



eMBMS 安全机制及内容保护研究

周 毅,刘 稼,史敏锐

(中国电信股份有限公司上海研究院 上海 200122)

摘 要: 通过对 3GPP 标准中 eMBMS 安全机制的研究并结合运营商自身的特点,给出了运营商部署 eMBMS 安全机制对 LTE 现网的影响。在此基础上对运营商如何部署安全机制提出了合理的建议。

关键词: LTE;安全机制;内容保护

doi: 10.3969/j.issn.1000-0801.2014.12.005

Research of eMBMS's Security Mechanism and Content Protection

Zhou Yi, Liu Jia, Shi Minrui

(Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China)

Abstract: Through the research of 3GPP's eMBMS security mechanism and being combined with the characteristics of operators, the influence of current network by the deployment of eMBMS security mechanism was given. On the basis of the research above, a proposal was made for how the operator deploys eMBMS security mechanism.

Key words: LTE, security mechanism, content protection

1 引言

LTE 的高带宽、低时延以及永远在线等特性已为人所熟知,但如何更好地使用这些 LTE 特性制造出 LTE 特有的杀手级应用呢? eMBMS (evolved multimedia broadcast multicast service,增强型多媒体广播多播业务)应能算其中之一。

3GPP 在 2010 年完成了基于 LTE 的 eMBMS 技术,即在 LTE 网络中承载多媒体广播业务和多播业务的技术方案,用于实现从数据业务源向特定范围内多个用户同时传送某类内容的数据业务的一种点到多点业务。相比 3G 时期的 MBMS,eMBMS 在逻辑架构、业务模式、传输方式和信道结构等方面进行了重大改进,更适应现阶段移动视频业务在 LTE 网络上的传送和使用。

但是 eMBMS 由于其技术特性,还存在一定的安全风

险。首先,eMBMS 是以广播的形式在无线网络中传播,这就意味着只要是在业务区范围内的所有终端都能接收 eMBMS 的业务内容,这样就会存在非授权用户接入的可能,造成网络资源的浪费;其次,eMBMS 的传输过程如果不采用一定的加密机制,就难免遇到来自网络的完整性攻击,使得数据在传输的过程中遭受修改和破坏;最后,如果不采用一定的内容保护举措保护 eMBMS 的业务内容,对于一些文件分发类的业务,会存在侵犯数字版权,非法复制的风险。下面就 eMBMS 安全机制的构架/原理以及运营商如何部署等方面进行详细的分析。

2 eMBMS 安全机制

2.1 eMBMS 安全机制定义

eMBMS 技术的安全机制由两部分组成:业务保护和内容保护。

业务保护和内容保护功能提供了一种在移动广播业务中,与底层传输网络无关的保护业务和内容的方法。

业务保护的目的是允许到某个业务的接入,如访问特定时间内特定的数据集。业务保护不对该业务传送的内容负责,也不提供任何方法来保护具有访问控制机制的管道外的内容。

内容保护功能保证每个独立的内容受到保护。

2.2 3GPP 技术架构

在安全方面,eMBMS 基本沿用 3G 时期 MBMS 的安全架构和机制^[1]。如图 1 所示,采用通用自举架构(generic bootstrapping architecture,GBA)通过鉴权、密钥管理和数据安全保护来保障 eMBMS 业务安全。因为 eMBMS 技术是一个包含了业务、传输以及接入的完整系统,所以与普通的单播相比,其安全机制不仅需要通过鉴权来验证用户接入的合法性,还需要通过加密和内容保护来确保传输和业务

的安全。

具体来说,eMBMS 安全机制分为 4 个层次^[2],如图 2 所示。

第 1 层:认证管理。

终端和网络之间相互认证,通过 Ub 接口执行 HTTP digest AKA 协议进行相互鉴权,网络侧 BSF (bootstrapping server function,引导服务功能)模块根据用户的鉴权元组信息实现对用户的鉴权,并生成共享密钥 K_s ,并通过 Ub 接口将密钥 K_s 传至终端。BSF 与 NAF(网络应用功能)相互认证,根据 NAF 请求,生成终端的认证密钥 MRK (MBMS request key)和用户密钥 MUK (MBMS user key)。终端侧根据共享密钥 K_s 也生成认证密钥 MRK 和用户密钥 MUK。其中,认证密钥用于终端向 BM-SC(广播多播业务中心)进行认证;用户密钥用于后续业务密钥 MSK (MBMS service key)的加解密运算。

