doi :10.3969/j.issn.1671-1122.2017.10.003

一种物联网端到端安全方案

马国峻[1,2]，白磊[2]，裴庆祺[2]，李向军[1]

（1. 西安文理学院信息工程学院，陕西西安 710065；2. 西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西西安 710071）

摘　要：物联网安全是物联网发展的最主要挑战之一。物联网中大量的资源受限节点存储空间不足、计算能力较差、通信链路不稳定，无法采用互联网标准的安全协议保障通信的端到端安全，成为物联网的薄弱环节。结合物联网的特性和发展趋势，文章提出了一种基于边缘计算的物联网安全架构，并在此架构的基础上提出了基于代理数据报传输层安全的端到端安全方案。分析和实验表明该方案可以让物联网中资源受限设备能采用互联网标准的安全协议进行端到端安全通信，且具有较好的规模性、可扩展性和实际的可行性。

关键词：物联网；端到端安全；资源受限设备；边缘计算

中图分类号：TP309　　**文献标识码：**A　　**文章编号：**1671-1122（2017）10-0013-09

中文引用格式：马国峻，白磊，裴庆祺，等 . 一种物联网端到端安全方案 [J]. 信息网络安全，2017（10）：13-21.

英文引用格式：MA Guojun, BAI Lei, PEI Qingqi, et al. An End-to-End Security Scheme of the Internet of Things[J].Netinfo Security,2017(10):13-21.

An End-to-End Security Scheme of the Internet of Things

MA Guojun[1,2], BAI Lei[2], PEI Qingqi[2], LI Xiangjun[1]

(1. *School of Information Engineering*, *Xi'an University*, *Xi'an Shannxi* 710065, *China*; 2. *State Key Laboratory of Integrated Service Networks*, *Xidian University*, *Xi'an Shannxi* 710071, *China*)

Abstract: Security problem is one of the main challenges of IoT. Many constrained devices of IoT are operating under low power, and with limited computational and network resources, and cannot use standard security protocols to protect end-to-end security, they become the weakness of IoT. An IoT security architecture based on edge computing and a proxy-based Datagram Transport Layer Security end-to-end security scheme based on the architecture were proposed. Analysis and experiment show that the scheme can enable the constrained devices to communicate with any remote devices using the Internet standard security protocol in a security way. At the same time, the scheme is scalable, feasible and practical.

Key words: IoT; end-to-end security; constrained devices; edge computing

收稿日期：2017-7-1

基金项目：国家自然科学基金 [61373170]

作者简介：马国峻（1978—），男，安徽，讲师，博士，主要研究方向为数字内容保护、智能移动应用开发、区块链应用与安全；白磊（1993—），男，河南，硕士研究生，主要研究方向为网络与信息安全、物联网安全；裴庆祺（1975—），男，广西，教授，博士，主要研究方向为信任管理、无线网络安全、区块链安全；李向军（1967—），女，河北，教授，博士，主要研究方向为数据挖掘与知识发现、机器学习。

通信作者：马国峻 1578291722@qq.com

0 引言

物联网定义包含两层意思：1）物联网的核心和基础仍然是互联网，物联网是在互联网基础上进行延伸和扩展的网络；2）物联网的网络组成和通信延伸并扩展到任何物体，利用周边普遍存在的各种各样的物体或设备（如RFID 标签、智能手机、传感器、执行器等），通过独特的寻址方案，组成了一个由互相连接的实体组成的世界性网络，网络中的实体可以随时随地的互相交互来完成各种任务进行信息交换和通信[1]，也就是物物相联。物联网通过智能感知识别技术、普适计算技术等通信感知技术，广泛应用于网络的融合中，因此被称为继计算机、互联网之后世界信息产业发展的第三次浪潮。作为一种革命性的技术，物联网被赋予了极大的期待，预期的应用领域包括智能物流、智能交通、精细农业、智能家居、环境保护、智能电力、零售管理、医疗保健、金融管理、公共安全、工业监管、智能建筑、城市管理、军事管理等，其中前七大领域是最为普遍的应用领域。可以说未来的生活、世界与物联网息息相关，不可分割。

近年来，随着网络技术的快速发展，物联网已经从一个概念走向现实。许多建筑和小区正在通过部署传感器来节约能源；智能锁、智能电表等智能设备正在进入千家万户；汽车、出租车、交通灯等设备通过联网来提高安全性和运输效率；人们使用智能手机配合可穿戴设备及植入式医疗设备检测自己的身体状况；工业生产通过连接互联网来提高管理水平和生产效率。然而，与近年来物联网发展速度不匹配的是物联网的安全依旧存在巨大漏洞，惠普安全研究的调查报告显示："目前约有 80% 的物联网设备允许使用弱密钥，70% 的物联网设备认证过程存在漏洞"。市场研究机构 Gartner Inc 在 2012 年发布的报告[2]称："物联网的概念至少还需要 10 年才能产生实质的生产力，主要是由于安全挑战、隐私策略、数据和无限标准以及物联网实现所需的应用和连接架构"。由于物联网网络基础设施和应用相分离的趋势，安全风险要比架构更加的紧迫[3]。

