基于射频指纹的 LoRa 网络安全方案研究

姜禹[1,2]，陈思卿[1]，孙雯[1]
（1. 东南大学网络空间安全学院，江苏 南京 211189；2. 网络通信与安全紫金山实验室，江苏 南京 211111）

摘　要：远距离无线电（LoRa, long range radio）凭其远距离、低功耗的优点在物联网中应用广泛，但目前 LoRa 网络还没有可靠的安全方案，无法保证通信安全。为此，基于射频指纹的唯一性和难以篡改性，提出接收请求接入的 LoRa 终端的射频信号，提取指纹并标注，与根据需求自定义的多尺度安全规则匹配来判断终端身份是否安全，采取对应安全措施。据此，对原有 LoRa 网关及 LoRa 网络架构进行改进，设计了全新的工作流程，提出了两种 LoRa 网络安全方案。提出的 LoRa 网络安全方案从物理层实现 LoRa 终端身份认证和接入控制，仅需针对原有网关及其工作逻辑进行改进，无须改造数量巨大的 LoRa 终端，在不影响原有 LoRaWAN 安全机制工作的基础上，给 LoRa 物联网应用添加新的安全措施和保障，具有很高的实用价值。

关键词：射频指纹；物理层安全；接入控制；LoRa 网关；LoRa 网络安全
中图分类号：TN915.05
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2021.00228

Research on LoRa network security schemes based on RF fingerprint

JIANG Yu[1,2], CHEN Siqing[1], SUN Wen[1]
1. School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China
2. Purple Mountain Laboratories, Nanjing 211111, China

Abstract: Long range radio (LoRa) is widely used in the IoT due to its advantages of long distance and low power consumption. However, LoRa network has no reliable security scheme currently, making it unable to guarantee the communication security. Therefore, based on the uniqueness and tamper-resistance of radio frequency fingerprint, it was proposed to receive radio frequency signals of the LoRa end nodes which requested access, extract the fingerprints from them, mark it and match with the customized multi-scale security rules according to demands to decide whether the identities of the LoRa end nodes were safe, taking security measures accordingly. Based on this, original LoRa gateway and LoRa network architecture were improved, new workflows were designed, and two LoRa network security schemes were proposed. The two LoRa network security schemes were proposed which implement identity authentication and access control of the LoRa end nodes from the physical layer. It is only needed to improve the original LoRa gateway in the LoRa network architecture and its workflow, which adds new security measures and guarantees for LoRa applications on the basis of not affecting the original LoRaWAN security mechanism, with no need to modify a huge number of LoRa end nodes. The security schemes proposed have high practical value.

Key words: RF fingerprint, physical layer security, access control, LoRa gateway, LoRa network security

收稿日期：2020−01−27；**修回日期：**2021−11−06
通信作者：姜禹，jiangyu@seu.edu.cn
基金项目：江苏省重点研发计划（No.BE2019109）；国家自然科学基金资助项目（No.61571110，No.61601114，No.61602113，No.61801115）；江苏省自然科学基金资助项目（No.BK20160692）
Foundation Items: The Key Research and Development Program of Jiangsu Province (No.BE2019109), The National Natural Science Foundation of China (No.61571110, No.61601114, No.61602113, No.61801115), The Natural Science Foundation of Jiangsu Province (No.BK20160692)

1 引言

物联网应用日益火热，低功率广域网络（LPWAN, low-power wide-areanetwork）技术应运而生。作为 LPWAN 的代表，远距离无线电（LoRa, long range radio）采用线性调频扩频技术和前向纠错编解码技术，具有通信范围广、距离远、功耗低、鲁棒性高等优点，颇具实际应用价值，受到国内外学术界和工业界的广泛关注[1]。

安全性是任何通信技术投入应用的基本要求，LoRa 也不例外。目前对 LoRa 安全性的研究主要集中在 MAC 层的 LoRaWAN 协议。文献[2]对 LoRaWAN 协议现存的 LoRa 组网必需的密钥更新机制进行了安全性分析，并基于此改进提出了一套全新的密钥激活机制；文献[3]通过数学推导得出 LoRaWAN 协议在终端请求－应答机制中应当保证的网络服务器的精准数值，并分析提出了相应的理论修改细节；文献[4]则重点关注了 LoRaWAN 协议规定的数据包格式中存在的时间标签信息缺失问题。然而，以上文献对 LoRa 的安全性研究还很片面，仅仅对 MAC 层的安全问题分析远远不够。文献[5]指出从终端物理接口很容易破解获取 LoRa 通信密钥的信息，而诸如此类的问题是单一的 MAC 层安全措施很难解决的。因此，应从不同层的角度出发研究 LoRa 安全问题，最终融合多层的多种安全措施完善 LoRa 的安全框架，而在这个过程中，对 LoRa 物理层的安全性研究必不可少。

射频指纹是一个典型的物理层概念，它是射频信号中包含射频设备的特征信息。射频设备的内部组成、电路走线、元件选择、物理属性甚至老化程度都会造成射频设备存在独特的非线性偏差，这些偏差使射频设备发出的信号包含其独特的物理层特征[6]。射频指纹是独一无二的，即使是同一工厂用同一设备和工艺生产出的同一批次的设备也会有生产标准容差造成的细微不同，进而导致射频指纹的不同。射频指纹的唯一性和难以篡改性使得它能够代表射频设备的身份，可以有效抵挡伪造、篡改等攻击[7]，作为物理层安全的一部分。基于射频指纹从物理层解决 LoRa 终端的身份认证和接入安全问题，提出两种改进了网关的 LoRa 网络架构安全方案。物理层防护提供了有别于传统安全架构的思路，该安全方案不但能够单独运行实现终端的安全接入，也能够配合上层的安全策略实现安全加固。从落地角度而言，该方案只需要改造网关设备，不需要改造大量的终端设备，为增强 LoRa 网络安全提供了全新的应用模式和技术手段。

