



# 基于 non-IP+SCEF 技术增强物联网终端安全性的研究

何晓, 黄海

(中国电信股份有限公司广州研究院, 广东 广州 510630)

**摘要:**研究了智能终端安卓系统,提出了基于证书链验证机制的智能终端安卓系统安全加固方案,并对安卓原生系统所表现出来的安全问题进行深入的分析与研究,比较了采用安全加固的系统较之安卓原生系统在安全性上表现出的优势。通过结合证书链机制,以完整性验证为核心的安全架构,能够达到最大限度保护智能终端安全的目标。

**关键词:**物联网;安全;非 IP;服务能力开放功能

**中图分类号:** TN929

**文献标识码:** A

**doi:** 10.11959/j.issn.1000-0801.2017035

## Research on enhancing the security of IoT terminals based on non-IP and SCEF technology

HE Yao, HUANG Hai

Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

**Abstract:** Android intelligent terminal system was studied, and Android security reinforcing scheme of intelligent terminal based on certificate chain authentication mechanism was put forward. The security problems that Android system showed were analyzed, and the advantage of the Android security reinforcing scheme was compared with Android system. The certificate chain authentication mechanism played a critical role as protecting the core of the terminals against some intrusion attacks in the security phases.

**Key words:** IoT, security, non-IP, SCEF

### 1 引言

随着物联网技术与业务的迅速发展,针对物联网的安全威胁也日益增大。2016年第三季度,网络信息安全处于高防御级别的美国,仍然发生了两起利用海量物联网终端实施大规模 DDoS 攻击的事件,传统 IP 网络的安全威胁已延伸到物联网领域,敲响了物联网终端安全的警钟。

如何防止海量的物联网终端受到攻击和感染,为非频繁小数据业务类型的物联网终端构建安全防护体系,避免物联网终端僵尸化成为物联网发展过程中不可回避的问题。

### 2 DDoS 攻击事件分析

分析 2016 年发生在美国的 DDoS 攻击事件,不难发现以下问题。

#### 2.1 攻击事件反映出的问题

(1)号称安全防护能力最强的国家也难以防止攻击事件的发生

网站以及美国 DNS 服务器提供商 Dyn 的 DNS 服务,均受到了基于 IP 网络的 DDoS 攻击,攻击来源于受 Mirai 恶意软件感染的约 5 万台物联网终端组成的僵尸网络,攻

击流量高达 600 Gbit/s,导致服务中断数小时。虽然美国的网络防攻击能力处于世界领先水平,但也未能有效防止攻击事件的发生,近半个美国的大型 Web 网站服务受到这次攻击事件的影响。可见,利用海量物联网终端实施攻击的威胁相当巨大。

### (2) 传统 IP 网的安全威胁已延伸到物联网领域

有别于以往手机类及消费电子类智能终端的攻击,黑客不再局限于以用户个体的隐私窃取、支付钓鱼、诈骗以及勒索等直接获利为目标,而是把目光延伸到物联网终端,其目的很明确,就是把海量的物联网终端构建成巨型的僵尸网络,用以实施大型 DDoS 攻击,此类攻击事件往往伴随着政治目的,其影响已上升到社会和国家层面,一旦蔓延,造成的恶劣影响和破坏力不容忽视。

### (3) 受感染终端大多为中国设备

在这些受感染的物联网终端中,大部分是中国大华和雄迈公司生产的网络摄像头设备。可见,防攻击能力相对薄弱的国内物联网终端已成为全球黑客的目标,如果类似攻击发生在国内,情况可能更为严重。

## 2.2 攻击原理

综合分析,不同类型的智能终端或物联网终端都有一个共同特征,就是它们都运行着 IP 协议栈并直接与 IP 网络通信,暴露在 IP 网络上。黑客通过 IP 网络,可以轻易发

现并攻击它们,终端一旦被攻陷,就加入了僵尸网络,成为攻击网络的一员,随时听候黑客的差遣。黑客的攻击方式一般有如下两种。

- 黑客通过 IP 网络直接远程攻击终端,原理如图 1 所示。
- 黑客通过近距离或本地攻击,先入侵少量终端,以此为跳板,继而攻击同一 IP 子网下的其他终端,原理如图 2 所示。

