基于 LoRa 无线网络的网络安全问题分析和实验验证研究

巩 潇 崔登祺 万彬彬 赵郑斌 李梦玮
(中国软件评测中心(工业和信息化部软件与集成电路促进中心),北京 100084)

摘要:LoRa 无线网络技术是一项广泛应用物联网平台的网络通信技术,能够以超低功耗提供长距离连接设施。由于 AES-128 加密技术用于从终端设备到应用服务器的有效负载传输,因此它提供了强大的安全功能。由于其自身网络体系架构的设计,网关是网络中的弱点,这给攻击者提供了可乘之机。提出了一种新的证书认证技术来保护网络中的网关。构建 LoRa 无线网络技术的实验仿真环境进行有效验证,大大提升了 LoRa 无线网络技术的安全性。

关键词:LoRa 无线网络;网络安全;防护策略;实验验证

Abstract: LoRa Wireless network technology is a network communication technology that is widely used on the Internet of Things platform, providing long-distance connectivity facilities with ultra-low power consumption. Because AES-128 encryption is used for payload transport from the end device to the application server, it provides strong security features. Due to the design of its own network architecture, gateway is the weak point in the network, which provides an opportunity for attackers. This paper proposes a new certificate authentication technique to protect the gateway in the network. In this paper, the experimental simulation environment of LoRa wireless network technology is constructed for effective verification, which greatly improves the security of LoRa wireless network technology.

Keywords: LoRa Wireless, network security, protection strategy, experimental verification

1 LoRa 无线网络概述

物联网平台依赖于多种类型的无线/有线网络传输将各种类型的物联网设备(智能终端)进行联合组网,形成一个无边界的网络空间[1-2],其广泛应用于人们日常生活和工业生产的各个方面,如智慧家居、智慧物流、智能工厂、智能电网等[2-5]。物联网设备基于有线/无线的网络传输构建了整体的物联网平台。由于物联网应用场景的不确定性,其网络空间是一个无边界可扩展的。LoRa 无线网络技术因为其低数据速率的成本优势,可进行超长距离的网络传输(最长单点可覆盖 50 km),在物联网平台中得到广泛应用[6]。

LoRa 无线网络技术的网络体系结构可以分为五层,如终端设备、网关、网络服务器、加入服务器和应用服务器[7-8],如图 1 所示,其中,常见的网络攻击有中间人攻击、网络洪泛攻击、网络流量攻击、物理攻击、射频干扰攻击和流量重放攻击等 6 种[9-11]。

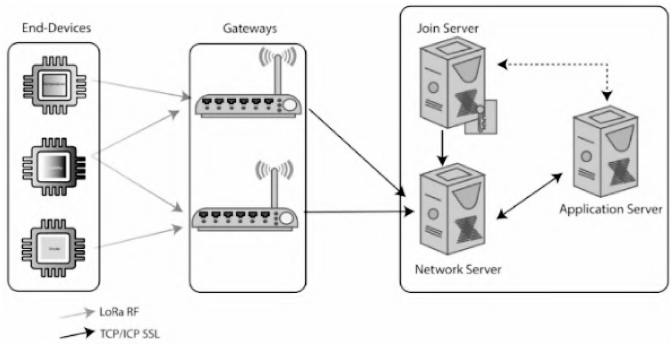

图 1 LoRa 无线网络体系架构

本文主要针对 LoRa 无线网络构建实验仿真环境,并模拟攻击者行为,进行安全性分析。

2 实验设计

2.1 实验环境的构建

本文中的用于复制 LoRa 无线网络生态系统的硬件,如终端设备和网关,是使用计算单元和 LoRa 无线电芯片完成的。本文的计算单元是树莓 Pi4 Model B (RPi4),如图 2 所示,配有 1.5 GHz 四核处理器和 4 GB RAM,再加上 16GB SD 卡等配套以及试验板、连接不同部件的跳线和电源。

