



Robustness Report on VoLTE
2011 VoLTE Interoperability Event

Abstract:

In September 2011, the MSF conducted a Voice over LTE (VoLTE) IOT event. The White Paper for the event may be viewed at :-

http://www.msforum.org/interoperability/MSF_VoLTE%202011_WhitePaper.pdf

One aspect of the VoLTE IOT event concerned robustness testing. This document is a report on that robustness testing from the MSF VoLTE IOT event. The tested targets were implementations of the LTE networks IPv4, UDP and SIP deployments within S-GW, P-GW and the IMS Core in order to demonstrate robustness in the network architecture. This Whitepaper focuses on describing the found issues and potential new test targets that need to be focused in the LTE Network deployments.

DISCLAIMER

The following is a technical report of the MultiService Forum. The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and the MultiService Forum is not responsible for any errors or omissions. The MultiService Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything contained herein to the contrary, neither the MultiService Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind whether based on theories of tort, contract, warranty, strict liability or otherwise, shall be assumed or incurred by the MultiService Forum, its member companies, or the publisher as a result of reliance upon or use by any party of any information contained in this publication. All liability for any implied or express warranty of merchantability or fitness for a particular purpose, or any other warranty, is hereby disclaimed.

About the MSF

The MSF is a global association of service providers, system suppliers, test equipment vendors, and users committed to developing and promoting open-architecture, multiservice Next Generation Networks. Founded in 1998, the MSF is an open-membership organization whose members are drawn from the world's leading IP communications companies. Historically, the MSF developed Implementation Agreements (IAs), promoting worldwide compatibility and interoperability of network elements, and encouraging input to appropriate national and international standards bodies. However, this role has become less of a focus as a standard architecture has emerged and protocol profiles are being defined in other SDOs and industry fora (e.g. 3GPP). The MSF primarily focuses on running IOT events to facilitate the deployment of next-generation multi-service networks, driven by its member needs. In addition, in 2009, the MSF decided to complement its established biennial Global MSF Interoperability (GMI) events by more targeted test events focused on critical and timely issues associated with deployment of IP communications. The VoLTE Interoperability Event 2011 is the third test event of this nature. For a history of MSF IOT events as well as information on planned upcoming IOT events, see <http://www.msforum.org/interoperability/GMI.shtml>.

Table of Contents

1 EXECUTIVE SUMMARY	4
2 TEST OUTCOMES.....	4
2.1 S-GW.....	5
2.2 P-GW.....	6
2.3 IMS CORE.....	6
3 IMPLICATIONS	8
4 CONCLUSION.....	8
ANNEX ABBREVIATIONS	9

1 Executive Summary

Codonomicon participated in to the MultiService Forum testing event in Dusseldorf Germany to do Robustness testing on the service components within the Voice over LTE networks. Robustness testing scenarios done by Codonomicon focused on the components that interact and have a direct effect on the end user services. The components tested within this environment where S-GW, P-GW and IMS Core Services (I-CSCF and P-CSCF). Tested protocols within these components were limited to three main protocols: IPv4, UDP and SIP (Options-Register) due to the limitations in time and possible interoperability issues.

During the testing it was noticed that there are issues within all components, which from end user and provider perspectives raises some concerns. This leads to situations where end users will not be receiving the services wanted and providers will lose revenue as a conclusion of this.

2 Test outcomes

This report is not a comprehensive remedy report but an overview on the situation seen in during the Interoperability testing event and to help create further steps to enhance the robustness and security of the VoLTE network for deployment.

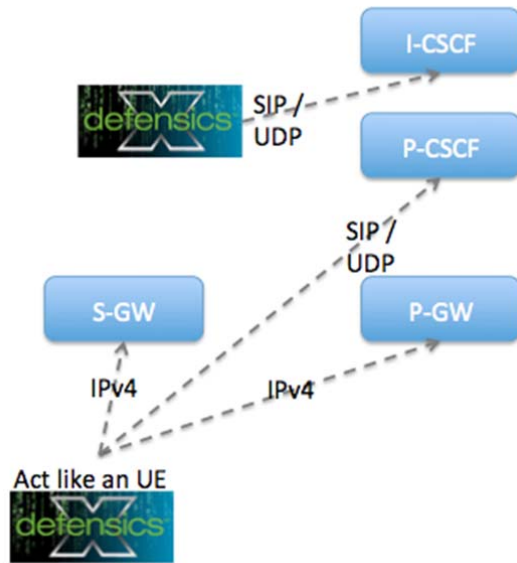
Results should be read so that even one fail is deemed as a failure. This is because there wasn't time to do in-depth analysis on the reasons why the system under test went failed to answer to valid requests. Denial of service in means that the system under test failed to respond to a valid request and the denial of service time reflects on how long it took for the system under test to come back online. Valid test case is a specific test for each protocol to test that the system is able to communicate and hasn't crashed.

