



---

**Question(s):** 5/17**STUDY GROUP 17 – CONTRIBUTION 0289****Source:** China Mobile**Title:** Proposal for a new work item: Technical measures and mechanism on countering the spoofed call in the visited network of VoLTE

---

With the rapid development of next generation network, the spoofed calls bring much more security and financial issues to end users and operators as well. There are new threats of the spoofed calls to end users and operators and also new opportunities to countering them.

This document proposes a new work item to recommend the technical measures and mechanism on countering the spoofed call in the visited network of VoLTE (Voice service over Long Term Evolution network). The work item will focus on the protection of the VoLTE users, keeping them away from the spam of the spoofed calls or warning them wary of the suspicious spoofed call in time.

It is proposed to establish the work item as a supplement to X.1245 “Framework for countering spam in IP-based multimedia applications”.

**1. Background**

Since the next generation network (4G) is developing rapidly, the VoLTE is already implemented or under implementation in some of operators, with a brand new mode of communications. Security issues are becoming more complicated compared to the traditional (circuit-switched) network. The

---

<b>Contact:</b>	Chen ZHANG China Mobile China	Tel: 86-10-52696688-3019 Fax: 86-10-52696688-3001 Email: zhangchen@chinamobile.com
<b>Contact:</b>	Meng ZHANG China Mobile China	Tel: 86-10-52696688-8304 Fax: 86-10-82606688-3001 Email: zhangmeng1@cmdi.chinamobile.com
<b>Contact:</b>	Xuetao DU China Mobile China	Tel: 86-10-52696688-3025 Fax: 86-10-52696688-3001 Email: duxuetao@cmdi.chinamobile.com
<b>Contact:</b>	Jie YUAN China Mobile China	Tel: Fax: Email: yuanjie@chinamobile.com

---

<b>Attention:</b> This is not a publication made available to the public, but <b>an internal ITU-T Document</b> 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.
--

spoofed calls can be generated more easily from caller which brings several threats to both operators and end-users.

Both in the traditional network and in the 4G network, the spoofed calls are generated due to the protocol vulnerabilities and the management vulnerabilities. But in tradition, once a spoofed call arrives at the visited network, operators can hardly point out whether the incoming call (mostly from other networks) is spoofed or not.

However, the core network architecture of VoLTE, that is IMS (IP Multimedia Subsystem), brings more flexibility so that operators can utilize more effective measures and establish a pragmatic protection mechanism to counter the spoofed calls.

## **2. Threats and Measures**

### **Part 1: Threats**

The spoofed calls always cause the most dangerous spam to fraud, blackmail, phish or threat, etc. Compared to the traditional voice service, the spoofed calls are more dangerous in the VoLTE.

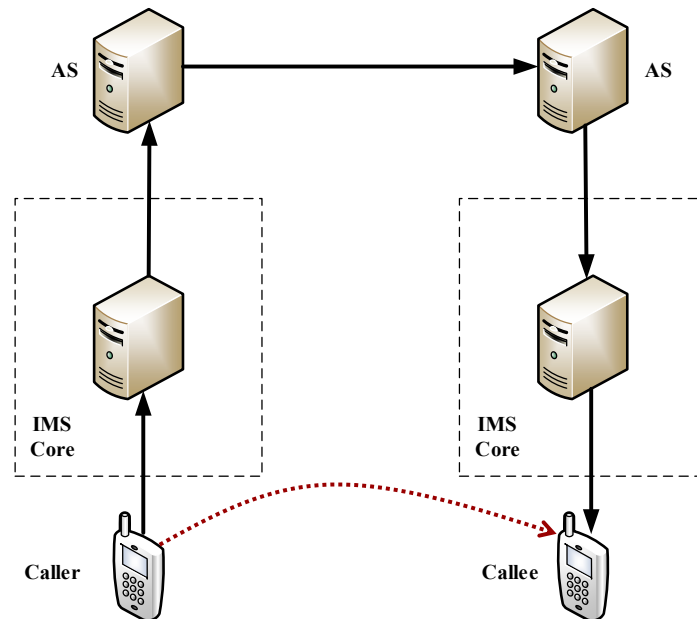
- Low Cost  
Due to the change of new network architecture and charging mode, communication fare becomes much cheaper than before, hence the cost of generating spoofed calls declines.
- Multiple Numbers  
Multiple numbers can be bundled into one SIM card in the IMS network, which increases the difficulty to find out the exact spoofed caller.
- Multi-party call  
Multi-party call involves multiple communication party, which increases the probability and spreading range of spoofed calls

### **Part 2: Measures**

There are several scenarios of spoofed calls, however, this proposal only discusses the measures to counter the following two kinds of spoofed calls:

- Completely duplicate a real caller number.
- Mimic a real caller number with nuance.

Based on the flexibility of IMS network and the extensibility of the voice call procedures, a new logic entity, anti-spoof AS in or beyond AS (Application Server) layer can be introduced to control the suspicious incoming calls, and the following measures can be used on the basis of the new logic entity.



### Measures based on IMS network

Since the architecture of IMS network is more flexible than that of the traditional network, it becomes easily for operators to monitor the status of a caller's each number and even block the spoofed calls directly by the anti-spoof AS.

### Measures based on RCS

Due to RCS or other kinds of messaging services, operators can keep communications with end-users more easily and real-time, hence operators can warn the end-users which calls are mimicked.

### Measures based on smartphone functions

Nowadays, smartphone functions are varied, which can provide validation function collaborated with anti-spoof AS to warn end-users whether the incoming call is suspiciously spoofed or not.

A mechanism can also be recommended with the integration of all available measures.

## 3. Proposal

It is proposed to establish a new work item as a supplement to recommend the technical measures and mechanism to counter the spoofed call in the visited network of VoLTE.

The content of this includes:

- Introduce the background of spoofed calls in VoLTE network.
- Analyze the threats existed in the VoLTE network.
- Propose countering measures and mechanisms.

## 4. Proposed structure

1. Scope
2. References
3. Definitions
4. Abbreviations and acronyms
5. Background

6. Threats analysis
  7. Measures proposed
-