Table of Contents

将IPv6 应用于低功耗无线个人局域网(6LoWPANs)：概述，设想，问题陈述，目标

在线阅读

Gitbook | Github

离线阅读

PDF | ePub | Mobi

英文原版

点击查看英文原版

强烈建议读完中文后再阅读英文。

当您认认真真读完一篇英文后，会发现原来读英文也如此轻松！

做贡献

如果您发现文档有任何错误，包括错别字，歧义等，您可以：

- 自己修改，提交 pull request，我会 merge 你的改动。
- 提问题(issue)，我会根据 issue 修改相应的内容。

更多关于物联网标准的中文文档，请移步：

物联网相关的标准文档(IEEE、IEFT RFC)中文版汇总

1 简介

低功耗无线个人局域网（LoWPAN）由符合 IEEE 802.15.4－2003 标准的设备组成。IEEE 802.15.4 设备的特点是近距离、低速率、低功耗和低成本。大多数使用 IEEE 802.15.4 的设备都在计算能力、存储、电源等方面受到一定的限制。

本文档对 LoWPAN 做了一个概述，并描述 IP 网络(尤其是 IPv6 网络)给 LoWPAN 带来的好处。本文描述了LoWPAN 对 IP 层和更上层提出的要求，并做了一些假想。最后，本文描述了在 LoWPAN 网络中使用 IP 通信的相关问题，并为解决这些问题定义了若干目标。当然，本文所列的条款未必全都适合于 IETF 的工作。然而，本文是为了给一个更大的问题做简要阐述。这不仅有助于 IETF 更好地组织内部工作，又有助于与其它外部组织相互合作。

2 概述

LoWPAN 是一个简单、低成本的通信网络，它允许低功耗、低速率的应用也能使用无线通信。LoWPAN 中通常包含若干设备，如无线传感器，这些设备协同作用，将物理环境和现实应用连接起来。LoWPAN 遵循 IEEE 802.15.4－2003 标准[IEEE802.15.4]。

LoWPAN 的一些特性如下：

1. 报文尺寸小。因为物理层的最大数据包是 127 字节，所以 MAC 层的最大帧长是 102 字节。链路层安全协议也占用了一定的空间（AES－CCM－128点用 21 字节，AES－CCM－32 占用 9 字节，AES－CCM－64 占用 13 字节），所以剩下给用户数据的空间可能只有 81 字节。
2. 支持 16 位短地址和 64 位 IEEE 扩展 MAC 地址两种地址模式。
3. 低带宽。对于物理层所定义的 2.4 GHz、915 MHz、868 MHz 三种频段，其对应的数据速率分别是 250 kbps，40 kbps 和 20 kbps。
4. 包括星型和 mesk 网络两种拓扑结构。
5. 低功耗。通常，网络中的部分设备（甚至全部设备）使用电池供电。
6. 低成本。这些设备通常是传感器、开关等。这一特性与其它一些特性相关，比如低处理能力、低存储空间等。因为设备的成本会随着时间而变化，所以“低”的具体数值是无法定义的。
7. 设备部署量大。这些设备的数量可能远远超过 PC 机。
8. 由于设备很可能以 ad-hoc 的方式部署，所以设备的位置通常都不能预先确定。此外，设备所处的位置可能不容易进入，设备也可能会被移动到新的位置。
9. LoWPAN 中的设备多是不可靠的，主要是因为：不可靠的无线连接、电池耗尽、设备锁定、物理干扰等。
10. 在很多环境下，连接到 LoWPAN 的设备为了节约电量可能长时间处于休眠状态，而在休眠时期不能进行通信。

接下来的章节会对 LoWPAN 特别地是 6LoWPAN（基于 IPv6 的LoWPAN 网络）的假设、问题陈述、目标进行具体的描述。

3 假设

基于 LoWPAN 的报文尺寸小这一特性，本文假定应用程序通常只发送很少量的数据。当然，协议本身并没有限制发送大量数据。

在本文所描述的 LoWPAN 基于 IEEE 802.15.4-2003。IEEE 802.15.4 的具体规范在未来可能会发生改变，因此上面提到的一些需求也可能随之改变。

