

面向 LoRaWAN 开发的工具支持：仿真与模拟的对比视角

彭晨曦，赵博文*

郑州大学数学与统计学院，郑州 450001，河南，中国

摘要：本文探讨了在设计与评估物联网网络时，各类远距离无线区域网络（LoRaWAN）仿真与模拟工具的使用。仿真工具因成本较低、易于对大规模网络建模而在研究者中广受欢迎，可便捷、快速地检验各种协议与行为的可扩展性；但它们往往难以体现真实部署中固有的不可预测性。模拟工具与云端工具弥补了这一不足：凭借其灵活性，它们能够更真实地逼近实际性能表现，并更便于与真实的网络硬件基础设施对接；不过其成本通常更高，且往往受制于使用者的技术水平。

关键词：模拟工具；物联网；远距离无线区域网络安全；仿真工具

Tool Support for LoRaWAN Development: A Comparative Perspective on Simulation and Emulation

ChenXi Peng, BoWen Zhao*

School of Mathematics and Statistics, Zhengzhou University, Zhengzhou 450001, Henan, China

Abstract: This paper explores the use of various long range wireless area network (LoRaWAN) simulation and emulation tools when designing and evaluating IoT networks. Simulation tools are often popular with researchers because they are less costly and can easily simulate large-scale networks, allowing for easy and faster tests of the scalability of various protocols and behaviors. However, they often lack the unpredictable nature of real deployments. Emulation and cloud-based tools fill this gap, but with their flexibility they provide a more realistic approximation of real-world performance and allow easier interfacing with actual network hardware infrastructure, although they generally incur a higher cost which is often controlled by technical skill level use.

Keywords: Emulation tools; Internet of things; Long range wireless area network security; Simulation tools

一、引言

物联网（IoT）由能够在无人直接干预的情况下生成并共享数据的受限物理设备构成，通常包含感知层、通信层、处理层与用户交互层[1-2]。在众多物联网通信技术中，远距离无线区域网络（LoRaWAN）已成为最受欢迎的技术之一，在需要长距离连接并兼顾低功耗的应用中受到广泛关注[1,3]。LoRaWAN 由 Semtech 公司开发，采用非授权频段并结合线性调频扩频（CSS）调制，从而在实现安全通信的同时延长设备电池寿命并提高通信效率[1-4]。其星形拓扑结构使终端节点可经由网关向中心网络服务器发送数据，从而实现网络的远程监测、控

制与扩展[5-8]。

LoRaWAN 通过空中激活 (OTAA) 或个性化激活 (ABP) 两种设备激活方式, 在部署安全性、灵活性与效率之间取得平衡。为适配不同的功耗与时延需求, LoRaWAN 提供认证、完整性保护与加密技术, 设备可实现为 A、B、C 三类之一。然而, 尽管 LoRaWAN 提供了安全机制, 网络仍易受窃听、数据篡改与非法访问等数据威胁与攻击[9]。

仿真器与模拟器是 LoRaWAN 结构设计、功能设计与优化中的关键要素。它们可对网络拓扑、信号传输、数据流、能耗与兼容性进行建模, 有助于识别瓶颈、验证协议并消除受攻击的脆弱性。开源平台通常更受青睐, 因其灵活、经济、不依赖特定厂商, 并经过严格测试以确保满足安全参数要求。尽管 LoRaWAN 技术的应用日益普及, 但由于平台众多且缺乏指导, 研究者在选择合适的仿真器与模拟器时仍面临困难[10-12]。图 1 给出了包含终端设备、网关、网络服务器与应用在内的 LoRaWAN 总体架构, 并说明了安全套接层 (SSL) 如何在传输控制协议 / 互联网协议 (TCP/IP) 与远距离 (LoRa) 两个层面上保障通信流的安全。为填补上述空白, 本文考察了若干知名 LoRaWAN 工具在性能、可扩展性、易用性、灵活性、设备类别支持、许可与集成能力等方面的表现, 旨在为工具选择提供有益建议, 并推动 LoRaWAN 协议与应用设计的进一步发展。本文其余部分安排如下: 第二部分为文献综述; 第三部分介绍研究方法; 第四部分给出关键结果与讨论; 第五部分为结论。

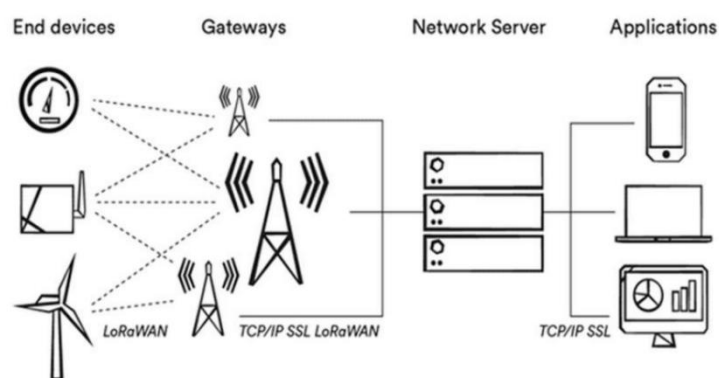


Figure 1 LoRaWAN Architecture

图 1 LoRaWAN 架构

二、文献综述

从现有文献可见, 在 LoRaWAN 环境的开发技术方面, 建立兼顾准确性与实用性的模型的需求日益凸显。为研究物联网应用的效果, 学界已对仿真模型与模拟器模型开展了大量研究。

(一) 相关研究

已有多项研究对 LoRaWAN 仿真器进行了评价, 但主要聚焦于特定框架内的性能特征。例如, 文献梳理了 NS-3 的各模块, 以帮助研究者选择合适的 LPWAN 组件; 文献[1]与[2]则给出了更为宽泛的分析, 强调设计需求、实验类型与性能约束。IDRIS 等进一步考察了三种常见仿真器在 CPU 负载、内存占用、冲突与投递率等关键指标上的表现, 但更广泛的评价仍属必要。ALMUHAYA 等比较了各类 LPWAN 技术并突出了 LoRa 的优势, 但其评估缺乏对仿真环境的细致比较。类似地, MARINI 等[5]使用 MATLAB 分析了 LoRaWANSim, 指出了仿真过程中的过度简化问题, 却未将其与其他方案进行基准对比, 这凸显了跨仿真层次开展比较研究的必要性。