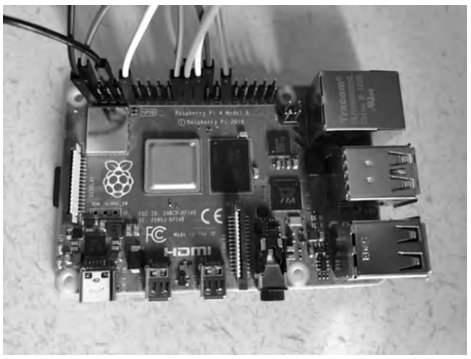

图 2 模拟的 LoRa 无线网络硬件

所用的 LoRa 无线电芯片是 Adafruit RFM96W LoRa 无线电收发器 433 MHz,如图 3 所示,这是在 LoRa 无限网络中使用远程通信所必需的。

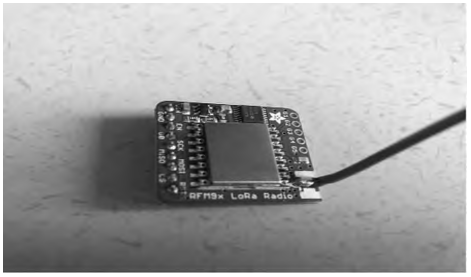

图 3 用于模拟的 LoRa 无线电芯片

关于天线,采用一根简单的 22 AWG 线,线的长度决定其频率,公式如下:

$$W_l=W_v\times F_r \tag{1}$$

其中 W_l 代表波长,W_v 是波速,F_r 是射频。

因此,对于网关,计算单元和 LoRa 无线电芯片是相连的。这是通过将无线电芯片与插头带引脚焊接在一起,然后将其连接到试验板上来实现的。当芯片牢固地安装在试验板上后,试验板通过公母线缆连接到 Raspberry Pi,如图 4 所示。

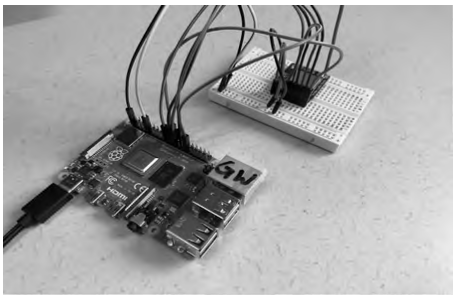

图 4 模拟的 LoRa 无线网关状态

LoRa 无线电芯片由控制不同功能的多个引脚组成。从左侧开始,我们有三个电源引脚:VIN、GND 和 EN。这些引脚处理分线的供电和无线电的关闭。

Raspberry Pi 带有两排 40 个通用输入/输出(GPIO)引脚;其中,我们用线缆将无线电芯片连接到 8 个等效引脚。

OpenSSL 软件安装在虚拟环境中的两个 Ubuntu 20.04.2 LTS 上,具有两个相同的设置,除了 OpenSSL 配置文件。当使用 OpenSSL 作为 CA 时,配置文件是必需的,因为它们包含的参数比终端中可能指定的要多。OpenSSL 配置文件提供了两个功能:模板,并在配置中强制实施证书策略。证书策略包含一组参数,如 countryName、commonName 等。它必须与证书签名请求(CSR)中的相应字段相匹配。

为了获得证书,客户端生成一个 CSR,其 DEVEUI 作为主题 Common<CN>,sha 256 作为消息摘要。如图 5 所示:

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = 0xFFFFFFFFFFFF
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:af:e1:3a:1a:d0:7f:9c:c5:a9:45:90:2a:dc:88:
                    ...
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Key Usage: critical Digital Signature, Key Encipherment
            X509v3 Extended Key Usage: E-mail Protection,TLS Web Client
    Authentication
            X509v3 Subject Key Identifier:
                67:FF:89:00:84:C7:40:ED:54:33:05:74:75:DE:C1:1E:4A:18:2D:F4
            X509v3 Subject Alternative Name:
                <EMPTY>

