浅析 LTE 无线通信网络安全漏洞及防御措施

◆高渊[1]　董宇翔[1]　张麾军[1]　陆艳军[2]

（1.中国移动通信集团重庆有限公司　重庆　401120；2.重庆理工大学　重庆　401120）

摘要：移动通信作为国家的关键基础设施，是全球科技核心竞争力必争之地，伴随着通信技术的快速发展，其在经济和社会方面的地位显著提高，带动了上下游产业、移动互联网和人工智能等新兴领域的崛起和发展。因此，在移动通信技术快速发展的今天，除了关注速率和系统容量，安全方面的问题更值得关注。目前，国内外对于 LTE 系统的安全问题的研究主要涉及密钥管理、加密算法及鉴权机制等方面。对通信系统的空中接口方面，仍需进一步完善。本文分析了 LTE 无线通信网络漏洞的基本原理及其产生的危害性。对部分场景提出了防御方案。

关键词：LTE 网络；信令；协议安全；攻击漏洞

通信行业的快速发展对企业数字化转型提供了有力的技术支撑，并且加快了自动驾驶、车联网等智能行业在人们日常生活中的应用，同时也将继续创新提高其市场规模。第四代移动通信技术通过对一些关键技术的提升，LTE 网络能够提供更大的网络吞吐量。LTE 及后续演进始终是全球移动通信先进技术研究中的热点之一。在移动通信技术的更新换代中，一直存在着一些潜在安全风险，虽然 LTE 系统中加强了安全方面的保护，比如非接入层的双向鉴权、加密，但安全风险仍不可忽视。

1　LTE 系统网络基本架构及安全机制

1.1 LTE 系统网络基本架构

LTE 网络架构的组成主要包括三部分，演进后的核心网（Evolved Packet Core，EPC），演进后的接入网（Evolved UMTS Terrestrial Radio Acecss Network，E-UTRAN）以及用户终端（User Equipment，UE），核心网包括移动管理实体（Mobility Management Entity，MME）、服务网关（Serving GateWay，S-GW）和 PDN（Public Data Network）网关组成。移动管理实体负责空闲模式的 UE 的定位，寻呼过程，非接入层（NAS）信令的加密和完整性保护，服务网关主要进行 eNode 间的切换，执行合法监听，进行数据包的路由和转发。接入网主要由基站（eNode）组成，起到连接 UE 和 EPC 的作用，主要实现无线资源控制功能。

1.2LTE 网络安全层次

在 LTE 网络中，eNB 的部署相对比较复杂，可能会遭受到恶意攻击。为了保证在接入网遭到攻击时不影响到核心网的安全，LTE 采用了分层安全的设计，即：将接入层（AS）安全和非接入网（NAS）安全分离，AS 负责 UE 与 eNB 之间的安全，NAS 负责 UE 与 MME 之间的安全。采用安全分层的方式使得 E-URTAN 安全层和 EPC 安全层之间的影响最小化，更好地保障 UE 接入时的安全。

鉴权和密钥协商（Authentication and Key Agreement，AKA）过程使用挑战应答机制，从而完成终端和网络之间的身份鉴别，通过身份的鉴别生成加密的密钥。通过身份鉴别和加密达到防御恶意攻击的目的，保护移动通信网络资源的安全。

LTE 网络的 AKA 过程和 UMTS 的基本类似，均通过 Milenage 算法完成终端和网络侧的双向身份鉴别。协议中参与该过程的主体部分有：用户设备（UE），移动性管理实体，归属签约用户服务器（Home Subscriber Server，HSS），UE 是信任 HSS 的，两者会共享密钥以及确定的加密算法。

2　LTE 网络攻击方式

LTE 网络中的安全攻击大体上分为主动攻击和被动攻击两类。被动攻击没有蓄意破坏目标网络的目的，其目的是窃听通信链路，并监控和研究网络业务等，由于该攻击具有的被动属性，使其不易被网络检测出来[1]。主动攻击主要有伪基站攻击、中间人攻击、拒绝服务攻击、重传等攻击类型。

（1）伪基站攻击：攻击者使用非法基站，以高功率方式吸引周围的终端驻留，对终端进行恶意攻击，比如拒绝服务、广播虚假消息、让终端无法执行业务；

（2）中间人攻击：攻击者以中继节点的方式截取合法通信的网元之间交互的信息。例如，攻击者可能对信息进行延迟、更改等操作，通过这种方法在攻击被发现之前，通信双方仍认为维持着正常通信，从而造成数据被盗窃[2]。

（3）重传攻击：攻击者将窃听到的有效信息经过一段时间后再传给消息的接收者。攻击者的目的是企图利用曾经有效的信息在改变了的情形下达到同样的目的，例如攻击者利用截获到的合法用户口令来获得网络控制中心的授权，从而访问网络资源。