包括文献[1]在内的多数已有研究局限于性能与可扩展性。互操作性与安全性评估较为稀缺; 近期研究虽涉及效率问题, 但对能耗感知的安全框架论述不深。加密与认证虽有探讨, 跨工具评价却依然有限。另一挑战在

于评价方法的不一致: 缺乏标准化基准, 比较结果的可靠性便会下降。硬件在环(HIL)模型正在兴起, 通过将干扰、拥塞等真实条件注入仿真环境来弥合这一差距; 但理论测试仍占主导, 环境变量常被忽略。引入机器学习方法有望改善动态威胁检测并优化工具选择。本文通过对现代 LoRaWAN 模拟器与仿真器的对比分析填补当前空白, 为依据具体应用需求与安全参数进行选择提供指导。

本文的目标并非评定出唯一的最佳平台, 而是帮助研究者与开发者选择最契合其项目目标的工具, 尤其是在需要兼顾安全性、可扩展性与特定应用需求时。

(二) LoRaWAN 前沿工具

本节分别介绍侧重于网络性能建模的仿真工具, 以及用于测试更贴近真实系统交互的模拟工具。表 1 至表 6 概括了各工具的关键特性, 包括性能指标、基础设施、设备支持与可用的安全机制。

1. LoRaWAN 仿真工具

本小节讨论若干现有的 LoRaWAN 网络构建与测试仿真工具。表 1 与表 2 从易用性、可扩展性、许可、支持、设备类别兼容性与集成能力等方面对这些工具进行了归纳, 旨在为研究者提供对比参考, 支持其作出知情的工具选择。

LoRaSim 是一款采用 MIT 许可的开放标准仿真器, 可在多种部署场景下对 LoRaWAN 网络进行性能分析。它支持可定制的流量模式、网络拓扑与射频配置, 并提供图形界面交互。该工具在研究中被广泛采用, 可进行协议测试与攻击仿真, 具备良好的可扩展性与跨平台集成能力。类似地, 遵循 GNU GPLv2 的 NS-3 是一款离散事件仿真器, 在科研与教学中被广泛使用。它可用于评估包括 TCP 拥塞算法、SDN 架构与路由模型在内的多种网络协议, 并支持可扩展部署; 结合完善的安全模块, NS-3 可在各种 LoRaWAN 配置下测试攻击缓解策略[1-2]。

另一款通用工具是 FloRa, 这是一款灵活的开源仿真器, 注重易用性以及与其他物联网平台的互操作性。尽管它并非针对特定技术且缺乏明确的安全协议, 但支持全部 LoRaWAN 设备类别, 并借助不断壮大的开发者与厂商社区实现可扩展的网络配置[1]。此外, 以 MIT 许可发布的 LoRaEnergySim 专注于 LoRaWAN 设备能耗建模, 可适配小型至大型网络, 支持全部设备类别并能与外部工具集成, 但不含加密与认证功能[2]。LoRaFree 同样提供基于浏览器的界面与可配置的网络管理, 支持设备认证与加密、全部 LoRaWAN 类别, 并可通过 WebSockets、HTTP 与 MQTT 等 API 与第三方平台互操作。该工具采用 Apache 2.0 许可, 允许不受限制地修改与分发, 但支持资源仅限于 GitHub 与社区论坛[4]。

同样地, 基于 Java 的开源仿真器 CupCarbon 提供图形化建模, 可对多种设备的无线传播、能耗与分组投递进行建模。它能够仿真包括 ESP32、Android 与 IoTNode 在内的数千个节点, 并可与 MATLAB、NS-3、OMNeT++ 等平台集成; 依据 GNU 通用公共许可证允许教学使用, 并提供丰富的文档与教程。与之类似, SimpleIoTSimulator 支持多种网络类型与设备(包括 LoRa 传感器与 MQTT 客户端), 提供向导式界面与消息回放功能, 可仿真大规模网络并分析加密、认证与密钥管理等关键安全机制, 同时配有文档、演示与在线资源。Mbed Simulator 则是一款开源方案, 支持包括 LoRa 传感器与网关在内的复杂网络配置, 并同时提供 Mbed OS 5 的在线与离线版本。它以 Apache 2.0 许可发布, 要求使用者在论文中加以引用。尽管其文档未明确说明内置安全特性, 但可与 MATLAB 等平台集成并支持全部设备类别, 通用性较强; 已有大量研究使用 Mbed Simulator 评估加密、认证与密钥管理等关键安全机制。

遵循 GNU 通用公共许可证的 OMNeT++ 在学术研究中被广泛用于非商业用途。它提供图形界面与命令行界面, 可用于模型设计、仿真执行与结果分析; 支持以 C++ 编写节点程序, 可处理数千个节点, 兼容全部 LoRaWAN 设备类别并可与外部平台集成。虽然其文档未突出面向 LoRaWAN 的安全模块, 但已被广泛应用于加密协议与

认证框架的研究。另一款重要工具是 Network Simulator，它是一款免费开源工具，界面友好，兼容多种拓扑、信道模型与调制方式，支持 LoRaWAN 全部三类设备，并向第三方应用提供 API。尽管兼容性很强，其文档对安全特性的说明不多；不过已有研究用它分析协议在受攻击时的安全性[1-5]。相应地，LoRaSimu 是一款遵循 LoRa 联盟使用条款的开源网页版仿真器，支持全部设备类别、可重构拓扑与全部载荷格式，并允许创建与修改网络模型。由于缺乏内置认证与加密功能[5]，且对第三方平台集成的支持有限，它并不完全适用于安全网络的仿真。

