研究与开发

一种轻量可信的物联网通信协议

马军锋[1]，刘芷若[1]，李观文[2]，杨飞[2]，党娟娜[2]
（1. 中国信息通信研究院，北京 100191；2.华为技术有限公司，北京 100094）

摘　要：随着万物互联时代的到来，面对海量异构终端的互联需求，传统基于应用层网关的协议栈转换方案存在性能差、无法保障端到端安全等问题。提出了一种轻量可信的物联网 IP 通信协议，是网络 5.0 产业和技术创新联盟协议与接口组的主要研究方向，避免应用层网关的部署，降低物联网设备的计算与存储开销，保障端到端通信安全。

关键词：万物互联；轻量化；安全
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2021229

A lightweight and trusted communication protocol for IoT

MA Junfeng[1], LIU Zhiruo[1], LI Guanwen[2], YANG Fei[2], DANG Juanna[2]
1. China Academy of Information and Communications Technology, Beijing 100191, China
2. Huawei Technologies Co., Ltd., Beijing 100094, China

Abstract: With the era of the internet of things (IoT), the protocol stack conversion scheme based on the application-layer's gateway has problems such as poor performance and end to end security that can't be guaranteed. A lightweight and trusted IoT IP communication protocol was proposed, which was the main research direction of Protocol and Interface Group in Network 5.0 Industry and Technology Innovation Alliance, the deployment costs of protocol conversion gateways was decreased, the computing and storage overhead of IoT devices was reduced, and end to end communication security was ensured.

Key words: internet of things, lightweight, security

1　引言

随着物联网产业的飞速发展，物联网设备深入人们生活和生产的方方面面，所采用的通信范围不再局限于单纯物联网络，而是需要与互联网通信。如智能家居场景的智能门锁、智能音箱等物联终端，需要访问互联网中服务资源，实现远程遥控等功能。

不同物联网设备采用不同的底层传输介质，导致其在访问互联网时往往需要依赖于一个应用层网关实现协议转换。但是，引入应用层网关将打破传统通信过程中的“端到端”原则，可能引入更多的安全威胁。另一方面，当前物联网正处于“烟囱式”发展的阶段，物联网设备的本地通信通常采用厂商定制化的私有协议，当实际部署环境中涉及多厂商设备时，需要分别部署对应的

收稿日期：2021−08−30；修回日期：2021−10−21

网关设备，导致其运维成本大幅提高。

为避免部署应用层网关带来的协议转换开销大、端到端安全无法保障等问题，业界提出“IP一网到底”的概念，旨在消除应用层网关，实现统一网络层的端到端通信[1]，其主要优势体现在如下4个方面。

- 当前网络基础设施可以完美支持IP协议栈，不必考虑网络重建成本及兼容性问题。
- IP技术已在大网中应用多年，被验证是成熟有效的，在物联网环境中仍采用IP的技术风险最小。
- 当前IP化的全球互联网生态已经形成，IP的开放性与包容性同样适用于物联网场景。
- 现有大量基于IP技术的工具可直接利用（特别是网络诊断及管理相关工具），不必增加额外的网络管理成本。

然而，传统IP定长、定界的设计并不适用于资源严重受限的物联网设备，其过高的报头开销导致报文数据传输效率低，增加设备能耗。据统计[2]，物联网通信的数据报文平均长度是25 byte，若采用标准IPv6协议传输（报头长度为40 byte），其传输效率仅有38%。另外，IP设计之初缺乏安全考虑，后续通过外挂补丁方式增加对安全的支持，如IPSec、TLS协议。这些安全协议需要在报文中增加安全头以及安全协商流程，以IPSec为例[3]，AH头为24 byte，ESP头大于24 byte，使得传输效率进一步降低到22%以下；而安全协商需要额外的IKE控制报文，进一步增加了带宽的消耗。

为此，IETF先后成立了6LoWPAN和6Lo工作组，提出一种可用于IPv6网络中高效传输物联网报文的报头压缩方法，但代价是设备需要付出额外的计算和存储开销来实现报文的压缩与解压缩。另外。即使基于该机制使用IPSec，整体传输效率依然很低，约30%。