在网络安全相关的众多相关技术中，保障设备与设备端到端通信的安全是非常基础和重要的部分。端到端的安全可以在所依赖的网络基础设施不在用户控制下时依旧保证通信的安全，考虑到通信的架构正变得越来越商品化，网络基础设施和应用分离是大势所趋，一个真正的端到端安全方案对物联网有着极为重要的意义。只有端到端通信的安全得到保障，用户、设备之间传输的数据才能避免被窃听者、电信供应商等非法获取，从而最大限度地保障用户的数据安全和隐私。在目前的互联网上，有众多的协议和机制用来保证端到端通信的安全，如 SSL/TLS、PGP、IPsec 等，这些安全机制保证了互联网上的端到端安全，但是它们无法直接应用到物联网中。

与传统互联网相比，处于物联网边缘的资源受限网络（如传感器网络）和资源受限设备（如传感器、RFID 标签、执行器），是物联网的重要组成部分，也是物联网安全的主要瓶颈。资源受限网络指那些目前难以实现互联网常用链路层特性的网络，资源受限网络通常具有低吞吐量、高丢包率、极度不对称链路等特点。而资源受限设备指那些目前难以实现互联网节点许多常见特性的设备，资源受限节点通常在能量、存储、处理能力上严重不足。虽然资源受限网络和资源受限节点并不相同，但是通常情况下资源受限网络中存在着大量的资源受限设备，资源受限设备是资源受限网络的主要瓶颈。对于这些资源受限设备来说，它们无法使用现有的互联网标准的安全协议和技术，因此成为网络攻击（如中间人攻击、拒绝服务攻击 DoS 等）的重要目标。

本文针对物联网中资源受限设备的端到端安全问题展开研究，在对物联网端到端安全机制研究进展分析的基础上，提出了一种基于边缘计算的物联网安全架构，并在此架构的基础上利用边缘计算设备对数据报传输层安全 (Datagram Transport Layer Security, DTLS) 协议的握手过程进行了代理，使物联网中的资源受限设备可以采用标准的互联网安全协议与远端任意设备进行直接通信。主要内容安排如下：

第 1 章介绍了物联网端到端安全机制的研究进展；第 2 章介绍了相关的基础知识；第 3 章提出了基于边缘计算的物联网安全架构和利用边缘计算设备对 DTLS 协议进行代理的过程；第 4 章对所提出的方案进行了分析和验证；最后对本文进行了总结和展望。

1 研究进展

考虑到物联网中的资源受限设备是物联网的主要安全

瓶颈，针对物联网安全的研究和早期无线传感器网络安全研究具有一定的相关性。然而，传感器网络的安全协议主要集中在链路层，以一种一跳一跳的方式保护数据安全。最简单的保护链路层安全的方法是使用一个网络内共享的密钥。例如，Zigbee 网络正是采用这种方法，Zigbee 还提供了对分簇和个人链路层密钥的支持。MiniSec[4] 是另外一种著名的传感器网络安全机制，提供了数据完整性、认证性和重放检验。和 Zigbee 相比，MiniSec 引入的包开销只有很少的字节。TinySec 曾经也是广泛流传的传感器网络链路层安全机制，但是研究表明它已经不再安全了 [5]。除了传感器网络的安全协议主要集中在链路层之外，在很多传感器网络的研究中并没有很好地考虑传感器的资源或者与现有协议的兼容性，这也导致针对传感器网络安全的研究不能很好地应用到物联网端到端安全中。

近年来，专门针对物联网环境下的端到端安全机制研究逐渐展开。针对物联网的端到端安全研究主要在基于云的物联网安全架构和基于网关的物联网安全架构下展开。基于云的物联网安全架构借助云计算强大的存储能力和计算能力弥补了资源受限设备计算性能差，存储能力不足的限制，其典型架构如图 1 所示。

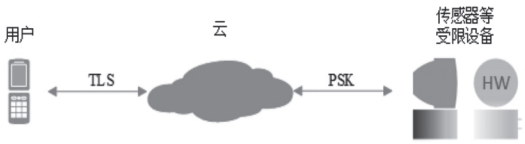

图 1 基于云的物联网安全架构

在基于云的架构下，云平台和资源受限设备之间通过预分发的密钥 PSK 保证数据传输的安全，通常情况下云平台和资源受限设备之间具有一对一的关系。用户和云平台之间通过互联网现有的安全协议 TLS 保证安全，资源受限设备和用户之间通常无法直接通信或者资源受限设备只能与有限的特定用户进行通信。采用基于云的物联网架构可以保证资源受限设备数据传输的安全，然而基于 PSK 的安全方案限制了资源受限设备与远端设备的通信，无法满足物联网开放性、可扩展性和规模性的特点，不符合物联网的发展趋势。

基于网关的安全架构是针对传感器网络研究的延续，该架构利用网关的计算和存储能力弥补了资源受限设备的不足，其典型架构如图 2 所示。在基于网关的安全方案中，早期研究中网关负责整个网络域内的安全，它不仅负责协议和数据的转换，还要负责对网络内部 / 外部所有节点的认证、访问控制、管理等工作。当外部数据进入资源受限网络中时，网关负责对数据进行解密，并将解密后的数据发送给对应的传感器节点；当传感器节点发送数据给外部设备时，网关负责将数据进行加密，并不是真正的端到端安全。