Table 1 LoRaWAN Simulation Tools Summary

表 1 LoRaWAN 仿真工具概览

工具	易用性	可扩展性	灵活性	许可	支持	设备类别	集成能力
LoRaSim [1][2][5]	界面简洁友好	小型至大型网络	拓扑与调制方式可配置	MIT (开源)	GitHub 社区、文档	A、B、C	OMNeT++、R、MATLAB
NS-3	需具备编程能力	小型至大型网络	高级定制、协议灵活	GNU GPLv2	活跃社区、邮件列表	A、B、C	NS-3、MATLAB、OMNeT++、Python
FloRa -	基于 OMNeT++ 框架的直观界面	小型至大型网络	支持动态 ADR、LoRa 专用设置	MIT (开放标准)	阿尔托大学与开发者论坛	A、B、C	SimuLTE、Veins、物联网平台
LoRaEnergySim [2]	界面直观	小型至大型网络	面向能耗、参数可定制	MIT (开源)	社区论坛	A、B、C	支持外部工具
LoRaFree [4]	网页版、界面友好	小型至中型规模	载荷与设备配置灵活	Apache 2.0	基于 GitHub 的支持	A、B、C	WebSockets、HTTP、MQTT API
CupCarbon	直观图形界面，支持 OSM	小型至大型网络	节点脚本 (Python/SenSc ript)、MQTT	GNU 通用公共许可	教程、GitHub、在线文档	A、B、C	NS-3、MATLAB、OMNeT++、FloRa
SimpleLoTSimulator	向导式图形界面	小型至大型网络	载荷与网关仿真可定制	许可使用，需引用	产品说明、演示视频	A、B、C	NS-3、CupCarbon、MATLAB、OMNeT++
Mbed Simulator	网页界面 + 离线 OS 5	小型至大型网络	支持 C++、可进行 MQTT 测试	Apache 2.0	GitHub、博客、视频教程	A、B、C	NS-3、MATLAB、CupCarbon、FloRa

另一款便于开发与试验大规模网络模型的易用工具是 LoRaWAN Simulator。除设备定制与载荷格式化选项外，它还支持 ABP、OTAA 与 ADR 等基本协议；由于提供加密与密钥管理选项，安全性成为其重点之一。该工具易于与其他外部软件包对接，并配有完善的文档，因而在学术与商业场景中均具可用性[1][5]。ChirpStack 是一款采用 Apache 2.0 许可的开源 LoRaWAN 网络服务器，在商业与科研部署中以可扩展性与灵活性著称。它支持安全通信协议，可承载数千台设备与网关，并配有现代化的网页界面；活跃的开发社区持续贡献，保证了其长期生命力与持续演进[9]。The Things Network (TTN) 是一项免费的、以 GPL 许可发布的开源计划，面向全球开放，旨在提供经济高效的 LoRaWAN 解决方案，具备可靠的数据存储、稳健的设备管理与安全的应用

集成; 其在学术界与产业界的普遍使用印证了其价值与经济性[6]。

TTN 支持种类繁多的设备与网关; 但对用户而言易用性仍是挑战, 相关成本也可能构成阻碍。其完善的客户支持以及对智慧城市与农业应用的适配性, 使其成为面向特定场景部署的合适选择[6]。此外, LoRaWAN Test Suites 为全部设备类别、自适应速率配置与扩频因子提供标准化的验证环境。它们不提供 API 集成, 也没有社区论坛支持; 但完整实现了加密、认证与授权协议, 因而适用于安全网络的认证与合规评估。

Table 2 LoRaWAN Simulation Tools Summary (Continued)

表 2 LoRaWAN 仿真工具概览 (续)

工具	易用性	可扩展性	灵活性	许可	支持	设备类别	集成能力
OMNeT++ -	图形界面与 命令行结 合, 适于精 细仿真	小型至大 型网络	可视化建模、 C++脚本可定制	GNU 通用 公共许可 证	手册、教程、 GitHub	A、B、 C	NS-3、MATLAB、 FloRa、CupCarbon
LoRaWAN Network Simulator [1][2][6]	图形化建模	小型至大 型网络	信道设置、支持 多种调制	经 LoRa 联盟开源	论坛、文档	A、B、 C	提供仿真器互操 作 API
LoRaSimu [5]	浏览器端建 模与分析	多节点场 景	载荷与网络参 数可配置	经 LoRa 联盟开源	联系表单、 反馈渠道	A、B、 C	NS-3、MATLAB、 CupCarbon、FloRa
LoRaWAN Simulator [1][5]	图形化建模 套件	多节点网 络	设备载荷与配 置可自定义	经 LoRa 联盟开源	联系表单、 反馈渠道	A、B、 C	NS-3、MATLAB、 CupCarbon、FloRa
TTN [6]	网页版, 易 于管理与测 试网络	大规模 LoRaWA N 部署	开放架构支持 安全通信与应 用集成	GNU GPL	社区文档、 论坛、开发 者支持	A、B、 C	NS-3、MATLAB、 FloRa、 CupCarbon、API
Loriot	图形界面支 持远程访 问、ADR、 地理定位、 云端 / 本地 部署	高度可扩 展, 企业 级	支持多种部署 模式与物联网 应用	商业专有	邮件、电话、 文档、知识 库	A、B、 C	NS-3、OMNeT++、 API、企业平台
Lorix One	云端设备 / 网关管理	可跨多设 备扩展	ADR、地理定 位、远程监控, 可与其他平台 集成	商业专有	邮件、电话、 文档 (可能 有限)	A、B、 C	API、物联网平台, 可与 TTN、Loriot 互操作
LoRaWAN Test Suites	命令行与图 形界面, 用 于合规与认 证测试	跨合规、 跨区域与 跨类别测 试	测试 A/B/C 类、 ADR 与扩频因 子	免费工具 集	用户指南; 无专门支持 门户	A、B、 C	仅 USB 或射频接 口, 无外部 API 集 成

表3与表4就性能需求、基础设施需求、设备仿真能力、所提供服务的鲁棒性水平,对现有的各类LoRaWAN仿真方案作了完整分析。其中,LoRaSIM、NS-3与FloRa等方案在借助投递率、时延与传输容量等分组路由指标来仿真网络效率与能效方面成果丰富。然而,多数仿真方案的不足之处在于:对旨在精确刻画数据分组加密的密码学模型仿真甚少,这部分能力要么超出方案自身的固有范畴,要么被交由TLS等外部库实现。而LoRaEnergySim与LoRaFree这两款轻量级方案则分别侧重于能效评估与网页端易用性。

类似地,OMNeT++与LoRaWAN Network Simulator等工具具有高度可定制性,可使研究者在贴近实际的拓扑下开展测试;它们同样具有模块化特征,既可用于工业界也可用于科研。LoRaSimu与LoRaWAN Simulator等网页版方案提升了场景构建的易用性与灵活性,但通常无法提供保障消息安全的强加密层。相比之下,ChirpStack与Loriot在云级与企业级部署方面表现最佳,其架构包含TLS/SSL加密、OAuth2认证与基于角色的访问控制,安全意识更强。Lorix One与LoRaWAN Test Suites将生态系统延伸至设备验证、合规与网关管理,但其中部分工具需依赖TTN或Loriot等外部平台才能完整实施安全策略。因此,表4既反映出从学术型仿真器向企业级框架持续演进的趋势,也凸显了在LoRaWAN研究与部署中建立标准化、安全且可互操作的仿真环境的必要性。

