



LoRa 广域网安全机制剖析

于小博, 朱红儒, 刘大鹏, 安勃
(阿里巴巴(中国)有限公司, 北京 100102)

摘要: LoRa 广域网 (LoRaWAN) 技术是目前主流的低功耗广域网技术。随着 LoRa 广域网技术越来越多地应用到各个垂直行业, 网络安全变得越发重要。主要针对 LoRa 广域网技术的安全机制进行了分析, 并且针对同类方案进行了技术对比分析。最后指出了 LoRa 广域网安全机制未来的技术发展方向。

关键词: LoRa 广域网; 低功耗; 安全

中图分类号: TN929.5

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019190

Analysis of LoRaWAN security mechanism

YU Xiaobo, ZHU Hongru, LIU Dapeng, AN Qing
Alibaba (China) Co., Ltd., Beijing 100102, China

Abstract: LoRaWAN is one of the most important low power WAN technologies. As LoRaWAN technology is massively applied in various vertical industries, network security becomes more and more important. The security mechanism of LoRaWAN technology was analyzed. In addition, the comparative analysis of similar schemes was carried out. The future research direction of LoRaWAN security mechanism was also pointed out.

Key words: LoRaWAN, low power, security

1 引言

据统计, 全球物联网连接数将以 17% 的年复合增长率继续快速发展, 预计到 2025 年将达到 215 亿。2018 年全球低功耗广域网连接数已经达到 3 700 万, 年复合增长率将达到 109%, 2023 年将增长至 11.5 亿, 超过承载在其他 2G/3G/4G/5G 技术上的连接数的总和。目前, 市场上两大主流的低功耗广域网技术分别为 NB-IoT 以及 LoRa (long range)。而 LoRa 广域网技术凭借其独特的

技术特性, 在诸多物联网应用场景 (如智慧楼宇、智慧城市等) 上发挥着重要的作用。

2 LoRa 广域网以及安全概述

LoRa 广域网是现在主流的低功耗广域网技术之一。LoRa 广域网通常以星形网络的方式部署。LoRa 广域网架构如图 1 所示, LoRa 广域网包括 LoRa 终端设备、LoRa 网关、网络服务器以及应用服务器。其中, 网关在终端设备和网络服务器 (network server, NS) 之间传递消息。网络

收稿日期: 2019-03-15; 修回日期: 2019-07-17

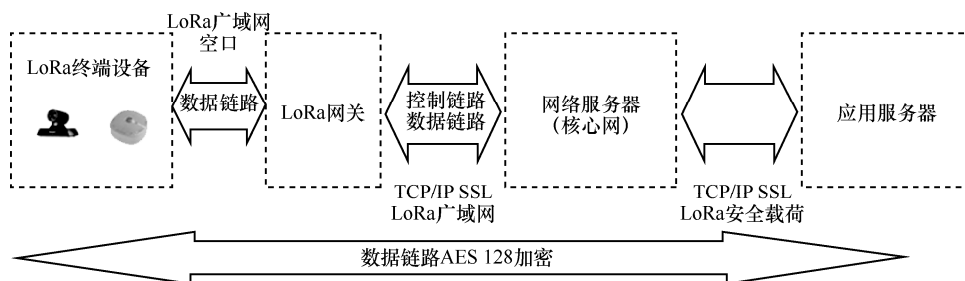


图1 LoRa广域网架构

服务器将数据分组从网络的每个设备路由到关联的应用服务器。

LoRa广域网具有以下几大特点^[1-3]。

- 远距离通信：LoRa广域网通过底层扩频通信技术可以有效地提高传输距离，LoRa广域网在城区的传输距离可以达到1~2 km，在农村地区可以达到10~15 km。
- 低功耗：LoRa广域网设备可以依靠电池供电，续航能力达到10~15年。
- 定位：LoRa广域网网络可以实现低功耗、免GPS的定位功能。
- 双向通信：LoRa广域网网络提供了多种方式的双向通信技术，如Class A/Class B/Class C。
- 安全性：LoRa广域网网络可实现端到端安全，终端具有唯一密钥。

LoRa终端设备通过空口将上行数据帧传输到LoRa网关，并且由LoRa网关将上行数据帧发送到网络服务器，最终由网络服务器将数据帧传输给相应的应用服务器。网络服务器可以根据当前的网络状况通过LoRa网关向LoRa终端设备发送MAC（medium access control）层指令，控制终端设备的空口参数，如发送频点、速率等。LoRa终端设备到应用服务器之间使用AES128加密算法实现端到端加密。

