
Content Analysis Spoofing Personal Blacklist Data Retention	Etisalat	7 Million	MO & MT (National & Intl)
Content Analysis Spoofing Data Retention	ME OpCo	27 Million	MO (National) MT (International)
Content Analysis Spoofing	African OpCo	9 Million	MT (International & National)
Content Analysis Spoofing	African OpCo	31 Million	MT (International & National)
Content Analysis Spoofing	ME OpCo	5 Million	MT (International & National)
Personal Blocklist	ME OpCo	2 Million	MO & MT (National & Internationa
Content Analysis Spoofing Data Retention	APAC OpCo	50 Million	MO, AO & MT (International & Na
Personal Blocklist	US OpCo	2 Million	MO & MT (National & Internationa
Content Analysis	US OpCo	33 Million	MO (National)

1.5 Growing mobile threats in India

- mobile users are being bombarded with massive numbers of spurious international missed calls originating **from Pakistan,Czechoslovakia, Middle East and African countries and also from India routed through international** numbers to defraud users who call back to these numbers. Such short and missed calls - known as 'wangiri' calls - is a larger part of an international syndicate involved in lottery winnings programme scams through mobile and Internet email

- Caller is told to have won a jackpot, lottery or is explained that the caller could be of some help to manage or dispose of a few
Million dollars of cash inherited. The caller is made to understand that he would be well rewarded and is asked to share his bank.
Account, credit or debit card details and other personal information

- Spam attack coming from National and International network without proper filtering capabilities in paced in operator network
  Causing major issue to subscriber.

- Subscriber loosing credit due MO Spoofing attack ,ucc messages getting delivered from national/international traffic primarily from Alphanumeric codes.
- Rogue Apps/Malware/virus leading Huge Data and SMS bills , increasing customer complaints
- Rogue banking application alerts are sending to subscriber leading to bank frauds.
- Bad IP reputation of operator network non delivery of mails, bad internet experience.
- No control on the content pushed by VAS partners
- Major challenge with respect to IUC billing

1.6 Consultation points.

1.6.1 Controlling UCC or anti social message content messagespost via P2P methor post removal of SMS cap on mobile originated traffic .

1.6.1.1 *Problem statement*

Today lot of small and medium size organization are using mobile originated SMS as medium for pushing unwanted , intrusive promotional alerts to subscribers irrespective of DND status and time .Operators has no mechanism in controlling these traffic specialy post removal of SMS cap on mo leg. For example property alerts ,advitisement etc.

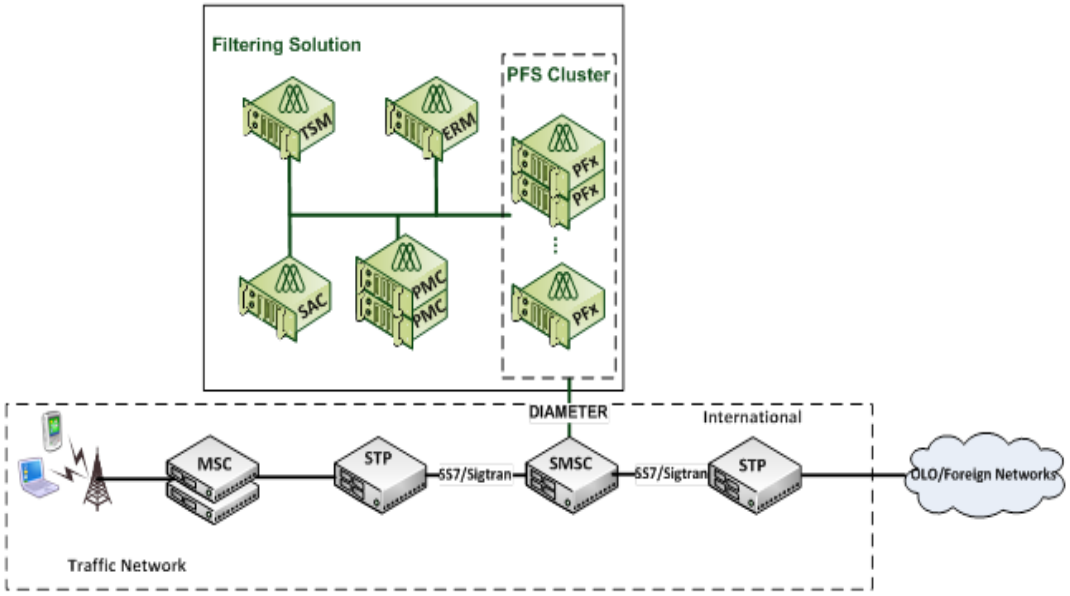
These traffic is primarly pushed via modems which allows multiple SIM cards acting like SIM bank application.