因此，本文提出一种轻量可信的物联网通信协议，是网络5.0产业和技术创新联盟协议与接口组的主要研究方向，避免应用层网关的部署，降低物联网设备的计算与存储开销，保障端到端通信安全。

2 轻量可信协议设计

为满足物联网设备的互联需求与安全需求，同时尽可能降低其部署开销，本文提出一种轻量可信的通信协议。该协议的关键技术包括灵活轻量的报文设计与网络安全可信机制两个方面。

2.1 灵活轻量的报文设计

在未来网络中，除了传统的主机以外，物联设备、内容资源、虚拟化服务、人都可以作为未来网络的通信实体。另一方面，以物联设备为代表的资源受限设备通信载荷通常较小，而局域网内通信时过长的地址又会导致报头开销过大，增加不必要的传输能耗，需要尽可能压缩域内通信地址。因此，本文提出灵活变长地址，打破传统IP报文长度与字段均固定的束缚，实现按需缩短或者扩展地址空间，满足以物联网通信为代表的短地址通信需求。可变长的编址方式使得网络设备可以按需采用不同的地址长度。网络中的路由器可以支持任意长度地址的路由查询操作，无须引入协议转换网关等设备，从而避免额外开销及网络可扩展性问题。

在物联网域内，不同通信实体可以通过短地址直接通信，满足设备资源或功耗需求；物联网终端访问互联网时，可进行无状态的长短地址转换，避免协议转换过程带来的操作开销和网络可扩展性问题。

2.2 网络安全可信的机制

内生安全可信网络[4]突破了传统以终端为核心的“外挂式”被动防御体系，采用以网络为核心的主动内生安全信任的设计理念，构建确定性的内生安全可信网络，满足未来互联网的网络行为可预期、强管理、端到端极度差异化的安全需求，为垂直行业进行安全赋能。以工业企业为例，在购置了大量的终端设备之后，通常需要对其购

置的设备进行统一管理，以便设备在接入客户网络时能够被正确识别，并且能与其他设备互联互通。但是，工业园区 IoT 终端数量大，安全部署困难，需人工大量参与。因此，本文为工业互联网海量异构的 IoT 设备提供了一种低成本、低开销的轻量级内生安全机制，实现新设备的自动化安全入网。

在轻量级内生安全机制中，内生安全是在 IP 层直接使能的基础安全机制，实现随路验证。其中，随路验证技术是智能门锁设备基于 ID 内嵌对称密钥技术，在发送数据报文同时携带验证信息，验证点逐包验证其合法性，降低因安全需求带来的信令开销及报文开销，相对于基于公钥以及复杂的安全机制，这种方式可以降低功耗，降低资源占用。

2.3　轻量可信协议的通信流程

以图 1 拓扑架构为例，IoT 终端通过 AP、接入设备、汇聚设备、核心设备以 IPv4 互联网访问 IoT 服务器。

2.3.1　环境配置

当 IoT 终端初次入网上电时，其内置出厂配置，包含初始设备身份信息 IDinit 及密钥 IDKinit，是获取入网许可的重要凭证。IoT 终端通过入网许可后，便可获得园区内唯一的身份信息、用于随路验证的密钥 DVK 以及 KeyID 信息。IoT 终端每次开机时，均需要通过认证过程，验证设备的身份信息，从而获得网络的访问权限。

一旦通过认证后，IoT 终端将发起短地址分配，从当前接入的 AP（含插卡）获得可用于后续通信的短地址。

2.3.2　上行报文通信流程

IoT 终端 A 已获得由 AP1 分配的短地址 2（1 byte），对应外网的完整地址为 1.2.1.2（4 byte）。此时 IoT 终端 A 向 IoT 服务器发起上行通信流程如图 2 所示。

步骤 1　IoT 终端 A 发出轻量可信报文 1，报文的目的地址是 IoT 服务器，源地址是本机的短地址 2，同时携带序列号 SEQ、验证码 AuthCode 与密钥编码 KeyID。其中，验证码 AuthCode 通过随路验证密钥 DVK 和对应的报文信息计算获得。