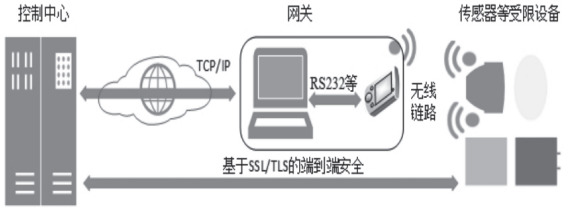

图 2 基于网关的物联网安全架构

随着物联网安全的研究越来越注重考虑物联网自身的特性，如物联网开放性和可扩展性，网关逐渐仅代替资源受限设备执行少量必要的计算。其中比较典型的如 YU[6] 等人提出使用可信的网关负责管理资源受限设备的公钥，并帮助资源受限设备协商与服务器进行 TLS 握手，建立通信密钥，资源受限设备的接入控制由该服务器负责，然而该方案使用 TLS 协议对于资源受限网络的链路特征来说是不合适的。BRACHMANN[7] 等人则采用网关进行 TLS/DTLS 协议转换的方法保证端到端通信和 LLN 网络的安全，网关只负责将远端设备发送给资源受限设备的 TLS 协议数据包转换为 DTLS 协议数据包，不改变数据包的内容，然而该方案并没有考虑基于公钥 / 证书的 DTLS 协议在资源受限设备上运行的可行性问题。GRANJAL[8] 等人提出了一个由网关中介的 DTLS 握手，在他们的方案中，网关参与并转发运输层的数据包，执行基于 ECC 公钥密码的握手，网关和资源受限设备间的通信是通过基于 PSK 的方法保护的。该方案在保证资源受限设备与远端设备通信安全的基础上具有很强的可行性，然而该方案如同其他基于网关的方案一样不适合大规模网络。采用网关的安全方案由于将大量的计算交给网关，当网络规模增大时，网关将成为系统的瓶颈。此外基于网关的安全方案导致网关成为一个高价值的攻击目标，当网关受到攻击（如 DoS 攻击）时可能导致整个网络的瘫痪。

其他一些专门针对物联网端到端安全的研究中，KOTHMAYR[9] 等人提出将可信模块 TPM 部署到所有的资源受限设备，并由 TPM 进行公钥相关运算，该方案提高了物

联网设备的成本，难以推广到所有设备中，此外此类方案也没有解决握手过程带来的通信开销。TAN[10] 等人提出了一种基于身份的轻量级密码方案 IBE-Lite，IBE-Lite 的基本思想是平衡安全隐私与可行性，然而该方案考虑资源受限节点对基站 / 用户数据的认证问题，而且该方案与现有的互联网安全协议不兼容，其实用性和规模性难以考量。

2 背景知识

2.1 资源受限设备

为了使本文的研究更加具有针对性，下面对本文所针对的资源受限设备进行说明。在 IETF 工作组的 RFC 7228[11] 中根据节点存储资源的不同将资源受限节点分为了三类，如表 1 所示。

表 1 资源受限设备分类

类名	RAM（数据空间）	ROM/Flash（代码空间）
Class 0	<<10 KB	<<100 KB
Class 1	~10KB	~100KB
Class 2	~50KB	~250KB

这些分类和目前商业上常用的资源受限的设备芯片相对应，在该分类中，Class 0 设备的存储资源和处理能力太过受限，因此它们很可能没有能力以一种安全的方式直接和互联网连接。Class 0 设备更可能需要借助网关、代理或者服务器的帮助来接入网络；他们通常无法以传统的方式保证安全或者管理，它们往往需要预配置非常少的数量集，并在此之后几乎不再改变。

Class 1 设备的代码空间和处理器能力都比较受限，他们无法很容易地和互联网节点采用全协议栈如 HTTP、TLS、TCP 等相关的协议进行通信，但是它们可以采用针对资源受限节点特殊设计的协议栈 CoAP、UDP 进行通信，并且不需要网关的帮助。通常情况下，这些节点可以支持安全功能并视作完整开发的节点加入 IP 网络，但是对于这些节点的设计需要非常珍惜代码空间、RAM 以及电量消耗。

Class 2 设备资源不太受限并且有能力支持笔记本电脑或者服务器上相同的协议栈。然而，即便是这种类型的设备也可以从轻量级的、能量高效的协议中收益。此外，网络消耗更少的能量就意味着应用程序可以使用更多的能量。因此，将针对资源更受限的节点而设计的协议应用到 Class 2 设备上可能会减少开发部署的花销，并增加互操作性。

能力和性能显著超出 Class 2 的设备可以直接使用现有的协议，不需要进行任何改变，因此在 RFC 7228 的定义中没有进行说明，本文的研究对象主要是 Class1 和 Class 2 设备的端到端安全通信问题。

2.2 DTLS 协议

DTLS 全称是 Datagram Transport Layer Security，即数据报传输层安全，主要用来保证基于 UDP 传输的数据安全。其基本设计理念是设计一个可用于 UDP 传输的 TLS 协议。DTLS 协议是互联网标准协议，由 IETF 工作组于 2006 年发布，之后在 2012 年 IETF 又发布了基于 TLS1.2 的 DTLS1.2 标准。