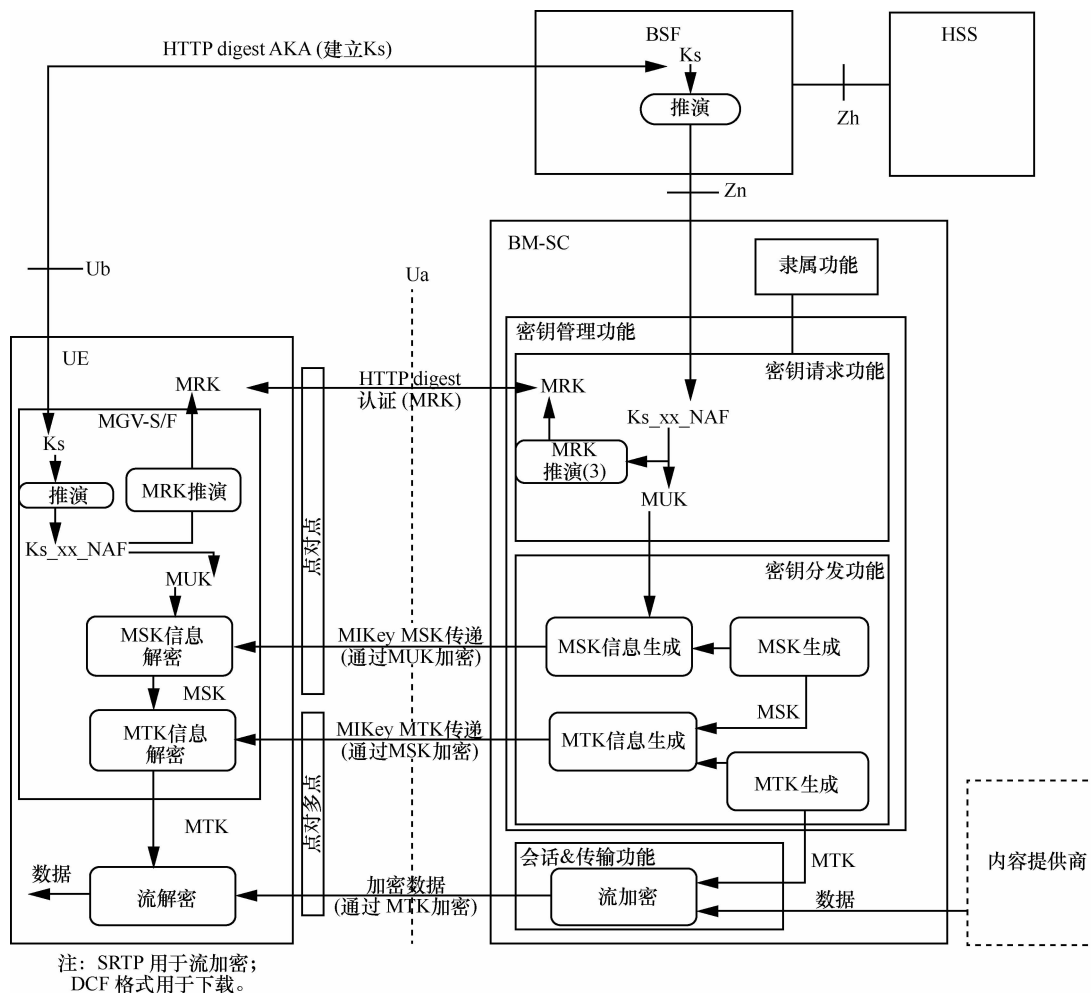


图 1 eMBMS 安全架构

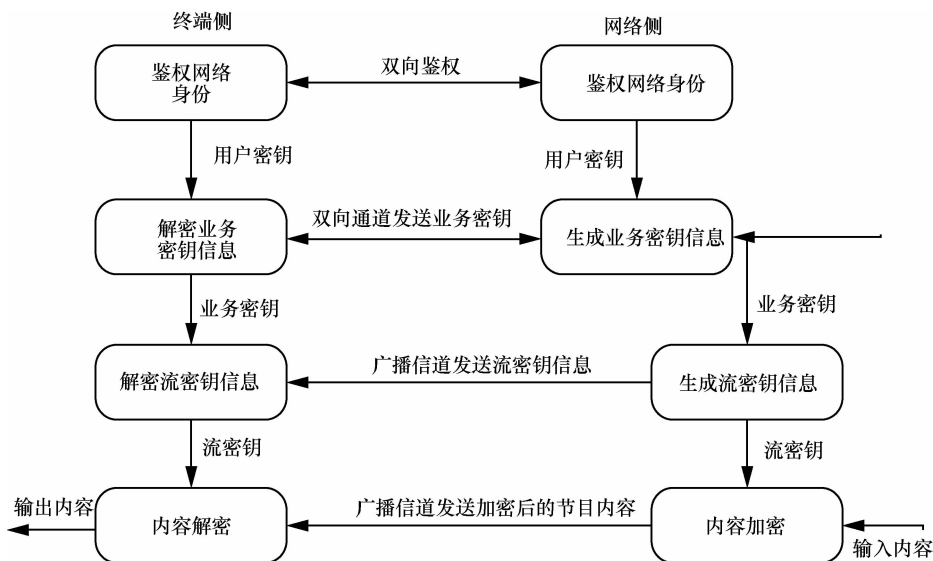


图 2 eMBMS 4 层安全体系

第 2 层:业务密钥管理。

业务密钥用于控制用户接入业务通信。MBMS 的业务加密密钥 MSK 是一个中间密钥,即它不直接加密内容,而是用于加密 MBMS 节目流密钥。网络根据用户订购关系将业务密钥基于 HTTP digest 协议,通过加密方式传送给用户。网络对业务密钥进行加密时使用的是第一层生成的用户密钥;同理,终端对业务密钥消息解密时使用的是本地生成的用户密钥。

第 3 层:流密钥管理。

节目流密钥 MTK(MBMS traffic key)用于对广播内容的加密。加密过的节目流密钥消息将在广播信道进行传递。网络对节目流密钥进行加密时使用的是第二次生成的业务密钥,终端节目流密钥消息解密使用的是本地生成的业务密钥。

第 4 层:MBMS 的业务数据加密。

网络侧使用第 3 层中生成的节目流密钥对节目流进行加密处理,加密后的节目通过 MTCH 信道分发,终端侧使用第 3 层经过解密得到的节目流密钥进行解密。

可以看到,MBMS 4 层安全机制包含了业务保护和内容保护两方面。其中前 3 层属于业务保护,第 4 层属于内容保护。

3 业务保护

通过上述分析可以看到,eMBMS 安全机制实质采用了两级密钥机制:业务密钥和流密钥。业务密钥:BM-SC 针