IPv4 interoperability was tested with a valid test case, where Test Suite sent a valid IPv4 packet with ICMP Request payload. The Test Suite then expected to get a valid ICMP Response within the timeout. The interoperability was verified both without fragmentation and with fragmentation. UDP interoperability was tested with a similar method, by sending a valid UDP packet with a valid SIP request (OPTIONS) as a payload, and expecting a SIP response within timeout. SIP interoperability was tested through sending a valid Options Request and expecting an OK response from the target system.

Notable is also that there are few "no interoperability" targets. These targets didn't allow communication from Codonomicon testing platform to the targets or the targets were offline when the testing was about to commence. Thus this means that these targets were scoped out of the testing.

Overall testing was done to 29 different targets out of 40 potential targets during the Interoperability testing event.

2.1 Test Setup



2.2 S-GW

The S-GW testing was done with IPv4 suite (version 2.5.0) from Codenomicon and testing the robustness of the IP implementation within the module. There were five vendors that had provided their solutions to this network component. Out of the five vendors we were able to test four and one vendor requested that robustness testing is not executed to them due to focus on other Interoperability tasks at hand.

The expectation of this test was a very clean result without any major failures as the IPv4 stack is one of the most tested network protocol.

It should be noted that UDP and IPComp failed to Interoperate with all the solutions (RFC 3173), thus these were left out on this scenario.

This test contained the default test case amount from the tool that would represent 21% coverage of potential test cases that can be generated through the tool. The test case count was 148 946.

Below is a list of the vendors and the results:

Vendor	Verdict	Result	Notice
A	Pass	0 fails	
B	Fail	1 fail	1.5s max Denial of Service time
C	Fail	8670 fails	11.5s max Denial of Service time
D	Fail	1 fail	11.5s max Denial of Service time
E	Inconclusive	N/A	Request to stop testing

2.3 P-GW

The P-GW testing was done with IPv4 suite (version 2.5.0) from Codenomicon testing the robustness of the IP implementation within the module. There were five vendors that had provided their solutions to this network component. Out of the five vendors we were able to test all five, but as one P-GW was physically the same machine as the S-GW the IPv4 results for this can be taken from the S-GW tests.

The expectation of this test was a very clean result without any major failures as the IPv4 stack is one of the most tested network element.

It should be noted that UDP and IPComp failed to Interoperate with all the solutions (RFC 3173), thus these were left out on this scenario.

This test contained the default test case amount from the tool that would represent 21% coverage of potential test cases that can be generated through the tool. The test case count was 148 946.

Below is a list of the vendors and the results:

Vendor	Verdict	Result	Notice
A	Pass	0 fails	
B	Fail	3 fails	1.5s max Denial of Service time
C	Skipped		Same device as S-GW
D	Fail	1 fail	11.6s max Denial of Service time
E	Fail	2 fails	1.8s max Denial of Service time

2.4 IMS Core

Within the IMS core the tests focused on testing the two elements P- and I-CSCF. These elements were tested through SIP UAS (version 4.6.2) and IPv4 plain UDP test tools (version 2.5.0). The expected outcome was that there would be some issues with the SIP implementations but it should be noted that full Interoperability was not achieved with all the vendors and this might have an effect of the test outcomes by giving better results through dropping packets that are coming from a not known host.

The test scenario with SIP UAS represented 5% test coverage of the potential maximum test cases that can be generated through the tool. This scenario was only for the Options-Sequence within SIP with possibility to test another 19 different sequences. This means the test coverage is below 1% within the MSF test event. Test case count for SIP was 67 773.

The UDP test scenario had 29% test coverage of the potential maximum test cases that could be generated through the tool. Test case count for UDP was 11 242.

For the I-CSCF there were four vendors tested with both SIP and UDP with one vendor preferred to be left out due to other Interoperability tests being done at the same time. Generally the results were what were expected with some failures but without major Denial of Service time. Combined with the low coverage it should be noted that this requires further evaluation to be done before a comprehensive answer can be given.