步骤 2　AP1 收到轻量可信报文报文 1 后，基于报文携带的短地址和 SEQ，查询 DevID 表做防重放检查（仅在网络边界设备执行）与限流，然后基于长短地址变换将源地址改写为 1.2.1.2（增加地址前缀），同时在报头中插入 DevID 字段，保留 SEQ、AuthCode 和 KeyID 字段，最终封装成可信报文 2。

步骤 3　AP1 默认上行接口转发轻量可信报文 2。

步骤 4　接入设备同样默认上行接口转发轻量可信报文 2。

步骤 5　汇聚设备收到轻量可信报文 2 后，进行随路验证，方法参见下行报文通信流程。

步骤 6　通过验证后，汇聚设备根据映射表获得源地址（1.2.1.2）对应的 IPv4 地址（10.5.5.198），封装 IPv4 报文并送往 IoT 服务器。

2.3.3　下行报文通信流程

在当前场景中，IoT 终端 A 已获得由 AP1 分配的短地址 2，对应完整地址为 1.2.1.2。此时 IoT 服务器向 IoT 终端 A 发送下行报文的通信流程如图 3 所示。

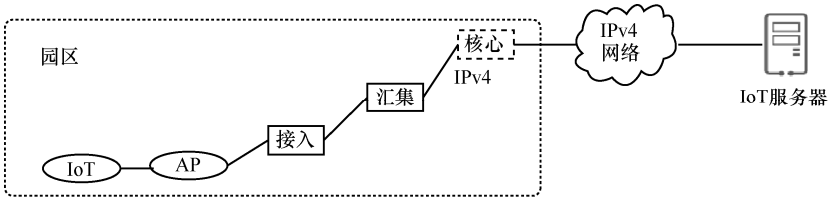

图 1　拓扑架构

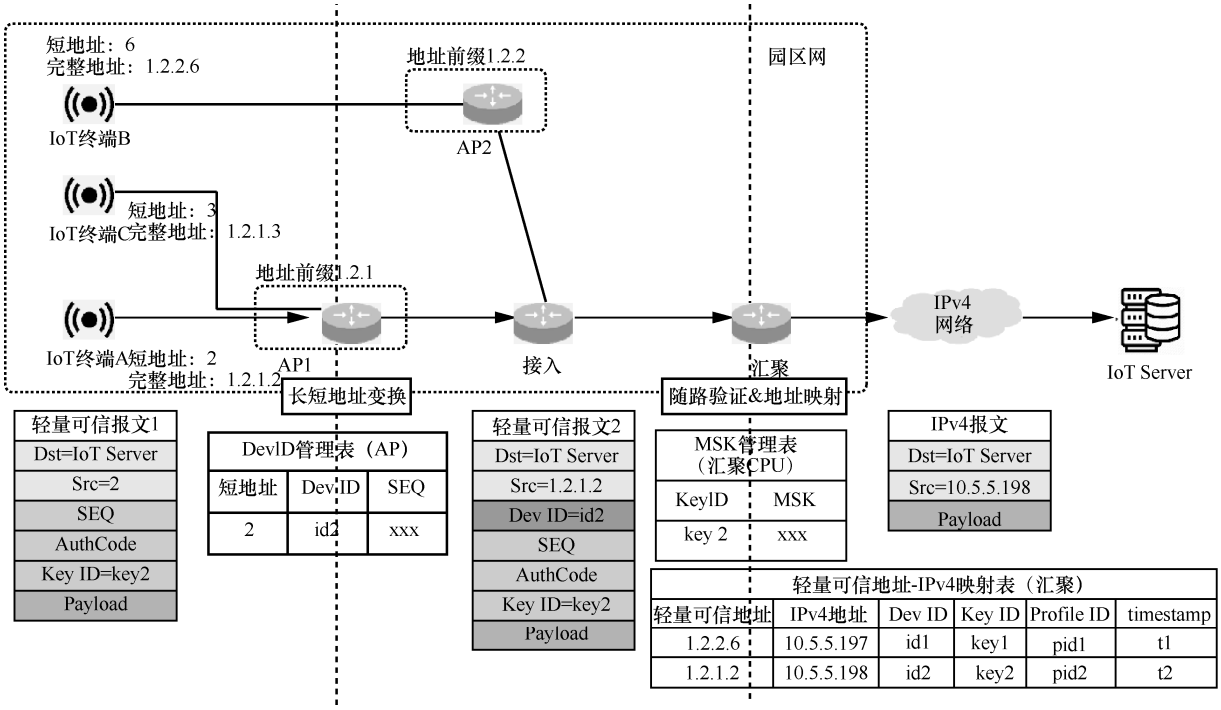

图 2　轻量可信协议的上行通信流程

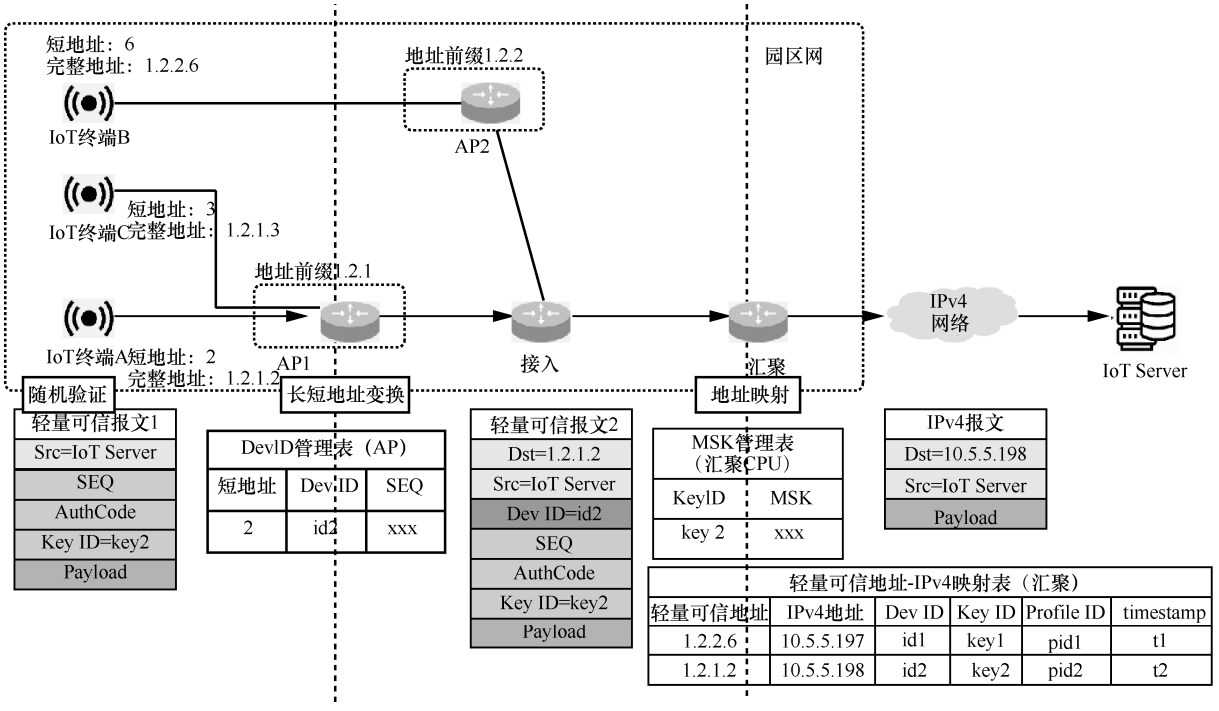

图 3　轻量可信协议下行通信流程

步骤 1　由 IoT 服务器主动发送 IPv4 报文，报文的目的地址是 IoT 终端 A 的 IPv4 地址 10.5.5.198。

步骤 2　汇聚设备收到 IPv4 报文后，根据地址映射表将目的地址（10.5.5.198）转换为完整轻量可信地址 1.2.1.2，然后根据转发规则获得接口

信息，上送 CPU。

步骤 3　汇聚设备根据 KeyID 查找 MSK 管理表得到对应的 MSK，通过 MSK 和 DevID 派生随路验证密钥 DVK 后生成 AuthCode，同时在报文中插入 SEQ 字段（取值为系统时间戳），然后根据出接口信息转发封装后的轻量可信报文 1。