利用传统的安全防御措施,无论是为操作系统和应用程序打补丁、关闭不必要的端口,还是做好账号/密码管理等,都不能完全弥补采用 IP 通信带来的缺陷。

电信运营商即将大规模开展物联网业务,使用 IP 技术进行通信的终端同样面临上述安全问题。既然专业的安全防御方法不能从根源上解决问题,那么能否换一种思路,从通信网络的架构切入,挖掘容易被忽略但又能把终端在网络中隐藏起来的方案,黑客找不到这些终端,自然就无法实施攻击了。

## 3 安全防御方案

3GPP R13 版本关于 NB-IoT (narrow band internet of things, 窄带物联网) 和 eMTC (enhanced machine type communication, 增强机器类通信) 基于蜂窝网的物理网通

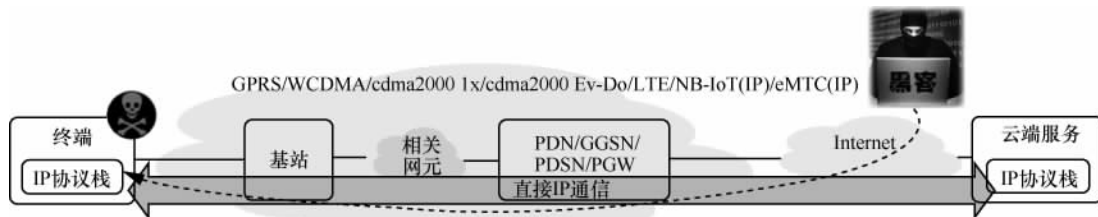


图 1 基于 IP 网络直接远程攻击终端示意

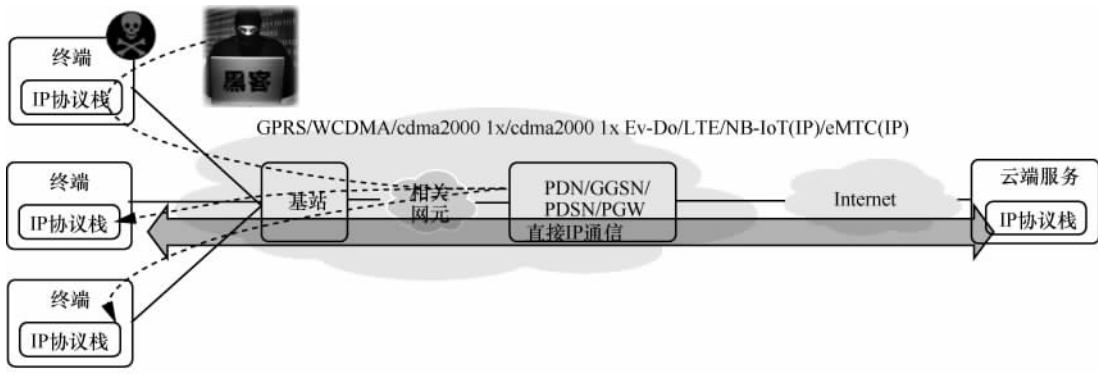


图 2 基于 IP 子网跳板攻击终端示意



信系统规范中,定义了一项新的数据通信技术——non-IP 技术。non-IP 技术在 NB-IoT 中是必选,在 eMTC 中是可选。non-IP 数据重要特征是无 IP 分组头,传输效率高,更重要的是,终端可以完全不需要 IP 协议栈,这意味着终端可以不暴露在 IP 网络上,从而避免一切基于 IP 技术的攻击和远程控制,也意味着黑客没有办法直接驱使这些海量的非 IP 化的终端发动基于 IP 网络的 DDoS 攻击,从根源上遏制了这些终端进入僵尸网络。黑客常年以来积累的诸如端口扫描、脚本注入、SQL 注入、密码穷尽等强大的攻击工具集(黑客的“核武器库”),都将派不上用场,因为它们都是基于 IP 技术的,黑客要破解 non-IP,不得不从零开始研究新的入侵手段和攻击方案。因此,non-IP 的使用,将为物联网的大规模商用发展赢得相当长的一段安全时间窗口。下面以 NB-IoT 系统为例,详细介绍这种新型的防御技术,eMTC 系统与之相似。