2 LoRaWAN 协议安全机制

工作在 MAC 层的 LoRaWAN 协议介绍了 LoRa 默认采取的安全策略[8]，每个 LoRa 终端拥有专属密钥 AppKey 产生的两个 128 bit 的会话密钥：NwkSKey 和 AppSKey。NwkSKey 用于确认 LoRaWAN 协议中数据包的真实性和完整性，AppSKey 提供了端到端加密确保通信的机密性，防止未授权者访问正在传输的应用数据。具体体现为，LoRa 终端接入认证方式随激活方式不同而有差异。协议规定 LoRa 终端有两种激活方式：空中激活（OTAA, over-the-air activation）和手动激活（ABP, activation by personalization）。在 OTAA 中，LoRa 终端拥有 DevEUI 和 AppEUI 两个专属标识，分别标识通信双方 LoRa 终端和服务器。LoRa 终端基于上述密钥和标识进行接入认证，确认身份后分配网络地址，允许接入网络。而在 ABP 中，LoRa 终端直接与特定的 LoRaWAN 协议配置安全通信所需的密钥和地址，不需要再接入认证确认身份安全[9]。此外，LoRaWAN 协议还规定数据包中需包含帧计数器以防重传攻击[10]。

即便如此，LoRa 通信仍存有较大的安全风险和漏洞。由上可知，密钥是整个 LoRaWAN 协议安全策略的核心，安全性与密钥及其管理息息相关。一旦攻击者获得密钥，LoRa 网络就将毫无秘密可言。近年来一些研究也表明，LoRa 现有安全策略对密钥的保护十分欠缺，攻击者想要非法破解 LoRaWAN 协议密钥并不困难。LoRaWAN 协议使用包计数器作为输入，重置后产生密钥流重用风险的概率很高[11]。并且没有制定密钥周期性更新和管理机制，每次更新密钥都只能重新接入或手动配置[2]。在 OTAA 中，会话密钥只有在每次重新接入网络时更新。而在 ABP 中，会话密钥的更新甚至需要管理者手动干预。不具备定期更新的机制会让会话密钥泄露的概率剧增，失去认证身份和保护会话安全的作用。并且一旦会话密钥被破解，在一段时间内会话内容都将暴露给攻击者[12]。此外，LoRa 终端也没有专门的安全存储模块存储密钥[13]，其微控制单元和无线模块之间的密钥交换也可以很容易地使用外部硬件拦截[5]。攻击者可以通过在 LoRa 网

络中加入高功率数据包破坏密钥随机性[14-15]。事实上，在网络安全系统中，密钥、身份标识等链路层特征是易于伪造的，意味着只针对数据链路层的安全防护必然存在风险。端到端的设备认证可以有效解决这一问题，但必须改造原有设备的特点让其投入生产实践的难度很大。LoRa 网络安全仍缺乏成熟的方案，引入新的 LoRa 终端接入认证方式很有必要。

3　LoRa 信号及射频指纹

3.1　LoRa 信号调制与解调

LoRa 信号调制使用啁啾扩频技术[16]，即在设定的带宽内让频率随时间线性变化来表示和传输信息，具有传输距离远、功耗低、包络稳定、鲁棒性高、抗多径抗衰落等诸多优势。频率随时间增加而线性增加的信号称为上啁啾，相反，频率随时间增加而线性减小的信号称为下啁啾。每一个符号的啁啾扩频都在一个固定长度的时间单元内进行，时间单元的长度由规定的带宽 BW 和扩频因子 SF 决定。设定带宽 $\mathrm{BW}\in\{125\ \mathrm{kHz},250\ \mathrm{kHz},500\ \mathrm{kHz}\}$，扩频因子 $\mathrm{SF}\in\{7,\cdots,12\}$，便可得到一个时间单元长度为 $T_s=\dfrac{2^{\mathrm{SF}}}{\mathrm{BW}}$（单位：s）。频带分成 $N=2^{\mathrm{SF}}$ 个等份，每个符号的取值 $s\in S\overset{\Delta}{=}\{0,\cdots,N-1\}$，意味着起始频率为 $f_1=\dfrac{\mathrm{BW}}{N}\cdot s-\dfrac{\mathrm{BW}}{2}=\dfrac{\mathrm{BW}}{2^{\mathrm{SF}}}\cdot s-\dfrac{\mathrm{BW}}{2}$。设定采样频率为 BW，频率随时间线性上升达到 $\dfrac{\mathrm{BW}}{2}$ 时便会翻转到 $-\dfrac{\mathrm{BW}}{2}$，之后频率继续上升。一个 LoRa 调制符号可以表示为

$$x_s(t)=\begin{cases}\mathrm{e}^{\mathrm{j}2\pi\left(\frac{\mathrm{BW}}{2T_s}t^2+(f_1)t\right)}, & 0\leqslant t\leqslant\dfrac{2^{\mathrm{SF}}-s}{\mathrm{BW}}\\ \mathrm{e}^{\mathrm{j}2\pi\left(\frac{\mathrm{BW}}{2T_s}t^2+(f_1-\mathrm{BW})t\right)}, & \dfrac{2^{\mathrm{SF}}-s}{\mathrm{BW}}<t\leqslant T_s\end{cases}\tag{1}$$