DTLS 协议是在 TLS 的基础上改进得到的，因此它和 TLS 协议具有相同的体系结构。DTLS 协议也是由一组协议组成的分层协议，共有五部分组成，分别是：记录层协议、握手协议、改变密码规格协议、警报协议和应用层数据协议。DTLS 协议的具体分层结构及它在 TCP/IP 协议栈中的位置如图 3 所示。

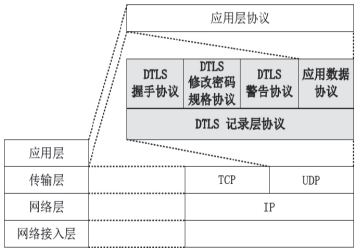

图 3 DTLS 协议分层结构

DTLS 记录层协议处于底层，它是一个封装协议，所有通过 DTLS 协议发送的数据都被添加了一个 13 字节长的 DTLS 记录层头部。这个头部指定了消息的内容（如是应用数据还是握手数据）、采用的协议版本、64 比特的序列号以及记录的长度。其中在 64 比特的序列号中，起始的 16 比特用来指定消息的 epoch，每次服务器和客户端完成了新的加密参数协商，epoch 就会加 1。其他协议（如握手协议、警告协议等）的数据是记录层协议载荷，处于记录层协议头部之后。进行数据发送的时候，记录层需要对数据进行分片、压缩（可选），计算 MAC 值以及加密，最后再加入上述的记录层头部。完成这些操作后，DTLS 对数据的协议封装完成，将数据交给传输层。在进行数据接收的时候则执行相反的操作。

握手协议用来协商端到端通信中使用的密钥材料和密

码套件，DTLS 共有三种类型的握手，分别是：无认证、服务器认证和全认证握手。在无认证握手中，通信双方不进行身份认证，在服务器认证握手中，只有服务器提供其身份信息，客户端对服务器进行认证；在全认证握手中，通信双方都需要提供身份信息，客户端和服务器进行互相认证。只有握手阶段完成后才能进行应用数据的发送。

DTLS 的握手阶段可以使用不同的方式进行身份认证，主要有预共享密钥 PSK、原生的公私钥对和基于证书的方式。基于预共享密钥 PSK 的方法采用客户端和服务器提前共享的密钥进行身份认证，由于采用对称密钥，认证开销较小，但是密钥的分发和管理比较困难，只适用于与固定服务器的认证，不具有扩展性和互操作性。基于证书的方案是目前互联网中使用的主流方法，具有较强的互操作性，但是开销较大，无法直接在资源受限设备上使用。

相对于 TLS 协议，DTLS 协议更加适合物联网中的资源受限设备和资源受限网络，这主要是由于 DTLS 是基于 UDP 协议开发的，TCP 相对对于简单的、不可靠的 UDP 协议来说带来了很大的开销，尤其是对于缺乏能量、电池供电的设备来说，这个开销很明显。而且 TCP 已经被证明在低带宽的场景中表现很差 [12]，这也反映在应用层标准协议 CoAP 中，它使用了 UDP 传输协议并绑定了 DTLS 作为它的安全机制。此外 TLS 协议在握手过程中数据包不能丢失，否则会终止握手，这对于易损的 LLN 网络来说是不现实的，而 DTLS 协议采用重传机制解决了 UDP 中数据包的丢失问题，这使它更加适合 LLN 网络。

2.3 边缘计算技术

随着物联网的发展，越来越多的涉及日常生活的数据在不断产生，在各种各样的物联网应用中，一些 IoT 应用可能需要非常短的反应时间（如智能医疗），一些 IoT 应用可能涉及个人的隐私数据，一些应用可能产生大量的数据（如智能监控）以至于对网络来说是个巨大的负担。当数据大量的在网络边缘产生并利用时，云计算通常是不够高效的，将不足以继续支撑这些应用的发展 [13]。由于网络边缘产生并消费的数据正在飞速增长，在网络的边缘对数据进行处理可能会更加高效。因此，近年来，微型数据中心 [14]、cloudlet[15]、雾计算 [16] 以及边缘计算的概念相继被引入以解决这些问题，这些概念虽然表述方式不同，但是本质基本一致，本文选择边缘计算这种表述方式以进一步说明。

边缘计算指使计算在网络边缘进行的一种技术，是在靠近物或数据源头的网络边缘侧，融合网络、计算、存储、应用核心能力的开放平台，就近提供智能服务。边缘边缘可以为数据源和云数据中心之间的任何计算和网络资源。例如，一个智能手机是智能穿戴设备和云之间的边缘；一个智能家庭网关是家庭和云之间的边缘；一个微型的数据中心或者 cloudlet 是移动设备和云之间的边缘。在边缘计算的模式中，物联网设备不仅是数据的消费者，也是数据的生产者。

边缘计算并不是云计算的替代性技术，而是云计算的补充，一方面边缘计算设备与物联网设备进行通行，可以执行计算卸载、数据存储、缓存和处理，以及将云的请求和服务传递给用户等功能；另一方面边缘计算设备可以和云实时通信，上传必要的数据到云平台，由云平台进行更深层次的数据融合。

3 基于代理 DTLS 的物联网安全方案

3.1 基于边缘计算的物联网安全架构

本文第 2 章通过分析指出，现有的基于云和基于网关的安全架构都不能很好地满足物联网安全需求，本节结合边缘计算的核心思想，及物联网的主要特性和安全需求，提出了一种基于边缘计算的物联网安全架构，如图 4 所示。