3 LoRa广域网安全机制研究现状及对比

现有文献从多个角度进行了LoRa广域网技

术安全方面的研究。例如，参考文献[4]针对物理层安全展开了研究。除此之外，一些文献针对MAC层的安全机制进行了研究，例如参考文献[5]针对MAC层安全机制提出了一种密钥自动生成机制，并且针对密钥生成机制进行了性能评估。参考文献[6]针对LoRa终端与终端通信的场景提出了一种低功耗的端到端密钥生成机制。参考文献[7]研究了如何将区块链框架引入LoRa广域网中来解决网络中的安全问题。

目前，业界主流的低功耗广域网技术除了LoRa以外，还有NB-IoT技术。NB-IoT是基于授权频段的低功耗广域网技术，是4G网络下，考虑物联网“小数据量，大连接”特点而产生的窄带通信技术。NB-IoT的安全机制与LoRa广域网相比具有以下特点。

(1) NB-IoT采用4G原有的AKA机制来进行终端和网络侧的双向鉴权。采用AKA的优点在于NB-IoT具有像4G一样的安全能力。而缺点在于AKA机制并没有从轻量级的角度对安全机制进行优化，这样会导致有低功耗需求的终端设备在安全计算方面消耗过多的资源。

(2) LoRa协议考虑到了应用层相关的安全机制，例如多播安全机制等，而NB-IoT没有考虑诸如多播安全等的应用层安全机制，这样会导致NB-IoT在应用侧的技术方案略显碎片化。

(3) 随着5G的到来，NB-IoT面临长期演进的技术问题，例如当核心网架构从EPS转换为SBA时，如何映射到相应的网络功能上来处



理 NB-IoT 消息并且保证消息传递过程中的安全等。而 LoRa 广域网的安全技术目前趋于稳定。总体来说, LoRa 相比 NB-IoT 具有更加轻量化且有效的安全机制。

4 LoRa 广域网的安全架构及流程

安全是 LoRa 广域网技术中的重要组成部分。在设计协议时就考虑到安全机制对保障 LoRa 网络的安全性是非常关键的。本文对 LoRa 广域网的安全机制进行了介绍和分析。

LoRa 广域网的安全架构如图 2 所示, LoRa 广域网的安全架构分为以下 3 个部分。

- **MAC 层安全 (I):** MAC 层安全主要保障终端设备与网络服务器之间的双向认证以及 MAC 控制命令的传输安全。
- **传输层安全 (II):** 传输层安全主要保障网关与网络服务器以及网络服务器与应用服务器之间的数据传输安全。
- **应用层安全 (III):** 应用层安全主要保障入网过程中的双向认证以及数据载荷端到端的加/解密。

LoRa 广域网为终端设备以及网络侧之间提供了认证、控制命令加密、数据载荷的端到端加密等安全机制。上下行数据帧的加密密钥可以保证一机一密。另外, 密钥不会在空口上进行传输, 这样保证了攻击者不会从上下行数据帧中截获密钥信息。LoRa 广域网依赖对称密钥机制来实现端到端的应用层以及网络层上的通信安全。

LoRa 广域网安全机制如下。

(1) 认证机制

认证机制为双向认证。终端与网络侧利用入网过程完成双向认证。终端首先向网络侧发送入网请求 (join request), 网络侧通过校验入网请求帧中携带的消息认证以及完整性校验码 (message authenticity & integrity check, MIC) 完成对终端的认证。随后, 网络侧向终端发送入网请求接受帧。终端根据入网请求接受帧来完成对网络侧的认证。入网过程完成后, 终端以及网络侧生成对应的会话密钥。会话密钥用来在后续的上下行数据传输中, 对终端以及网络侧进行认证。

(2) 加密和完整性机制

主要采用分组加密的方法。终端设备通过预存储的根密钥派生的相应会话密钥进行消息的加/解密或者完整性保护。LoRa 广域网主要采用 AES128 算法进行加/解密。LoRa 广域网的安全流程主要在网络服务器、应用服务器与终端之间进行。应用服务器管理无线终端设备的激活过程^[3]。应用服务器会在收到终端设备发送的入网请求后, 执行网络层会话密钥 (NwkSkey) 和应用层会话密钥 (AppSkey) 派生。它将网络层会话密钥传送给网络服务器。终端在接收到网络侧发送的入网接受帧后生成对应的网络层会话密钥以及应用层会话密钥。随后, 终端设备凭借 NwkSkey 以及 AppSkey 分别与网络服务器以及应用服务器建立安全通道。