Apart for promotional messages SIM bank application is also used political and anti socialmessages .

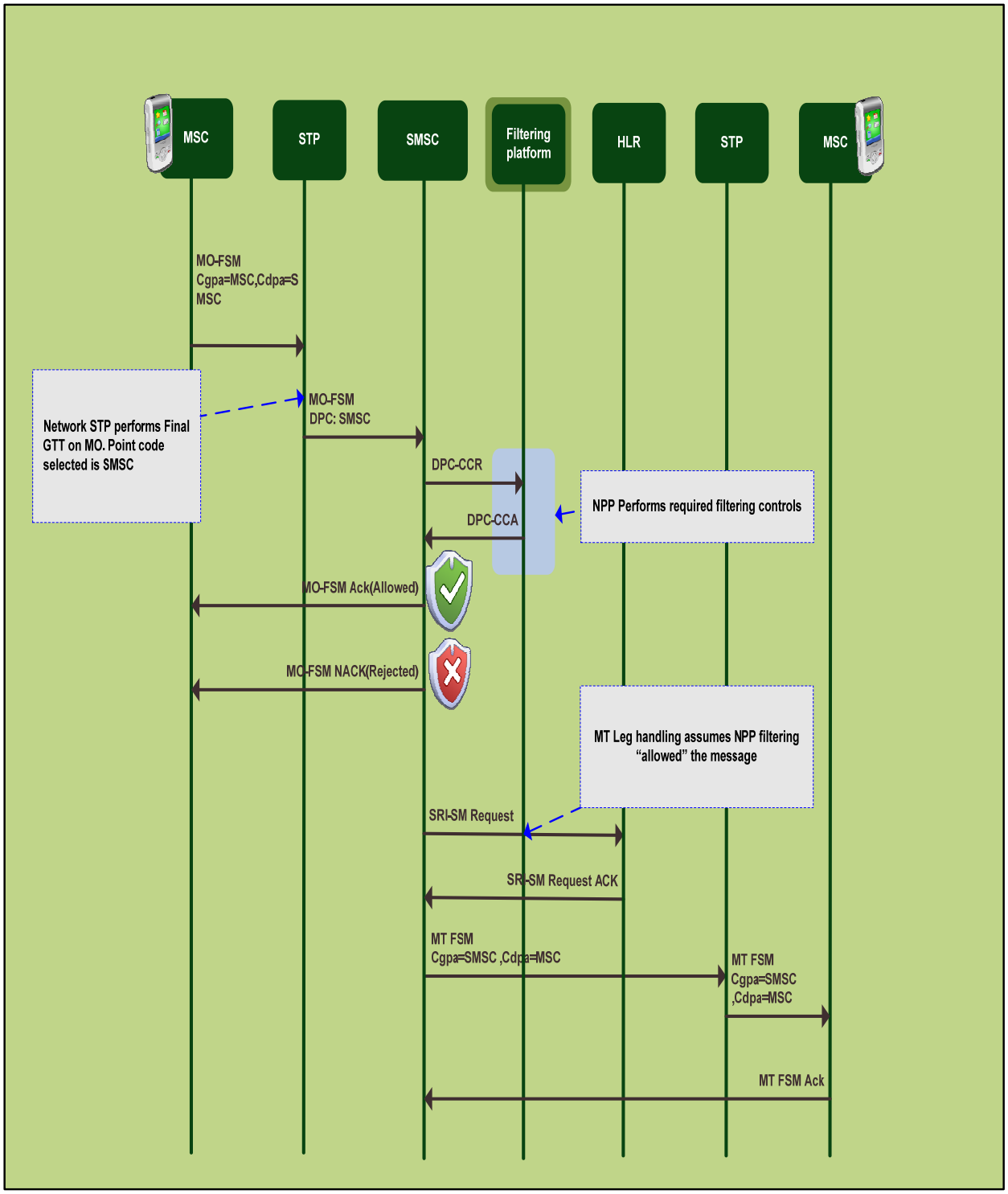
1.6.1.2 *Solution.*

To control UCC traffic via P2P messages it is required mobile network should have infratstructure in placed to do automatic message and traffic level analysis. Platform should be able to identify and block spam traffic automatically before allowing message delivery to B-party. If the message content is identified as spam message should be discarded .