部分假设基于 LoWPAN 网络中设备的处理能力有限这一特性。因此当设备的处理能力变强、消耗的电能减少时，上述所提到的一些条件可以适当放松。

LoWPAN 中的设备可以分为两类：资源极其受限的设备（精简功能设备，简称 RFD）；功能稍强的设备（全功能设备，简称 FFD）。全功能设备通常拥有更多的资源，且可能以传输线供电的方式供电。因此，全功能设备可以用来辅助精简功能设备提供一些功能，如网络协调、报文转发、连接其它类型的网络等。

使用 IP 技术主要有以下好处：

1. IP 网络的普遍性使得设备可以利用现有的网络基础设施。
2. 基于 IP 的技术是已经存在的，且是广为人知的、并证明是可行的。
3. 一个不可否认的非技术性但重要的因素是 IP 网络技术是公开、免费的，这是有好处的，或至少相对于专有的技术方案来说，IP 技术更容易让大众理解。
4. 已经存在很多关于 IP 网络的工具，比如诊断、管理、调试等。
5. 基于 IP 的设备能够很容易的与其他 IP 网络连接，不需要中转设备，如转换网关、代理。

4 问题

基于第二章中提到的特性，下面的章节将阐述 LoWPAN 中关于 IP 的主要问题。

4.1 IP 连接性

LoWPAN 中 IP 连接性的需求受到下列条件的影响：

1. LoWPAN 网络中的许多设备需要网络进行自动配置并高度无状态描述。对于这一点，IPv6 已经有了解决方案。
2. 大量设备需要大量的地址空间。IPv6 能满足这个需求。
3. 由于 LoWPAN 的报文尺寸小，因此可以根据需要，将 IPv6 地址格式归入 IEEE 802.15.4 地址。
4. 简化了与其它网络的连通性，比如因特网。

然而，因受报文大小限制，要尽可能地将 IPv6 和上层报文头进行压缩。

4.2 拓扑结构

LoWPAN 必须支持包括星型和 mesk 在内的各种拓扑结构。

Mesk 拓扑意味着报文需要经过多跳路由才能达到目的地。在这种情形下，中间设备在链路层扮演报文转发的角色（与网络层的路由器类似）。这种中间设备一般都是 FFD，因为它们比 RFD 具有更好的电源供应和更高的计算能力。路由协议的需求如下：

1. 由于 LoWPAN 的报文尺寸小，路由协议必须只占用少量（或者不占用）报文数据，且最好与跳数无关。
2. 路由协议应该只有少量的路由报文数据（少交换数据），平衡拓扑的变化和电量消耗。
3. 为了满足低成本和低功耗的目标，路由协议对于计算能力和存储的要求尽量降低。因此，存储和维护大路由表是不可能的。
4. 支持电池供电或有线供电的 FFD 或 RFD 所组成的网络拓扑。这意味着要考虑到对睡眠节点的路由。

与 mesh 拓扑一样，星型拓扑也包含一个具有报文转发功能的设备子集。这些设备可能会使用除 IEEE 802.15.4 之外的其它网络接口，比如以太网、IEEE 802.11。我们的目标是将这些构建在不同技术之上的网络进行无缝集成。当然，这是一开始使用 IP 的最主要原因。

4.3 受限的报文大小

应用程序发送的报文要尽可能小，最好能保证应用程序的数据加上各层的头部能在一帧之内传输，这样就能减小不必要的分片和重组。更进一步，在设计或选择协议时，必须保证单个“控制/协议报文”能够填充在一个 802.15.4 帧之内。按照这些原则，低端设备在对 IPv6 进行子 IP 重组（参考第 5 章）时将面临一些挑战，因为这些设备没有足够的内存或者存储空间来存储 1280 个字节的报文。

4.4 受限的配置和管理

如前面所述，LoWPAN 网络中部署的设备的数量可能是极其庞大的。此外，这些设备一般都只有很弱的显示和输入的功能。而且，有些设备部署的地方是很难进入的。因此，LoWPAN 所使用的协议应尽量减小配置项，使设备容易启动，最好是开箱即用。此外，由于设备所固有的不可靠性，网络具有自动修复功能。在保证能够控制大量的密集部署的设备的前提下，网络管理的开销要尽量小。

4.5 服务发现

LoWPAN 需要一个简单的服务发现网络协议来发现、控制和维护设备所提供的服务。在某些情况下，特别是密集部署时，整合几个节点来提供一个服务是有好处的。为了实现这样的功能，需要设计新的协议。