Table 3 Summarized Limitations of LoRaWAN Simulation Tools

表3 LoRaWAN 仿真工具局限性归纳

工具	性能	指标	基础设施	设备支持	服务	安全性
LoRaSIM [1][2]	对网络/设备行为的仿真逼真度高	分组投递、时延、能耗、拓扑变化	桌面图形界面;支持OMNeT++、MATLAB、R	A、B、C	信道建模、调制测试	仿真可定制;无内置加密与认证
NS-3	协议丰富,可仿真高级协议栈	误码率、丢包、吞吐量、能效	Linux 命令行/脚本(C++、Python)	A、B、C	路由协议、实时仿真	需手工建模协议;TLS依赖外部库
FloRa -	面向能效与ADR	时延、吞吐量、ADR指标	OMNeT++结合INET框架	A、B、C	面向物联网:SimuLTE、Veins集成	仅具备基本的LoRaWAN安全验证
LoRaEnergySim [2]	轻量级能耗建模	功耗、传输时延、节点寿命	桌面端,硬件要求低	A、B、C	载荷定制、频率/数据速率调节	无完整协议仿真;仅侧重能耗
LoRaFree [4]	实时的浏览器端仿真	丢包、时延、节点距离	网页端并可云端集成	A、B、C	网络可视化、性能剖析	仅具基本功能;缺少加密与认证
CupCarbon	面向城市尺度、含移动传感器的仿真	RSSI、分组速率、移动性、位置建模	Java 图形界面,集成OpenStreetMap	A、B、C	SenScript、物联网建模、真实设备模拟	基于MQTT的加密;缺少安全信道建模
SimpleIoT Simulator	网关—载荷交互	成功率、时	向导式图形界	A、B、	自动场景生成、	安全特性随套餐而异;加

	互建模	延、网关使用情况	面；付费工具	C	节点交互	密文档有限
Mbed Simulator	面向 LoRa 节点的嵌入式 / 云端仿真	在线时长、MQTT 投递、电池影响	在线 / 离线；支持 Mbed OS 5	A、B、C	MQTT 测试、经 C++ 进行云端同步	支持 TLS 加密与 Mbed 信任锚

Table 4 Summarised Limitations of LoRaWAN Simulation Tools (Continued)

表 4 LoRaWAN 仿真工具局限性归纳（续）

工具	性能	指标	基础设施	设备支持	服务	安全性
OMNeT++ -	模块化平台，可深度定制	节点交互、成功率、时延	桌面应用；INET、Veins、SimuLTE 扩展	A、B、C	模块化仿真、可视化网络建模	随模块而异；加密逻辑可定制
LoRaWAN Network Simulator [1][2][6]	全协议栈 LoRaWAN 建模	节点覆盖、帧接收、拓扑扩展	桌面 / 服务器端；基于 LoRa 联盟	A、B、C	拓扑测试、协议支持	仅具基本安全建模；扩展使用需引用
LoRaSimu [5]	高保真的分组与网络仿真	网关接收、信号强度、损耗	网页版仿真引擎	A、B、C	网关、节点与 MAC 层仿真	基于协议；缺少安全通信层
LoRaWAN Simulator [1][5]	交互式拓扑与节点测试	帧重传、投递、节点距离	网页平台（符合 LoRa 联盟规范）	A、B、C	场景编辑、网关仿真	仅可测试安全行为；缺少完整加密仿真
ChirpStack [9]	云级性能并提供网络服务	吞吐量、网关负载、连接可靠性	分布式服务器 + 网页管理界面	A、B、C	MQTT 集成、设备开通	TLS/SSL 传输、OAuth2、令牌认证、基于角色的访问控制
Loriot	面向混合模式的企业级平台	在线时长、投递率、ADR 成功率、地理位置	公有云与本地部署可选	A、B、C	监控、网关控制、自定义 API 支持	基于角色的访问、加密数据流、安全的 API 管理
Lorix One	云托管运营下灵活稳健	分组吞吐量、网关连通性、在线时长	经 Lorix 或合作方集成的云端界面	A、B、C	网络集成、远程控制、网关开通	基于 LoRaWAN 的加密；完整安全需经 TTN 或 Loriot 集成
LoRaWAN Test Suites	面向认证与协议测试的精确工具	RSSI、误包率、频偏、功率电平	USB 或射频接口；命令行 / 图形测试套件	A、B、C	合规性与基准验证	提供认证 / 加密测试用例；不强制实施安全传输

2. LoRaWAN 模拟工具

本小节讨论 LoRaWAN 部署中的若干关键模拟平台, 见表 5 与表 6。模拟器复现硬件功能, 可在虚拟设备上对固件测试、协议验证与调试。相比仿真器, 模拟器的实现要求更高, 但在评估动态与安全系统方面能提供更强的真实感。

Table 5 Summarised LoRaWAN Emulator and Certification Tools

表 5 LoRaWAN 模拟与认证工具概览

工具	易用性	可扩展性	灵活性	许可	支持	设备类别	集成能力
COOJA -	图形与命令行界面建模; 可用 C 语言 (Contiki OS) 编程	小型至大型网络	支持多种设备与拓扑	BSD 许可; 需引用	教程、邮件列表、GitHub、用户手册	A、B、C	NS-3、MATLAB、OMNeT++、FloRa、CupCarbon
ThingsBoard [9]-	网页界面, 用于建模与分析	高度可扩展, 支持多节点	可用 Java、C++、Python 编程; 支持 OTAA、ADR、ABP 支持网络拓扑	Apache 2.0 许可	安装指南、GitHub、教程	A、B、C	提供云端 / 平台集成 API
LoRaWAN Emulator	图形界面用于构建、仿真与测试安全网络	多设备与多节点配置	与安全 LoRaWAN 协议 (OTAA、ADR、ABP)	开源; 需致谢	帮助文档、视频、联系表单	A、B、C	可与外部工具集成; 支持安全通信
LoRaWAN Gateway Emulator	仿真终端与网关; 消息负载大	支持多场景	数据速率、类别与频率可配置	MIT 许可	GitHub 仓库提供文档与问题跟踪	A、B、C	无外部 API 或服务集成
Packet Sender	网关仿真并可生成 LoRaWAN 分组	可处理高消息量	支持 LoRaWAN 1.0.2 与 1.0.4; 可调时延与功率	MIT 许可	GitHub 仓库	A、B、C	UDP 分组转发; 无 API 集成
MultiTech Conduit	网页界面用于设备 / 网关管理	可管理数千台 LoRaWAN 设备	支持 LoRaWAN 1.0 与 1.1; 实时日志、帧 / 信道配置	商业; 提供免费试用	支持门户、文档、论坛	A、B、C	gRPC/REST API 可接入云端与数据库
Semtech LoRa Cloud	面向设备接入与监控的云服务	全球规模部署	自适应数据速率 (ADR)、地理定位、跳频	商业订阅	支持门户与社区论坛	A、B、C	可与数据库及各类平台云端集成
Actility ThingPark	具备完整物联网连接套件的网络平台	支持公网 / 专网	LoRaWAN 1.0.2 与 1.0.4; 自定义 API 集成; 支持 LTE-M/NB-IoT	商业; 提供免费试用	门户、社区论坛、市场支持	A、B、C	提供外部服务 API; 支持蜂窝物联网