对每个 MBMS 会生成一个业务密钥,MSK 的传输和更新都是通过点对点的方式完成,确保其安全性。业务密钥在相对较长的时间内保持不变。流密钥:BM-SC 通过 MSK 对 MTK 加密后,采用点对多点的方式,对 MTK 进行广播传递。每个加入此 MBMS 的用户利用之前收到的 MSK 来解密该消息,从而获得当前 MBMS 使用的 MTK。MTK 变化频率很快。

通过这样两级密钥机制,可以保证 MBMS 密钥能够及时地更新到每个用户,同时又避免了小区内大量用户进行密钥传输占用过多的系统资源。

3.1 相关业务流程

3.1.1 认证流程

认证流程发生在终端开启客户端后,发现本地不存在共享密钥 Ks 的情况下,会触发 GBA 认证流程^[3]。

3.1.2 业务密钥分发流程

eMBMS 是基于 USIM(3GPP 中给定了 3 种卡的形式:SIM、ISIM 和 USIM,每种卡的鉴权方式存在一些不同,但 LTE 环境下国内各运营商均采用 USIM 卡的形式,所以这里只选取 USIM 卡的方式)实现业务密钥的分发。有两种方式:终端请求方式和网络主动推送方式。

其中终端请求方式主要用于终端新加入广播业务时向 BM-SC 索要业务密钥的过程;网络主动推送方式主要用于平台侧的业务密钥更新、节目更新等过程。

3.2 业务安全机制设备要求及建议部署方案

从上述的描述当中可以看到 eMBMS 两级密钥的安全

机制,能很好地确保广播业务的安全私密性,并在一定程度上控制了网络的额外消耗。但是对于平台和终端侧而言,要实现 eMBMS 的安全机制还是需要增加额外的功能需求。下面就这两方面进行介绍。

