



LTE 下一代中继的安全

朱红儒, 齐旻鹏

(中国移动通信有限公司研究院 北京 100053)

摘要:介绍了 LTE 中继的背景与面临的威胁,对中继中存在的安全问题进行分析,并提出了相应的安全需求。在此基础上,提出了中继的安全解决方案,通过这些安全解决方案,可以有效地提升中继的安全防护能力。

关键词:无线通信;安全;中继;认证;加密

doi: 10.3969/j.issn.1000-0801.2013.10.024

Security Analysis of Relay in LTE-Advanced

Zhu Hongru, Qi Minpeng

(China Mobile Research Institute, Beijing 100053, China)

Abstract: The background and the threats of relay were introduced. The security problems about relay node and related security requirements were analyzed. Based on these requirements, some security solutions were made. These solutions can make relay more secure.

Key words: wireless communication, security, relay, authentication, encryption

1 概述

LTE-Advanced 是 LTE 技术的后续演进。在 LTE-Advanced 中,3GPP 提出了几种关键技术,其中,接力传输即指在传统蜂窝网的基础上对城市热点地区容量进行优化,并且需要扩展盲区、地铁及农村的覆盖。

中继(relay)是 LTE-Advanced 系统中为了满足接力传输提出的一个功能特性。中继就是通过基站在移动台之

间增加中间节点——中继站(relay node),对基站的发射信号或者终端的发射信号进行再生、放大处理后,再转发给终端或者基站,甚至下一个中继站,从而提高信号传输的质量和可靠性的网络增强型技术。中继不但可以为蜂窝网络带来容量提升、覆盖扩展等性能增强,更可以提供灵活、快速的部署,弥补回传链路缺失的问题,以响应网络快速部署的需求。

中继和 LTE 在结构上的区别如图 1 所示。

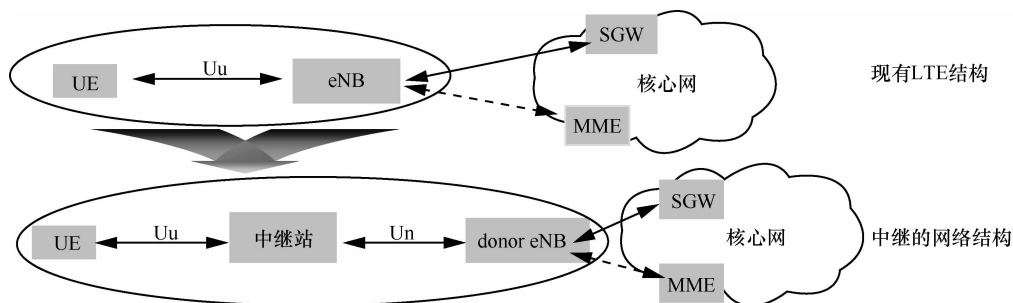


图 1 LTE 和中继的结构区别

中继有两个功能,从 UE 来看,中继就是一个 eNB;从 LTE 的 eNB 来看,中继就是一个 UE。其中 Un 口是中继到 donor eNB 之间的接口。donor eNB 是未加中继前与 UE 直接相连的 eNB;添加中继后与中继站通过无线连接;而中继在 donor eNB 和 UE 之间,为 UE 和 donor eNB 间消息传输提供中继作用。

从协议栈的角度来看,控制面和数据面的展示如图 2 所示。

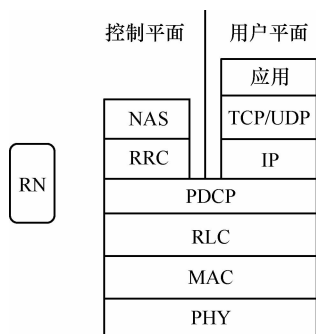


图 2 中继的协议栈

综上所述,中继的结构如图 3 所示。

中继的应用能大大帮助 LTE 时代的偏远地区、热点地区以及高速移动中的负载问题,对人们的生活大有裨益。

2 中继面临的安全威胁

当在 LTE-Advanced 系统中引入中继站后,它将面临以下问题。

(1) 伪装的中继对接入的用户进行攻击

攻击者从合法的中继中获取 UICC 卡并插入非法的中继上,如图 4 所示。由于没有对中继设备进行设备认证,网

络不能检测出恶意中继,这也就使得用户可以附着到恶意中继上,用户的安全也就受到破坏。因此执行中继设备认证是必要的。

(2) 中继和 donor eNB 之间 Un 接口上的中间人攻击

在这种攻击中,中间人节点被插入中继和 donor eNB 之间,中间人节点是由从合法中继上获取的合法 UICC 充当中间人,而合法中继设备上的 UICC 卡则是攻击者伪造的 UICC 卡,即合法的 UICC 卡插到中间人节点上,如图 5 所示。