它的离散时间表示如式(2)

$$x_s[n]=\begin{cases}\mathrm{e}^{\mathrm{j}2\pi\left(\frac{1}{2\cdot2^{\mathrm{SF}}}\left(\frac{\mathrm{BW}}{2f_s}\right)^2n^2+\left(\frac{s}{2^{\mathrm{SF}}}-\frac{1}{2}\right)\left(\frac{\mathrm{BW}}{f_s}\right)n\right)}, & n\in\{0,\cdots,\dfrac{2^{\mathrm{SF}}-s}{\mathrm{BW}}f_s-1\}\\ \mathrm{e}^{\mathrm{j}2\pi\left(\frac{1}{2\cdot2^{\mathrm{SF}}}\left(\frac{\mathrm{BW}}{2f_s}\right)^2n^2+\left(\frac{s}{2^{\mathrm{SF}}}-\frac{3}{2}\right)\left(\frac{\mathrm{BW}}{f_s}\right)n\right)}, & n\in\{\dfrac{2^{\mathrm{SF}}-s}{\mathrm{BW}}f_s,\cdots,2^{\mathrm{SF}}-1\}\end{cases}\tag{2}$$

其中，f_s 是采样频率，$n=tf_s$。

因为采样频率 f_s=BW，式(2)可简化为

$$x_s[n]=e^{\mathrm{j}2\pi\left(\frac{n^2}{2\cdot2^{\mathrm{SF}}}+\left(\frac{s}{2^{\mathrm{SF}}}-\frac{1}{2}\right)n\right)},\quad n\in S\tag{3}$$

通过高斯白噪声信道后，接收端收到的信号为

$$y[n]=h\cdot x_s[n]+z[n],\quad n\in S\tag{4}$$

其中，h 是信道的传递函数，$z[n]\sim\mathrm{CN}(0,\sigma^2)$ 是高斯白噪声。将收到的信号先与 s=0 的上啁啾信号 $x_0[n]$ 的复共轭相乘，计算结果的离散傅里叶变换（DFT）为 Y，最终得到 LoRa 信号解调结果即传输符号为 $\hat{s}=\arg\max_{k\in S}(|Y[k]|)$。

3.2　LoRa 信号射频指纹提取

射频指纹工作在物理层，难以克隆和篡改，因此可以对 LoRa 终端的射频指纹进行识别和验证，以控制终端接入的安全，此方法具有比传统无线网络认证方法更高的安全性。现有的射频指纹提取方法包括基于瞬态指纹特征、稳态指纹特征[17-18]和星座轨迹图[19]的指纹提取。其中，基于瞬态指纹特征的指纹提取对接收信号的信噪比要求较高，基于稳态指纹特征的指纹提取需要对接收信号做精准的频率同步，基于星座轨迹图的指纹提取相对适合 LoRa 终端的射频指纹提取。星座图是数字信号在复平面中绘制表示的图形。星座图的横、纵坐标分别是 I 路和 Q 路，信号投影在 I 路的分量称为同相分量，投影在 Q 路的分量称为正交分量，数字信号的幅度和相位信息包含在它的星座图中。数字通信中如果接收方采样率高于发送方，将此过采样的信号绘制在复平面中即得到星座轨迹图。过采样使得星座轨迹图可以显示采样点的变化，反映信号特征及其变化规律，包括造成射频指纹唯一性的很多非线性偏差因素，因此，可以基于星座轨迹图提取射频指纹。

考虑在理想信道环境下，发射的基带信号为 $X(t)$，接收的基带信号为 $Y(t)$，则

$$Y(t)=X(t)\mathrm{e}^{-\mathrm{j}2\pi\Delta ft+\varphi}\tag{5}$$

其中，Δf 为收发双方的载波频率偏差，φ 为接收信号相位误差。接收的信号含有频率偏差 Δf，导致基带信号的每一个采样点都有一个相位旋转因子 $\mathrm{e}^{\mathrm{j}2\pi\Delta ft}$，该相位旋转因子随着采样点位置 t 的不同而变化，因此会造成信号星座轨迹图整体的旋转。对数据间隔时间 n 进行差分操作，可得

$$\begin{aligned}D(t)&=Y(t)\cdot Y^*(t+n)\\&=X(t)\cdot e^{\mathrm{j}2\pi\Delta ft+\varphi}\cdot X^*(t+n)\cdot e^{-\mathrm{j}2\pi\Delta f(t+n)-\varphi}\\&=X(t)\cdot X^*(t+n)\cdot e^{-\mathrm{j}2\pi\Delta fn}\end{aligned}\tag{6}$$

其中，X^*为 X 的共轭，且当差分间隔 n 为一个符号的间隔时，差分后信号 $D(t)$的幅值稳定，辐角与相位误差 φ 无关，只与载波频偏 Δf 和差分间隔 n 相关。固定差分间隔，则 $D(t)$信号的辐角与频偏具有线性关系，4 个不同设备前导码部分的星座轨迹图如图 1 所示，其中，白色部分表示经过差分后的数据点所在位置。

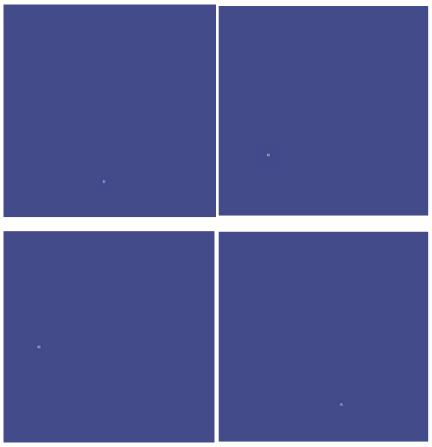

图 1　4 个不同设备前导码部分的星座轨迹图

每个 LoRa 终端设备每次发出的信号的星座轨迹图都不尽相同，但属于同一终端的星座轨迹图具有相似性。星座轨迹图中点分布的总体轮廓和形状、各区域点分布的密集程度等都伴随终端独一无二，包含了每个终端独有的射频指纹特征。根据区域点分布的密集程度，使用模式识别中的 K 均值聚类算法计算聚类中心提取指纹。具体方法是将星座轨迹图均匀分块，根据各块中轨迹点的数量对该块赋值 1 或 0，随后采用大均值聚类算法对赋值为 1 的块进行聚类，获得规定数目的聚类中心，并定为指纹。比较两个指纹，计算两个指纹的聚类中心欧氏距离和，当值小于规定的门限时即判断指纹相同，属于同一终端，否则判断属于不同终端，指纹获取及判别流程如图 2 所示。