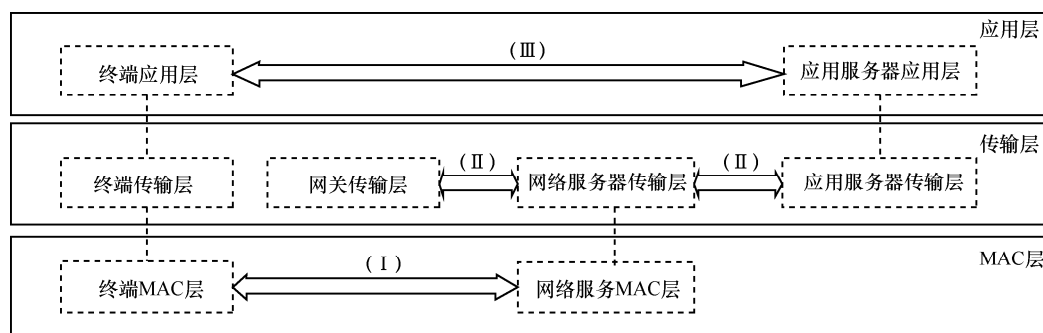


图2 LoRa 广域网的安全架构

5 LoRa 广域网密钥衍生机制

终端与网络服务器之间预置根密钥。每一个终端都具有唯一的根密钥。在入网过程中,终端与网络服务器之间根据根密钥动态生成不同类型的共享密钥,LoRa 广域网密钥产生过程如图3所示。

在现有的 LoRa 广域网技术^[1]中,终端只拥有一个应用根密钥 Appkey。根密钥可以通过产线预置的方式预置在终端上。如图3所示,应用层以及网络层传输所需的会话密钥都是通过应用根密钥来生成的。其中,aes128_encrypt代表 AES128 加密算法。会话密钥的种类如下。

(1) 应用层会话密钥

应用层会话密钥主要用于加密应用层数据。

加/解密在应用服务器以及终端之间完成。

(2) 网络层会话密钥

网络层会话密钥主要用于生成 MIC 或者加密 MAC 指令。

如上文所述,LoRa 广域网中会话密钥的生成主要是在入网过程中完成的,因此入网过程是保障 LoRa 广域网安全机制的一个关键过程。入网过程中的密钥衍生机制如图4所示。

终端设备在开机之后,首先需要接入 LoRa 网络。因此,终端设备首先需要进行入网过程,如图4步骤1所示,终端根据当地 LoRa 网络所使用的频率参数向网络发送入网请求帧。由于此阶段终端设备和网络之前还未协商出共享密钥。因此,入网请求帧的消息体是不加密的。但是为保证空口传输的完整性,入网请求帧会携带一个