合法中继将连接到中间人节点,中间人节点再连接到合法的 donor eNB,中间人节点可以透明地传输、接收、查看、更改合法中继和合法 donor eNB 之间的流量信息,而合法的中继和 donor eNB 都不会察觉到。因此连接到此中继上的所有用户都将受到破坏。即使用户相关密钥受到服务于 UE 的 MME 和中继之间的 IPSec 保护,中间人节点依然能够侦听、更改、插入用户的流量信息。

(3) 对中继与 donor eNB 之间的 Un 接口上流量信息的攻击

中继和 donor eNB 间的接口是基于 LTE 空口的标准,中继和 donor eNB 间的所有流量需要有可选的机密性保护,但中继和 donor eNB 间的所有非 RRC 信令信息则没有完整性保护。机密性保护可以用于接口上的流量信息的加密保护,但如果此安全保护不适用于中继节点,则需要考虑其他提供机密性保护的方法。此种保护方式对于来自 UE 的用户流量可以接受,但对于中继发送给网络的信令信息(S1-AP 或 X2-AP 接口)则不能接受。这意味着对于 Un 接口的安全保护,既需要对标准的 E-UTRAN 中

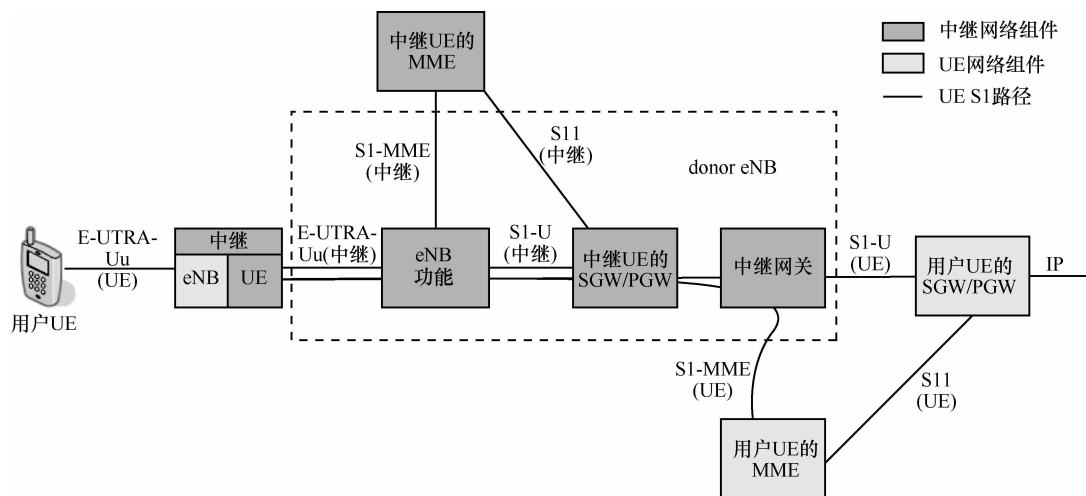


图 3 中继的结构

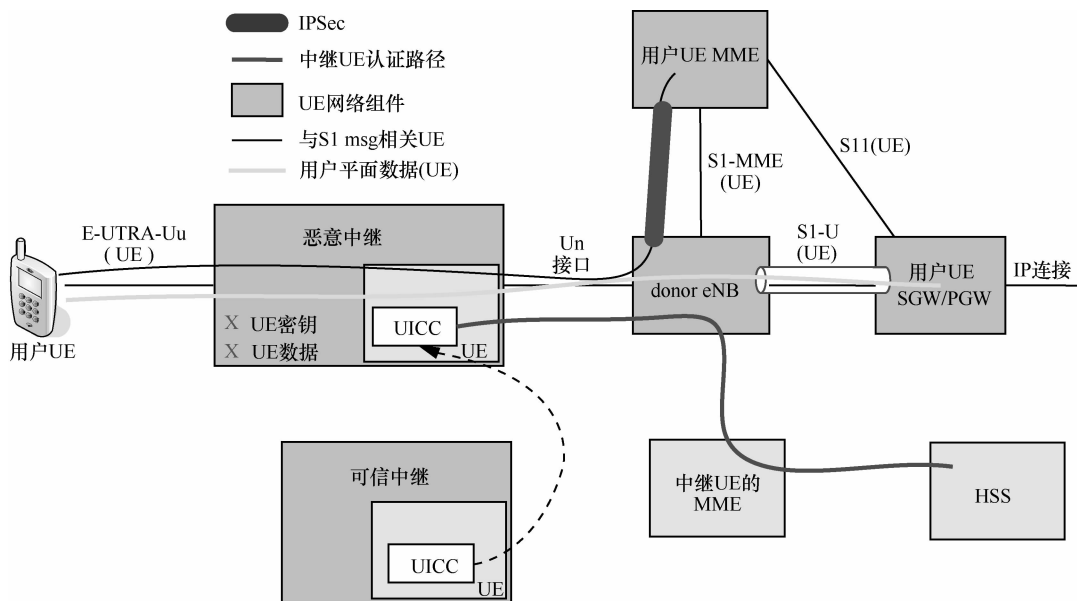


图4 攻击者伪装成中继发起对接入用户的攻击

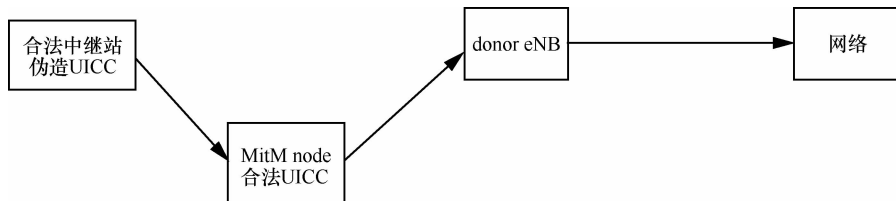


图5 中间人攻击

UE-eNB 接口的保护进行增强, 还需要对 Un 接口上的 S1-AP、X2-AP 接口信息加以保护。