星座图分块数量、赋值 0/1 的门限、聚类中心数目和最后指纹判决的门限都根据实际使用的 LoRa 终端类型和具体需求来确定，并且判决门限可通过不断的训练改进，使判决结果的准确率更高。

4　基于射频指纹的 LoRa 安全网关设计

4.1　LoRa 网关扩展

LoRaWAN 协议规定标准的 LoRa 网络架构由 4 部分组成，分别是 LoRa 终端、网关、网络服务器和应用服务器，如图 3 所示，呈星形拓扑结构。LoRa 终端多为与传感器组成的传感器节点。终端节点采集完数据后通过单跳 LoRa 无线通信与网关建立连接，按照 LoRa 通信协议进行传输。协议中 LoRa 网络有 Class A、Class B、Class C 3 种工作模式[20]。Class A 是所有 LoRa 终端必备的基础模式，规定节点只有在每次上行后允许打开两个接收窗口；Class B 除了 Class A 的两个接收窗口外还会根据网关发送的 Beacon 信标周期性地打开一个接收窗口；Class C 则在没有发送需求时一直开放接收窗口。网络服务器在 MAC 层工作，中转网关和应用服务器之间的消息，并对消息进行包含安全性检查在内的处理，对网关及通信网络进行控制和调节。应用服务器是 LoRa 网络架构中数据传输的目的地，针对数据管理网络提供应用服务。

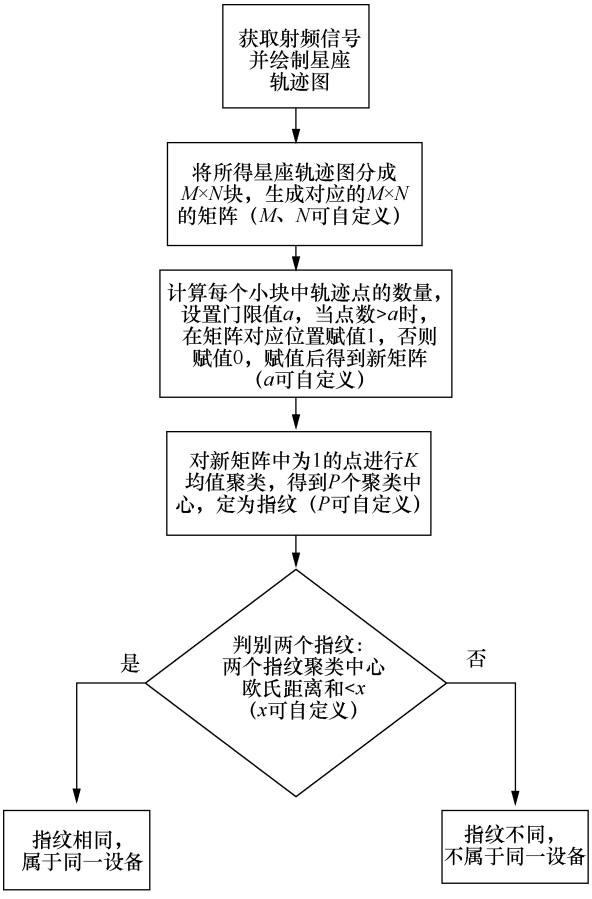

图 2　指纹获取及判别流程

在整个 LoRa 网络架构中，LoRa 网关和一般网关类似，承担中继和转发的责任。LoRa 网络中网关是终端节点和云端服务器的中继，负责接收并转发终端节点和云端服务器间的通信数据。全过程中

LoRa 网关只是将数据在 LoRa 通信和网络通信之间转换，并未对数据做任何附加的处理。由图 3 可以发现，所有终端节点发送和接收的数据若想到达服务器，必先经过 LoRa 网关。换言之，LoRa 网关是所有 LoRa 终端节点数据传输的必经关卡，因此具备管理通信链路、解决终端接入安全问题、维护网络架构安全的潜力。

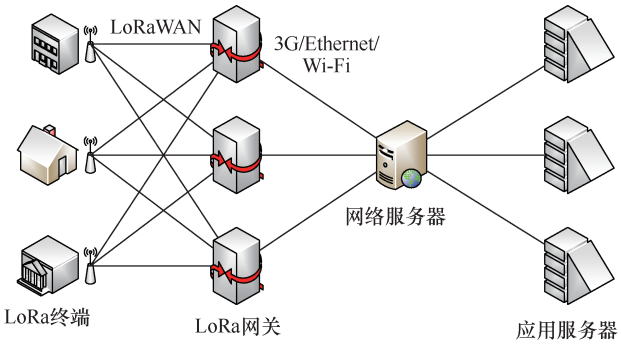

图 3　LoRa 网络架构

设计在 LoRa 网络架构中，于 LoRa 网关处对 LoRa 终端发出的射频信号制作射频指纹，配合原有的链路层身份标识，作为终端的身份凭证判定其安全与否。只有当终端被判定符合安全规则时，才允许其与云端服务器传输数据。通用软件无线电外设（USRP, universal software radio peripheral）可以接收 LoRa 终端信号，进而获取星座轨迹图并制作指纹。因此可将 USRP 与原来的网关一起组成新的网关，网关扩展 USRP 后的 LoRa 网络架构如图 4 所示。

