Draft Recommendation ITU-T X.ticvs

Technologies involved in countering voice spam in telecommunication organizations

Summary

Voice communication is a fundamental service provided by telecommunication networks. With the development of voice communication, voice spam has also been increasing with numerous negative effects on end users and network operators. In general, voice spam has content ranging from commercial advertisement to offensive pornographic material, which has various kinds of negative effects on end users and network operators. Voice spam may allure, annoy, bully or even intimidate users as well as network resources. To avoid these negative influences, and to protect user's rights and maintain network stability, network operators may wish to increase their efforts to counter voice spam.

The objective of Recommendation ITU-T X.ticvs is to review technical solutions to counter voice spam. This Recommendation gives an overview of voice spam, and summarizes the existing anti-spam technologies which are used by users and telecommunication networks alike, and the collaboration mechanism between them. Additional proposed technical solutions are also recommended based on the technologies and this collaboration mechanism.

Keywords

Spam, voice spam

Attention: This is not a publication made available to the public, but **an internal ITU-T Document** intended only for use by the Member States of ITU, by ITU-T Sector Members and Associates, and their respective staff and collaborators in their ITU related work. It shall not be made available to, and used by, any other persons or entities without the prior written consent of ITU-T.

Contents

1. Scope 3

2. References 3

3. Definitions 3

3.1 Terms defined elsewhere 3

3.2 Terms defined in this Recommendation 4

4. Abbreviations and Acronyms 4

5. Conventions 5

6. Overview of voice spam 5

6.1 Voice communication scenarios 5

6.2 Characteristics of voice spam 6

7. Technologies for countering voice spam 7

7.1 General aspects 7

7.2 Network-side technologies 7

7.2.1 Signalling record 8

7.2.2 Analysis 10

7.2.3 Interactive verification 11

7.2.4 Controlling 12

7.3 User-side technologies 13

7.3.1 Whitelists/blacklists 13

7.3.2 Call-delay 13

7.3.3 Feedback 13

7.4 Collaboration mechanism 13

7.5 Proposed solutions 14

Appendix I Comprehensive measures on countering voice spam 15

Appendix II A suggestive solution for interactive verification 17

Appendix III Policy considerations in countering voice spam 18

III.1 Users 18

III.2 Operators 18

III.3 management entities and third party organizations 18

Recommendation ITU-T X.ticvs

Technologies involved in countering voice spam in telecommunication organizations

1. Scope

This Recommendation gives an overview of voice spam and reviews existing technologies used to assist countering voice spam, including network-side and user-side technologies and the collaboration mechanism between them. In addition, this Recommendation also proposes additional practical anti-spam solutions, such as signalling records, interactive verification, controlling measures, etc.

This Recommendation focuses only on countering voice spam that has originated from the circuited-switched area in telecommunication networks. The technologies for countering voice spam originating from the IP-based area should be referred to ITU-T X.1244 and ITU-T X.1245.

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1240] Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail spam.*

[ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications.*

3. Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **Circuit-Switched Network** [b-Y.1001 (2000)]: A network which provides connections for the exclusive use of the users for the duration of a call or service by interconnecting transmission channels or telecommunication circuits.

3.1.2 **IP-Based Network** [b-E.370 (2001)]: A network in which the Internet Protocol is used as the ISO layer 3 protocol (OSI Reference Model).

3.1.3 **Operator** [b-ITU-T M.1400]: An organization responsible for identification and management of telecommunication resources. An operator must be legally recognized by the telecommunication administration of the country, or delegation thereof. An operator may or may not correspond to a trading partner.

3.1.4 **Spammer** [b-ITU-T X.1231]: the entity or the person creating and sending spam.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **Voice spam:** unsolicited, automatically dialled, pre-recorded phone calls, usually with the objective of marketing commercial products or services. The content of voice spam ranges from advertisement of goods to offensive pornographic materials. Voice spam has several various kinds of harmful effects onto users and operators.

3.2.2 **Honeypot:** A software program (maybe in a terminal) that emulates a terminal or a group of terminals so as to detect suspicious voice spammers and even assist verifying them. The output of these systems can be used to evidence gathering.

3.2.3 **Management entity**: an entity which may have one or more responsibilities for governing, auditing or guiding the work of countering voice spam.

3.2.4 **Third party organization**: an entity which can consult, assist or coordinate the work of countering voice spam.