3.2.1 对平台的要求

对于平台来说,在 eMBMS 系统最重要的作用是完成业务指南的生成与分发、业务管理和内容管理、用户订购关系管理与计费等功能。但如果需要实现 eMBMS 的二级密钥安全机制,就需要额外增加平台的功能模块以及相应接口。具体来讲,主要是增加功能模块 BSF (bootstrapping server function, 引导服务功能) 以及其与 HSS 的接口 Zh、与终端的接口 Ub, 增加 BM-SC 的安全子功能。

(1)BSF 的主要功能是执行 3GPP GBA 体系中的 BSF 功能,根据用户的鉴权元组信息实现对用户的鉴权,并生成共享密钥 Ks,供后续终端和 NAF 适用。就 eMBMS 系统而言,如上面认证流程所述,BSF 主要是根据请求的用户标识在 HSS 处获得用户的 GUSS (GBA user security setting),并通过 AKA 协议完成对终端的认证,最终得到共享密钥 Ks。

(2)Ub 是终端与 BSF 之间的接口,主要功能是提供终端与 BM-SC 之间的双向鉴权以及共享密钥的传输。

(3)Zh 是 BSF 与 HSS 之间的接口,主要功能是获取用户的鉴权数据与 GUSS 数据,用于后续的认证过程中。

(4)BM-SC 安全子功能主要包括了密钥请求功能和密钥分发功能。密钥请求功能主要包含了检索 GBA key、MSK 请求流程以及相关用户的用户认证等;密钥分发功能主要包含了 MTK 分发流程和 MSK 分发流程。

3.2.2 对终端 (USIM 卡) 的要求

对于终端来说,在 eMBMS 系统中主要是 eMBMS 无线信号的检索并接收,广播节目的解码并播放等功能。但如需实现 eMBMS 的二级安全机制,需要额外增加终端 (USIM 卡) 的 MGV-F (MBMS key generation and validation function, MBMS 密钥生成与验证功能) 功能模块,用于密钥的生成与认证过程;另, eMBMS 的安全机制还需要终端中间件的支持,所以需要终端芯片提供商开放其中间件,用于数据配置使其支持 eMBMS 安全机制。

3.2.3 建议部署方案

由上述的叙述中不难看出,要实现 eMBMS 的二级密钥安全机制需要在平台和终端侧做出一定程度的升级。在平台方面,实现安全机制需要通过软硬件的升级增加 BSF 功能模

块和平台安全子功能,一来增加了业务实施的成本,二来增加了部署和开展业务的复杂度;在终端方面,实现安全机制需要增加终端 (USIM 卡) 的 MGV-F 功能模块。也就是说现行的各运营商 LTE 的 USIM 卡都不能直接支持 eMBMS 的安全机制,需要更换含有 MGV-F 的 USIM 卡才能支持 eMBMS 安全机制的需求,这对于业务的开展是非常不利的。

但是如果不采用任何的安全机制, eMBMS 还是会存在一定的风险,前面已经提到,这里不再赘述。

那么对于运营商如何部署 eMBMS 的安全机制,这里建议采用分业务初期和业务成熟期两个不同的阶段来部署。

一般 eMBMS 发展初期只是在特定的区域 (如体育比赛场馆、演唱会现场等) 内试行 (据 GSA 2014 年 8 月份的报告显示,全球共有 16 个运营商正在测试或部署 eMBMS,所选用的 eMBMS 都是直播类业务),所涉及时间、范围以及使用的用户都属于可控的范围。所以为了实现业务的快速部署,此阶段不采用 eMBMS 标准的二级密钥安全机制,采用简单的客户端 (用户名、密码) 或是其他简单的认证方式来控制系统授权的用户可顺利接入,先不引入 eMBMS 的业务加密等安全机制,这样就不需要增加平台的安全功能模块,也不需要更新用户 USIM 卡。以中国电信在 2014 年南京青奥会试行 eMBMS 为例,因其是在青奥会比赛场馆内广播比赛,其业务开展的范围、试行的时间以及使用的用户都是可控的,所以其是采用客户端用户名、密码的方式来解决安全问题。

在 eMBMS 成熟期,业务范围已经大大超过初期,可能已经覆盖城市的大部分区域,业务的种类也是多种多样,签约用户也具有一定的规模。此阶段应引入 eMBMS 标准的二级密钥安全机制。确保 eMBMS 的安全,也方便运营商进行业务的管理。

4 内容保护

eMBMS 内容保护功能主要包含了流媒体加密功能和数据加密功能,目前 3GPP 的标准分别采用 SRTP (secure realtime transport protocol, 安全实时传输协议) 和 OMA DRM (digital rights management, 数字版权保护技术) V2.0-DCF (digital content format, 数字内容格式) 作为流媒体加密和数据加密的标准。