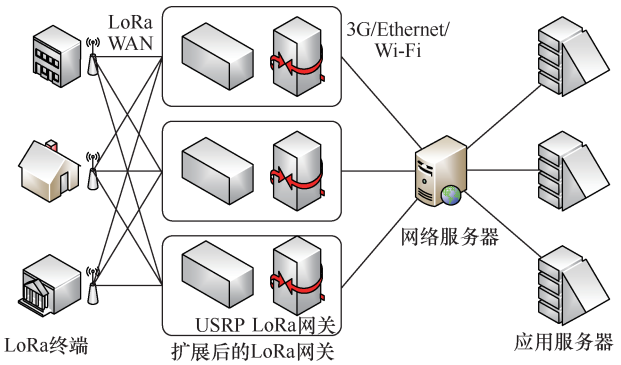

图 4　网关扩展 USRP 后的 LoRa 网络架构

原网关扩展加入 USRP 后的新网关工作步骤如下。

1) 事先将安全规则存储在网关中，安全规则包括安全 LoRa 终端的链路层身份标识和对应的指纹。若后续还有新的安全终端接入，其链路层身份标识和指纹可扩展加入安全规则。

2) 使用 USRP 接收 LoRa 终端射频信号，获取指纹并提取 LoRa 终端链路层身份标识，一并发送网关。网关将 USRP 发来的终端指纹和对应的链路层身份标识绑定，标记为当前在线终端。

3) 同时，网关也接收终端信号并解析成链路层数据包，提取链路层身份标识，和预存安全规则中的安全身份标识进行比对。若无匹配结果，判断该 LoRa 终端身份不安全，跳转步骤 5)；若匹配，跳转步骤 4)。

4) 网关将自己提取的 LoRa 终端链路层身份标识和 USRP 发送的链路层身份标识作匹配，这样就将网关解析得到的链路层数据包和指纹绑定。随后将这一绑定了指纹的数据包与步骤 3)中和预存安全规则匹配的身份标识对应的指纹比对，从而判断网关接收的 LoRa 终端数据包是否完全符合安全规则：若不匹配，判断该 LoRa 终端身份不安全，跳转步骤 5)；若匹配，则判断该 LoRa 终端身份安全，网关可将该合法数据包转发至网络服务器。

网关接收网络服务器下行数据并解析成链路层数据包，提取链路层身份标识，和预存安全规则进行匹配，获取安全规则中的合法终端指纹并绑定，再与在线 LoRa 终端进行比对：若对应链路层身份标识绑定的指纹不匹配，判断该 LoRa 终端身份不安全，跳转步骤 5)；若匹配，则判断该 LoRa 终端身份安全，允许网关将网络服务器的数据包转发至该 LoRa 终端。

5) 网关对不安全的 LoRa 终端数据包进行阻断，对不安全的 LoRa 终端阻止其继续接入网关。

扩展 USRP 后的 LoRa 网关工作流程如图 5 所示。

新的网关在物理层控制终端接入安全，在消息上传到服务器前或服务器消息下行到终端前拒绝不安全的终端的请求，减少隐患，使网关不只是接收转发的中间点，还在 LoRa 网络架构中承担重要的安全责任，帮助维护 LoRa 网络安全。

4.2　LoRa 网关替换

在 LoRa 网关添加控制终端接入安全的射频指纹提取功能，除了将 USRP 加入 LoRa 网络架构和原来的网关一起组成新的网关以外，还可以让具备提取指纹能力的 USRP 取代原有网关在整个网络中的位置。如果只是将 USRP 和 LoRa 网关组合在一起做简单的“一加一”，会丧失掉原先标准 LoRa 网络架构的精简性。USRP 具有获取射频信号并制作

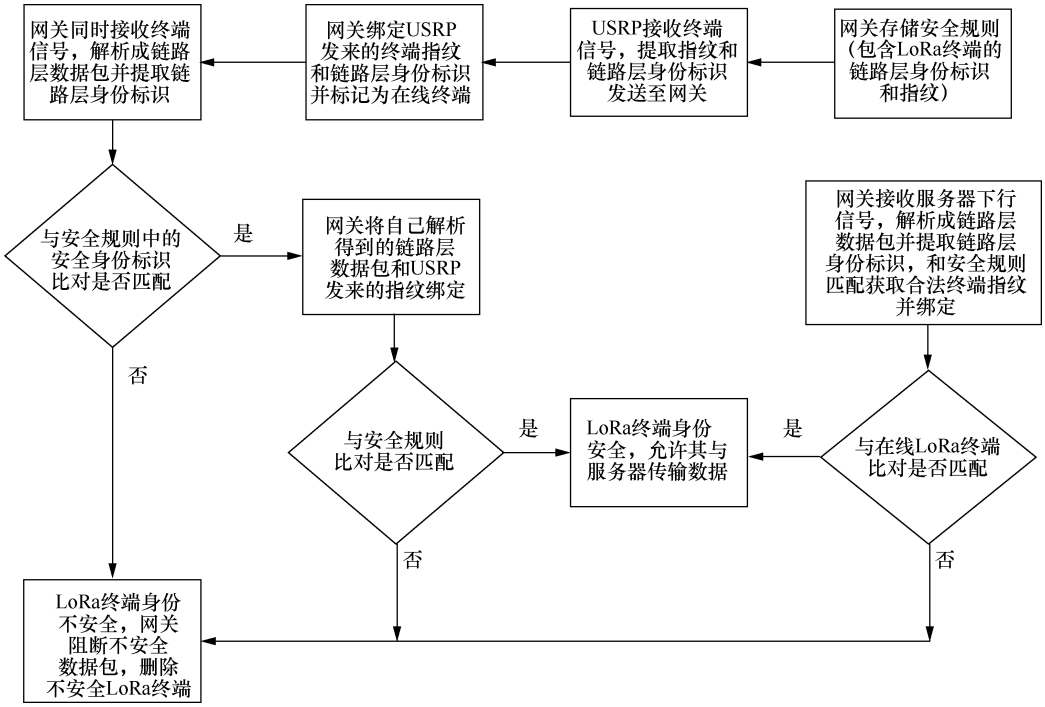

图 5　扩展 USRP 后的 LoRa 网关工作流程

指纹的能力，因此使 USRP 实现原有网关的中继转发功能，以取代网关在 LoRa 网络中的位置，不扩大整个架构的规模。USRP 取代网关后的 LoRa 网络架构如图 6 所示。