3　防御措施

3.1 伪基站攻击防御

为了防止恶意攻击者进行伪基站攻击，网络系统要能够完成网络侧的身份鉴别和信令消息的完整性保护。在 LTE 网络系统中，终端、接入网、核心网等核心设备能够实现终端和网络侧的双向鉴权，并且可以保证空口信令消息的完整性。

（1）在 LTE 网络系统中，终端用户对网络侧的鉴权通过全球唯一用户识别卡检查核心网下发的 AUTN 实现。通过终端的 SIM 卡和 HSS 中携带的共享密钥算出 AUTN，最后通过真实的核心网和 eNB 设备下发给终端用户。终端用户的 SIM 卡根据 K 运用一样的算法产生 AUTN，使其和合法网络中的 AUTN 比较判断网络是不是合法。

由于 K 只有终端侧与合法网络才会有，伪基站没有办法获得正确的 AUTN 来通过 USIM 卡的鉴别。因为伪基站并没有在服务提供商进行注册，从而无法获取合法网络真实有效的 AUTN，最终无法通过终端用户对它的鉴权。

（2）LTE 网络在实现终端对网络侧鉴权的时候需要保护终端与网络之间的不缺失性，对空口传输的消息进行保护，防止恶意攻击者发送虚假的消息。在 LTE 网络系统中采取了更加复杂的密钥结构，生成密钥 KNAS_INT 和 KRRC_INT 分别对应 NAS 层和 RRC 层信令进行完整性保护[4]。与前文提到的 AUTN 类似，IK 是由 HSS 和 USIM 卡依据 K 分别计算出下发给基站和终端用户，之后基站和终端用户将使用 IK 防止空口传输的消息产生缺失。

对于终端而言，对空口消息的一些处理并不会很极端，不具备完整性和鉴别未通过的空口消息，终端不会接收处理并直接丢弃。因为伪基站无法根据 K 生成有效的 IK，导致其发送的信令消息无法被正确的处理从而达到保护完整性的目的。

3.2 终端位置泄露防御

终端位置信息防泄漏是让位置服务提供商和恶意攻击者不能或者无法轻易获得终端用户的真实位置相关信息[3]。目前针对终端位置泄露的防护技术主要有位置模糊、身份隐藏和信息加密三类。位置模糊技术通过扩大或改变终端用户的真实位置，通过降低用户位置信息的精确度来保护终端位置的隐私，身份隐藏技术保留终端的位置信息，将终端用户的身份信息通过技术手段隐藏起来，信息加密技术通过加密算法在终端位置信息使用的时候隐藏用户的信息，即使攻击者获得终端用户的相关信息也无法识别出终端的真实信息和位置。

（1）位置模糊技术

该技术可以降低终端位置的空间粒度，模糊位置信息以及降低终端位置信息的空间粒度，从而到达终端在进行消息交互的时候不泄露

自身的真实坐标。本文主要提出两种未知模糊的技术，包括虚假位置和模糊技术。

虚假位置是指终端用户用多个假冒的位置代替自己的真实位置来发送服务请求。通过这种技术，如果终端需要向其他设备发送自身的坐标信息时，可以不直接发送自己的真实坐标，而是利用相应的技术手段形成一些虚假的信息替代真实的坐标信息发送出去，这样对方就不会获取到真实的坐标，对端必须进行检测筛选接收到的所有有关位置的信息，将本端筛选的结果返回给终端用户，由终端用户根据自己的真实位置决定所需要的服务结果。但是，这种方法将增加对端设备的性能损耗，一定程度上会造成一些额外的开销。

模糊空间是指用一个空间区域代替用户的真实地理坐标。区域的大小根据终端用户的隐私保护需求和要求的服务质量来决定。同虚假位置类似，位置服务器仅知道终端在这个模糊的空间区域，无法获得真实的位置坐标。但是，由于发现目前模糊空间降低了用户的位置精确度，会导致服务质量降低。

（2）身份隐藏技术

攻击者获得了终端的实际位置信息，但无法确定具体用户的情况下发生的损失相对较小，因此更好地隐藏用户的真实身份信息的方法也是解决终端位置泄漏的有效方法。目前有三种主要的匿名技术：假名技术、混合领域技术 ID 隐藏技术。

（3）信息加密

简单来讲就是将看得见的信息利用一定的方式使其变成看不出真实信息的技术，保护用户的敏感信息。这种技术也可以达到保护用户信息的目的，使得终端的坐标信息是经过加密的信息，恶意攻击者就不能获取到终端的位置坐标等相关信息，这种防护技术对计算和通信的开销不是很高，除此之外，查询的过程不需要借助于不安全的服务器。