4.1 内容保护标准

(1) OMA DRM DCF

DRM 是指在网络及数字化环境下,借助加密与安全



封装技术、PKI(public key infrastructure,公钥基础设施)认证、权限管理技术等,使数字内容的权利主体获得对其客体的控制权,从而防止非授权使用,保护权利人利益的一种综合性技术体制。所涉及的相关领域包括电子书技术、流媒体技术、访问控制技术、防复制技术、内容保护等方面。

DRM 各个不同领域具有相应的子标准^[4]。MPEG4 组织在 20 世纪 90 年代就提出了内容保护的标准。到了 MPEG21 的时候,加了一个对权力描述的语言和权力数据库;在全球各主要运营商、设备商、应用提供商共同推动和参与下,成立了 OMA(开放移动联盟)组织,现已推出了 OMA DRM V2.0-DCF 标准,此标准在目前所有标准中最成熟、参与者最多、影响力最大;再一个就是 SVP(secure video processor,安全视频处理器),这个是专门对于数字电视的芯片解决方案,它的优势强调的是安全性和价格。接下来就是 DMP(digital media project,数字媒体计划)、XrML(extensible rights markup language,可扩展权利标记语言)等,这些都是近年来很有名的标准。

其中,OMA DRM 规范主要包括 DRM 系统、数字内容封装和版权描述 3 部分^[5]。

系统部分:DRM 关注消息交互、密钥交换以及设备管理等。

数字内容封装部分:数字内容的封装格式和一些与使用相关的头信息。

版权描述语音部分:定义对数字内容使用的限制、许可信息和相应的密钥信息。

并且在规范中定义了基本下载、超级分发、流媒体等几个常用的消息流程。其中在内容分发和基本下载的过程中规范专门提及了针对移动数字内容(如音乐、软件、文本等)的下载。

(2)SRTP

SRTP(secure realtime transport protocol,安全实时传输协议)是在解决 VoIP 网络的不安全性的前提下产生的,在 RTP(realtime transport protocol,实时传输协议)的基础上所定义的一个协议,旨在为单播和多播应用程序中的实时传输协议的数据提供加密、消息认证、完整性保证和重放保护^[6]。

4.2 使用场景

流媒体加密技术通常用于 eMBMS 流媒体分发中的流媒体加密,而数据加密技术一般用于 eMBMS 数据文件

分发业务的数据加密。

流媒体分发是指内容提供商将在任何地方的视频(内容包括实况转播以及手机电视)发送至 eMBMS 业务平台,再由业务平台将视频内容通过 eMBMS 多播频道传输至基站,最后由基站广播至开通了 eMBMS 的用户终端进行播放。对于内容保护,BM-SC 收到内容提供商的音视频内容后,使用 SRTP 对内容进行加密,然后发送给 MBMS GW,其中 SRTP 的密钥包含在 MTK 中。

文件分发是指用户终端软件的下载更新。利用 eMBMS 的广播特性,终端软件发布者可以租用 eMBMS 多播频道进行智能终端应用软件、物联网终端软件等的更新。由发布者将更新软件发送至 eMBMS 业务平台,再由业务平台将更新软件的数据通过 eMBMS 多播频道传输至基站,最后由基站广播推送至开通了 eMBMS 的用户终端进行软件更新。对于内容保护来说,BM-SC 收到数据文件后,使用 OMA DCF 协议对数据进行加密,然后使用 FLUTE 协议^[7]把加密后的数据文件发送给 MBMS GW。

4.3 内容保护机制设备要求及建议部署方案

从上述描述可以看到,SRTP 和 OMA DRM DCF 作为 eMBMS 的流媒体加密和数据加密的标准,能够很好地保护广播业务的内容;而其密钥又包含在原有的 MTK、MSK 中,对网络没有额外的消耗。但是对于平台和终端侧而言,要实现 eMBMS 的内要保护机制需要增加额外的功能需求。下面就这两方面进行介绍。

4.3.1 对平台的要求

对于平台来说,要实现 eMBMS 的内容保护,主要需要支持 SRTP 和 OMA DRM DCF 两种协议对相关 eMBMS 内容进行加密。所以,对 BM-SC 新的功能要求如下。