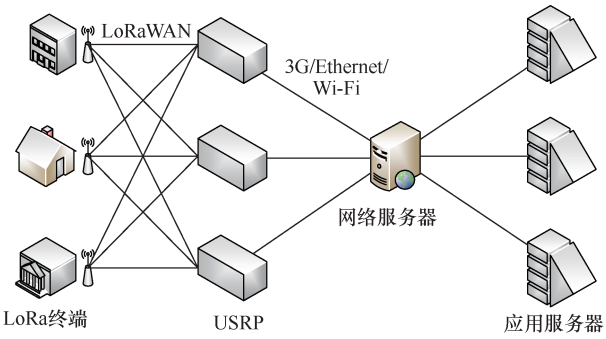

图 6　USRP 取代网关后的 LoRa 网络架构

与 USRP 和原网关组成新网关的方案相比，USRP 取代网关成为新网关后的工作步骤略有不同，具体如下。

1) 事先将安全规则存储在 USRP 中，安全规则包括安全 LoRa 终端的链路层身份标识和对应的指纹。若后续还有新的安全终端接入，其链路层身份标识和指纹可扩展加入安全规则。

2) 使用 USRP 接收 LoRa 终端射频信号并获取指纹，解析成链路层数据包并提取 LoRa 终端链路层身份标识。将终端指纹和对应的链路层身份标识绑定，标记为当前在线终端。

3) USRP 将绑定的指纹和链路层身份标识同预存的安全规则中对应的身份标识和绑定的指纹进行比对，从而判断 USRP 接收的 LoRa 终端数据包是否符合安全规则。若不匹配，判断该 LoRa 终端身份不安全，跳转步骤 4)；若匹配，则判断该 LoRa 终端身份安全，USRP 可将该合法数据包转发至网络服务器。

USRP 接收网络服务器下行数据并解析成链路层数据包，提取链路层身份标识，和预存安全规则进行匹配，获取安全规则中的合法终端指纹并绑定，再与在线 LoRa 终端进行比对。若对应链路层身份标识绑定的指纹不匹配，判断该 LoRa 终端身份不安全，跳转步骤 4)；若匹配，则判断该 LoRa 终端身份安全，允许 USRP 将网络服务器的合法数据包转发至该 LoRa 终端。

4) USRP 对不安全的 LoRa 终端数据包进行阻断，对不安全的 LoRa 终端阻止其继续接入 USRP。

USRP 取代原有网关的 LoRa 新网关工作流程如图 7 所示。

实现原有网关的中继转发功能需要完整地实现 LoRa 物理层收发链。虽然 LoRa 的技术细节是专有的、封闭的，但近些年大量的逆向工程工作和相应的软件无线电（SDR, software defined radio）

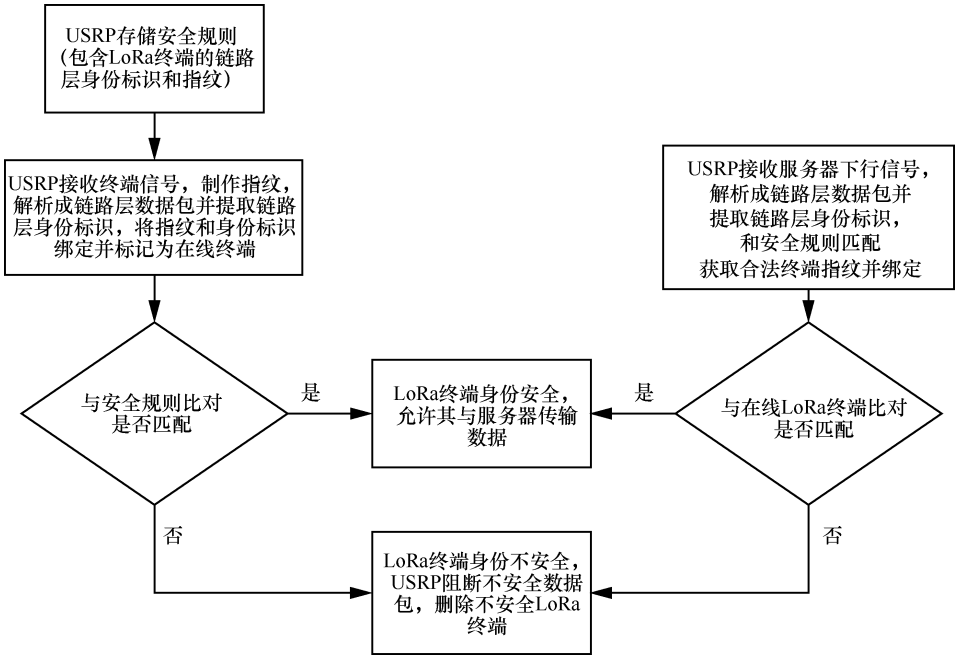

图 7　USRP 取代原有网关的 LoRa 新网关工作流程

实现揭示了 LoRa 物理层的许多重要细节[21-22]，给复现 LoRa 物理层收发链创造了可能。作为硬件的 USRP 搭配的 GNU Radio 是一个自定义无线电收发、创建通信系统的开源软件系统。LoRa 物理层收发链如图 8 所示，提供了一种 LoRa 物理层收发链的 GNU Radio SDR 实现方式，具有所有必需的发送和接收组件，可以很好地让 USRP 实现 LoRa 信号的收发，达到取代原有网关的目的。

LoRa 物理层发送链按先后顺序依次包括白化、汉明编码、交织、格雷编码和 LoRa 调制 5 个模块。接收链则与发送链对应相反，先编码对应后解码，后调制对应先解调。LoRa 物理层接收链按先后顺序依次包括 LoRa 解调、格雷解码、解交织、汉明解码和解白化 5 个模块。