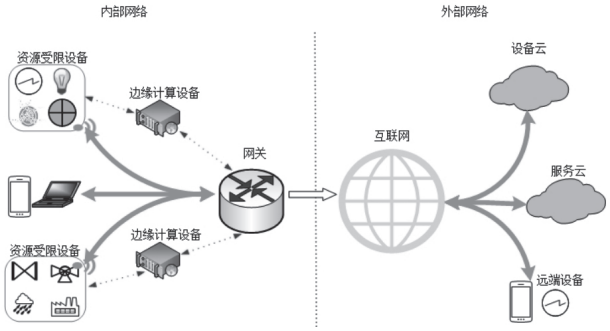

图 4 基于边缘计算的物联网安全架构

在该架构中主要有以下组成部分。

1）资源受限网络

即图 4 中的内部网络，它是由资源受限设备和普通网络设备组成的网络，网络中的资源受限节点通过传感技术监测环境的各种信息并提供给需要的消费者，同时节点自身可能也是消费者，从其他设备 / 云端获得数据。资源受

限节点和网关节点之间通过无线或有线通信协议连接，但通常是无线通信技术如 Bluetooth、WiFi、IEEE 802.15.4 等；资源受限节点的寻址采用 IPv6 技术，传输层协议采用 UDP 协议，应用层采用 CoAP 协议（普通网络设备采用现有的网络通信技术，在此不再赘述）。

2）边缘计算设备

边缘计算设备是一种新的硬件，它处于网络的内部，在互联网的边缘提供计算、存储、边缘智能、数据协同融合等服务。边缘计算设备可以根据网络的规模灵活地配备资源和数目。当资源受限网络中节点数目较多时，可以配备性能强大的边缘计算设备，也可以配备多个边缘计算设备，每个边缘计算设备负责部分资源受限节点；当资源受限网络中节点数目较少时，可以将网关作为边缘计算设备。由于处于网络的内部，边缘计算设备与资源受限节点是属于同一实体的，如在智能家庭场景中，边缘计算设备和资源受限节点都属于房屋主人；在智能建筑场景中，每个公司可以为自己配备边缘计算设备。因此可以认为边缘计算设备是一个可信的实体，为网络内的资源受限设备提供认证、授权等服务。

3）网关

作为本地网络和互联网的衔接桥梁，网关支持上述多种不同的通信技术，由于资源受限设备采用 TCP/IP 协议栈（对于 TCP/IP 协议栈的支持性已在第 2 章介绍），因此资源受限设备发送数据到互联网将不需要网关的协助。但是在一些特殊的情况下如外部发向资源受限设备的数据可能需要由网关协助提供 6LoWPAN 分片操作，这一操作发生在网络层和链路层之间，不会影响双方通信的端到端安全性。为了保护本地网络的安全，网关上部署防火墙等安全安全技术，过滤非法的通信，作为保证本地网络安全的第一道屏障。

4）外部网络

外部网络包括云服务中心、服务供应商、普通用户 / 设备等。虽然边缘计算设备具有较强的存储、计算等能力，但是随着时间的增加本地网络将产生大量的数据，将这些数据发送到云服务中心进行存储、深度挖掘等将会更加合适，但是是否需要这一操作取决于资源受限网络所属实体采用的隐私策略。服务供应商可以提供广泛的服务和保障，如医疗、安监、食品配送等服务，服务供应商通常需要向资源受限网络订阅数据，根据接收到的数据提供相应的服务。远端设备既可以是数据的生产者也可以是数据的消费者，可以向资源受限网络中的设备发送数据以下达命令，也可以从资源受限网络中的设备接收数据以获取资源。

3.2 基于边缘计算设备代理 DTLS 的端到端安全机制

要想使 Class 1 和 Class 2 设备采用互联网标准的安全协议 DTLS 保证其通信的端到端安全性，并且不限定资源受限设备的通信对象，则必须解决资源受限设备采用公钥 / 证书作为凭证进行 DTLS 握手的通信和计算开销。本节提出利用边缘计算设备对 DTLS 握手流程进行代理解决这一问题。方案主要分为以下几个步骤：启动初始化和重定向、握手代理阶段、会话转移阶段，下面对这三个过程分别进行介绍。

1）启动初始化和重定向

由于物联网的异构性，网络中不仅有大量资源受限设备也有许多普通设备，普通设备和部分资源受限设备可能出于自身性能或隐私保护的考虑不使用代理握手，因此网关需要知道那些设备的握手过程需要代理，此外网关还需要知道执行代理操作的是哪一个边缘计算设备。此外为了保护资源受限节点和为其提供代理服务的边缘计算设备之间的通信安全，需要首先在两者之间共享一个对称密钥，由于资源受限节点和边缘计算设备处于同一网络内，因此可以在节点加入本地网络，初始化配置的过程中采用物理接触或无线通信等方法进行。