3GPP R13 新增了控制面优化(control plane optimization, CP 优化)和用户面优化(user plane optimization, UP 优化)两种数据传输方案:CP 优化方案通过 NAS 信令传输数据,减少了终端、空口和核心网的信令开销,并为 non-IP 的数据传输增设了 SCEF(service capability exposure function, 服务能力开放功能)网元,SCEF 在 NB-IoT 中的具体网络位置如图 3 所示;UP 优化方案增加了 RRC 挂起和恢复两

种状态,减少了空口信令交互。

在终端附着网络的过程中,会携带建立数据通道的参数,这决定了终端在完成附着后,以何种类型的方式进行数据通信,每种方案对应的参数配置和数据路径见表 1。

由表 1 可知,方案 1、方案 4 和方案 7 属于传统 IP 通信方式,终端获得 IP 地址并直接接入 IP 网络;方案 6 只提供短信通信方式,不涉及数据通信,不在本文研究范围内;方案 2 和方案 5 都属于 non-IP 通信,网络出口点是 PGW;方案 3 也属于 non-IP 通信,但网络出口点是 SCEF。下面介绍与 IP 和 non-IP 相关的 3 类方案的机制、优点、缺点、安全性和适用场景。

### 3.1 控制面或用户面的 IP 通信方案(方案 1、方案 4 和方案 7)

该类方案通过控制面 NAS 信令或者用户面传输用户数据,NAS 层单独或 NAS+PDCP 层共同负责用户数据安全,PGW 为终端分配 IP 地址,终端具有 IP 协议栈并获得 IP 地址,网络出口点是 PGW,终端直接与 SCS/AS 进行 IP 通信。终端与云端直接 IP 通信方案如图 4 所示,该类方案的优/缺点、安全性及适用场景介绍如下。

- 优点:基于传统 IP 通信,终端侧与云端应用开发门槛低;经过优化的控制面和用户面方案,可减少终端、空口和核心网的信令消耗。
- 缺点:IP 技术的开放性导致运营商仍只承担通信管

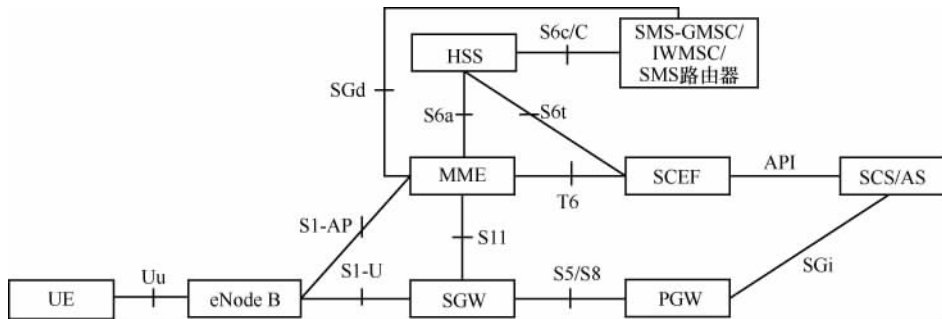


图 3 NB-IoT 网络架构

表 1 附着过程建立数据通道参数与数据路径对应

| 方案序号 | 附着参数                                                              | 数据路径                                   |
|------|-------------------------------------------------------------------|----------------------------------------|
| 1    | PDN connection: C-plane; IP type = IP; APN = “PGW PDN” (EBI)      | UE-eNode B-MME-SGW-PGW-SCS/AS          |
| 2    | PDN connection: C-plane; IP type = non-IP; APN = “PGW PDN” (EBI)  | UE-eNode B-MME-SGW-PGW-SCS/AS          |
| 3    | PDN connection: C-plane; IP type = non-IP; APN = “SCEF PDN” (EBI) | UE-eNode B-MME-SCEF-SCS/AS             |
| 4    | PDN connection: U-plane; IP type = IP; APN = “PGW PDN” (EBI)      | UE-eNode B-SGW-PGW-SCS/AS              |
| 5    | PDN connection: U-plane; IP type = non-IP; APN = “PGW PDN” (EBI)  | UE-eNode B-SGW-PGW-SCS/AS              |
| 6    | attach without PDN connection: SMS only(no EBI)                   | UE-eNode B-MME-SMS-GMSC/IW MSC/SMS 路由器 |
| 7    | legacy EPS S1-U PDN connection: IP; (EBI)                         | UE-eNode B-SGW-PGW-SCS/AS              |