白化模块将消息序列与伪随机序列位异或，以消除传输消息中的直流偏置。LoRa 基础白化矩阵对应编码率为 CR=4/8，当 CR=4/7 和 CR=4/6 时分别去掉基础矩阵的最右一列和最右两列得到白化矩阵。而因为当 CR=4/5 时 LoRa 采用的纠错编码技术由汉明码换成了奇偶校验码，所以 CR=4/5 时白化矩阵的最右一列与基础白化矩阵对应列有所不同。LoRa 使用的具体白化矩阵可参考文献[22]。当 CR=4/5 时可发现矩阵的奇偶校验位由前 4 位白化后计算得出的，这意味着白化是 LoRa 发送链中的第一个模块。

纠错编码通过增加码字冗余减弱信道噪声的影响，提高通信传输的鲁棒性。在 LoRa 中，冗余量由编码速率 CR 控制，共 4 种，分别是 $\mathrm{CR}\in\left\{\frac{4}{5},\frac{4}{6},\frac{4}{7},\frac{4}{8}\right\}$。对于 $\mathrm{CR}=\frac{4}{6},\frac{4}{7},\frac{4}{8}$，这 3 个较低的编码率，LoRa 使用($k$,$n$)汉明编码，其中，$k$ 是数据长度，取值为 4，n 是码字长度，取值 $n\in\{6,7,8\}$。(4,7)汉明编码和(4,6)汉明编码的码字分别是(4,8)汉明编码删除 1 位和删除 2 位的删减版本。与白化模

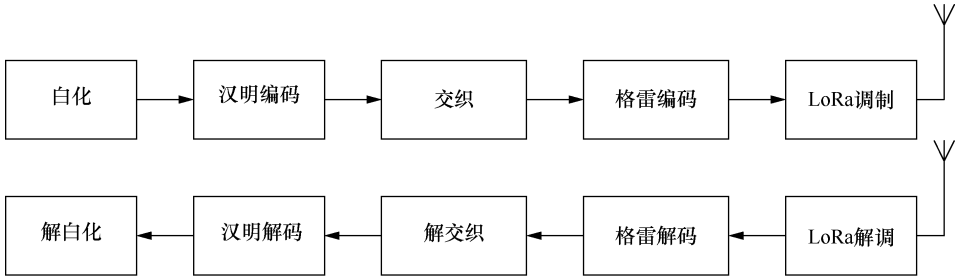

图 8　LoRa 物理层收发链

块的情况对应，当 CR=4/5 时，LoRa 采用的纠错编码技术与其他 3 种编码率的不同，此时 LoRa 使用奇偶校验码代替(4,5)汉明编码。纠错编码具体生成矩阵和校验矩阵可参考文献[22]。

交织模块将因噪声和衰落而产生的错误分布在多个码字上，打破错误比特之间的相关性，从而提供更好的抗噪声性能。这是旨在纠正码字随机错误的纠错编码无法做到的。LoRa 使用的交织器是一种对角交织器，对角交织器能把输入矩阵的一行分散到输出矩阵的对角线上。LoRa 使用的对角交织器可将最大 SF 个由符号错误引起的错误比特，分配到多个纠错码字里。由于大多数码字仅有可能包含一个误码，LoRa 使用纠错编码和交织的组合能够保证很高的正确解码率。

格雷编码将任何数字形式的符号映射成二进制序列，映射后原本相邻的符号对应的二进制序列后仅有一位不同。这一特性适合应用在传输中相邻符号之间容易发生混淆错误的通信调制技术。据此，LoRa 使用格雷编码保证当发生相邻符号混淆时，经过格雷映射之后仅会产生一位的错误，而编码率为 $CR = 4/7$ 和 $CR = 4/8$ 的纠错编码可以纠正一位的错误，将格雷编码与之组合非常合适。

接收链的各个模块分别与发送链对应，并且具有一定相似性，不再赘述。需要说明的是，在 GNU Radio 的 LoRa 物理层收发链模块中，包括扩频因子 SF、编码率 CR、带宽 BW 等参数都可以根据用户需求选择。

由此可见，USRP 可以实现网关的 LoRa 物理层收发功能，结合其获取星座轨迹图制作指纹的能力，非常适合作为新的网关控制终端接入，负责 LoRa 网络架构的安全。

4.3 性能比较及分析

本文提出了两种基于射频指纹的 LoRa 安全网关设计实现方案，从功能角度，两种方案均实现了针对 LoRa 终端的物理层安全接入防护，两种接入方案对比见表 1。

网关扩展的方案由于在原网关上进行改造，可以保留原网关的技术指标，可以很好地兼容原有的通信系统，但是具体实现需要对现有设备进行软硬件改造，存在一定的复杂度和不可控因素，如果由生产设计环节介入或者由生产厂商配合，网关扩展是一种很好的安全提升解决方案。网关替换方案可以直接使用现成的 USRP 平台实现，但是软件实现需要很大的工作量，性能指标也和平台的指标参数直接相关。其优点是具有很大的设计自由度，方便研究和算法及功能定制。

表 1 两种接入方案对比

	LoRa 网关扩展	LoRa 网关替换
解调性能	好	一般
通信距离	远	一般
终端兼容性	好	一般
接入算法自由度	一般	高
指纹识别率	一般	高
改造内容	硬件及软件改造	软件开发
软件改造工作量	适中	较大
硬件改造工作量	大	无