This can be achived by integrating advance message/traffic analysis platform with existing SMSC using Diameter/SMPP/Cops interface.


Filtering Solution
PFS Cluster
TSM
ERM
PFx
PFx
SAC
PMC
PMC
PFx
DIAMETER
International
MSC
STP
SS7/Sigtran
SMSC
SS7/Sigtran
STP
OLO/Foreign Networks
Traffic Network

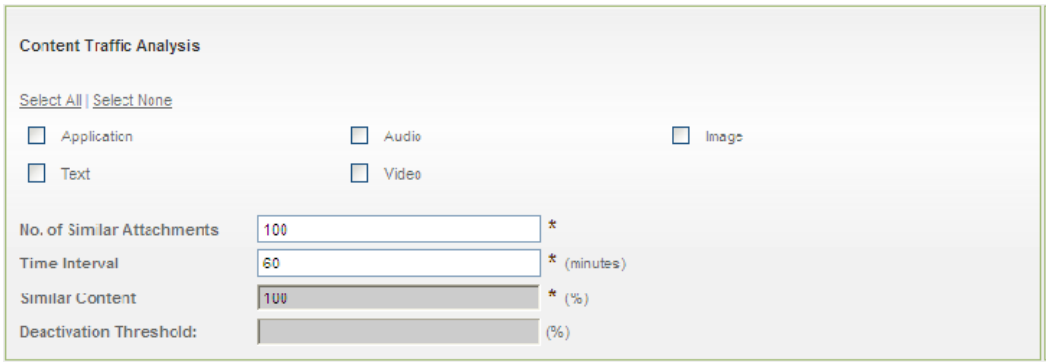
Call flow .


MSC
STP
SMSC
Filtering platform
HLR
STP
MSC
MO-FSM Cgpa=MSC,Cdpa=SMSC
Network STP performs Final GTT on MO. Point code selected is SMSC
MO-FSM DPC: SMSC
DPC-CCR
NPP Performs required filtering controls
DPC-CCA
MO-FSM Ack(Allowed)
MO-FSM NACK(Rejected)
MT Leg handling assumes NPP filtering "allowed" the message
SRI-SM Request
SRI-SM Request ACK
MT FSM Cgpa=SMSC ,Cdpa=MSC
MT FSM Cgpa=SMSC ,Cdpa=MSC
MT FSM Ack

1.6.1.3 *Filtering capability.*

Following are the adavance and multiple level filtering required to identify and control UCC/Anti social messages coming vial P2P messages. These advance filtering capability not only identify spam message but also help in blocking them permanently .

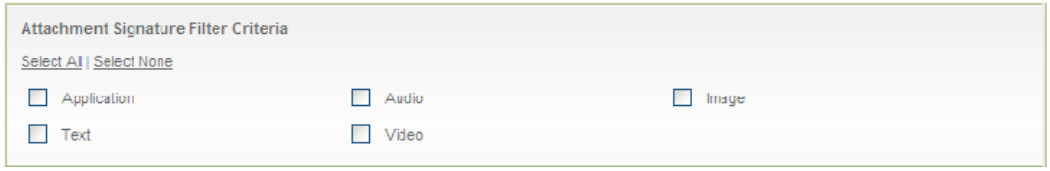
1. **Content traffic analysis :-**Capability to automatically detect SMS messages/signature that are considered to be variant of the same message.Comparison is based on the features of a message. Features are n-grams created from the normalised and tokenised message. The signature is the feature set of the message.
   This enhance capability detects spam variants that might advertise in the same essential content but with variations in message spelling, vocabulary, abbreviation, character aliasing, and so on. It works by identifying a threshold number of similar message attachments occurring within a defined timeframe. Ones platform detects spam message using this filter it would do following actions.
   - Block
   - Raise SNMP trap
   - Send Email to Admin with SMS attachment for analysis
   - Add signature to database for permanent blocking of the message