4. Abbreviations and Acronyms

This Recommendation uses the following abbreviations and acronyms:

CAMEL	Customized Applications for Mobile Enhanced Logic
CCLTP	Call CLear Time Point
CCOTP	Call COntinued Time Point
CDMA	Code Division Multiple Access
COSN	Call Originated Subscriber Number
COTP	Call Originating Time Point
CRBT	Colour Ring Back Tone
CS	Circuit -Switched
CTSN	Call Terminated Subscriber Number
DMP	Device Management Platform
GMSC	Gateway Mobile Switching Centre
GSM	Global System for Mobile Communications
HLR	Home Location Register
ID	IDentification
ISIS	Information Sharing System
IMS	IP Multimedia Subsystem
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
IP	Internet Protocol
IVR	Interactive Voice Response
MSC	Mobile Switching Centre
OTAP	Over- the- Air Platform

PSTN	Public -Switched Telephone Network
SCP	Service Control Point
SIM	Subscriber Identity Module
SLETP	Signalling Link Establishment Time Point
SLRTP	Signalling Link Release Time Point
SS7	Signalling System No.7
STP	Signalling Transfer Point
UMTS	Universal Mobile Telecommunications System
VLR	Visitoring Location Register
VMS	Voice Mail Server
VoIP	Voice over Internet Protocol

5. Conventions

None

6. Overview of voice spam

Voice spam is unsolicited, automatically dialled, pre-recorded phone calls, usually with the objective of marketing commercial products or services. The content of voice spam ranges from advertisement of goods to offensive pornographic materials. Voice spam may have several harmful effects on users and operators.

6.1 Voice communication scenarios

Voice communication is a fundamental service provided by telecommunication operators. Originally, voice communication was based on the traditional circuit-switched (CS) networks. With the development of Internet, it has expanded to include voice over Internet protocol (VoIP) across Internet protocol (IP)-based networks.

Four voice communication scenarios are considered below, determined by the technologies used (in Figure 1):

- Scenario 1: CS-CS: Traditional mobile /fixed circuit-switched voice communications
- Scenario 2: CS-IP: Voice communication originated from mobile /fixed circuit-switched user and terminated at an IP telephony user
- Scenario 3: IP-CS: Voice communication originated from an IP telephony user and terminated at a mobile /fixed circuit-switched user
- Scenario 4: IP-IP: Voice communication between IP telephony users

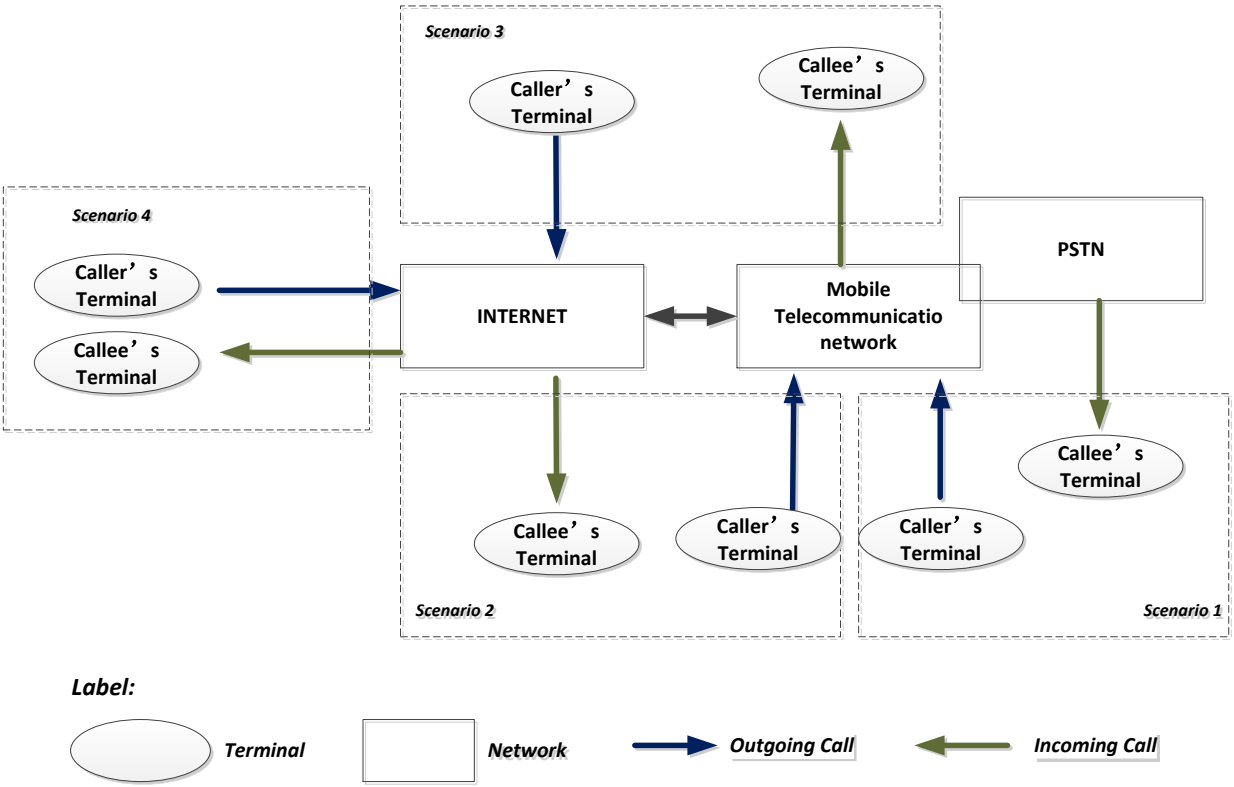

Figure 1 - Voice communications in telecommunication networks

NOTE – Terminal here in Figure 1 may include mobile phone, fixed phone, laptop, personal computer and so on, which can access circuit-switched /IP-based networks.In general terms, most users do trust the source of voice telecommunication. Consequently, voice spammers are willing to use traditional circuit-switched voice communication to initiate voice spam. In addition, technologies on countering voice spam in scenario 3 and scenario 4 are recommended in [ITU-T X.1244]. Therefore, this Recommendation only focuses on countering voice spam in scenario 1 and scenario 2.