尽管一些比较老的加密技术可以保证数据不被窃取，但是基本都是借助公有密钥的技术，提供服务的一方想要实现信息加密就必须拥有终端用户的可用公有密钥，但是属性基加密（ABE）的提出解决了这方面的不足。将身份标识看作是一系列的属性，将 ABE 中解密者身份信息与信息加密者的信息匹配，只有匹配一致时，才可以获取加密者加密的信息。ABE 技术能够在位置信息公布时提供加密，仅允许有特殊属性的终端用户才能解密。基于属性隐私保护的移动传播方案，能够确保终端用户信息的保密，加解密机制依赖于用户权限，通过相互身份验证保护终端位置隐私。

4　总结

本文分析了 LTE 网络系统架构及其安全机制，主要包括网络基本架构、无线接口协议栈、系统安全层次三方面。通过对 LTE 网络安全的分析介绍了密钥与协商过程以及 LTE 网络中主要存在的网络攻击方式。对 LTE 网络中存在的安全漏洞进行了分析，主要提出了 DoS 攻击、广播虚假公共告警信息、中间人攻击以及终端位置泄露等安全漏洞场景，并且针对伪基站攻击和终端位置泄露提出了防御方法。在不断提升 LTE 网络吞吐量和速率的同时要更多地关注网络完全问题，只有这样才能将通信技术运用到更广泛的领域，通信技术才能推动社会的不断进步与发展，从而更好地服务于人类的生活。

参考文献：

[1]王勇，骆玉奇，杨立伟.LTE 宽带通信在无线专网的应用[J].信息通信技术与政策，2020（08）：93-96.

[2]张秀杰. LTE 无线通信网络中的安全接入方法研究[D].南京邮电大学，2018.

[3]许志强.分析 LTE 网络结构的特性[J].数码世界，2018（10）：23.

[4]王怀南. LTE 网络节点信息探测方法研究[D].山东大学，2018.

5G 时代无线电监测站无人机云平台技术研究

◆宁悦　吴啸晨

（中国电子科技集团公司第二十八研究所　江苏　21000）

摘要：自无人机云平台技术诞生后，无人机应用情况越发广泛，为了促使现代无线电环境足够规范，我国对于无线电监测站实际需求有所上涨，尤其是在我国正式宣布 5G 时代的到来后，空中无线电的实际情况开始越发混乱，我国无线电监测站也开始迎来全新转折点。这时如果无人机云平台技术在无线电监测站之中得到落实，便可促使我国在 5G 时代下的空中无线电实况得到有效控制。基于此，本文首先介绍了 5G 技术概念、特点以及核心工艺，其次提出无人机发展现况与相关问题，再次提出 5G 时代无线电监测站无人机云平台的设计方案，最后表明 5G 时代无线电监测站无人机云平台之中的核心技术，仅供参考。

关键词：5G 时代；无线电监测站；无人机云平台技术

在近几年经济持续发展下，我国 4G 通信技术已经十分完善，5G 通信技术也开始进入社会大众视线内，云平台、人工智能以及大数据等产业发展必然会更加顺利，现代社会已经正式迎来信息改革，并升级为将 5G 技术作为核心的智能时代。由于 5G 技术具备诸多优势，将其落实到无线电监测无人机云平台设计之中，一定可以促使我国空中无线电监管能力得到大幅加强，促使无线电监测站发展前景更加客观。因此，以下也将 5G 技术作为关键，进一步探析如何在无线电监测站无人机云平台设计之中落实 5G 技术。

1　5G 技术概念、特点及核心工艺

1.1 基本概念

所谓 5G 技术是指现代社会中的最新通信技术，英文为 5th-Generation，属于 2G 技术、3G 技术以及 4G 技术的升级。在 5G 时代之中，所有运营商将服务范围划分为各个小区域，这些小区域就可以称为蜂窝，图像、声音等信号在移动终端中变成数字化形式，通过转换器进行传输。在蜂窝之中所有具备 5G 技术的移动设备，都可以利用电波、天线、发射与接收装置实现通信，当手机用户从一个地区转移到其他地区后，便可将用户移动终端转变为此地区蜂窝之中。于 2019 年 10 月末，我国三大运营商同时宣布 5G 套餐，并在 2019 年 11 月初允许 5G 套餐正式使用[1]。

1.2 技术特点

在信息历史之中 5G 技术是第七次革新，前几次革新无一不为社会大众提供诸多便利，此次 5G 时代来临也不例外，甚至可以说此次 5G 通信技术自身特点完全比以往通信技术更加有质量。第一，用户流量与谅解的视角密度得到全面加强；第二，网络频谱实际效率与 LTE 相互对比至少提高十倍左右；第三，网络整体容量可得到提高，足以让上千亿台设施同时连接，可以满足物联网对于通信的实际需求；第四，接口延时实践控制为 1 毫秒左右，可以为汽车领域和医疗领域实现汽车自动驾驶与远程治疗；第五，除了为手机用户提供通信