    Signature Algorithm: sha1WithRSAEncryption
         73:b4:c4:ed:93:9e:f4:9d:a7:1f:90:40:71:07:5d:3a:d9:f1:
         ...
```

图 5 证书获取状态截图

此后,中间 CA 基于 CSR 发布一个新的证书。根 CA 的证书吊销列表(CRL)每七天自动接收一次更新,或者在证书被吊销时接收一次更新。相反,中间 CA 的 CRL 每 7 小时接收一次更新。CRL 由发布实体签名,并且通过将签名与从发布实体的公钥生成的签名进行比较,接收者可以容易地验证 CRL。此外,来自发布 CA(即 intermediate-CA)的 CRL 将放在 JS 旁边,并通过 MQTTv3 为 LoRaWAN 设备进行访问。

2.2 实验方法

基于已构建的 LoRa 无线网络环境的安全性,采用如图 6 所示的实验验证流程。从图中可以看出,JS 接收来自 GW 和 NS 的请求,并将它们转发给中间 CA。然后,根 CA 认证请求,并向 GW 和 NS 提供确认。

这将通过收集每个测试场景的包交付率(PDR)来执行。PDR 是一个指标,用于显示到达的数据包占网络中发送的数据包总数的百分比。观察 PDR 可以了解当网络受到恶意攻击或受到建议的解决方案保护时会发生什么情况,以及这会如何影响网络流量。

$$PDR=\frac{P_{Received}}{P_{Sent}} \quad (2)$$

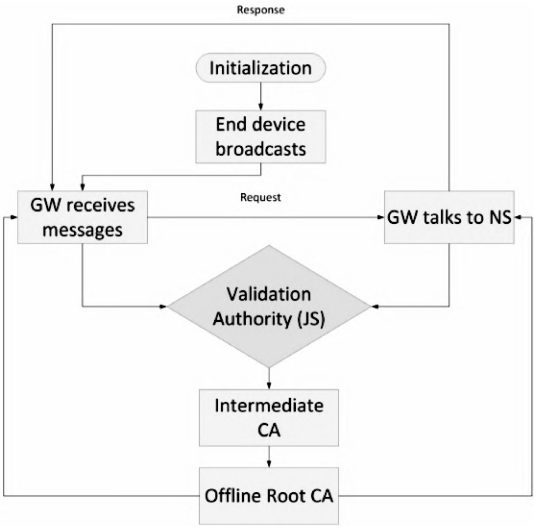

图 6 实验验证流程图

验证过程采用常见的 LoRa 无线网络攻击(中间人攻击)。因此,当终端设备发出一定数量的数据包时,这些数据包会按顺序注册并增加帧计数器。因此,如果它接收到帧计数器较低的消息,它就会被丢弃。因此,通过选择性转发攻击,恶意参与者可以扣留大部分数据包,只要它发送的帧计数器高于前一个帧计数器,例如,只发送第一个和最后一个数据包。因此,如果中间人行为者比合法行为者更快,无论是通过更近还是直接禁用附近的合法 GW,这将意味着它可以控制传输流,并大大降低网络的效率。

这可以通过部署两个网关来验证,其中一个是授权网关 GW-A,另一个不是 GW-B。然后,终端设备发送一系列消息,这些消息将被接收并转发到 NS。首先从授权网关 GW-A 附近开始,大多数包裹在到达 NS 之前将首先通过 GW-A,在 NS 处它们将最终被接收。网络服务器将只看到一个可接收的帧计数器,它高于前一个,并接收传输。然而,当来自 GW-A 的包最终到达时,它们将以较低的帧计数器按顺序到来,ns 最终因为重复而拒绝该帧计数器,这最终意味着 NS 将仅接收整个消息的一小部分。

3 结果和讨论

接收信号强度指标(RSSI)是一个参数,旨在表示设备收听、检测和接收传输的能力。这是基于信号的相对质量以及由于天线或电缆特性造成的任何潜在损失。

通过测量 RSSI,可以收集数据,给出噪声水平的粗略估计,这可能会影响信号强度。图 7 显示了相同的基线场景,其中收集了 RSSI 值,然后绘制成图。可以看出,对于初始距离,RSSI 已经开始超过 80 dBm 值,这是一个较低的额定值。随着终端设备移动得更远,这种情况会继续恶化。在大约 1000 m 处,不再有任何包裹被递送到 GW-A,这与几乎达到 100 dBm 的 RSSI 值相关联。类似的趋势也可以在 GW-B 上看到:随着 ED 的靠近,RSSI 强度增加。

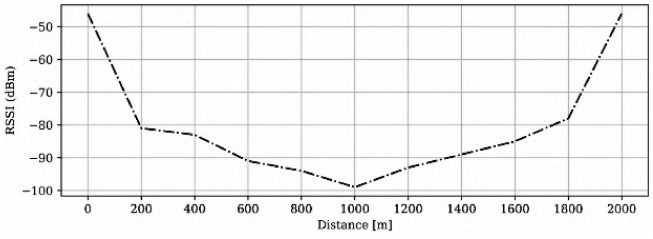

图 7 LoRa 无线网络 RSSI 值与无线距离的关联

(下转第 82 页)

fect extraction and classification of mobile phone screen based on machine vision [J]. Computers and Industrial Engineering, 2020, 146