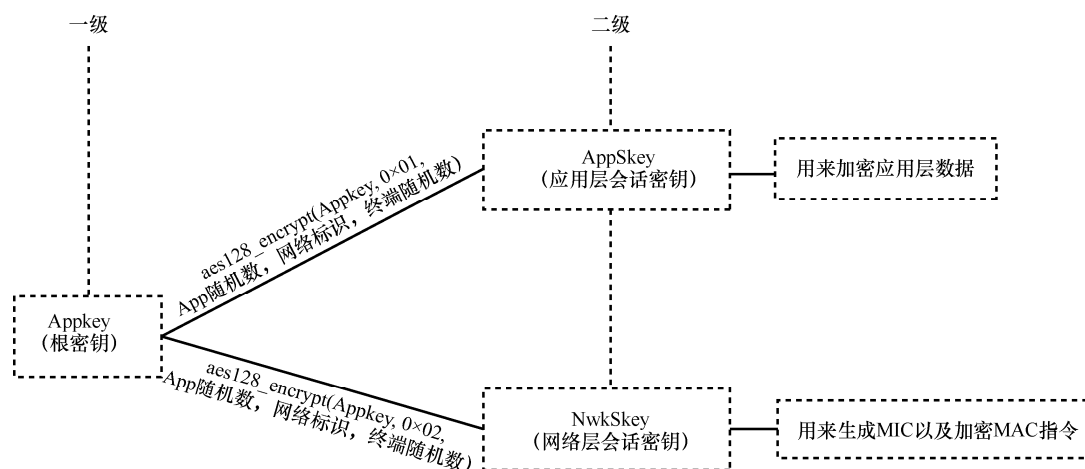


图3 LoRa 广域网密钥产生过程

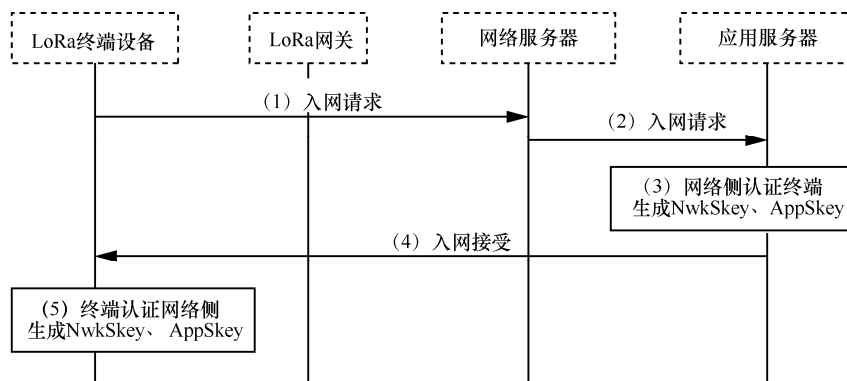


图4 入网过程中的密钥衍生机制



MIC。为了使网络服务器侧可以进行相应的完整性校验。入网请求帧的 MIC 生成方式为：

```
cmac = aes128_cmac(Appkey, MHDR | AppEUI |  
DevEUI | DevNonce), MIC = cmac[0..3]
```

其中，aes128_cmac 代表 AES128 CMAC 算法。网络服务器在收到入网请求帧后，将该入网请求帧转发给相应的应用服务器。

应用服务器在接收到入网请求帧后，会根据终端设备对应的标识找到相对应的根密钥，并且利用根密钥对入网请求帧的 MIC 进行校验。应用服务器通过校验 MIC 完成对终端的认证。之后，应用服务器根据相应的信息来生成会话密钥 NwkSkey 以及 AppSkey。两个会话密钥分别保证终端设备与网络服务器以及终端设备与应用服务器之间信息传输的安全性。为了使终端设备也获取相对应的会话密钥，应用服务器根据入网请求帧来生成对应的入网接受帧 (join accept)，并且通过网络服务器发送给终端。由于终端在接收到入网接受帧后，可以通过相应的参数来推演出相应的会话密钥，因此，入网接受帧采用加密的方式进行传输。入网接受帧的加密方式为：

```
aes128_cmac(Appkey, AppNonce | NetID |  
DevAddr | DLSettings | RxDelay | CFList | MIC)
```

同时，应用服务器将 NwkSkey 发送给网络服务器。

终端接在收到入网接受帧后，用 Appkey 来校验入网接受帧的 MIC，并且完成对网络侧的认证。至此，终端设备和网络侧完成了双向鉴权。随后，终端设备根据入网接受帧来生成对应的两个会话密钥 NwkSkey 和 AppSkey。密钥的衍生将 Appkey、应用随机数 (AppNonce)、网络标识 (NetID) 以及终端随机数 (DevNonce) 作为输入参数。

终端入网成功后，会用衍生出的 NwkSkey 验证下行数据帧中的 MIC 或者生成上行数据帧中的

MIC，而不再使用 Appkey 来进行 MIC 的验证和生成，这样可以保护根密钥的安全性。

总体而言，LoRa 广域网考虑到了终端到网络服务器以及应用服务器端到端的安全机制。权衡终端设备功耗以及安全等级，系统主要采用 AES128 加解密算法。然而，LoRa 广域网的安全性依然存在一些待解决的问题。

6 LoRa 广域网安全机制的下一步工作

6.1 DDoS 攻击防护

LoRa 广域网缺乏对 DDoS (distributed denial of service) 攻击的防护机制。例如，在 LoRa Class B 协议中，beacon 帧的传输起到了时间同步等重要作用。然而，beacon 帧的传输没有采取任何安全措施。攻击者可以通过仿冒 beacon 帧的方式来发送假的 beacon 帧给终端设备，造成终端设备的传输故障。在 DDoS 攻击防护的问题上，对称密钥存在着密钥分配的问题。而引入 PKI 机制将是一种解决 DDoS 攻击的有效方法。例如，网关在收到一个上行数据帧时，可以通过私钥来验证上行数据帧的合法性。如果失败，网关可以拒绝向网络服务器发送上行数据帧。然而，如何引入 PKI 机制将是一个关键的研究课题。