Below is a list of the vendors and the results:

Vendor (I-CSCF)	Protocol	Verdict	Result	Notice
F	SIP	Fail	1 fail	No full Interoperability
C	SIP	Fail	13 fails	0.5s max Denial of Service time. Full Interoperability
A	SIP	Inconclusive	N/A	No testing done
B	SIP	Inconclusive	N/A	No Interoperability

Vendor (I-CSCF)	Protocol	Verdict	Result	Notice
F	UDP	Fail	78 fails	3.5s max Denial of Service time
C	UDP	Inconclusive	N/A	No Interoperability
A	UDP	Pass	0 fails	
B	UDP	Inconclusive	N/A	No Interoperability

The P-CSCF testing had ten test targets and with six vendors taking part. Two of the vendors preferred to be left out due to other Interoperability tests being done at the same time.

Below is a list of the vendors and the results:

Vendor (P-CSCF)	Protocol	Verdict	Result	Notice
A 1	SIP	Fail	14 fails	33.7s max Denial of Service time, full interoperability
A 2	SIP	Inconclusive	N/A	Requested to stop testing
F 1	SIP	Fail	460 fails	3.6s max Denial of Service time
F 2	SIP	Fail	1883 fails	11.6s max Denial of Service time
C	SIP	Fail	12 fails	0.5s max Denial of Service time
B	SIP	Inconclusive	N/A	No interoperability
G 1	SIP	Inconclusive	N/A	No Interoperability
G 2	SIP	Inconclusive	N/A	
H 1	SIP	Inconclusive	N/A	No Interoperability
H 2	SIP	Fail	1 fail	0.5s max Denial of Service time

Vendor (P-CSCF)	Protocol	Verdict	Result	Notice
A 1	UDP	Pass	0 fails	
A 2	UDP	Inconclusive	N/A	No Interoperability
F 1	UDP	Inconclusive	N/A	No Interoperability
F 2	UDP	Inconclusive	N/A	No Interoperability
C	UDP	Pass	0 fails	
B	UDP	Inconclusive	N/A	No interoperability
G 1	UDP	Pass	0 fails	
G 2	UDP	Pass	0 fails	
H 1	UDP	Inconclusive	N/A	No Interoperability
H 2	UDP	Pass	0 fails	

3 Implications

There are two main scenarios that can be viewed through the testing results: a) a person with malicious intent willingly wants to bring down the network with anomalous packets or b) there is a component issue within the network (End user or Inter network) that starts to send malformed packets, which would have an effect to the other network components by causing disturbance in the services. The maximum denial of service time during the testing was not a major implication as the systems under test were able to come back online without major crashes.

The test result imply that there are issues in the network that need to be tested further and seen as potential issues in the future within the network. This is especially important in the S-GW and P-GW components and their IPv4 deployments. As these components are reachable through the public networks their robustness is essential to ensure uninterrupted end user services. The few targets that were not interoperable were targets that were not present in the network at the time of testing or due to time limitations interoperability was not feasible to establish.

The IMS core is more secure in general and it can be made more secure through filtering traffic before the components within the IMS core. The filtering can be done on malformed packets but occasionally the filtering can fail or it hasn't been implemented at all. SIP traffic testing is important, as it is responsible to deliver the value added service to the end users, which has a direct effect on the perceived quality by the end users.

4 Conclusion

In conclusion the VoLTE components handled the malicious packets and traffic reliably without complete service crashes. Although there were clear Denial of Service situations, which would need to be evaluated further before live implementations, but all the systems were able to recover from the situations. In the end even if the systems were able to come back alive the implication to end user is during the downtime is not being able to access the services they needed at that point in time.

Codonomicon recommends that Vendors would look into the protocol deployments they are going to do in their LTE networks and validate that the components can handle the malicious traffic. Recently it has become a trend to do these types attacks against services by certain groups thus to prevent service downtimes these matters should be tested during development to minimize potential issues to end users and network infrastructure.

Codonomicon would like to thank vendors for their help and understanding in the test situation.

Annex Abbreviations

3GPP	3 rd Generation Partnership Project
eNodeB	Evolved Node B
EPS	Evolved Packet System
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
HSS	Home Subscriber Server
I-CSCF	Interrogating Call Session Control Function
IMS	IP multimedia Subsystem
IP	Internet Protocol
IPR	Intellectual Property Rights
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LTE	Long Term Evolution
MME	Mobility Management Entity
MMTelAS	Multimedia Telephony Service
MSF	MultiServiceForum
P-CSCF	Proxy Call Session Control Function
P-GW	PDN Gateway
PCRF	Policy and Charging Rules Function
S-CSCF	Serving Call Session Control Function
S-GW	Serving Gateway
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SUT	System Under Test
UDP	User Datagram Protocol
VoLTE	Voice Over LTE