2. **Signature filtering.**

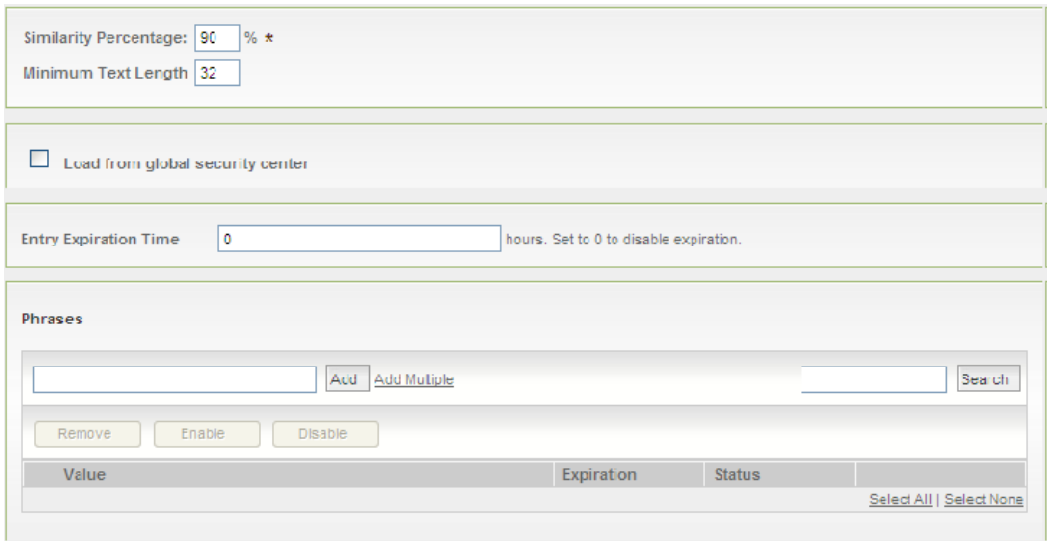
Platform supporys in built signature database. This database is automatically updated ones platform indentifies new spam message.Platform also supports manualy add signature which are know to be of spam.

Platform blocks known SMS threats based on signature or call for action to add particular spam in to signature database for permanent blocking. Analyses text, audio, video, application, and image attachments, and compares them to a database of restricted signatures. The Signature Manager enables the creation of signatures from greylisted or retained attachments. It also allows attachments to be reviewed and possibly added to a blacklist or white list.

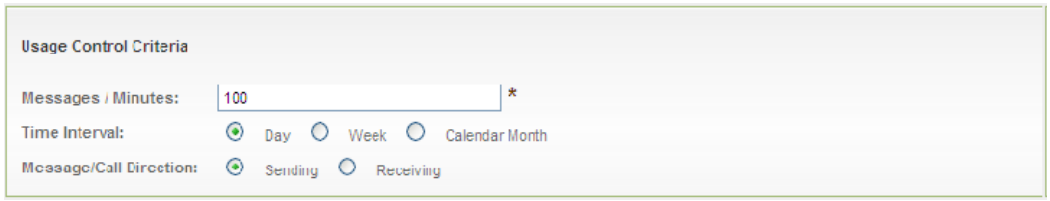


3. **SMS Fingerprint.**

Used to match known threats(Spam,fraud,virus) Blocks or allows messages with words or phrases that have a configurable percentage similarity to a predefined list of phrases.
Detects patterns in the SMS text payload. The pattern recognition provides a percentage match. The pattern recognition identifies percentage matches based on similar text attributes in a list of predefined phrases can also specify the minimum required length of any message for which text patterns should be checked
The Fingerprinting filter uses a list of predefined phrases for the purposes of determining any text pattern matches. These phrases can be either specified within the filter itself or downloaded from the global security center

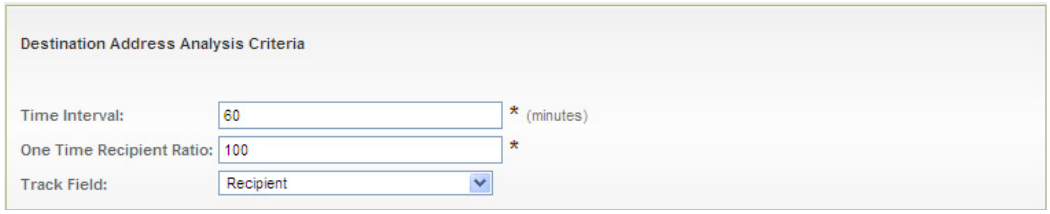


4. **Usage Control**
   A Usage Control filter restricts the number of messages that a subscriber may send or receive, on a daily, weekly, or monthly basis.