另外，两种方案在使用过程中并不影响原系统平台的通信功能，当 LoRa 终端通过多址接入产生数据碰撞时，通信功能受阻，此时安全功能无须介入。

5 结束语

目前，LoRa 网络安全方案仍存有较明显的缺陷，引入射频指纹这个物理层概念给 LoRa 网络安全研究提供了一个新的方向。根据 USRP 接收信号提取指纹的能力，改进 LoRa 网关，提出了两种全新的 LoRa 网络安全方案，对解决 LoRa 终端的身份认证和接入安全问题有所帮助。目前的安全规则只包括链路层身份标识和射频指纹两种匹配尺度，后续还可扩展加入链路层数据负载中的网络层地址、传输层端口与应用层身份标识符等尺度，使多重安全标准和安全方法结合工作，更好地保护 LoRa 网络安全。除此之外，指纹算法、LoRa 物理层收发链的复现也需继续研究改进，以应对物联网复杂多变的通信情况，更切实地了解 LoRa 技术并针对性地改进安全方案。

参考文献：

[1] NEUMANN P, MONTAVONT J, NOËL T. Indoor deployment of low-power wide area networks (LPWAN): a LoRaWAN case study[C]//2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Piscataway: IEEE Press, 2016: 1-8.

[2] SANCHEZ-IBORRA R, SÁNCHEZ-GÓMEZ J, PÉREZ S, et al. Enhancing LoRaWAN security through a lightweight and authenticated key management approach[J]. Sensors, 2018, 18(6): 1833.

[3] ZULIAN S. Security threat analysis and countermeasures for LoRa-

WAN join procedure[EB]. 2015.

[4] KIM J, SONG J. A dual key-based activation scheme for secure LoRaWAN[J]. Wireless Communications and Mobile Computing, 2017, 2017: 1-12.

[5] ARAS E, RAMACHANDRAN G S, LAWRENCE P, et al. Exploring the security vulnerabilities of LoRa[C]//2017 3rd IEEE International Conference on Cybernetics (CYBCONF). Piscataway: IEEE Press, 2017: 1-6.

[6] DANEV B, ZANETTI D, CAPKUN S. On physical-layer identification of wireless devices[J]. ACM Computing Surveys, 2012, 45(1): 1-29.

[7] 袁红林, 胡爱群. 射频指纹的产生机理与惟一性[J]. 东南大学学报(自然科学版), 2009, 39(2): 230-233.
YUAN H L, HU A Q. Fountainhead and uniqueness of RF fingerprint[J]. Journal of Southeast University (Natural Science Edition), 2009, 39(2): 230-233.

[8] DE CARVALHO SILVA J, RODRIGUES J J P C, ALBERTI A M, et al. LoRaWAN—A low power WAN protocol for Internet of Things: a review and opportunities[C]//2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech). Piscataway: IEEE Press, 2017: 1-6.

[9] BEHRAD S, TUFFIN S, BERTIN E, et al. Network access control for the IoT: a comparison between cellular, Wi-Fi and LoRaWAN[C]//2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN). Piscataway: IEEE Press, 2019: 195-200.

[10] SANTAMARIA M, MARCHIORI A. Demystifying LoRa WAN security and capacity[C]//2019 29th International Telecommunication Networks and Applications Conference (ITNAC). Piscataway: IEEE Press, 2019: 1-7.

[11] YANG X Y, KARAMPATZAKIS E, DOERR C, et al. Security vulnerabilities in LoRaWAN[C]//2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI). Piscataway: IEEE Press, 2018: 129-140.

[12] SANCHEZ-IBORRA R, SÁNCHEZ-GÓMEZ J, PEREZ S, et al. Internet access for LoRaWAN devices considering security issues[C]//2018 Global Internet of Things Summit (GIoTS). Piscataway: IEEE Press, 2018: 1-6.

[13] BUTUN I, PEREIRA N, GIDLUND M. Security risk analysis of LoRaWAN and future directions[J]. Future Internet, 2018, 11(1): 3.

[14] BASU D, GU T B, MOHAPATRA P. Security issues of low power wide area networks in the context of LoRanetworks[EB]. 2020.

[15] CHACKO S, JOB M D. Security mechanisms and Vulnerabilities in LPWAN[J]. IOP Conference Series: Materials Science and Engineering, 2018, 396: 012027.

[16] VANGELISTA L. Frequency shift chirp modulation: the LoRa modulation[J]. IEEE Signal Processing Letters, 2017, 24(12): 1818-1821.

[17] DEMERS F, ST-HILAIRE M. Radiometric identification of LTE transmitters[C]//2013 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE Press, 2013: 4116-4121.

[18] ROMERO H P, REMLEY K A, WILLIAMS D F, et al. Electromagnetic measurements for counterfeit detection of radio frequency identification cards[J]. IEEE Transactions on Microwave Theory and Techniques, 2009, 57(5): 1383-1387.

[19] PENG L N, HU A Q, JIANG Y, et al. A differential constellation trace figure based device identification method for ZigBee nodes[C]//2016 8th International Conference on Wireless Communications & Signal Processing (WCSP). Piscataway: IEEE Press, 2016.

[20] CHEONG P S, BERGS J, HAWINKEL C, et al. Comparison of LoRaWAN classes and their power consumption[C]//2017 IEEE Symposium on Communications and Vehicular Technology (SCVT). Piscataway: IEEE Press, 2017: 1-6.

[21] GHANAATIAN R, AFISIADIS O, COTTING M, et al. Lora digital receiver analysis and implementation[C]//ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Piscataway: IEEE Press, 2019.

[22] JOACHIM T. Complete reverse engineering of LoRa PHY[EB]. 2019.

[作者简介]

姜禹（1981– ），男，博士，东南大学网络空间安全学院副教授，主要研究方向为物理层安全、无线网络安全、RFID 技术、物联网技术等。

陈思卿（1996– ），男，东南大学网络空间安全学院硕士生，主要研究方向为物理层安全、无线网络安全、RFID 技术、物联网技术等。

孙雯（1988– ），女，博士，东南大学网络空间安全学院讲师，主要研究方向为物理层安全、无线网络安全、人工智能、物联网技术等。