6.2 中继安全

LoRa 广域网中继是一个业界普遍关注的热点技术。终端设备可以通过设置 LoRa 广域网中继器来转发终端以及基站之间的上下行数据。LoRa 广域网中继技术主要是为了解决网络边缘信号覆盖差的问题，使得网络边缘的终端数据帧也可以通过中继器发送到网关，进而将数据帧发送到网络服务器。中继器与终端设备之间的传输安全是一个待解决的课题。具体地，中继器可能受到终端设备的 DoS 攻击，造成过多的误唤醒，从而导致中继器的电量过度消耗。因此，可以考虑在中继器以及终端设备之间引入一个轻量级的密钥保

护机制。密钥保护机制需要考虑生成过程的轻量化以及实际部署的复杂度等问题。另外,由于中继密钥保护机制不影响网络侧的实现,所以保障中继密钥保护机制可以最大限度地兼容不同版本的LoRa广域网协议。

中继问题在蜂窝网系统中同样也受到了关注。参考文献[8]针对蜂窝网的中继问题展开了系统的研究和分析。为使中继方案在未来融合场景中广泛应用,需在不同类型的低功耗广域网部署中考虑类似的密钥衍生以及分发机制。

6.3 密钥体系增强

LoRa广域网中的两个对称密钥的生成输入参数几乎一致,攻击者可以通过一个密钥很轻易地导出另外一个密钥,从而导致传输过程中数据内容的安全隐患,这也是将来要解决的一个问题。

6.4 网络侧安全机制增强

目前在LoRa广域网的覆盖场景中,出现了诸多要求较低时延的应用,例如智慧停车、智能门锁等。为了满足上述应用低时延的要求,可以在LoRa广域网的边缘部署边缘平台。如何实现LoRa核心网与边缘平台之间的鉴权以及数据加密是另外一个待解决的问题。

7 结束语

LoRa广域网是目前主流的低功耗广域网技术之一。而安全机制是网络运行的最基本保障。本文阐述了目前LoRa广域网用到的安全机制,并且对密钥衍生机制做了具体的分析以及介绍。此外,在未来LoRa广域网技术演进过程中,还需要考虑诸多待解决的安全问题,如DDoS攻击防护、LoRa中继安全机制、密钥体系增强以及网络侧安全机制增强等。

参考文献:

- [1] LoRa广域网技术协议 v1.0.3[S]. 2018. LoRaWAN specification v1.0.3[S]. 2018.
- [2] 刘玮,董江波,任冶冰. NB-IoT 的关键性能[J]. 电信科学, 2018, 34(Z1): 111-117. LIU W, DONG J B, REN Y B. Key performance of NB-IoT[J]. Telecommunications Science, 2018, 34(Z1): 111-117.
- [3] LoRa广域网后端接口技术协议 v1.0[S]. 2017. LoRaWAN backend interfaces v1.0 specification[S]. 2017.
- [4] XU W, JHA S, HU W. LoRa-Key: secure key generation system for LoRa-based network[J]. IEEE Internet of Things Journal. 2018(12): 1.
- [5] ZHANG J, MARSHALL A, HANZO L. Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks[J]. IEEE Transactions on Vehicular Technology, 2018, 67(12): 12462-12466.
- [6] KIM J, SONG J. A secure device-to-device link establishment scheme for LoRaWAN[J]. IEEE Sensors Journal, 2018, 18(5): 2153-2160.
- [7] OZYILMAZ K R, YURDAKUL A. Designing a blockchain-based IoT with Ethereum, Swarm, and LoRa: the software solution to create high availability with minimal security risks[J]. IEEE Consumer Electronics Magazine, 2019, 8(2): 28-34.
- [8] 朱红儒,齐闵鹏. LTE下一代中继的安全[J]. 电信科学, 2013, 29(9): 122-126. ZHU H R, QI M P. Security of LTE next-generation relay[J]. Telecommunications Science, 2013, 29(9): 122-126.

[作者简介]



于小博(1985-),男,博士,阿里巴巴(中国)有限公司标准化部高级工程师,国家标准化管理委员会委员,主要研究方向为无线系统分析与仿真、MAC层调度以及路由算法、MAC层协议优化、下一代网络资源管理以及跨层协议设计。

朱红儒(1976-),女,阿里巴巴(中国)有限公司标准化部总经理、研究员,主要研究方向为通信安全,电子商务以及移动通信网/物联网等安全、标准化及国际化等。

刘大鹏(1980-),男,阿里巴巴(中国)有限公司标准化部高级专家,主要研究方向为物联网、IP网络与基础协议等技术领域的国际标准化工作。

安勃(1989-),男,阿里巴巴(中国)有限公司标准化部标准化专家,主要研究方向为智能音箱、物联网连接蓝牙、ZigBee协议、虚拟现实/增强现实等。