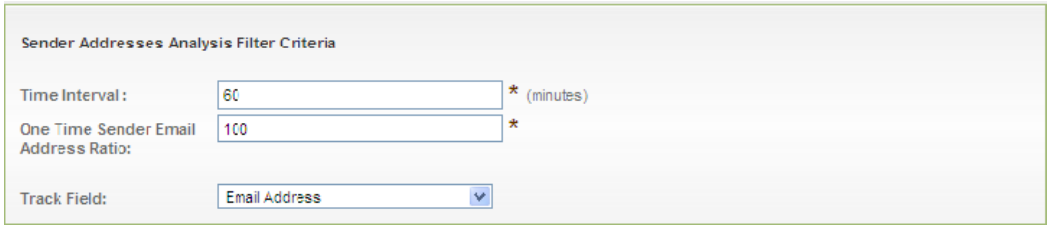


5. **Destination Address Analysis**

   Analyse the recipient list patterns of a message sender during a configurable period. This type of filtering occurs at the message stage. If the ratio of one-time recipients compared to the total number of recipients exceeds a configurable threshold, the message can be optionally blocked. (A one-time recipient is a recipient to whom only one message is sent by the sender during the configurable time period.) This filter is used to detect spamming behaviour where senders send messages to an auto-generated list of recipients



6. **Sender Address Analysis**
   A Sender Addresses Analysis filter analyses the sender address patterns of a message sender during a configurable period. If the ratio of one-time sender addresses used compared to the total number of messages sent exceeds a configurable threshold



7. **Differential Sending rate traffic Analysis.**
   A Differential Sending Rate Traffic Analysis filter analyses and detects changes or surges in sending rate where the sender is a MSISDN, SMSC (for SMS-MT and SMS-SRI messages), or MSC (for SMS-MO messages). Platform allows to configure the action that will be taken when a MSISDN, SMSC, or MSC triggers this threshold. choose any combination of the following filter actions:

Block—Prevent the entire offending message from being sent.

Raise SNMP Trap—Provide details of the threshold exceeded (image, audio, application, video or text) via the amsThresholdExceeded alarm.

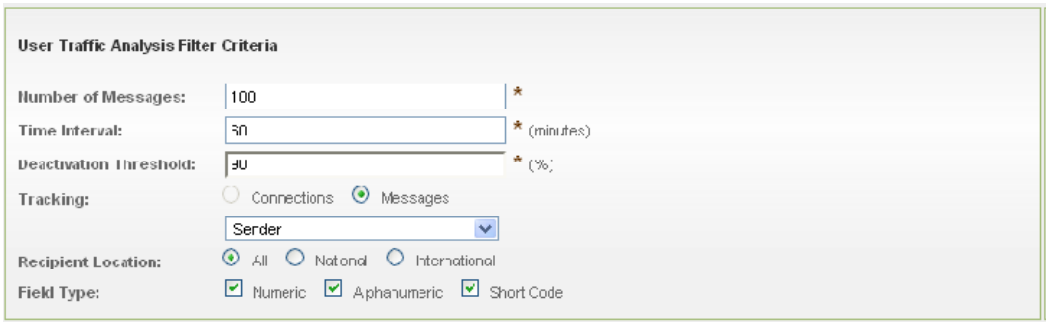
Send Email to Admin—Send an e-mail to a preconfigured administration e-mail address. This e-mail contains the attachment that triggered the threshold as well as details of the threshold crossed. See the Filtering Engine Installation and User Guide for more information on how to configure this e-mail address.

Send SMS to User—Send a preconfigured text message to the user to inform them that they have exceeded the permitted message threshold.

Add User to Greylist—Add the user to the Grey List for further consideration and adjudication.

8. **User traffic Analysis**

   Analyse the send and receive patterns of a particular user to see if these suggest spamming behaviour. This type of filtering occurs at the message stage. It works by monitoring the number of messages sent or received by a single user during a configurable period. You can choose to analyse patterns for subscriber MSISDNs, alphanumeric identifiers, short codes, or any combination of these



   Following action can be done as out of the filter getting tripped.

   Block.

