# AI & Machine Learning thwarts threat to enterprise messaging ecosystems

Deshbandhu Bansal, chief operating officer, Messaging Solutions at Comviva Technologies looks at the importance of controlling messaging

Enterprise loves messaging; it allows them to engage their customers in the most cost effective manner, moreover, in today's highly competitive markets messaging provide businesses with a channel to drive customer life-time value with highly interactive and engaging communications, designed to cater to each individual's unique persona and requirements.

Similarly, the growth of messaging has allowed operators to create new sources of revenue besides rising up the value chain in the messaging economy. Since the messaging opportunity is so critical for operators, as well as the enterprise segment, there is a growing interest in AI & Machine Learning to ensure the continued growth and health of the overall messaging ecosystem.

## RISING DEMAND FOR ENTERPRISE MESSAGING

One of the biggest factors for messaging popularity is the increasing penetration of

> "Grey Route compromises the ability of the operator to monetise the messaging opportunity leading to operator losses running into billions."
>
> **Deshbandhu Bansal**, Chief Operating Officer, Messaging Solutions at Comviva Technologies.

Deshbandhu Bansal - chief operating officer, Messaging Solutions at Comviva Technologies.

**For more stories, check out commsmea.com. Follow CommsMEA on Twitter: @COMMSMEA**

mobile. According to GSMA Intelligence, today there are more than 8.97 billion mobile connections, surpassing the world population by more than a billion. Similarly, there are 2.71 billion smart-phone users today, constituting almost 35 per cent of the global population.

Secondly, SMS has made B2C communications easier. Businesses can reach out to anybody with a mobile phone with short messaging services. SMS is also a high ROI messaging channel, where SMS open rates are measured in seconds. Studies have shown that four out of five customers will read an SMS within 30 seconds, which is a higher rate than any other medium. Now, if we compared this number to email open rates, it will become easy to understand why SMS has become so critical for enterprise communications today.

Thirdly, the growth of analytics, combined with the customer's willingness to share their data if it leads to better service, have made it easier for enterprises to understand the impact and ROI of each messaging platform, and fine-tune it to different customer personas and requirements.

## OPERATOR OPPORTUNITY

With operator's voice and SMS business declining rapidly, there is a growing need for operators to generate fresh revenue streams. In this context, A2P is critical for operators, as it guarantees consistent revenues for them in the near future, especially with the app ecosystem growing by leaps and bounds. However, in order to fully monetise the A2P opportunity, the operator will have first have to tackle the problem of Grey Routes.

In order to understand the Grey Route problem, we will have to distinguish between a P2P message, which is the transfer of SMS messages between two individuals, and A2P message, which is the transfer of SMS between and application and an individual. The problem arises when the A2P message is masked as a P2P message, with the objective of saving A2P termination charges, or if the message sender wants to

hide his identity for the purpose of spamming.There are several ways to mask an A2P message, such as GT spoofing, SIM farms. In GT faking: the message's global title is altered, hiding its identity. In SIM farms, hoards of SIMS are collected and used for sending out A2P messages in the guise of P2P messages.

When enterprises or aggregators try to send commercial messages via illegitimate or zero rated routes, it is known as grey routes. Grey Route compromises the ability of the operator to monetise the messaging opportunity leading to operator losses running into billions.

Besides revenues losses, Grey Routes have an impact on the operator's ability to drive quality traffic on its networks. Also, without the means to distinguish between good and bad traffic, the operator is unable to prioritise message delivery. The resulting traffic congestion, may eventually lead to slower message delivery in critical industries such as banking, where a customer wants to be notified immediately for every withdrawal, for example, at the ATM. In the event of this happening, it is the enterprise that has to bear the brunt of the irate customer. Similarly, if the sender is using the system for spamming, it puts the operator's credibility under the sword.

## THE WAY FORWARD

Traditionally, operators have been using rules based SMS firewalls for safeguarding the network from misuse. Rules based firewalls use a combination of blacklisted numbers, key word search, URL destinations for categorising messages. However, sophisticated scammers are easily able to overcome traditional detection and prevention techniques based on deterministic rules, limited pattern search and blacklists. Another problem with these deterministic platforms is that they are not 100 per cent accurate, which means that legal traffic may also be blocked if they meet the criteria set by the platform. On the customer experience front, it may lead to poor experience, as they miss out on promotions. Therefore, in the interest of the overall messaging ecosystem, it is time to take a more nuanced approach to the problem.

In this context, AI capabilities take a more comprehensive view. Using new advances in the field of natural language processing, the AI-based SMS firewall auto classifies a message into different categories. Unlike conventional platforms which provide limited pattern search, AI platform leverages the past training with millions of similar messages and it analyses words using pattern matching techniques and the context in which the words are used to predict the category to which a given message belongs. Once the messages are categorised, the operator can enforce policy control on a much granular level, which will help to protect the subscribers from spam and fraud, arrest revenue leakages and reduce operational effort for the operators ensuring low subscriber churn from their network.