6.2 Characteristics of voice spam

Voice spam may spread content ranging from commercial advertisement to offensive pornographic materials, which may cause harmful effects on users and network operators:

- Voice spam may include tiresome, deceptive, bullying or threatening contents
- Users and operators may suffer from wasting resources
- Users and operators may need to spend time, money and effort on countering voice spam.

The most widely recognized forms of voice spam are classified but not limited into two types:

- **Type One (silent call)**: A silent call is a telephone call with the intends of telemarketing, that is generated by a predictive dialer (or dialers) with no intent of an agent immediately handling the call.. In this instance the call may be terminated by the dialer, and the called party receives a silence ("dead air") or a tone from the telephone company which indicates the call has been dropped. The term “abandoned call” has the same meaning. Usually, this kind of call will expect a call-back.
- **Type Two (harassing call)**: A telephone call with the intends of telemarketing, which may also harass, annoy, alarm, or intimidate with the content of porn, threat, illegal

information, sham advertisement and so on. Usually, this kind of call will not be dropped until put through.

7. Technologies for countering voice spam

7.1 General aspects

None of the solutions can be entirely successful independently. In order to mitigate the negative influence from voice spam, it is necessary to implement a comprehensive range of solutions with correlative technologies, which are categorized into network-side technologies and user-side technologies to cover scenario 1 and scenario 2 described in clause 6.1.

Network-side technologies are key for operators, i.e., in public switched telephone networks (PSTNs), universal mobile telecommunications systems (UMTSs), global system for mobile communications (GSMs) and code division multiple access (CDMA) networks. Compared to the network-side technologies, user-side technologies are much more flexible and dependent on user initiatives. Feedback from users is a necessary supplement to the network-side technologies. Therefore, an effective collaboration mechanism between the two technologies should be also established.

7.2 Network-side technologies

Every phone call initiates in the access network by signalling. In order to detect the suspicious voice spammer, the basic method is to collect signalling data, analyze it and verify it. This method should be considered comprehensively. Generally speaking, a call set-up phase involves a handshake between two ends of a communication. During the call setup phase, the only identification of the caller/called party is caller identification (ID). This leads to the following observation.

1) Any call handling decisions should be made in real-time before call setup completion.

Voice spam presents complex technological challenges, and therefore solutions to eliminate it need to be supported by appropriate procedures coupled with technological measures. A fundamental network-side procedure for countering voice spam might include the following processes given in **Figure 2**:

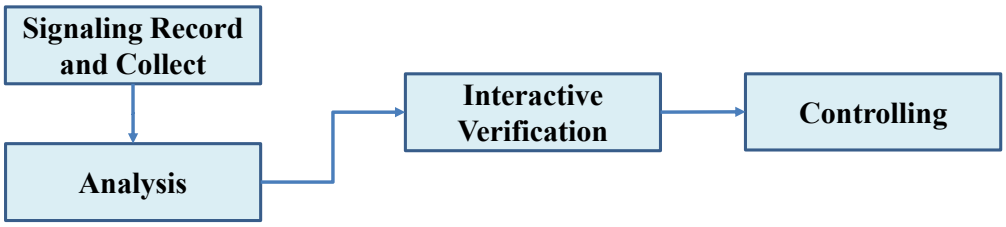

Figure 2 - Network-side procedure of countering voice spam

- **Signalling Record and Collect**: To record and collect the original signaling data in real-time.
    - **Analysis:** To identity suspicious voice spammers and list their numbers.
- **Interactive Verification**: To obtain direct verification to find out the real voice spammers in the suspicious list.
- **Controlling**: To restrict or disable voice spammers which have been confirmed by the verification process in order to protect normal users.

The user-side procedure has almost the same processes but with simpler measures in each part. In some cases, interactive verification can be neglected.

According to the procedure, there are several technologies to deal with each part respectively. It should be noted that none of the technologies discussed in the following clauses will act as a "silver-bullet" or be the sole solution to the voice spam problems. On the contrary, all of the technologies are complementary and will be more effective when grouped together.

This Recommendation will introduce and classify technologies by their deployment positions, that is, network-side and user-side technologies and by the processes (mentioned in Figure 2).