利用资源受限节点和边缘计算设备之间共享的密钥提供加密保护，需要代理的资源受限节点可以安全地将自身的密钥套件、密钥材料等发送给边缘计算设备。收到资源受限节点的代理请求后，边缘计算设备将代理关系发送给网关，网关维护一个资源受限设备和边缘计算设备的对应关系表，记录下边缘计算设备和资源受限节点之间的代理关系。之后网关接收到数据时需要查询该表，如果数据包的目的节点在该表内则执行重定向操作，如图 5 所示。

在重定向操作中，网关首先需要读取 DTLS 记录层头部的 CONTENT_FIELD 部分，实际上网关也确实可以读取这一数据，因为 CONTENT_FIELD 是明文信息，如果 CONTENT_FIELD = 32，则该数据为应用数据，网关直接

转发数据给资源受限节点，否则网关将该数据包重定向到对应的边缘计算设备。

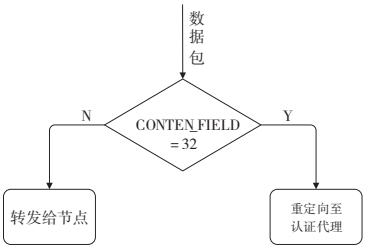

图 5 网关重定向操作

2）握手代理阶段

在本文方案中，握手代理方案是可选的，只有在初始化的过程中节点告知网关采用代理握手的方案，才执行 DTLS 代理握手。具体的 DTLS 代理握手流程如图 6 所示。

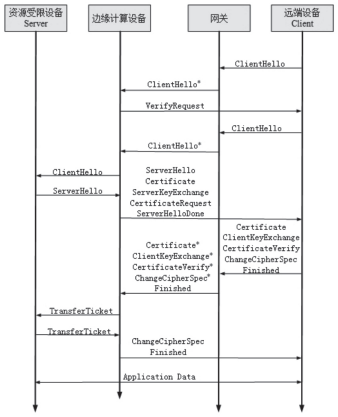

图 6 基于代理的 DTLS 握手流程

（1）首先一个远端节点（客户端）发送一个 ClientHello 消息来发起和资源受限节点（CoAP 服务器）的通信。网关接收到 ClientHello 消息后会执行重定向操作，将 ClientHello 消息及之后相关的所有握手消息重定向到对应的边缘计算设备，同时还会在消息中附上本消息真实的目的地址。

（2）边缘计算设备回复远端节点一个 VerifyRequest 消息。这个消息包含有边缘计算设备产生的 cooike，用来阻止拒绝服务攻击 DoS。考虑到一个边缘计算设备需要负责多个设备，且边缘计算设备只是资源相对丰富，因此该措施是必要的，负责过多的 DTLS 握手可能会耗尽边缘计算设备的存储、计算、带宽等资源。之后如果远端节点回复的 ClientHello 消息中包含有相同的 Cookie，则握手继续进行，否则终止该握手过程。

（3）如果远端节点回复了包含正确 Cookie 的 ClientHello 消息，边缘计算设备将发送 ClientHello 消息给资源受限设备，并在消息中包含客户端随机数，这个随机数之后会被用来计算远端设备和资源受限设备之间通信的密钥。通过这一步骤，边缘计算设备可以告知资源受限节点目前正在代理它进行 DTLS 握手操作，并且将在之后与资源受限节点进行会话转移（session transfer）；此外该边缘计算设备通过该消息还可以检查资源受限节点的可达性，如果资源受限节点被占用，无力接受新的连接，则边缘计算设备可以代替资源受限节点终止本次握手，这样便保证了资源受限节点和边缘计算设备均可以终止握手。

（4）资源受限节点回复 ServerHello 消息给边缘计算设备，该消息中包含会话 ID 和其产生的服务器随机数。该随机数与客户端随机数一起组成了会话密钥材料。边缘计算设备发送包含有该服务器随机数的 ServerHello 消息给远端的节点。同时在这一航程（flight）中边缘计算设备还会发送 ServerKeyExchange、证书和 ServerHelloDone 消息。在 ServerKeyExchange 消息中包含有 ECDH 公钥用来创建预 – 主安全密钥。在此需要注意，不管是 ClientHello 消息还是 ServerHello 消息都分别包含了客户端和服务器支持的密码套件。如果需要的话，在该航程中还可以发送 CertificateRequest 消息来要求远端节点提供证书证明自己的身份。

（5）远端节点根据边缘计算设备发送证书的真实性后，回复它的证书以及 CertificateVerify 消息来证明自己的身份，同时在该行程中一起发送 ClientKeyExchange、ChangeCipherVerify 消息及 Finished 消息。其中 ClientKeyExchange 消息中包含有预 – 主密钥，该密钥被双方设备用来计算共同的主密钥。之后双方的会话将建立在该秘密的基础上。

至此，边缘计算设备代理的 DTLS 握手操作已完成，之后边缘计算设备将把安全环境发送给对应的资源受限设备。

3）会话转移

会话转移通过 DTLS 协议的恢复机制实现，边缘计算设备收到远端节点发送的 Finished 消息后，发送 SessionTransferTicket 消息给被代理设备，该消息中包含有

所建立会话相关的参数如客户端 id、预 – 主密钥，本次通信使用它和被代理设备之间共享的密钥进行加密保护。

被代理设备通过边缘计算设备发送的相关参数创建和远端节点的连接状态，之后回复另一个 SessionTransferTicket 消息给边缘计算设备，该消息包含了它上一个接收到的消息的 MAC 值，来向边缘计算设备确认已经收到该消息。