(4) 伪造的中继对网络的攻击

恶意中继能够将如下 4 种类型的消息插入网络中。

- MME 和中继之间的 NAS 信令。由于恶意 UE 也会发起同样的攻击, 因此对于中继安全性分析来说并不重要。
- S1-AP 或 X2-AP 信令。
- 代表用户插入的数据。
- 用户面数据获得免费的 IP 连接。

可以通过在上述类型消息被接收前加强中继设备认证来减轻此种威胁, 也可通过其他方式来减轻此类威胁。

(5) 中继和 UICC 间的接口攻击

中继和 UICC 间的接口数据没有受到保护, 这意味着尽管攻击者无法破坏中继, 也可以通过中继与 UICC 间的接口转发获得密钥材料。攻击者获得这些密钥, 即能够获得通过这些密钥保护的数据, 也能够将插入的伪造数据利用这些密钥保护。特别地, 攻击者可以建立威胁(2)中所述

的中间人节点。

(6) 中继平台控制

除了 MME 与 UE 间的 NAS 信令消息外, 所有的消息都可以明文进入中继平台。因此, 一旦攻击者控制了中继平台, 则监听、篡改消息都是可行的。

(7) DoS 攻击

当攻击者移走 UICC, 没有 UICC 的中继则不能被网络认证, 因此合法的中继不能接入网络提供服务。攻击者也可以将 UICC 插入其他的中继中, 那么接入网络的拓扑变化也会引起其他 eNB 的接口问题。

(8) 初始附着后停留在 UE 状态

恶意的中继在执行完认证后停留在 UE 状态, 既不离网也不发起 S1 接口建立流程。这种中继不履行 eNB 的职能, 只作为 UE 接收或请求网络服务。此种威胁如不加以防范, 将导致计费问题。