MQTT Broker	基于 MQTT 的服务器, 用于客户端 / 设备通信 命令行 / 图形界面, 用于 LoRaWAN 设备认证	多租户、可扩展架构	符合 LoRaWAN 规范; 支持 ADR 与自定义 API / 数据处理	开源与商业并行	支持门户、论坛	A、B、C	TLS/SSL 加密, 云端与数据库集成
LoRaTester		支持多种配置文件	支持 ADR 与扩频因子; 可进行物理设备测试	免费使用	无专门门户; USB 接口	A、B、C	无外部 API 支持; 用于协议合规验证

采用 BSD 许可的开源平台 COOJA 可仿真多种设备与网络拓扑, 既提供命令行界面也提供图形界面。它基于 C 语言与 Contiki OS, 并与 MATLAB、NS-3、OMNeT++、FloRa、CupCarbon 等应用高度集成。此外, COOJA 能够较为真实地模拟安全关键场景, 并支持全部 LoRaWAN 设备类别。ThingsBoard 则提供可扩展的网页界面, 并在 Apache 2.0 许可下支持使用 Gatling 进行性能测试。它支持以 Java、C++ 与 Python 进行节点级编程, 并支持 OTAA、ADR、ABP 等主要 LoRaWAN 协议; 基于角色的认证、访问控制与加密机制均属其安全模型的组成部分[9]。LoRaWAN Emulator 为多节点网络拓扑仿真提供了模块化平台, 支持与各类设备的安全通信, 并依照 LoRa 联盟的使用准则运行; 除复现网络对潜在攻击的容错能力外, 该模拟器还可与外部系统通信[1]。

同样地, Gateway Emulator 支持 A、B、C 三类设备, 采用 MIT 许可开源发布, 可复现数据速率、消息类型与频率设置等参数。由于既可作为终端又可作为网关使用, 它通过 UDP 发送海量数据。其功能包含面向设备管理的授权、加密与认证特性, 但不提供任何外部服务[1]。同为 MIT 许可开源实现的 Packet Sender 依据 LoRaWAN 1.0.2 与 1.0.4 规范仿真终端与网关功能, 可通过 UDP 转发分组以开展压力测试, 从而观察网络在重负载下的表现以及吞吐量与可靠性是否开始劣化。它涵盖全部设备类型并允许用户调整性能参数, 但不提供更高级的安全特性, 也不便于 API 对接。MultiTech Conduit 提供了一款完全可编程的 LoRa 网关, 专为较大规模的工业物联网(IIoT)系统设计, 具备实时帧日志、网页界面与更快的动态信道切换能力; 它同时适用于 LoRaWAN 1.0 与 1.1 设备, 并提供 REST API 与 gRPC 以便接入云端或数据库, 还通过内置的认证与加密工具保障数据安全。

Semtech LoRa Cloud 是构建于 LoRa Edge 平台之上的云端管理方案, 服务范围涵盖认证测试、全球覆盖与设备定位, 完整支持 A、B、C 类 LoRaWAN 设备。该平台遵循 LoRaWAN 1.0.2 与 1.0.4 标准, 可通过与主流云基础设施集成提供安全的数据管理与设备连接; 安全性通过标准化的访问控制、认证与加密加以保障, 确保设备与数据均得到可靠保护。相比之下, Actility 的 ThingPark 平台在提供 LoRaWAN 支持的同时, 还通过一体化的物联网网络管理方案兼容 LTE-M 与 NB-IoT 等蜂窝技术。它覆盖完整的设备管理生命周期, 并处理定位服务、数据路由与配置管理等网络运营事务; 完全兼容 LoRaWAN 协议, 可通过 API 方便地与其他系统集成。其架构面向安全性与可扩展性设计, 适用于工业物联网、智慧城市与精准农业等大规模部署。Semtech 侧重边缘能力与云原生服务, 而 ThingPark 更侧重于复杂多技术环境下的网络管理与全生命周期支持。

MQTT Broker 组件基于 MQTT 协议仿真服务器通信过程, 提供多设备、多网关通信。该模块支持与云服务及其他 API 的连接, 架构灵活, 既可搭配开源平台也可用于商业部署。该代理具备使用 TLS/SSL 的安全数据传输以及基于凭据认证的访问控制列表等特性, 并支持 LoRaWAN 协议下的全部设备类别。此外, LoRaTester 用于对符合 LoRaWAN 区域与国际标准的设备进行一致性与互操作性测试, 支持全部设备类别以及 ADR 与扩频因

子。尽管其部署需要一定的技术能力，该平台仍通过可定制参数与数据保护策略为提升安全措施提供了进一步空间。

综合来看，已有研究表明仿真与模拟构成了结构化的开发环境，二者在物联网系统验证过程中各有侧重。LoRaSim、NS-3 与 FloRa 等仿真环境提供了经济便捷的验证途径，在开发初期最为适用，可在网络配置与协议分析阶段进行深入的参数调节；但这类环境无法复现硬件环境所固有的真实工况。LoRaWAN Emulator 与 Gateway Emulator 等模拟环境通过同步的实时节点—网关通信弥补了上述不足，使完整的固件验证流程以及包括 ADR 重协商在内的各项参数测试能够以极小的开销实时进行。TTN、Loriot 与 Actility ThingPark 等工业平台则作为生产级平台，具备标准化的加密参数、内置的设备管理与网关管理、安全的数据交易与云端分析能力；这类平台运行稳定且可扩展，但在开发初期不便于进行协议层面的探索。总体而言，仿真环境、模拟平台与工业平台构成了一个协同的生态体系：仿真环境适用于理论验证，模拟平台适用于工程验证，工业平台则适用于实际运营。