[4]ZHENG J, YU W, DING Z, et al. Real-time batch inspection system for surface defects on circular optical filters[J]. Applied Optics, 2022, 61(32): 9634-9645
[5]MANSI S, JONGTAE L, HANSUNG L. The Amalgamation of the Object Detection and Semantic Segmentation for Steel Surface Defect Detection[J]. Applied Sciences, 2022, 12(12)
[6]AKGÜL J. A Novel Deep Learning Method for Detecting Defects in Mobile Phone Screen Surface Based on Machine Vision[J]. Mobile Phone Screen Surface Defect, 2023, 27(2): 442-451
[7]YANG W, ZHANG Y, DONG Y, et al. Development of machine vision system for off-line inspection of fine defects on glass screen surface[J]. IEEE Transactions on Instrumentation and Measurement, 2022, 71: 5016008.1- 5016008.8
[8]SIMONYAN K, ZISSERMAN A. Very Deep Convolutional Networks for Large-Scale Image Recognition[C]// International Conference on Learning Representations, 2015
[9]WOO S, PARK J, LEE J-Y, et al. Cbam: Convolutional block attention module[C]// Proceedings of the Proceedings of the European conference on computer vision (ECCV), 2018
[10]朱聪,于广婷,李柏林,等.一种新的精密光学镜片表面疵病宽度测量方法[J].计算机应用与软件,2014,31(12):259-261,286
[11]LIU D, YANG Y, WANG L, et al. Microscopic scattering imaging measurement and digital evaluation system of defects for fine optical surface[J]. Optics Communications, 2007, 278(2): 240-246
[12]谢世斌.基于机器视觉的玻璃表面质量检测若干技术问题的研究[D].杭州:浙江大学,2016
[13]YANG L, HUANG X, REN Y, et al. Study on steel plate scratch detection based on improved MSR and phase consistency[J]. Signal, Image and Video Processing, 2023, 17(1): 119-127
[14]SU H, WANG X, HAN T, et al. Research on a U-Net bridge crack identification and feature-calculation methods based on a CBAM attention mechanism[J]. Buildings, 2022, 12(10)

[收稿日期:2023-10-16]

(上接第 68 页)