3 中继的安全需求

由于中继面临着上述问题, 为了解决这些问题, 中继在使用时应当满足以下安全需求。

- 认证。中继在接入网络时应当与网络侧进行双向认证。认证是确认中继身份的最基础保障。通过中继与网络侧的双向认证,可以有效地避免攻击者假冒中继接入网络,从而对用户和网络发起攻击。中继的认证应是基于(U)SIM 卡的认证,从而满足复用 LTE 接入认证机制的要求。
- 设备类型鉴别。网络侧应能够区分附着的终端是 UE 还是中继,以避免无线资源被滥用。识别和区分的方式可以是显式或隐式的。
- 设备绑定。中继要与(U)SIM 卡一对一绑定,防止(U)SIM 卡被非法拔出进而导致一系列的攻击。
- 接入控制。中继只有在认证通过之后才能转发和接收用户的信令和数据信息。中继应当与普通用户区分开。通过这些需求,可以有效地防止空口资源被滥用。
- 完整性。中继对传输的控制信令提供完整性保护。控制信令包括中继本身产生的 RRC、NAS 信令,也包括转发的来自于用户的 RRC、NAS 信令。通过对控制信令提供完整性保护,中继可以有效地保障信令在空口传输的有效性,保障信令不会受到篡改、伪造等攻击。
- 加密。中继对传输的信令和数据提供可选的加密保护。控制信令依然如上所述。由于中继与 donor eNB 之间传递的数据是转发的用户的信令和数据,所以对数据的加密保护主要是指对用户数据的保护。

4 中继的安全体制

为了满足上述安全需求,在中继系统中,应当采用下述安全机制。

- 基于(U)SIM 卡的认证,即复用 LTE 网络中的 AKA 认证机制。在中继接入网络时,由于从网络侧来看,它就是一个 UE,所以这时使用 LTE 网络的 AKA 认证机制,即可有效保证对中继的认证,并且可以完全使用现有系统,不需要进行改造。为防止移除或替换 UICC 卡所带来的安全威胁,应考虑对中继和 UICC 进行绑定。绑定可能是物理的,例如将 UICC 和中继焊接成为一体;也可能是逻辑的,例如在 UICC 和中继之间建立安全通道。
- 安全通道的保护。当 UICC 和中继之间通过建立安全通道的方式保证机卡绑定时,应使用 ETSI 102.484 中定义的终端设备与 UICC 卡之间的安全通道(secure channel)。出于对卡片操作系统的改动

影响考虑,ETSI 规定的 4 种机卡安全通道中选择使用基于 APDU 的安全通道方式。而机卡通道的建立需要在 UICC 与中继之间预先共享一个密钥,或者通过证书的方式来保证。

- 安全通道的建立。当使用预共享密钥时,应按照 ETSI 规范建立安全通道。当使用证书方式时,如果证书已经预置,则按照 ETSI 规范要求建立安全通道;如果证书需要在线下载,那么此时 UICC 上应当还存在一个专为证书下载提供服务的(U)SIM 应用,使得中继可以利用该(U)SIM 应用与网络相连并下载证书。
- 对中继身份类型的鉴别。在中继接入网络之前,UICC 上的(U)SIM 应用应预先在 HSS 中被配置为中继专用的(U)SIM 应用。当中继接入网络时,应在接入消息中携带设备类型,由网络侧判断完成对中继身份类型的鉴别。
- 对转发信令及数据的逐段式保护。在现有中继站架构中,用户发到中继的信令和数据需要转发给 donor eNB,然后由 donor eNB 再向其他网元转发。因此中继站转发的所有信令和数据,都需要在 donor eNB 上重新处理,即 donor eNB 需要能够看到所有中继转发的信令和数据。因此,中继转发用户的信令和数据,必须采用逐段式的保护方法,才能在 donor eNB 上解开从而得到处理。如果采用端到端的保护方式,donor eNB 将无法解密和处理。
- 对转发信令、数据的加密和完整性保护。出于处理性能的影响,中继最终选择对 AS 安全机制增强的保护方式对中继转发的控制面信令提供加密和完整性保护,对用户面提供加密保护,即在中继和 donor eNB 之间的 AS 安全上下文中增加一个用户面的完整性保护密钥,即 KUPint。并且要求 donor eNB 在发给中继的 AS SMC 命令中选定的加密算法和完整性算法将同时适用于信令和数据,但具体到每一个信令承载和数据承载,则可以独立地开启或关闭加密和/或完整性保护,如图 6 所示。

此外,为了保证中继站与 OAM 管理系统间的安全,在中继站与 OAM 之间使用端到端的保护机制,例如,可以采用 TLS/IPSec 等保护方式进行保护。考虑到如果中继设备与 donor eNB 设备是不同厂商的产品,而不同厂商之间不愿意对方看到自己的设备配置信息,那么逐跳保护的安全连接就不能满足中继网管的安全需求,此时需要采用端到