步骤 4　接入设备根据转发规则，继续转发轻量可信报文 1 至 AP1。

步骤 5　AP1 收到轻量可信报文 1 后，根据转发规则获得接口信息，然后为目的地址（1.2.1.2）去除 AP1 的地址前缀（1.2.1）形成短地址 2，封装成轻量可信报文 2 并转发报文至 IoT 终端 A。

步骤 6　IoT 终端 A 收到报文后，需要先进行防重放检查与安全校验（仅在终端执行），检查通过后再做进一步解析。

2.3.4　随路验证流程

（1）密钥派生机制

基于主密钥 MSK 派生终端随路验证密钥 DVK，如图 4 所示。主密钥 MSK 由权威机构维护，并下发到验证点即汇聚设备，终端设备在入网时获取随路验证密钥 DVK 和 KeyID 信息。KeyID 用于指示生成 DVK 对应的 MSK。此外，支持周期性更新主密钥 MSK 以及设备随路验证密钥 DVK，防止长期使用单一密钥，导致密钥泄露。

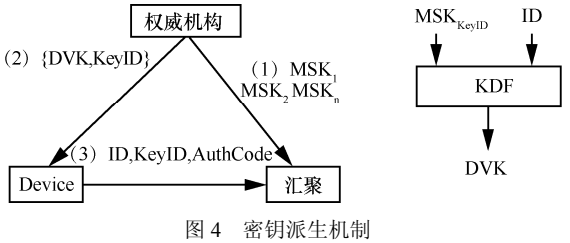

图 4　密钥派生机制

（2）验证码的生成和验证

终端根据图 5 左侧方法生成验证码 AuthCode，汇聚设备根据右侧方法生成 AuthCode'。

其中，sID 为终端 ID，sLoc 为终端短地址。

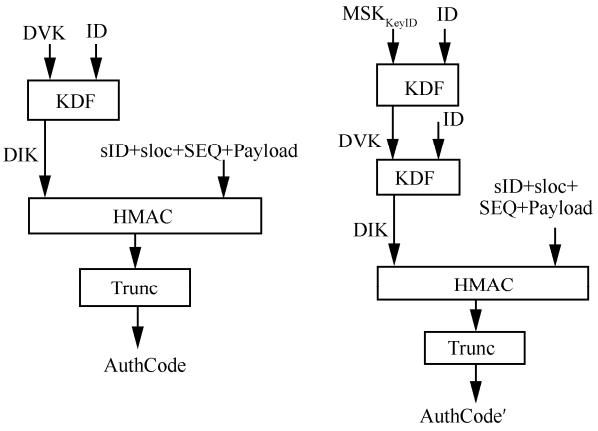

图 5　验证码生成和验证机制

汇聚根据报文的 KeyID 找到对应的 MSK，再以 ID 为输入派生出终端对应的 DVK，之后使用与终端一样的方法生成验证码 AuthCode'，需要注意的是 sLoc 为短地址，需要从报文中的终端长地址读取最后一级地址值（短地址）后再进行计算，然后通过 AuthCode'验证报文中的 AuthCode。

（3）防重放机制

终端设备和 AP 在认证过程中得到防重放计数器 SEQ 初始值，终端发包时，报文携带 SEQ 值，每发一个报文 SEQ 值加一，AP 维护接收窗口[SEQ_{MAX}，SEQ_{MAX}+ SEQ_WINDOW_SIZE]，依据该报文 SEQ 值是否在接收窗口内来判断其合法性。其中，SEQ_{MAX} 为已收到报文的 SEQ_T 最大值，SEQ_WINDOW_SIZE 为接收窗口大小，这两个参数可以通过命令配置。