7.2.1 Signalling record

Signalling record is to collect call detail record data in a (quasi) real-time way for analysis, which can include time-related or phone number related data, such as:

- Call originating time point (COTP): time point of caller generates a phone call
- Signalling link establishment time point (SLETP): time point of signalling link establishment between caller and callee
- Call continued time point (CCOTP): time point of phone call continued and put through by callee
- Call clear time point (CCLTP): time point of call cleared by caller or callee
- Signalling link release time point (SLRTP): time point of signalling link released after call clear
- Call originated subscriber number (COSN): normally known as Caller Number, the number of call originated by caller
- Call terminated subscriber number (CTSN): normally known as Callee Number, the number of call terminated by callee

The value of the same data, especially time-related data, may slightly differ by the positions of the collecting points.. However, the nuance mentioned above can always be ignored in practice.

NOTE – Only popular data sources (based on signalling system No. 7 (SS7), intelligent network (IN), IP multimedia subsystem (IMS), colour ring back tone (CRBT), voice mail server (VMS), etc.) will be listed below, though there are other alternative data sources, such as R2, and missed call alert systems.

7.2.1.1 SS7 signalling

NOTE – The signalling collection point is a logical net element, which can be formed from different kinds of entity elements.

SS7 signalling can be a useful source to assist in monitoring voice spam. It is practical to insert a signalling collection point to duplicate signalling information and parameters, and record them. The signalling collection point is connected in parallel with the signalling link, so the signal is effectively "beam split", although only a small part of signal power will be consumed by the collecting point. In this situation, the failure of the signalling point shall not have any negative effects on the signalling link.

There is also another method to collect SS7 signalling by inserting a hidden signalling node between two explicit signalling nodes. This means, that the hidden signalling node will first "block" the signal in order to record it and then relay the signal without any change but with the nuance on latency. However, the technology has the risk of a single point of failure. Therefore, a reliable failure and backup capacity is required.

The great advantage of using SS7 signalling records is that they contain the detailed call data from which various indicators can be deduced (see clause 7.2.2). However, if the voice call traffic increases and the network expands, the number of signalling collection points shall increase synchronously to cover all/major signalling sources in order to keep an acceptable range of monitoring, which may lead to a higher cost of countering spam.

It is recommended to deploy the signalling collection points in a core /local networks. To achieve an overall collection, these points shall cover all the Mc and Nc interfaces of switchers. Furthermore, to achieve a balanced collection, these points shall just cover all the NC interfaces. If the focus is only on national long-distance calls or international calls, long-distance /international Signalling Transfer Points (STPs) shall be covered.

7.2.1.2 Intelligent network (IN)

A method based on service control point (SCP) is to collect the customized application for mobile enhanced logic (CAMEL) or intelligent network application protocol (INAP) signalling for analysis. SCP is a key node in IN and determinant factor to decide how to process phone calls.

Once, a user is contracted for the IN service, the outgoing call will trigger SCP to inquire about the called user's visiting location register (VLR) information before setting up communication links. As IN services are popular with some operators, it is easy to collect and record the signalling data of the call generated from IN-contracted users.

As the signalling collection points can be at/around SCP, the method needs less signalling collection points compared to that of SS7. Whether these IN-contracted users are roaming or not, they can be monitored easily by this method.

There is a limitation to this method. If penetration of the IN service stays at a low level, only small part of the users' behaviours will be monitored. However, this situation can be solved by helping each user to subscribe implicitly to a customized IN service, which will forward the inquiry request unconditionally to SCP when an outgoing call is generated.

This method is restricted by the common IN service process; therefore, only limited data could be collected, such as COTP, SLETP, COSN and CTSN (see clause 7.2.1). Nevertheless there is space for improvement if a more complex IN service process is introduced, for example, if all the signalling signals of telephony are relayed by SCP.

The method of IP Multimedia Subsystem (IMS) can be similar to the above discussion, as IMS shares similar signalling procedures with IN.

7.2.1.3 Colour Ring Back Tone (CRBT)

CRBT is a specific user-oriented service provided by some operators. Once a user contracts the CRBT service, other users will hear pre-ordered music clips instead of the ringing tone. As a result, the signalling record and collect data can be achieved in the CRBT hosts.

This method is restricted by the service process; therefore, only limited types of data can be collected in the service hosts, such as COTP, CCOTP, CCLTP, COSN and CTSN (see clause 7.2.1) and there is almost no more improvement of CRBT process to collect more types of data.

Only if a voice spammer bothers a CRBT user, the spammer could be monitored, and therefore a high service penetration is a pre-condition to make the method practical. If the situation is satisfied, the investment in the signaling record and collections should be comparatively low.

7.2.1.4 Voice Mail Servers (VMS)

VMS handles calls in situations of call forwarding no reply, call forwarding busy, call forwarding unconditional, etc. In most cases, VMS is irresponsive to a silent call unless the criterion is

unconditional. While it may provide voice recordings of a calling party if a spam caller intends to get the call connected and spam a callee directly, then it may support the interactive verification process powerfully by the voice recordings from user feedback or authorization (see clause 7.3.3).