- 增加 BM-SC 的内容加密功能,能使用 SRTP 和 OMA DRM DCF 协议加密 eMBMS 节目内容。
- 增加 BM-SC 点对点的文件修复功能。当终端在数据下载过程发现从广播信号中接收的某些数据分块错误时,将向 BM-SC 发送 HTTP 消息以请求这些数据分块,BM-SC 收到终端请求后将以单播的形式向其发送数据分块。

4.3.2 对终端的要求

因为内容保护的密钥是包含在原有的 MTK、MSK 中,所以内容保护机制对终端的要求与业务安全中类似,详见第 3.2.2 节,这里不再赘述。

4.3.3 部署建议

由上述的叙述可知,要实现 eMBMS 的内容保护机制需要平台侧和终端侧做一定程度的升级,与业务保护类似。

所以建议运营商部署 eMBMS 的内容保护机制的过程分两步走:业务初期和业务成熟期。

一般 eMBMS 发展初期只是在特定的区域(如体育比赛场馆)内试行,所涉及的用户不会太多。为了实现业务的快速部署,此阶段不采用 eMBMS 的内容保护机制,就只通过简单的业务认证来确保内容的安全。

在 eMBMS 成熟期,业务范围已经大大超过初期,签约用户也具有一定的规模。此阶段应引入 eMBMS 标准的内容保护机制来确保 eMBMS 的安全,也方便运营商进行内容的管理。

5 结束语

本文分析研究了 eMBMS 安全机制(包含业务安全机制和内容保护机制)。通过对 3GPP 中 eMBMS 安全机制的标准架构、密钥体系等方面的分析,引出 eMBMS 对原有设备的新增要求以及运营商部署建议等方面的内容。

基于该技术研究,电信运营商可分时部署 eMBMS 安全机制,更好地发展 eMBMS 业务。

参考文献

- 1 3GPP TS 33.246. Security of Multimedia Broadcast/Multicast

Service (MBMS)(Release 11), 2012

- 2 中国通信标准化协会. YD/T 1785-2008 移动多媒体广播业务总体技术要求, 2008
- 3 3GPP TS 33.220. Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture(GBA)(Release 12), 2013
- 4 吕井华. 移动数字出版版权保护使用控制技术研究. 北京邮电大学硕士学位论文, 2013
- 5 OMA-RD-BCAST-V1-0-20080226-C. Mobile Broadcast Services Requirvemonts Candidiate Version 1.0, 2008
- 6 RFC 3711. The Secure Real-Time Transport Protocol (SRTP), 2004
- 7 3GPP TS 26.346. Multimedia Broadcast/Multicast Service (MBMS); Protocols and Codes(Release 12), 2013

[作者简介]



周毅,男,中国电信股份有限公司上海研究院平台技术部工程师,主要研究方向为 LTE 核心网、eMBMS 等。

刘稼,男,中国电信股份有限公司上海研究院平台技术部高级工程师,主要研究方向为 LTE 核心网等。

史敏锐,男,中国电信股份有限公司上海研究院平台技术部高级工程师,主要研究方向为 LTE 核心网等。

(收稿日期:2014-11-03)

·简讯·

2014 中国未来网络发展与创新论坛暨全球 SDN 开放网络高峰会议南京开幕

2014 年 12 月 8 日至 9 日,2014 中国未来网络发展与创新论坛暨全球 SDN 开放网络高峰会议在南京召开。

由于互联网对推动社会发展起到了重要作用,因此我国对抢占未来网络发展先机也给予了高度重视。2013 年 8 月,全球首家 SDN 测试认证中心(SDNCTC)在北京揭牌成立,并面向全球开展 OpenFlow 测试认证服务。

2014 年 12 月 8 日,2014 未来网络与 SDN 峰会成功举办,得到全球互联网之父 Vint Cerf、ONF 执行主席 Dan

Pitt、中国工程院陈左宁、邬贺铨院士等国内外顶级专家的大力支持。同时,中国联通、中国移动、中国电信等主流运营商,英特尔、思科等设备商以及全国各大高校院长等齐聚大会,共商未来网络产业发展。

在峰会上,全球顶级专家围绕未来网络体系架构、融合及业务创新进行了深入探讨。

为了集聚更多国内学者共同致力于未来网络事业的发展,本次论坛面向学术界广泛征集网络体系架构、软件定义网络(SDN)等领域最新研究成果以及有关新应用与新方法的论文、案例等。本次征文共收到 300 余篇论文,经过多项评审,80 余篇高水平论文被录用。这对推动我国未来网络业务创新具有重要意义。