3　原型系统搭建

为验证轻量可信协议的可行性以及灵活轻量与安全可信的特性，本文基于未来网络试验设施，搭建以智能门锁为典型应用的物联网原型测试场景。

3.1　基于未来网络试验设施的智能门锁应用场景

未来网络实验设施国家重大科技基础设施（CENI）是我国在信息通信领域的重大科技基础设施。深圳分系统作为 CENI 大科学装置的一部分，建设覆盖北京、深圳、上海、珠海、南京、

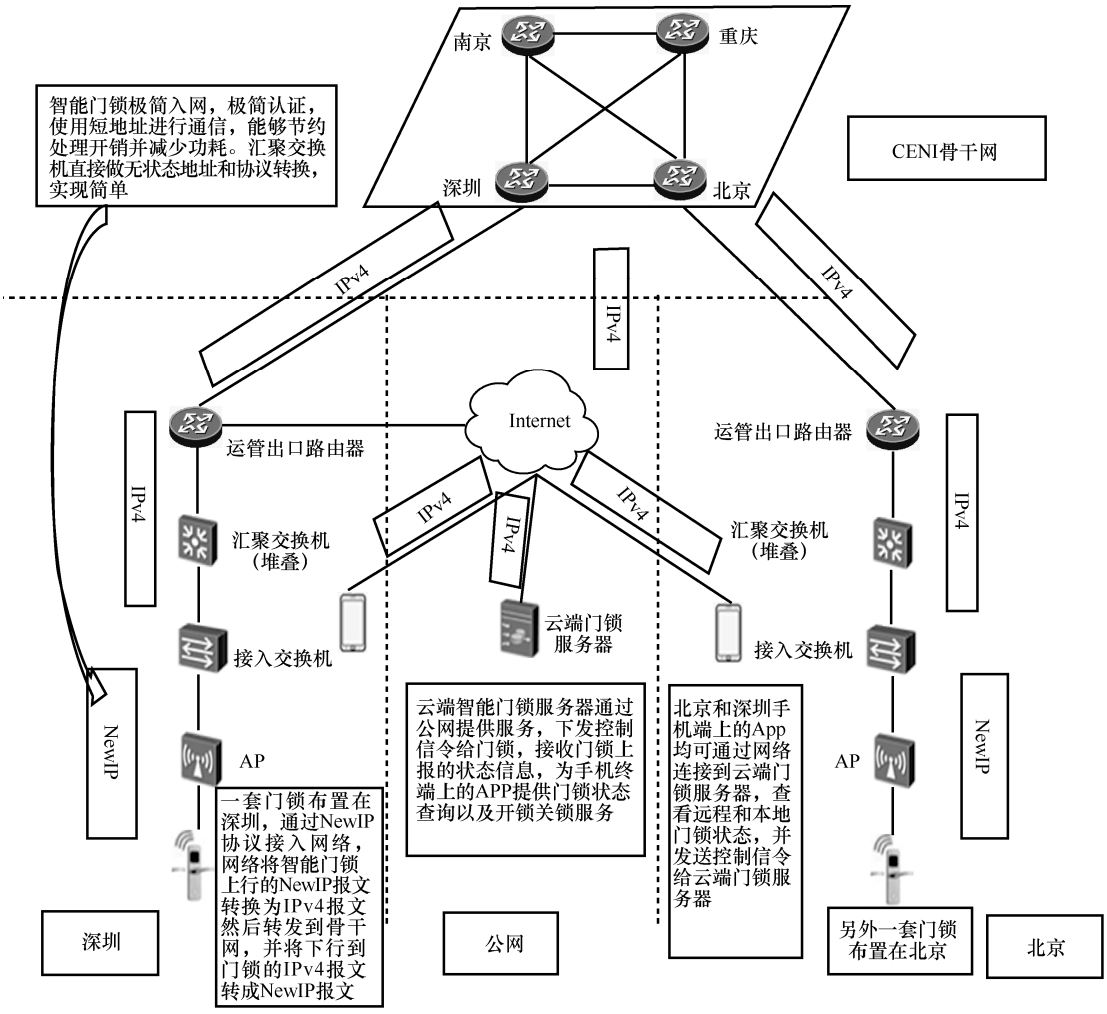

图 6　基于未来网络试验设施的智能门锁应用场景

成都、重庆、西安 8 个城市的 8 个骨干网络节点和 20 个边缘网络。如图 6 所示，为验证和测试本文提出的轻量可信协议，依托 CENI 试验设施深圳分系统，在北京和深圳两地搭建以智能门锁为测试场景的物联网原型系统。