之后边缘计算设备发送 ChangeCipherVerify 和 Finished 消息给远端设备，并删除关于此次连接相关的状态、参数等。之后被代理设备和远端设备之间便可利用已建立的 DTLS 连接进行安全交互。

4 方案分析和验证

结合物联网的自身特性，下面分别从端到端安全性、是否限定通信对象、是否支持标准协议、可用性、规模性五个方面对本文提出的方案进行分析。

首先从端到端安全性来说，基于代理的 DTLS 安全方案以 DTLS 协议为基础，对 DTLS 协议的握手流程进行了代理，代理过程中边缘计算设备与远端设备进行完整的基于公钥或证书的 DTLS 握手，由于采用标准的互联网安全协议，该握手流程的安全性可以保证。边缘计算设备与远端设备完成握手建立安全环境后，将安全参数通过它和被代理设备（资源受限设备）提前协商的密钥加密后传递给被代理设备，可以保证安全参数的安全转移。之后被代理设备与远端设备之间的端到端通信是通过握手产生的安全参数保护的，进行的是 DTLS 协议保护的端到端安全通信，因此具有 DTLS 协议的安全性，如保证通信数据的机密性、完整性和可用性，抵抗重放攻击、抵抗 DoS 攻击等。

在对标准协议的支持上，本文所提出的物联网端到端安全方案基于 DTLS 协议，为互联网标准的安全协议，其底层协议传输层 UDP 协议、网络层 IP 协议、适配层 6LoWPAN 协议、MAC 层和物理层 IEEE 802.15.4 协议均为互联网标准协议和技术，对标准协议完全支持，与互联网现有机制互相兼容，这有利于该方案的推广使用并促进不同厂商、不同设备之间的互联互通和数据融合。

在是否限定通信对象方面，本文方案利用边缘计算设备代理资源受限设备进行 DTLS 协议的握手过程，减少了资源受限设备用于握手阶段和公钥运算的资源消耗，因此使用中可以采用基于公钥或证书的 DTLS 协议进行身份的验证及会话密钥协商，而不局限于基于 PSK 的 DTLS 协议，不限定资源受限设备的远端通信对象，确保资源受限设备与任意远端设备进行安全通信。

在规模性方面，本文方案采用边缘计算设备进行握手的代理操作，避免了网络规模增大时网关成为瓶颈。此外在一个网关内部可以部署多个边缘计算设备，这意味着即便某个边缘计算设备被攻击，也只影响部分节点，不会导致整个网络的瘫痪。

在可行性方面，本节通过在资源受限设备上分别实现基于 PSK 和基于 ECC 的 DTLS 协议来对方案的实际可行性进行进一步的分析。可行性分析主要针对存储和计算能力，具体体现在 RAM/ROM 的消耗和握手时间上。

实现所采用的硬件平台为 TI 公司生产的 CC2538 芯片，CC2538 具有 32 KB RAM 和 128~512 KB ROM，其最高主频为 32 MHz，最大的闪存为 512 KB，RAM 为 32 KB，满足 IETF 对 Class 2 设备的分类标准。该芯片为片上系统，芯片上集成了 32 位的 ARM Cortex M3 内核和满足 IEEE 802.15.4 的射频模块，在工作的过程中，射频模块接收电流仅为 20 mA，发射电流 24 mA，睡眠模式下则仅有 1.3 μA 的电流，具有低功耗的特性，可以满足资源受限节点对低功耗的需求。

实现所采用的软件平台为开源的物联网操作系统 Contiki，它专门针对资源受限的设备和网络进行设计，支持多任务操作。Contiki 致力于帮助小的低价格、低功耗微控制器连接到互联网，整个系统仅需要几字节便可以运行，在一个较为典型的配置中，Contiki 系统只需 2 KB 的 RAM 与 40 KB 的 ROM，非常适合物联网末端环境。

对于 DTLS 的实现，借助了开源的 tinyDTLS 库，它支持基于 PSK 的 TLS_PSK_WITH_AES_128_CCM8 和基于 ECC 的 TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8。

表 2 列出了硬件节点上只运行 Contiki 系统、运行 Contiki 系统及基于 PSK 的 DTLS 协议、运行 Contiki 系统及基于 ECC 的 DTLS 协议这三种情况下 RAM 和 ROM 空

间的存储资源消耗情况。

表 2 DTLS 存储资源消耗

系统	代码空间（ROM）	只读数据（ROM）	读写数据（RAM）
Contiki	52.3 KB	6.0 KB	7.2 KB
Contiki + DTLS PSK	81.4 KB	17.6 KB	9.4 KB
Contiki + DTLS ECC	87.2 KB	18.3 KB	10.5 KB

从表 2 中可以看出，当在 Contiki 系统上运行基于 PSK 的 DTLS 协议时，消耗 9.4 KB 的 RAM 和 89.0 KB 的 ROM 空间，可以满足在 Class1 设备上运行，并留有一定空间给应用程序。当在 Contiki 系统上运行基于 ECC 的 DTLS 协议时，消耗 10.5 KB 的 RAM 和 105.5 KB 的 ROM，增加了 1.1 KB 的 RAM 和 6.5 KB 的 ROM 消耗。采用基于代理的 DTLS 安全方案时资源受限节点只需要维护 DTLS 的安全环境并执行 Session 恢复的过程，消耗的存储资源小于基于 PSK 的 DTLS 握手过程，因此所提出的方案在存储上具有可行性。