Table 6 Summarised Limitations of LoRaWAN Emulator and Certification Tools

表 6 LoRaWAN 模拟与认证工具局限性归纳

工具	性能	指标	基础设施	设备支持	服务	安全性
COOJA - Contiki 仿真	适用于基于 Contiki 的仿真	分组投递、时延、能耗、仿真时间	基于 Java 的图形 / 命令行界面；需 Contiki OS	A、B、C	网络行为测试、拓扑建模	仿真中具备基本加密；可经 Contiki 协议栈定制
ThingsBoard [9]	高性能遥测与可视化	在线时长、流速率、节点时延、连通性指标	可扩展的网页平台；支持集群部署	A、B、C	规则引擎、节点管理、实时数据处理	TLS 加密、基于角色的访问、令牌 / 证书认证
LoRaWAN Emulator	LoRaWAN 仿真高效，复杂度中等	节点交互、分组状态、消息投递	网页架构：无需网关即可测试	A、B、C	ADR/OTAA/ABP 建模、入网测试	支持安全信道仿真与协议合规测试
Gateway Emulator	可应对消息密集场景	网关时延、吞吐量、类别切换	本地部署：仿真网关与设备	A、B、C	网关仿真、流程建模	无集成安全机制；主要用于功能测试
Packet Sender	分组仿真与构造可靠	成功率、时延、IP / 端口投递	基于 UDP 的本地工具；无云端后台	1.0.2 与 1.0.4 设备	手工分组测试	无加密与认证；需借助外部配置
MultiTech Conduit	针对网关流量与协议处理优化	在线时长、流量、接收率、时延	VPN / 云连接的网关基础设施	A、B、C	路由、云端集成、网关管理	安全的 gRPC/REST API、加密、认证
Semtech LoRa Cloud	可扩展、全球覆盖且遥测能力强	电池寿命、MAC 命令、流量规模	云平台，支持 LoRa Edge 设备	A、B、C	设备跟踪、MAC 开通、调制	强认证、安全接入与通信
Actility	面向公网 / 专	时延、在线	托管 / 本地部	A、B、	高级分析、设备	端到端加密、身份管理、

ThingPark	网的高性能平台	时长、流量分析、仪表盘指标	署; 支持 LTE-M/NB-IoT	C	管理、集成市场	认证
MQTT Broker	高吞吐消息传递与中间件集成	代理时延、访问日志、消息丢失率	中间件经 HTTP/UDP 与服务器 / 网关集成	A、B、C	LoRaWAN 数据流处理、云存储支持	TLS/SSL、访问控制列表、客户端认证
LoRaTester	面向设备认证的精密测试	功耗、信号距离、传输效率	基于 USB 的独立测试工具	符合协议的设备	固件升级仿真、激活测试	支持安全验证; 缺少完整加密与强制实施

(三) 已识别研究空白小结

尽管可供选择的 LoRaWAN 工具众多, 全面而有针对性的安全性比较却屈指可数。已有研究视角往往偏窄, 聚焦于时延或吞吐量等性能评价, 而未系统考察仿真器、模拟器与基础设施平台在集成、可扩展性与安全特性方面的表现。多数工具还缺乏将定量评分与专家验证相结合的统一评价框架。业界所需的是一种把技术评估与可视化综合 (如热力图或雷达图) 相结合的方法, 使研究者与从业者能够针对物联网系统设计与部署的特定阶段找出最合适的工具。

现有关于 LoRaWAN 开发工具的文獻仍显示出基于仿真的实验与面向部署的评价之间存在差距。以往研究多聚焦于网络可扩展性、协议优化或工具易用性等具体议题, 全面的、具备安全意识的对比分析仍然有限。本综述在统一的分析框架内对 LoRaWAN 仿真、模拟与部署工具进行系统分类与评价, 从而首次为研究者与从业者在实验与实际物联网实现中选择合适平台提供了结构化依据。基于文献中识别出的研究空白, 下一部分介绍本文所采用的方法, 用以从可扩展性、集成与安全三个主要维度系统评估 26 款 LoRaWAN 相关工具。

三、研究方法

本研究采用结构化方法, 从可扩展性、集成能力与安全性能三方面系统评估 26 个仿真与模拟平台。整个研究过程被划分为五个阶段: 数据收集、数据分类、工具验证、分析以及随后的可视化。为确保方法学上的严谨性, 各阶段说明如下。

(1) 数据收集: 数据收集首先在 IEEE Xplore、ScienceDirect、ACM DL 与 Google Scholar 等学术数据库中开展前沿检索, 以识别与 LoRaWAN 最相关的仿真与模拟工具。为保证有效性, 本文设定了一组标准, 要求工具支持 OTAA、ABP、ADR 等基本通信参数, 其仿真 / 模拟能力须兼容 A、B、C 类设备, 并具备基本或高级安全功能。最终确定 16 个仿真平台与 10 个模拟平台。

(2) 工具分类: 随后对所分析的数据进行分类, 以确定最终工具集合所属的各个类别。分类借助多个维度完成, 这些维度通过同行评议渠道与论坛加以确定, 包括: ①易用性, 考察安装与界面的简便程度; ②可扩展性; ③配置能力; ④协议可修改性, 考察其许可为免费 / 开源还是版权受限; ⑤支持与教程的完备程度; ⑥对 A、B、C 类设备的兼容性; ⑦能否与 OMNeT++、NS-3、MATLAB 等平台集成。

(3) 对比评价: 该阶段旨在比较各候选工具的易用性、可扩展性与安全能力。本文采用定性分析与半定量评分相结合的混合评价方法, 评分采用 1 至 5 的五级量表。评分方式因候选技术为仿真平台还是模拟平台而异: 模拟平台就加密、认证过程与协议级安全按 0 至 5 分评定; 仿真平台则采用三级量表, 1 表示弱、2 表示中等、