智能门锁依次通过 AP、接入设备和汇聚设备连接到未来网络试验设施，作为其典型的物联网边缘场景。门锁终端的操作和状态将主动上报智能门锁服务器。该系统支持手机远程开锁，由智能门锁服务器向门锁终端直接发送开锁命令报文，实现门锁的开、关等动作。

基于灵活变长的地址设计，智能门锁服务器发送控制报文的目的地址可直接填写门锁的长地址，与门锁建立端到端的连接。当报文进入边缘网络后，通过汇聚和接入设备转发到 AP。此时，AP 嵌入相应的安全信息、并根据长短地址转换规则，将报文的长地址转换为短地址后再发送给门锁，降低门锁的通信开销。当门锁终端收到报文时，可依据报文内嵌的安全检查信息，做轻量级的安全校验和防重放，提升通信过程的安全保障能力。

3.2　智能门锁测试环境

在未来网络试验设施的边缘搭建智能门锁原型系统如图 7 所示。

其中，智能门锁终端采用 Telink TLSR 8258 型号芯片，其拥有 512 KB Flash 及 32 KB RAM，

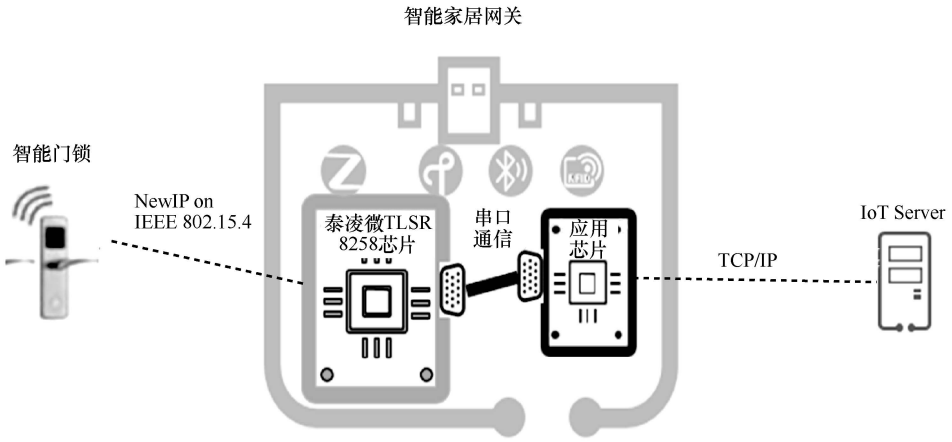

图 7　智能门锁原型系统

其上运行本文设计的轻量可信协议栈，可使用短地址直接与门锁服务器通信。AP 的通信模块同样采用 Telink TLSR 8258 型号芯片，同时 AP 可实现报头的网络层地址长短转换。接入和汇聚设备采用华为 CX600。门锁服务器架设在公有云上，可通过互联网远程下发控制指令到门锁终端上。

4　测试结果及分析

如图 8 所示，通过现场测试，可以使用手机 App 查看门锁状态并远程控制门锁的开启，证明了轻量可信协议的部署可行性。

图 8　手机 App 远程控制智能门锁开启

为进一步验证轻量可信协议栈的优势，本文分别从灵活轻量和安全可信两方面分析测试数据，论证其特性。

4.1　灵活轻量

在原型系统测试过程中，门锁服务器下发的控制指令的目的地址为门锁终端的 4 byte 长地址，在报文达到 AP 后，经过网络层的长短地址转换后，门锁终端实际收到的报文目的地址仅为 1 byte 的短地址，验证了本文提出的轻量可信协议栈支持灵活可变的报文传输，可以更好地应对不同应用场景下的通信需求。