道的角色,难以从海量终端和数据中深挖价值。

- 安全性:终端直接与IP网络通信,易被黑客发现并攻击。
- 适用场景:基于控制面的方案适合非频繁小数据传输,基于用户面的方案适合各种类型的数据传输。

### 3.2 控制面或用户面的 non-IP 隧道通信方案 (方案 2 和方案 5)

该类方案通过控制面 NAS 信令或者用户面传输用户数据,NAS 层单独或 NAS+PDCP 层共同负责用户数据安全,PGW 为终端分配 IP 地址但不分发给终端(基于 UDP/IP 的 PtP 隧道),或者不为终端分配 IP 地址(其他类型 PtP 隧道),终端不需要 IP 协议栈且不需要获得 IP 地址,网络出口点是 PGW,终端经过 PGW 与 SCS/AS 通过 IP 隧道通信,不直接进行 IP 通信。控制面或用户面 non-IP 传输+PGW IP 隧道方案如图 5 所示,该类方案的优/缺点、安全性及适用场景介绍如下。

- 优点:使用 non-IP 技术,用户数据无 IP 分组头,转发效率高;经过优化的控制面和用户面方案,可减少终端、空口和核心网的信令消耗。

少终端、空口和核心网的信令消耗。

- 缺点:终端侧与云端应用需要适应新的隧道开发模式;隧道转发的模式令运营商仍只负责管道运营。
- 安全性:PGW 与 SCS/AS 间建立授信隧道通信,终端不直接与 IP 网络进行通信,有效隐藏终端,不易受到黑客攻击。
- 适用场景:基于控制面的方案适合非频繁小数据传输,基于用户面的方案适合各种类型的数据传输。

### 3.3 控制面 non-IP 能力开放方案 (方案 3)

该类方案通过控制面 NAS 信令传输用户数据,NAS 层负责数据安全,终端不需要 IP 协议栈且不需要获得 IP 地址,网络出口点是服务能力开放单元 SCEF,终端经过 SCEF 与 SCS/AS 进行 API 通信。控制面 non-IP 传输+SCEF 服务能力开放方案如图 6 所示,该类方案的优/缺点、安全性及适用场景介绍如下。

- 优点:使用 non-IP 技术,用户数据无 IP 分组头,转

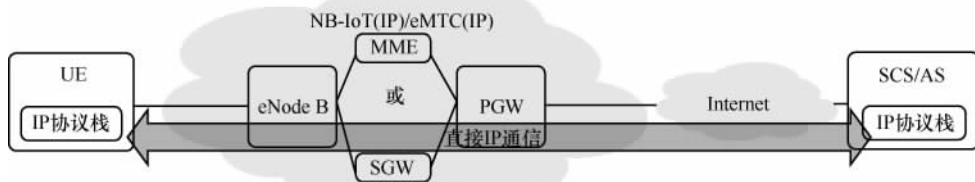


图 4 终端与云端直接 IP 通信方案

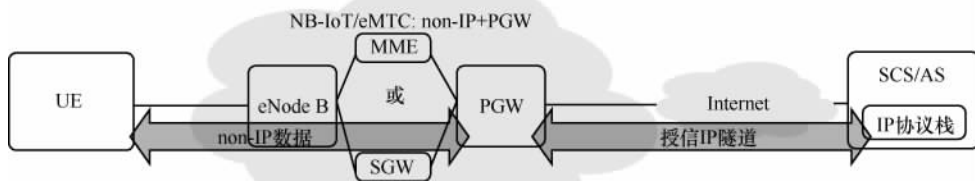


图 5 控制面或用户面 non-IP 传输+PGW IP 隧道方案

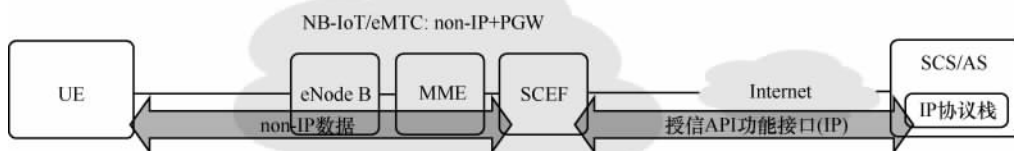


图 6 控制面 non-IP 传输+SCEF 服务能力开放方案



发效率高;减少了终端、空口和核心网信令消耗;SCEF汇聚了 non-IP 的终端和数据,并以 API 形式向云端应用方提供服务,而非直接把数据转发出去,运营商在这个节点上可以沉淀数据并进行大数据分析,从中挖掘出具有商业价值的信息,由于使用了 API 形式开放服务,而不是简单的数据转发,为实施更灵活、更多样化的资费策略奠定了基础,运营商不再沦为纯管道的角色。