Similar to CRBT, service penetration and usage of VMS is a pre-condition to make the method practical.

7.2.1.5 Honeypot

The honeypot method is used for setting up a quantity of successive or random phone numbers to attract voice spammers. Besides data collecting, the honeypot method can also facilitate the analysis procedure as well as the interactive verification procedure.

Since the honeypot method can be put through by any caller (outgoing call), it can collect some particular types of data, such as COTP, CCOTP, CCLTP, COSN and CTSN (see clause 7.2.1). The honeypot will calculate and transfer the data for some analytical measures which are described in clause 7.2.2.

7.2.2 Analysis

In order to make an analysis of countering voice spam by using the monitoring system, the collected original data needs to be calculated and transformed into some meaningful indicators such as the connection rate, the call released time, the ringing duration, etc. In order to differentiate voice spammers from normal users, the indicators should be counted continuously for a specific period, normally known as the time window (duration). Operators may adjust the duration to an appropriate value based on the maintenance experience.

All the indicators can be deduced logically into a more comprehensive indicator called “the rule”, which can be used in some algorithm to analyze the voice spammer’s behaviour with higher accuracy. The rule model for judging the voice spammer is shown in **Error! Reference source not found.**.

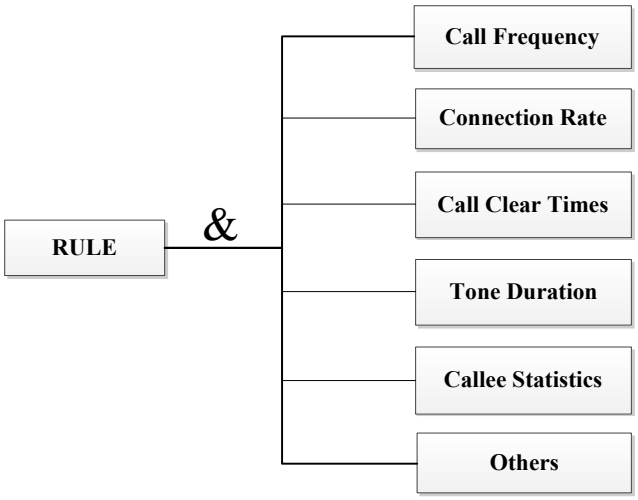

Figure 3 – Rule model

The rule model is deduced from several indicators by the logical AND operation. Since data sources are from different sources and may be collected together, not all the indicators can be supported at the same time. A feasible solution to the problem would be to set the unsupported indicators to “TRUE” or “1” to ignore them. For example, after collecting data and transforming them into

indicators, the honeypot just needs the indicator of the tone duration to process the required analysis procedure and to set the other indicators' value to "TRUE" or "1" to omit them.

Indicators and its definition contained in the Rule Model are listed below:

- Call frequency: Number of calls in a particular period
- Connection Rate: Rate of the call communication or the signalling link establishment
- Call clear times: Number of times when the caller or callee releases the call on their own initiative
- Tone duration: Time duration of the ringing tone
- Callee statistics: Statistics on the callee characteristics, such as uniform distribution, arithmetic progression, etc.

The threshold value of indicators should be adjusted by the operators based on the realistic service scenarios to balance the accuracy and cost. Furthermore, the concrete rules should be defined to match the different types of voice spam.

For example, there are two types of widely recognized voice spam: they are silent calls and harassing calls. A silent call (also called an abandoned call) is a telephone call initiated by a dialler who does not have an agent immediately available to handle the call. In this instance, the call may be terminated by the dialler, and the called party receives a silence ("dead air") or a tone from the telephone company which indicates that the call has been dropped. Usually, this kind of call will expect a call-back. A harassing call is a telephone call that intends to harass, annoy, alarm, bully or intimidate with the content of porn, threats, illegal information, and sham advertisement, etc. Normally, these calls will not be dropped until put through.

Silent calls and harassing calls (see clause 6.2) can show different indicator features respectively in term of the proposed rule model. A higher value of call frequency or call clear times and a lower value of connection rate or ringing duration could sound more suspicious to be a silent call spammer. On the other hand, a harassing call may focus on a specified callee; it tends to keep the ringing duration longer and it obtains a higher connection rate comparatively.

In some circumstances, a group of silent callers will open the "unconditional forwarding" service to inform the network to forward the incoming calls unconditionally to a specific number, by which an interactive voice response (IVR) platform is working. The IVR platform can even send back the spam voice to the incoming caller by a ring tone. It would be helpful for the analysis to check whether the suspicious callers opened the "unconditional forwarding" service and what the destination number was.

It is a fact that there exist some more complicated and effective analysis models in countering voice spam, such as a model integrated with human society analysis, caller billable records analysis and so on. Anyway, the rule model could be a basis for evolving more comprehensive models.