传统协议栈与轻量可信协议栈开销的对比见表 1。可以发现，在存储开销方面，传统协议栈需要占用 180 KB 的 Flash，而轻量可信协议栈仅需 112 KB，节省约 40%的存储开销。同时，传统协议栈由于报头较长（平均 33 byte），而门锁终端通信报文的有效载荷平均也为 33 byte，实际传输效率仅为 50%，而轻量可信协议采用灵活报文设计后，压缩报头开销至平均 20 byte，可将该传输效率提升至 62%，总体传输效率提升了 24%。

表 1　传统协议栈与轻量可信协议栈对比

	轻量可信协议栈	传统协议栈
存储开销	112 KB	180 KB
传输效率	20/(20+33)=62%	33/(33+33)=50%

因此，采用轻量可信协议，可以显著降低物联网设备的通信开销，提升其通信数据的传输效率。

4.2 安全可信

原型系统关于安全可信功能的测试，首先在门锁中预置正确的安全信息，包括设备 ID、随路验证密钥、防重返计数器初始值，在手机 App 能够查看智能家居网关下有门锁接入，能够查看门锁的状态，远程控制开锁和关锁。

而当门锁中预置的安全信息错误，或未预置安全信息时，门锁无法加入网络，App 无法看到该门锁，网关侧日志能够看到安全验证错误的提示。

根据抓包分析可以看到，轻量可信协议每个报文中的安全字段为 13 byte，包括基于对称密钥安全机制生成的验证码（4 byte）、防重放计数器（4 byte）。而门锁接入认证只需两个控制报文，分别为 44 byte 和 68 byte。轻量可信协议与 IPSec 的比较见表 2，轻量可信协议报文安全开销远小于 IPSec，使用对称密钥机制大大降低了设备的计算开销，适用于资源受限物联网设备。

表 2 轻量可信协议栈与 IPSec 对比

	轻量可信协议栈	IPSec
安全字段	13 byte	＞48 byte

5 结束语

面对未来海量物联终端的网络互联需求，本文提出了一种轻量可信的通信协议，通过灵活轻量的报文设计，降低物联网低功耗设备的通信开销，提高数据传输效率。同时，针对常见的网络安全威胁，引入轻量级安全可信机制，保障物联网通信的端到端安全。本文基于未来网络试验设施搭建了原型系统，验证了轻量可信协议的可行性，并通过分析测试数据，论证了该协议具备灵活轻量与安全可信的特性，满足物联网设备低开销、高安全的通信需求。

参考文献：

[1] JIA Y, TROSSEN D, IANNONE L, et al. Challenging scenarios and problems in Internet addressing[EB]. 2021.
[2] CHATTERJEE A. Internet of things (IoT)[EB]. 2017.
[3] RFC. Security architecture for the Internet protocol[R]. 2005.
[4] 江伟玉, 刘冰洋, 王闯. 内生安全网络架构[J]. 电信科学, 2019, 35(9): 20-28.
JIANG W Y, LIU B Y, WANG C. Network architecture with intrinsic security[J]. Telecommunications Science, 2019, 35(9): 20-28.

[作者简介]

马军锋（1975− ），男，中国信息通信研究院技术与标准研究所副总工程师、高级工程师，主要研究方向为 IP 网络架构及路由技术、下一代互联网、SDN/NFV、边缘计算、未来网络等。

刘芷若（1992− ），女，中国信息通信研究院技术与标准研究所工程师，主要研究方向为 SDN/NFV、边缘计算、网络智能化、未来网络等。

李观文（1992− ），男，华为技术有限公司高级工程师，主要研究方向为未来网络架构与路由、天地一体化网络等。

杨飞（1975− ），男，华为技术有限公司主任工程师，主要研究方向为网络技术。

党娟娜（1982− ），女，华为技术有限公司主任工程师，主要研究方向为下一代 IP、内生安全的应用等。