通过使用低成本且可获得的 RFM9x LoRa 收发器结合 Raspberry Pi,Lora 无线网络体系架构中的网关实际上变成了单通道。单通道网关只能接收特定扩频因子和通道上的有效载荷。此外,与高端 LoRa 芯片相比,单通道网关的覆盖范围较小。在基线测量中,实验过程发现在中等视距内,200 m 后 PDR 急剧下降。1000 m 后,我们没有收到任何数据包。从 RFM9x 获得的 RSSI 读数对确定信号强度和质量至关重要,但并不准确。同样重要的是要注意,由于上述原因,单通道网关不符合 LoRa 无线网络标准。

为了有效对 LoRa 无线网络的安全性风险进行防护,基于上述的分析,采用一种全新的防护策略,新增了一个网关,导致原本的单独网关从单通道变为双通道。图 8 展示了匹配新的防护策略的实验数据的变化。实验室发现,无视线的初步测试区域。R-GW 永久放置在距 ED 200 m 处,L-GW 以 200 m 的增量放置,直至 800 m。流氓网关比合法网关接收到更多的数据包。这是因为靠近末端装置的固定位置。因此,当终端设备广播数据包时,流氓网关会立即收到数据包。换句话说,合法网关从终端设备收到的远程数据包较少。在 200 m 处,网络服务器接收了 4500 多个数据包。然而,由于本文采用的认证算法,只有来自合法网关的数据包被接收(大约 1500 包),其余的被丢弃(大约 3000 个分组)。

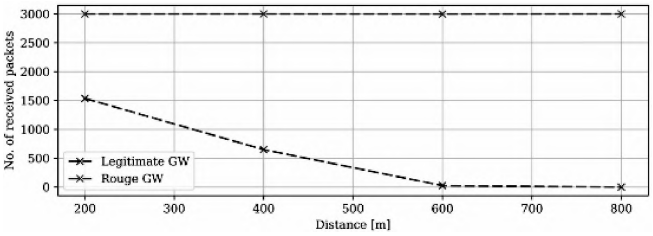

图 8 对 LoRa 无线网络进行防护策略后的趋势

4 结束语

本文构建 LoRa 无线网络技术的实验仿真环境进行有效验证,实验发现来自非法网关的 66.67%的数据分组被丢弃,大大提升了 LoRa 无线网络技术的安全性。将来,一种轻量级的证书分配技术可能会在初始身份验证期间有效减少 LoRa 无线网络传输的负载,更进一步地提升 LoRa 无线网络的安全性和可用性。

参考文献

[1]李权接,赵延明,张泽瑞,等.基于 LoRa 无线通信的分布式桥梁监测系统设计[J].传感器与微系统,2021,40(1):104-106,109
[2]曹安民.LoRa 物联网技术的发展展望与应用探讨[J].广播电视网络,2022,29(4):79-83
[3]姜顺荣.物联网中信息共享的安全和隐私保护的研究[D].西安:西安电子科技大学,2016
[4]张小娟.智慧城市系统的要素、结构及模型研究[D].广州:华南理工大学,2015
[5]WU QINGQING, ZHANG SHUOWEN, ZHENG BEIXIONG, et al. Intelligent Reflecting Surface-Aided Wireless Communications: A Tutorial[J]. IEEE Transactions on Communications, 2021, 69(5): 3313-3351
[6]梁广俊,辛建芳,王群,等.物联网取证综述[J].计算机工程与应用,2022,58(8):12-32
[7]MARCO DI RENZO, ALESSIO ZAPPONE, MEROUANE DEBBAH, et al. Smart Radio Environments Empowered by Reconfigurable Intelligent Surfaces: How It Works, State of Research, and the Road Ahead[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(11): 2450-2525
[8]张琪,蒋宇娜,葛晓虎,等.基于最优运输理论的物联网边缘计算资源优化机制[J].物联网学报,2021,5(2):60-70
[9]徐浪,陈小莉,田茂,等.基于 Turbo 码和 ODPD 判决法的 LoRa 改进方法[J].电子测量技术,2020,43(7):142-147
[10]蒋卫恒.基于协作的无线窃听信道安全通信与功率分配[D].重庆:重庆大学,2015
[11]吴彤.无线网络物理层安全传输策略研究[D].北京:北京交通大学,2016

[收稿日期:2023-08-28]