7.2.3 Interactive verification

Required by the management entities or the user service agreement, the callers' number in the suspicious list shall be verified before some controlling measures are taken. There are two alternative ways to operate verification in terms of the requirement.

First, the telecommunication organizations shall keep updating the suspicious list and submit it to management entities and accept feedback from it.

Second, if it is permitted by the user service agreement or the management entities, the operator could undertake a dialling test on a caller number from the suspicious lists in order to obtain direct

verification. Using the results of the dialling test, usually known as the voice record file, the authorized audit staff will attempt to point out whether the record is spam or not.

However, the accuracy and quality of the interactive verification affects the controlling procedure.

As mentioned above, a honeypot can handle the interactive verification itself, i.e. if the calculation result of the indicators implies the outgoing call to be a silent call (see clause 6.2), the honeypot will call back to prove the evidence of the verification; in contrast, when the harassing call is confirmed by the indicators' analysis, the honeypot will put through the phone call and record it.

Furthermore, the coordination between a group of silent callers and a/several IVR platforms may confuse the operators about the real source of the voice spam. Sometimes, the IVR platforms and the silent callers belong to different operators respectively. After achieving a spam voice record, it will be meaningful to trace the potential connection between a silent caller and an IVR platform by making a request to the home location registry (HLR), for example.

7.2.4 Controlling

Controlling is to restrict or disable/shut down voice spammers confirmed by verification to protect normal users. Two methods are discussed below.

7.2.4.1 Whitelists/blacklists

Whitelists/blacklists, usually known as key account lists, are time consuming to create and require continued updating. The life cycle of each item in a whitelist/blacklist needs to be well-managed to keep it accurate and effective. Each item in a whitelist/blacklist needs also to be well-maintained in a secure way during its life cycle.

As described in [ITU-T X.1240], the quality of blacklists varies enormously depending on the professionalism of the compiler. Blacklists inevitably contain inaccuracies that prevent some legitimate calls from getting through to the receivers. Although their utilization raises many concerns, blacklists are a quick solution to refuse a connection between voice spam sources and receivers (phone users).

Blacklists including user numbers or number segments are usually deployed in a gateway mobile switching centre (GMSC), in SCP, in switches and other network entities. Generally, blacklists from the same operator network can be deployed in SCP, switches or other network entities, while blacklists from other operator networks can only be deployed in the GMSC whose blacklist capacity may be too limited to store a large list of numbers. To solve the problem simply, hidden signalling nodes (see clause 7.2.1.1) can be used behind GMSC.

Whitelists may need to interact with the authorized database maintained for already identified legitimate callers to exclude unintended genuine callers having similar characteristics as voice spammers. These callers may be call centres, notification services, feedback/data collection services such as due payment reminders, feedback of management entities sponsored schemes, awareness programmes, emergency-/disaster-related programmes, etc.

7.2.4.2 Trace back mechanism

This mechanism traces back the real physical location of voice spammers. It could be useful sometimes to point out the exact location or address of the voice spammer if necessary.

According to the existing techniques, operators can locate the voice spammer's real location based on information provided by the mobile switching centre (MSC); however, this technique can only locate the approximate area. More accurate location could be provided by the operator's location information service, such as assisted global positioning service.

7.3 User-side technologies

User-side technologies should be an effective supplement to network-side technologies. And the measure of feedback can provide detailed information of voice spammers (as discussed below), which is an especially important backup for operators. User-side technologies may need the aid by some smart mobile phones' particular features, the support to which may be different by vendors.

7.3.1 Whitelists/blacklists

User can utilize the connection-control feature in phones to block specific numbers or number segments as blacklists, while at the same time they will allow particular numbers (set by the users or synchronized by some mobile applications) to be always put through when they are treated as whitelists.

This method could work based on the whitelist/blacklist when synchronized by the network side, whereas the user side is usually subject to personal preferences because users can maintain their own lists.

7.3.2 Call-delay

Call delay is a signalling-level technique which specifically works for silent calls (see clause 6.2).

After the signalling link is established between a caller and a callee, the ring tone will be periodically generated from the link. Some silent calls will be produced and users will receive a silence ("dead air") or a short duration of the tone which indicates the call has been dropped.

With the support of a smart mobile phone, users can block the silent call at the terminal side (user side). Since users can set a value of the tone duration (threshold) for every incoming call at the signalling layer, silent calls may be omitted as to the tone duration is less than the threshold. However, the calling record will be saved in the mobile phone's call log list to allow the user to double check, in case of ignoring the "short-ring-tone" normal call.

7.3.3 Feedback

After receiving voice spam, users can provide a feedback to the operators indicating the voice spam number and other detailed information. The feedback channels include sending text messages, phone calls and e-mails or even an official website to the customer service department (or other equivalent departments) of operators. All the channels should provide convenient and easy-to-follow procedure for users to provide a feedback. A user-friendly channel could be constructed by applications in terminals or subscriber identity module (SIM) cards and platforms such as device management platform (DMP), over the air platform (OTAP) in the network.