3 表示强,用以刻画其加密实现与对 LoRa 安全要求的遵循程度。评价聚焦于两个视角:面向测试与实验的适应性,以及在可扩展性与互操作性方面的部署就绪度。

(4) 验证:本文采用三角互证进行验证,将所得结果与既往同类对比分析的规范性研究以及相关开发机构的报告相比对,从而提高内部效度并降低评价者偏差的影响。同时进一步参考同行评议论文,确保所观察到的属性与所声称的结果之间不存在偏差,进而增强结论的可靠性与所提评价框架的有效性。

(5) 可视化综合:对经过验证的结果进行可视化综合,以便于理解与决策。数据以性能表格、热力图与雷达图等形式呈现,有助于把握本文所述各类仿真器与模拟器的优势与不足。

四、结果与讨论

本部分结合定性洞察与定量分析,考察 LoRaWAN 的仿真、模拟与完整部署三类框架各自的表现。NS-3、LoRaSim 等仿真工具通常是研究者的首选:成本低、易于修改,在验证新思路或初步评估性能时相当灵活。例如,研究者可以尝试一种新的数据速率调节方式,或在不使用任何实际设备的情况下测试数千个虚拟传感器。但其不足同样明显:这类工具无法完整反映真实网络的运行状况,难以刻画邻近设备干扰或现实中随机出现的分组丢失。模拟工具与部署平台则更进一步,FLoRa 或云端测试床等平台可在更大规模、更接近真实的条件下进行测试,安全性更好,可处理多种设备类型,并能与其他系统良好协作。简言之,仿真适合受控测试与学习,而要确保 LoRaWAN 方案能够应对真实环境,模拟与部署工具必不可少。

(一) 结果

1. LoRaWAN 仿真工具

仿真工具是在实际部署前对网络行为进行建模、测试与验证的必要手段,可提供经济灵活的环境,用以评估不同配置下的时延、能耗、分组投递与可扩展性等性能指标。例如,COOJA、NS-3 与 CupCarbon 使研究者与开发者能够考察 LoRaWAN 协议的运行机制,如网络参数优化与大规模性能评估;它们对研究环境因素、移动性与干扰对通信效率的影响也很有帮助。

从易用性、可扩展性、灵活性、支持与集成五项核心特征出发,比较了 16 款 LoRaWAN 仿真与部署工具。TTN、Loriot 与 NS-3 在可扩展性与集成方面表现优异,说明其适用面更广;LoRaWAN Test Suites 与 LoRaSimu 在支持与可扩展性方面排名靠后。

TTN 与 Loriot 等部署平台凭借集成的加密、认证与访问控制取得最高分;NS-3 与 OMNeT++等仿真器得分较低,因其重心在于建模而非安全策略的实施。这意味着,仿真器非常适合开展研究或试验,而部署平台在安全的生产级环境中表现更佳。不过,即便最实用的仿真器也存在弱点:高度依赖模型假设,在高流量下容易失效,通常忽略硬件约束,并且可能仅支持部分协议特性;此外它们需要专门的技术知识,部分工具还涉及许可费用。

2. LoRaWAN 模拟工具

模拟器为硬件与网络交互测试提供了更接近真实的条件。仿真在一定程度上依赖抽象,而模拟则可近乎实时地复现真实的传输行为、设备交互与网关通信,使开发者能够在受控条件下开展固件测试、协议合规验证与系统性能评估。值得一提的还有 LoRaWAN Emulator、Gateway Emulator 与 MultiTech Conduit,它们在部署就绪度评估、设备互操作性与认证测试方面颇为有用。

ThingsBoard、MultiTech Conduit、Semtech LoRa Cloud 与 Actility ThingPark 在可扩展性、灵活性与集成能力方面得分持续较高,均适用于大规模部署。相比之下,LoRaWAN Gateway Emulator、Packet Sender 与 LoRaTester

的集成与支持有限, 表明它们更适合特定任务, 而非完整的系统仿真或部署。

本文采用三级量表(1=弱, 2=中等, 3=强), 聚焦加密、认证与合规性。可见 ThingsBoard、ThingPark 与 Semtech LoRa Cloud 提供了稳健的加密(如 TLS)、强认证(如证书、RBAC)与完整的标准合规性, 因而适用于安全的生产级部署。MQTT Broker 与 COOJA 等中等水平的工具在特定方面(如加密或仿真)具有优势, 但在合规性或认证方面存在不足, 因此只宜用于测试或非关键场景。Packet Sender 与 LoRaTester 因缺失基本安全特性而在各维度得分均较低, 只应在受控环境中使用。图 6 反映了总体安全态势: 形状越大越均衡表示工具越强, 形状不对称则揭示了取舍关系。该图有助于决策, 但简化了现实的复杂性; 增加审计日志等维度可进一步完善。

(二) 讨论

由表 1 至表 6 可见, 可扩展性、协议支持、设备兼容性与安全需求是选择 LoRaWAN 开发工具时的主要关注点。LoRaSIM、NS-3 与 FloRa 等仿真环境为分组投递、时延与能耗提供了经济高效的高性能建模。其中, NS-3 以协议灵活性以及与 C++、Python 脚本的集成见长, 与 OMNeT++、SimuLTE 结合还可提供更广泛的城市物联网仿真能力。尽管各有所长, 这类仿真工具往往缺乏原生加密模块, 需要手工实现 TLS 或 DTLS 协议。如表 5 所示, LoRaWAN Emulator、Gateway Emulator 与 Packet Sender 等模拟器可在更贴近真实的条件下开展实时测试, 仿真节点交互、消息吞吐量与 ADR/OTAA 行为。LoRaWAN Emulator 等工具支持安全信道建模与协议合规测试, 而 Packet Sender 等则侧重功能性分组生成, 未集成加密。

TTN、Loriot 与 ThingPark 等基础设施平台提供企业级性能, 对网关连接、云端集成与设备开通提供广泛支持。TTN 支持开源的可扩展性, 并通过 AES 加密与访问密钥实现安全入网机制。ChirpStack 与 ThingsBoard 等平台则以 TLS/SSL、OAuth2 与基于证书的认证弥合了这一差距。可扩展性与集成能力方面的差异同样明显: MultiTech Conduit 与 Semtech LoRa Cloud 可承载数千个终端节点, 支持 REST/gRPC API 并提供地理定位服务; 相比之下, 仿真器运行于孤立环境, 与真实设备的交互有限。在实践中, 选择合适的 LoRaWAN 工具取决于具体的开发阶段、所需的建模细致程度以及项目的安全与可扩展性需求。因此, 采用组合策略——以仿真器进行协议设计、以模拟器进行系统行为测试、以基础设施平台进行部署——是构建可靠、安全的 LoRaWAN 物联网系统的一条务实而灵活的路径。