- 缺点:终端侧与云端应用需要适应新的 API 开发模式。
- 安全性:SCEF 引入了 non-IP 数据传输授权检查技术,SCEF 根据终端的外部标识或 MSISDN,检查是否为该终端创建了 SCEF 承载。SCEF 检查请求 non-IP 数据投递的 SCS/AS 是否被授权允许发起 non-IP 数据投递,并且检查该 SCS/AS 是否已经超出 non-IP 数据投递的限额(如 24 h 内允许 1000 byte),或已经超出速率限额(如 100 byte/h)。只有当上述安全检查通过后,SCEF 才做后续的投递工作。基于以上的安全机制,SCEF 可以安全地对 3GPP 网络中的 non-IP 数据与互联网云端应用方的 IP 数据进行转换,有效地在 IP 网络中隐藏了终端,终端不直接与 IP 网络通信,而是在 IP 网络中隐身了,黑客难以对其实施攻击。
- 适用场景:非频繁小数据传输。

### 3.4 方案对比分析

对比以上几类方案,在安全性、传输效率、信令优化、开放性、产业成熟度以及对运营商利弊等方面各有优缺点。运营商希望选择一种既能解决安全问题,也能在商业模式上打破运营商纯管道运营角色困局的技术方案。

物联网主要的应用场景如自动抄表、环境监控、车场管理、智慧城市、物流跟踪等,其通信特征主要是非频繁的小数据传输,此类终端数量和业务规模相当巨大,并涵盖了大多数的物联网业务应用场景,运营商应牢牢地抓住这类业务。运营商面对每一次新技术选择时,除了满足高效快速开展业务外,还要兼顾网络和业务可持续发展,过于开放的技术架构虽然能“短平快”地产生规模效应,但也意味着后续商业价值的分流。

综上所述,基于 IP 通信的方案(方案 1、方案 4 和方案 7),终端暴露于 IP 网络中不能满足所需要的安全性要求;

基于 non-IP 的隧道方案(方案 2 和方案 5),non-IP 技术能在网络中很好地隐藏终端,虽能满足安全性要求,但隧道模式无法帮助运营商突破纯管道运营者的困局。

基于控制面 non-IP 的能力开放方案(方案 3),non-IP 技术能在网络中很好地隐藏终端,SCEF 也承担了 non-IP 网络与 IP 网络之间的安全转换角色,能有效防御来自 IP 网络的恶意刺探和攻击,因此,基于 non-IP+SCEF 的方案能很好地满足安全要求,也能满足物联网非频繁小数据的主要业务需求。从网络位置上看,SCEF 的定位近似但不等同于物联网连接管理平台或物联网云服务平台,也就是说,对于还没拥有成型的连接管理平台或云服务平台的运营商,SCEF 也是一种选择,可帮助运营商突破纯管道运营的困局,扩大管道业务以外的利益。non-IP 和 SCEF 都已经在标准层面得到定稿,只要运营商明确需求并推动产业链参与跟进,就能有效降低开发与运营的门槛。

## 4 结束语

2016 年,运营商开始规模建设并试点物联网业务,物联网终端的快速发展以及网络扩张所带来的安全隐患不可忽视,需要从终端、网络 and 平台等各方面寻求综合解决方案,虽然目前 IP 技术仍是主流通信技术,但从发生的安全大事件来看,通过各种基于 IP 的传统防御手段遏止物联网终端僵尸化,仍有很大的不确定性。因此,通过在终端、空口和核心网启用 non-IP 技术,在网络出口点部署 SCEF 网元相结合的方案,不仅是一种通信方案,还将是解决物联网终端僵尸化的安全方案之一,该思路开拓了 NB-IoT 和 eMTC 在安全领域的全新研究方向,为物联网的安全发展赢得时间窗口。同时,运营商可基于这种物联网安全解决方案,打造“安全物联网”的品牌,实现安全差异化,吸引更多的行业用户。