   Raise SNMP Trap

   Send Email to Admin

   Send SMS to User

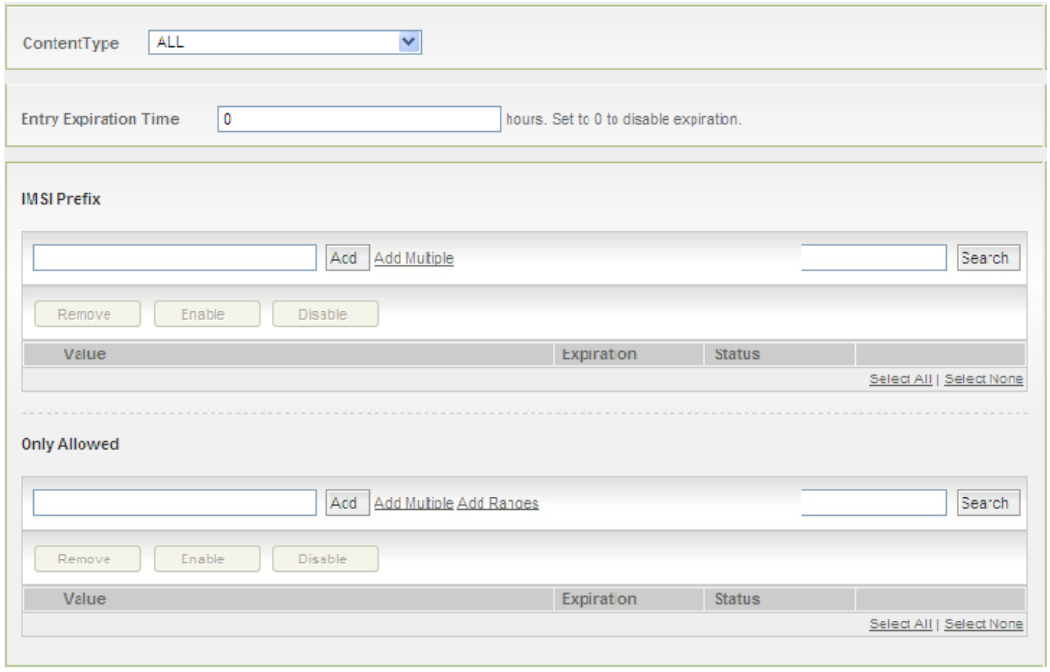
   Add User to Greylist

9. **Content Matching**

   Content Matching filter analyses text in a message and compares it to a configurable dictionary of banned words. Plarform supports dictionary

management capability where allow an operator to specify a list of restricted words or characters. When a message is received, the Content Matching filter can either replace offending text with asterisks, simply log the message details, or both.Platform supports multiple dictionary configuration and each filter can be mapped to separate dictionary .

10. **Content Type Trusted source.**
    A Content Type Trusted Source filter can block various types of SMS message content by preventing off-net messages that contain that type of content. These messages destined for home network subscribers are only accepted if they originate from specific global title addresses, but not if they originate off-net



type of content following options are available.

OTA (over-the-air)

– Text
– Binary
– MWI (message waiting indicator)
– V-Card
– V Calendar
– EMS (enhanced messaging service)
– WAP (wireless application protocol)
– Nokia Smart Message
– Sim Tool Kit Header
– Unknown

11. ***Message Content Trusted Source Filter***
    A Message Content Trusted Source filter blocks fake voicemail alert SMS messages. This protects on-network subscribers from calling premium numbers in the message, which have been substituted for the voicemail number. This filter applies to SMS messages that have a home network destination IMSI

12. ***Data Retention.***
    Is a feature that provides the ability to record and store all communications for a defined period of time (typically for legal purposes). The data stored can be used to identify the source, destination, time, duration and content etc of each communication. Data retention can be in the form of call detail records (CDRs), message data , complaintsetc

13. ***Quarantine.***
    Is an feature that stores messages that have been identified as potentially threatening. The administrator can examine each quarantined message and to forward it to the intended recipient if it is deemed safe

1.6.2 Registering UCC complaint for easy and effective lodging of complaints

- **Problem**:-In the current scenario process of registering unsolicited commercial communication complaint requires sending SMS to 1909 , with manual typing complex format in sms body .Complaint redressal through sms to 1909 is not consumer friendly . Apart from complex format it does provide key information like source network also in most of the case subscriber is not able to provide complete information.

  Solution:-SpamGuard enables mobile users to automatically report and block SMS spam from their phone with ‘one-click’. SpamGuard is

the only SMS spam solution that is built from the handset up into the network and actively involves the subscriber in the reporting and blocking of spam.

A simple and easy to use ‘one-click’ SMS spam reporting app The ability to provide direct feedback to the network operator

MKT4295-03 -
SpamGuard Product D