Furthermore, once the service department of the operators has received the feedback, an authorized auditor should check whether the feedback information is real and effective, and apply a similar procedure of interactive verification before taking proper further action. If there is a voice recording as proof from VMS and the access to the recording is authorized by the owner, the verification could be more effective and more efficient.

7.4 Collaboration mechanism

Operators may co-operate with management entities, other operators or users to establish some corresponding co-operation and communication mode, in order to counter voice spam.

Operators may establish or support an information sharing system (ISS). This particular system could cover the basic voice spam information exchanges with other organizations, including the suspicious/verified spam caller list, classification of each voice spam, the countering technologies, etc.

Management entities may consider the implementation of ISS and the establishment of an information exchange mechanism or even the organization of formal meetings for operators and third party organizations to share up-to-date information.

Users could share their blacklists with the server at the network side by uploading or downloading the blacklists. However, operators should have a verification mechanism through which they could detect whether an item in a personal blacklist is a real voice spammer or not. Operators should provide an interface for uploading and downloading blacklists. This mechanism could be interacted with customer feedback. Meanwhile, management entities should audit the updated information to avoid inappropriate information.

In order to implement the information sharing mechanism, operators may submit the verified blacklists, on a recurring basis to management entities and to block the established blacklists enforced by management entities.

Moreover, management entities may consolidate all the received blacklists from all the operators and apply appropriate actions and procedures. In addition, management entities may take more responsibilities, such as restraining voice spam at source, while ensuring operators to implement their duties.

7.5 Proposed solutions

None of the solutions can be entirely successful independently. In order to counter voice spam effectively, network-side and user-side technologies should be deployed comprehensively in each procedure.

In order for high accuracy, it is possible for the signalling record procedure to integrate various data sources together. However, a comprehensive data-source will be extremely expensive implementation.

The following situations should be considered.

Firstly, SS7 signalling could be a single choice because it covers all the signalling links to obtain the most useful data rather than other data sources (mentioned in 7.2.1), in order to guarantee the effectiveness of countering voice spam.

On the other hand, a data collecting system based on IN, CRBT or VMS may be a cost-balanced alternative, if operators have already launched IN, CRBT or VMS services. However, data sources from CRBT or IN networks may not cover all the specific data as discussed in clause 7.2.1. Hence, a data source from these services could be complementary.

The model proposed in clause 7.2.2 is easy-to-use and is not costly; it is also commonly deployed in countering voice spam. To increase the accuracy of the analysis, more sophisticated rule models and algorithms can be used. For example, statistics on the codes of calling release causes and statistics on the codes of rejected calls could narrow significantly the suspicious list.

However, comprehensive rule models or algorithms may lead to a high degree of system complexity and long time-consuming procedures, which in turn, increase the delay of the whole procedure of countering voice spam, which may ultimately decrease customer satisfaction. Given all that, a wise choice of proper rule models or algorithms is a quite significant factor for operators.

The interactive verification procedure may be different from nation to nation. Hence, management entities may assist operators to establish a proper verification procedure based on their national practice.

As can be seen from the controlling procedure stated earlier, the user-side and network-side methods should be better integrated to mitigate the volume of voice spam. The customer service department of the operators could play a significant role in the controlling procedure and meet customers' demands.

Appendix I

Comprehensive measures on countering voice spam

(This appendix does not form an integral part of this Recommendation.)

Since countering voice spam is not a simple technical problem, various approaches should be applied together:

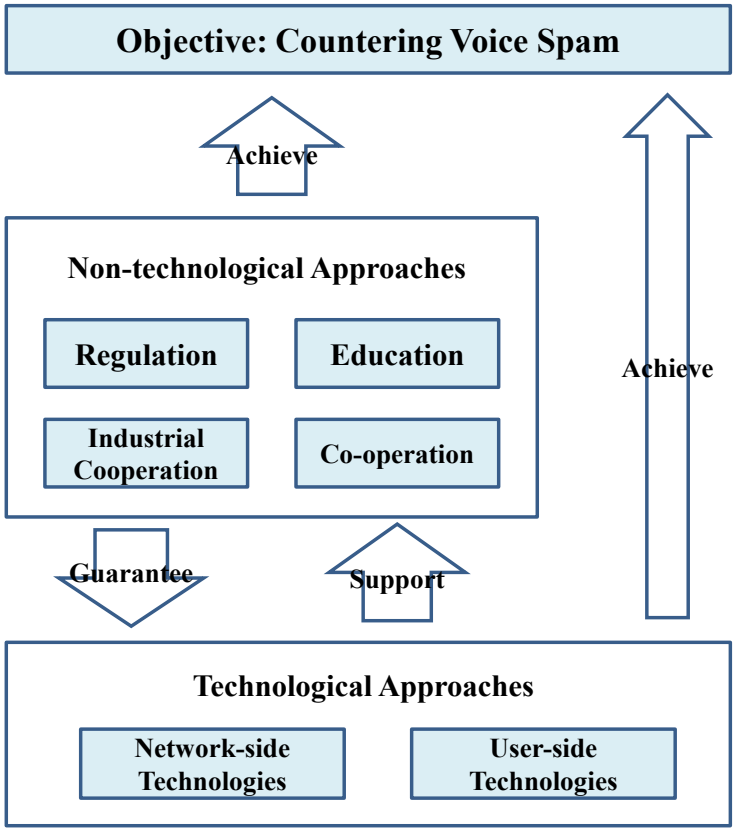

Figure 4 - Structure of Countering Voice Spam

- Regulations can help protect users and operators from voice spam.
- Industry cooperation is necessary so that various kinds of technologies are appropriate to be developed and installed by industry participants.
- Cooperation can help operators and management entities to share information about effective adoption of the regulations and technology development.

- Education is important for users to minimize economic loss incurred by voice spam.

Appendix II

A suggestive solution for interactive verification

(This appendix does not form an integral part of this Recommendation.)

Generally speaking, every interactive verification implies the dialling of a suspicious caller number, the recording of the ring-back tone before being connected and of the voice after the connection, and then the auditing of the content to check whether it is voice spam or not. If all these steps are done manually, this could exhaust tremendously the human resources of the operators. Therefore, an optimized approach shall be considered to balance the cost.

The interactive verification can be operated in a central way to dial records and audit semi-automatically the voice proofs of the amount of suspicious voice spammers, who were distributed sparsely maybe in every corner of the network.

The centralized approach executes the dialling and the recording job automatically in high concurrency and only allows the auditors audit the successful voice proofs without white noise and other useless ring-back tones.

Appendix III

Policy considerations in countering voice spam

(This appendix does not form an integral part of this Recommendation.)

Voice spam is a dangerous tool used to advertise, fraud, and to harass, etc., which may occur in daily communications. In order to counter voice spam effectively, different approaches in various aspects of the participating groups should be considered, though various types of technologies are introduced in this Recommendation. These are users (or subscribers), operators, management entities and third party organizations. Thus, this appendix describes several aspects which should be considered in countering voice spam.

III.1 Users

Users are the final victims in the voice spam communication chain, and they have a great demand to block spam. Hence, users should implement some approaches applied in the whole process of countering spam. The following provides several suggestions which may vary based on the situation:

- Users should install anti-spam applications on their own devices, such as on smart mobile phones, if possible. For better effectiveness, the anti-spam application must be up to date.
- Users should send feedback to the telecommunication operators or third party organizations of all the detailed information of the voice spammer as soon as they receive voice spam.
- - Users should be much more conscious in their daily communications and protect personal information from being exposed to spammers.

III.2 Operators

Operators are the significant parts in the whole procedure of countering voice spam. Since voice spam may reduce the users' satisfaction rate severely and cause much waste to network resources, operators should be aware of voice spam to protect their networks and provide better services.

- Operators should monitor the whole communication network to detect potential voice spam, which may incur abnormal signalling transmissions or traffic patterns.
- Operators should pre-install the latest version of anti-spam applications in all the devices that could be the targets of voice spam through their own distribution or sale channels. For third-party distribution channels, operators should guarantee that all the devices are fully protected by up-to-date applications.
- Operators should provide awareness and training campaigns and encourage users to submit feedback about voice spammers by providing detailed information to third party organizations; such feedback can be operated by some incentive programs.
- Operators should be involved in building alliances with management entities and third party organizations to consolidate their efforts in countering voice spam.

III.3 management entities and third party organizations

Management entities and third party organizations may supervise or guide operators directly and even providenecessary backup.

- Management entities and third party organizations may train or provide training and awareness campaigns to users and operators to counter voice spam.

- Management entities and third party organizations should conduct more research on voice spam trends and should endeavor to find more effective countering approaches or technologies on the newest pattern of voice spam.
- Management entities and third party organizations should unclog advertisement or promotion channels to normalize current voice communication environment, or regulate chartered advertisement dialling systems for the promotion entity.
- Management entities and third party organizations should share the latest blacklists with operators and even with users; this blacklist should be maintained with the support of operators and users.
- Management entities should provide the circumstances to reinforce the strength for countering voice spam under the protection of the users' benefits.

Bibliography

[b-ITU-T E.370] Recommendation ITU-T E.370 (2001), *Service principles when public circuit-switched international telecommunication networks interwork with IP-based networks*.

b-ITU-T M.1400] Recommendation ITU-T M.1400 (2013), *Designations for interconnections among operators' networks*.

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam.*

[b-ITU-T X.1245] Recommendation ITU-T X.1245 (2010), Framework for countering spam in IP-based multimedia applications.

[b-ITU-T Y.1001] Recommendation ITU-T Y.1001 (2000), *IP framework - A framework for convergence of telecommunications network and IP network technologies*.