## 参考文献:

- [1] 3GPP. Architecture enhancements to facilitate communications with packet data networks and applications (release 13): 3GPP TS 23.682[S/OL]. (2016-12-10)[2016-12-10]. [https://www.baidu.com/link?url=ltCYaC0JN0\\_NkFgyGi6I33\\_PViwmH78SQ3ytlrOBdA9NEUVHVB9qbNW6eNBN\\_9yqcIZGfK\\_8TWAXU5C-9eGbH-VOK&wd=&eqid=de14\\_a62d0008d\\_4210000000358844583](https://www.baidu.com/link?url=ltCYaC0JN0_NkFgyGi6I33_PViwmH78SQ3ytlrOBdA9NEUVHVB9qbNW6eNBN_9yqcIZGfK_8TWAXU5C-9eGbH-VOK&wd=&eqid=de14_a62d0008d_4210000000358844583).
- [2] 3GPP. General packet radio service (GPRS) enhancements for

- evolved universal terrestrial radio access network (E-UTRAN) access (release 13): 3GPP TS 23.401 [S/OL]. (2008-10-10)[2016-12-10]. [http://www.etsi.org/deliver/etsi\\_TS/123400\\_123499/123401/08.03.00\\_60/ts\\_123401v080300p.pdf](http://www.etsi.org/deliver/etsi_TS/123400_123499/123401/08.03.00_60/ts_123401v080300p.pdf).
- [3] 3GPP. Non-access-stratum (NAS) protocol for evolved packet system (EPS); stage 3 (release 13): 3GPP TS 24.301[S/OL]. (2009-03-10)[2016-12-10]. <http://max.book118.com/html/2015/1019/27540606.shtm>.
- [4] 3GPP. Evolved universal terrestrial radio access (E-UTRA) and evolved universal terrestrial radio access network (E-UTRAN); overall description;stage 2 (release 13):3GPP TS 36.300[S/OL]. (2007-12-10)[2016-12-10]. [http://xueshu.baidu.com/s?wd=paperuri:\(be81e93a0601e10eb42f7c072c2c2b6a\)&filter=sc\\_long\\_sign&sc\\_ks\\_para=q%3DEvolved+Universal+Terrestrial+Radio+Access+%28E-UTRA%29+%3B+LTE+Physical+Layer-General+Description&tn=SE\\_baiduxueshu\\_c1gjeupa&ie=utf-8&sc\\_us=5075368087671280276](http://xueshu.baidu.com/s?wd=paperuri:(be81e93a0601e10eb42f7c072c2c2b6a)&filter=sc_long_sign&sc_ks_para=q%3DEvolved+Universal+Terrestrial+Radio+Access+%28E-UTRA%29+%3B+LTE+Physical+Layer-General+Description&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_us=5075368087671280276).
- [5] 3GPP. Evolved universal terrestrial radio access (E-UTRA);radio resource control (RRC);protocol specification(release 13): 3GPP TS 36.331 [S/OL]. (2007-12-10)[2016-12-10]. <http://xueshu>.

[baidu.com/s?wd=paperuri:\(be81e93a0601e10eb42f7c072c2c2b6a\)&filter=sc\\_long\\_sign&sc\\_ks\\_para=q%3DEvolved+Universal+Terrestrial+Radio+Access+%28E-UTRA%29+%3B+LTE+Physical+Layer-General+Description&tn=SE\\_baiduxueshu\\_c1gjeupa&ie=utf-8&sc\\_us=5075368087671280276](http://baidu.com/s?wd=paperuri:(be81e93a0601e10eb42f7c072c2c2b6a)&filter=sc_long_sign&sc_ks_para=q%3DEvolved+Universal+Terrestrial+Radio+Access+%28E-UTRA%29+%3B+LTE+Physical+Layer-General+Description&tn=SE_baiduxueshu_c1gjeupa&ie=utf-8&sc_us=5075368087671280276).

#### [作者简介]



何峣(1977-),男,中国电信股份有限公司广州研究院高级工程师,主要研究方向为物联网终端通信、安全、测试技术等。



黄海(1973-),男,中国电信股份有限公司广州研究院高级工程师,主要研究方向为视频流媒体、物联网相关技术及应用。