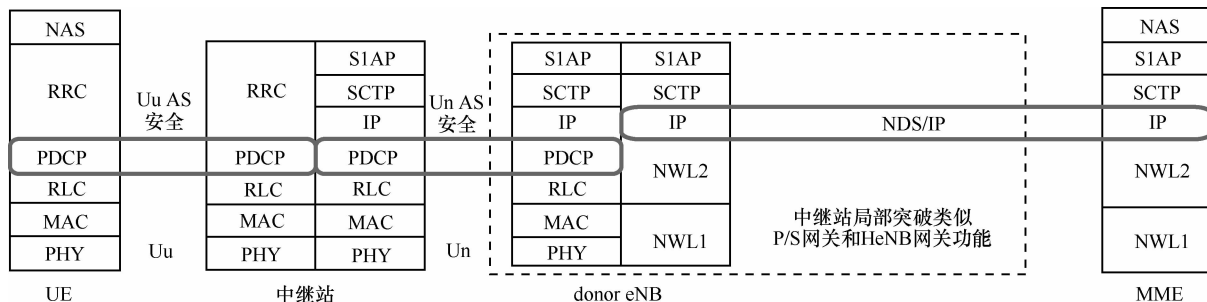


图6 中继对转发信令和数据的加密和完整性保护

端的安全保护机制。但端到端安全机制将会带来中继设备需要与每一个 OAM 服务器维护一条安全连接的缺点,这将在 OAM 服务器数量较多时带来不便。为了克服这个问题,可以在 OAM 侧引入安全网管 SeGW,使得中继与 OAM 侧的安全连接终结于 SeGW,从而避免过度复杂的安全解决方案。

5 结束语

在 LTE-Advanced 系统中引入中继,以解决热点小区覆盖的问题以及扩大小区覆盖的范围问题,也带来了新的安全问题。通过对中继的安全威胁分析,提出了对应的安全需求和解决方案。但是应当看到,针对中继的安全研究才刚刚起步。目前的中继还处于发展阶段,对现有 LTE 系统的影响还需要进一步的研究,其安全问题也需要进一步挖掘和确定。此外,中继的使用场景还会不断扩展,诸如移

动中继、多中继中继等场景下的安全问题也将会随着使用方式的逐步确定而明确。中继的安全研究需要随着中继不断演进而继续深化和发展。

[作者简介]



朱红儒,女,中国移动通信有限公司研究院技术经理、高级工程师,主要研究方向为密码学、可信计算、移动通信网/物联网/WLAN 等网络安全技术。

齐旻鹏,男,中国移动通信有限公司研究院项目经理、工程师,主要研究方向为移动通信网/物联网安全技术。

(收稿日期:2013-06-04)

(上接第 121 页)

操作规范等多种因素相关。因此,需要进行综合权衡考虑,这样才能得出较为准确的校正结果,为后续准确的网络规划和优化奠定基础。

参考文献

- 1 OFcom. Second consultation on assessment of future mobile competition and proposals for the award of 800 MHz and 2.6 GHz spectrum and related issues. <http://stakeholders.ofcom.org.uk/consultations/award-800mhz-2.6ghz/summary>, 2012
- 2 Channel models: a tutorial V1.0. http://www.cse.wustl.edu/~jain/cse574-08/ftp/channel_model_tutorial.pdf, 2007
- 3 Urban Transmission Loss Models for Mobile Radio in the 900 and 1 800 MHz Bands (Revision 2). COST 231 TD (90)119 Rev, 2. European Cooperative in the Field of Science and Technical Research EURO-COST 231
- 4 张华,李懿,尧文彬等. 2.6 GHz 频段传播模型校正及分析. 电信工程技术与标准化, 2011,24(9):5~8
- 5 Volcano training. [http://www.siradel.com/1/volcano-software-](http://www.siradel.com/1/volcano-software-suite.aspx)

suite.aspx. June 18, 2010

- 6 王庆扬,陈晓冬. 2.5 GHz 和 3.5 GHz 频段的 WiMAX 传播模型研究与校正. 电信科学, 2008, 24(6): 52~54
- 7 Shabbir N, Sadiq M T, Kashif H, *et al.* Comparison of radio propagation models for long term evolution (LTE) network. International Journal of Next-Generation Networks (IJNGN), 2011, 3(3):25~41
- 8 Shahajahan M, Hes-Shafi A Q M. Analysis of propagation models for WiMAX at 3.5 GHz. Blekinge Institute of Technology, Sweden, 2009

[作者简介]



赵明峰,男,博士,中国移动通信集团设计院有限公司四川分公司工程师,通信学会会员,主要研究方向为下一代移动通信、无线网络网络安全。

(收稿日期:2013-06-30)