在握手时间上，当运行基于 ECC 的完整 DTLS 握手时，需要约 5 s 才能完成完整的握手流程，运行基于 PSK 的完整 DTLS 握手时需要约 3 s 完成握手。采用基于代理的 DTLS 安全方案时，资源受限设备不需要参与 DTLS 的握手过程，因此在计算上具有可行性。

5 结束语

本文首先结合物联网的发展趋势，提出了一种基于边缘计算的物联网安全架构，然后在该架构的基础上提出了基于边缘计算设备代理的 DTLS 端到端安全方案，通过分析说明了所提出的安全方案在保证物联网中资源受限设备采用互联网标准的安全协议与任意远端设备进行端到端安全通信的基础上，还具有较好的规模性和可扩展性，并通过实现说明了该方案的可行性。然而，本文方案仅能保证物联网设备端到端通信的安全性，实际上针对物联网安全还需要进行更多更深入的研究，如物联网设备本身的安全、物联网设备的入网初始化、移动物联网设备的安全等多个方面。可以说物联网安全的研究才刚刚起步，更广泛更深入的研究需要更多科研工作者的共同努力。（责编 吴晶）

参考文献：

[1] 文伟平，郭荣华，孟正，等 . 信息安全风险评估关键技术研究与实现 [J]. 信息网络安全，2015（2）：7-14.

[2]LEHONG H. Hype Cycle for the Internet of Things [R]. Stamford: Gartner Inc,G00234864, 2012.

[3] 张晓惠，林柏钢 . 基于平衡二叉决策树 SVM 算法的物联网安全研究 [J]. 信息网络安全，2015（8）：20-25.

[4]Luk M, Mezzour G, Perrig A, et al. MiniSec: A Secure Sensor Network Communication Architecture[C]// IEEE. International Symposium on Information Processing in Sensor Networks, April 25-27 2007, Cambridge, MA, USA. New York: IEEE, 2007:479-488.

[5] 高君丰，崔玉华，罗森林，等 . 信息系统可控性评价研究 [J]. 信息网络安全，2015（8）：67-75.

[6]YU H, HE J, ZHANG T, XIAO P, et al. Enabling end-to-end Secure Communication Between Wireless Sensor Networks and the Internet [J]. World Wide Web, 2013, 16(4):515-540.

[7]BRACHMANN M, KEOH S L, MORCHON O G, et al. End-to-End Transport Security in the IP-Based Internet of Things[C]// IEEE. International Conference on Computer Communications and Networks, July 30-August 2, 2012, Munich, Germany. New York: IEEE, 2012:1-5.

[8]GRANJAL J, MONTEIRO E, SILVA J S. End-to-end Transport-layer Security for Internet-integrated Sensing Applications with Mutual and Delegated ECC Public-key Authentication[C]// IEEE. Ifip NETWORKING Conference, May 22-24,2013, Brooklyn, NY, USA. New York: IEEE, 2013:1-9.

[9]KOTHMAYR T, SCHMITT C, HU W, et al. DTLS based Security and Two-way Authentication for the Internet of Things[J]. Ad Hoc Networks, 2013, 11(8):2710-2723.

[10]TAN C C, WANG H, ZHONG S, et al. IBE-Lite: a Lightweight Identity-based Cryptography for Body Sensor Networks.[J]. EEE Transactions on Information Technology in Biomedicine A Publication of the IEEE Engineering in Medicine & Biology Society,2009, 13(6):926-932.

[11] BORMANN C, ERESUE M, KERANEN A.RFC 7228: Terminology for Constrained Node Networks[EB/OL]. https://tools.ietf.org/pdf/rfc7228.pdf, 2014-5-1.

[12]DAWSON-HAGGERTY S, TAVAKOLI A, CULLER D. Hydro: A Hybrid Routing Protocol for Low-Power and Lossy Networks[C]// IEEE. First IEEE International Conference on Smart Grid Communications, October 4-6, 2010, Gaithersburg, MD, USA. New York: IEEE, 2010:268-273.

[13]SHI W, CAO J, ZHANG Q, et al. Edge Computing: Vision and Challenges[J]. IEEE Internet of Things Journal, 2016, 3(5):637-646.

[14]GREENBERG A, HAMILTON J, MALTZ D A, et al. The Cost of a Cloud: Research Problems in Data Center Networks[J]. Acm Sigcomm Computer Communication Review, 2008, 39(1):68-73.

[15]JARARWEN Y, TAWALBEH L, ABABNEH F, et al. Resource Efficient Mobile Computing Using Cloudlet Infrastructure[C]// IEEE. International Conference on Mobile Ad-Hoc and Sensor Networks, December 11-13, 2013, Dalian, China . New York: IEEE, 2013:373-377.

[16]BONOMI F, MILITO R, ZHU J, et al. Fog Computing and its Role in the Internet of Things[C]// ACM. Edition of the Mcc Workshop on Mobile Cloud Computing, August 17, 2012, Helsinki, Finland.New York: ACM, 2012:13-16.