在为 LoRaWAN 应用权衡仿真器与模拟器时, 还需考虑若干取舍。仿真器在 LoRaWAN 实验中更为理想且灵活, 但往往难以完整复现真实的 LoRaWAN 交互; 模拟器则可通过构建更贴近现实的 LoRaWAN 测试床来弥合这一差距, 但在某些情况下资源消耗更大; 基础设施平台可优先保障可扩展性与安全性, 但对迭代设计或快速原型而言成本较高。理解模拟器与仿真器之间的这些差异, 有助于研究者与开发者作出明智选择, 使工具与特定 LoRaWAN 物联网项目所处阶段、规模与安全需求相匹配。

(三) 未来研究方向与局限

本小节指出若干已识别的未来研究方向。尽管当前的 LoRaWAN 仿真与模拟工具具备可观的能力, 仍有若干局限有待进一步研究。

(1) 可扩展性与准确性仍是重大挑战。现有仿真器往往难以复现真实条件, 在受动态干扰、信道争用与能耗特性波动影响的大规模物联网部署中尤为如此。未来模型应纳入自适应信道分配、真实的干扰仿真与功率优化框架, 以提升保真度与响应能力。

(2) 将 LoRaWAN 拓展至非地面网络(如卫星—无人机—地面混合系统)是另一个有前景的方向。把 LoRaWAN 工具与天基一体化通信的最新进展(包括面向 NOMA 叠加的遍历容量建模)相衔接, 有望为偏远地

区与天基物联网应用开辟新途径; 面向地面—卫星混合场景设计的模拟平台, 对此类部署的原型验证将至关重要。

(3) 安全性虽日益受到重视, 但仍缺乏统一而先进的支持。多数工具在现代密码协议、入侵检测系统以及对干扰等主动威胁的抵御能力方面实现有限。引入后量子密码、人工智能驱动异常检测与自适应安全模块, 可显著增强仿真与模拟环境中的防护能力。

(4) 在能耗方面, 虽然 LoRaEnergySim 等工具可进行能耗剖析, 但在实时自适应能量采集与优化技术方面仍存在空白。嵌入面向动态能效的机器学习模型, 可延长传感节点寿命并提升网络可持续性, 在偏远与资源受限的部署中尤为重要。

(5) 互操作性仍是关键领域。许多 LoRaWAN 工具仍各自为政, 限制了跨平台评价与协同开发。建立标准化的 API 与中间件框架将促进数据交换与 workflow 集成, 使研究者与从业者能够把仿真的深度与模拟的真实感结合起来, 实现更全面的测试与部署。

五、结论

本文对当前的 LoRaWAN 仿真与模拟工具进行了全面的对比分析, 评价了其易用性、可扩展性、安全特性、许可与集成能力。研究表明, NS-3、OMNeT++ 与 LoRaSim 等仿真工具提供了灵活、经济的环境, 适用于学术研究与协议层面的研究, 可在 A、B、C 类设备上评估时延、分组投递与能耗; 但其准确性受限于简化的环境建模, 且往往缺乏对端到端安全的内置支持。相反, TTN、ChirpStack、Loriot 与 Lorix One 等模拟平台可在真实条件下提供高保真测试, 支持可扩展部署、安全通信以及与网关和云基础设施的集成; MultiTech Conduit 与 ThingPark 等工具则通过先进的遥测、稳健的设备开通与生命周期管理进一步拓展了上述能力。COOJA、ThingsBoard 与 LoRaWAN Emulator 等基础设施与可视化工具通过实时遥测、图形化建模与不同层次的安全机制, 架起了仿真与实现之间的桥梁。尽管许多平台已支持 TLS 与 OAuth2 等协议, 仿真环境仍常常依赖人工的安全配置。上述发现凸显了对更具适应性与安全性的 LoRaWAN 工具的需求: 这类工具应纳入人工智能驱动的入侵检测、密码学增强与互操作框架, 以统合仿真与模拟工作。仿真、模拟与基础设施平台之间的区别, 反映了网络设计、测试与部署的不同阶段。本文建议采用混合策略: 以仿真器进行设计、以模拟器进行验证、以基础设施平台进行实际实现, 从而构建稳健、可扩展且安全的 LoRaWAN 网络。未来研究应聚焦于提升仿真准确性、卫星集成与自适应能耗建模; 同时, 标准化的评价方法 (尤其是硬件在环测试) 对于确保 LoRaWAN 工具在新兴物联网应用中持续可靠且切合实际至关重要。

参考文献

- [1] 何雅玲. 工业余热高效回收换热装备. 工程热物理学报, 2024, 43(03): 561-570.
- [2] 周创兵. 岩质边坡稳定性智能监测方法. 岩土力学, 2022, 43(03): 599-608.
- [3] LoRa Alliance. Online simulation of LoRaWAN devices. <https://www.youtube.com/watch?v=NJyGYh2WeZ8>.
- [4] Bernardinetti G, Mancini F, Bianchi G. Disconnection attacks against LoRaWAN 1.0.X ABP devices. 2020.
- [5] 陆建华. 6G 通信超宽带传输技术. 电子学报, 2022, 50(03): 513-522.
- [6] 周秉根. 风电叶片复合材料成型工艺. 复合材料学报, 2025, 39(03): 1067-1078.
- [7] 李爱群. 老旧建筑抗震加固改造技术. 工程力学, 2022, 39(04): 1-10.
- [8] 刘吉臻. 新能源火电耦合调峰系统. 动力工程学报, 2022, 42(04): 265-273.
- [9] 张友军. 船舶动力系统减振降噪技术. 船舶工程, 2023, 44(03): 1-7.

- [10] 杨孟飞. 星载计算机容错设计技术. 中国空间科学技术, 2020, 42(02): 1-8.
- [11] 王树国. 机器人关节驱动器高精度控制. 机器人, 2022, 44(02): 1-8.
- [12] Hammache M, Kacimi R, Beylot A L. Unifying LoRaWAN networks by enabling the roaming capability. Proceedings of the Conference on Local Computer Networks (LCN), 2021: 371-374.