4.6 安全

尽管 IEEE 802.15.4 使用了 AES 保证了链路安全，但它在程序启动、密钥管理和上层协议的安全性方面没有作任何具体的规定。当然，LoWPAN 设备必须根据应用的需要仔细考虑一个完整的安全性方案。请参考后面安全相关的章节做更具体的讨论和深入的安全需求分析。

5 目标

下面所提到的目标具有一般性，并不限定在 IETF 任务里。同样的，这不仅仅涉及到只有 IETF 才能完成的工作（例如传输 IP 的具体需求、现实中传输IP报文最好的配置、相关的上层协议等）。它同样指向了跟其他标准更相关的工作（例如与 IEEE 802.15.4 相关的变化描述或配置文件、W3C 等）。当目标是在IETF的范围内时，它用来指出什么样的工作是需要完成的，不管是否在一个（或多个）新的（或已存在的）工作组里完成的。当目标不在 IETF 的范围内时，在这里提到是为了交给其他的组织 [LIAISON]。

请注意，一个共同的目标是减小报文开销、带宽开销、处理器需求、和电量消耗。

下面是按优先级列出的一些 LoWPAN 目标：

1. 分片和重组层：正如概述里提到的一样，协议数据单元可能只有 81 字节大小。这明显比 IPv6 的最小报文 1280 字节还要小得多，为了符合第 5 章的 IPv6 要求，在 IP 层下面必须提供一个分片和重组的适配层。
2. 报头压缩：考虑到在最坏情况下，一个 IEEE 802.15.4 帧可用于传输IP报文的大小只有 81 字节，并且 IPv6 报头长度为 40 字节（在没有报头选项的情况下），这就只剩下 41 字节给上层协议了，如 UDP 和 TCP。UDP 使用 8 字节的报头而 TCP 使用 20 字节。别外，如上面所提到的，还需要一个分片和重组层，这将会占用更多的字节，留给数据的字节就更少了。这样，如果要使用这样的协议，这将会导致大量的分片和重组，即使数据包长度只有 10 个字节。这表明需要进行报头压缩。因为有大量的已发行的和正在制定中的关于报头压缩的标准化文件，6LoWPAN 必须考虑使用现有的报头压缩技术，并且，如果有需要的话，制定新的标准。
3. 地址自动配置：[6LoWPAN]指定了自动配置无状态 IPv6 地址的方法。无状态自动配置（相对于有状态的）更适合于 6LoWPANs，因为它在主机上减少了配置信息的流量。这就需要一种方法来从 IEEE 802.15.4 设备上分配的 EUI－64[EUI64]来生成“接口标识符”。
4. Mesh 路由协议：一种支持多跳mesh网络的路由协议是必需的。现已有很多发布的点对点多跳路由协议。一些例子包括[RFC3561]、[RFC3626]、[RFC3684]这些都是实验性的。同样，这些协议是为使用有比较在的报头的基于IP地址而设计的。例如，特别按需距离矢量（AODV）[RFC3561]路由协议使用48字节报头进行基于 IPv6 地址的路由请求。考虑到报文大小的限制，传输这个报文而不用分片和重组是比较困难的。因此，为了使路由报文只限在一个 IEEE 802.15.4 帧内，在选择现有的路由协议（或设计新的协议）时应该要认真考虑。
5. 网络管理：使用IPv6进行报文传输的一个重要原因是为了尽可能的使用现有的协议。网络管理功能对于LoWPANs来说是很重要的。然而，管理方式必须符合受限资源和在4.4节提到的最小配置和自动修复功能。在传统的网络中，简单网络管理协议（SNMP）[RFC3410]被广泛的使用在数据资源和传感器的监控上。SNMP 功能对于LoWPAN 来说

可认为“同样的”，为了利用现有的工具。然而，由于受到存储容量、处理能力和报文大小的限制，使用 SNMPv3 是否合适还是需要进一步的研究，或者在 SNMPv3 上加一个适配层，或者使用另一个不同的协议。

6. 实施注意事项：在 IEEE 802.15.4 上传输 IP 报文或许是更有好处的，如果通过“某种”方式来实施。因此，实施注意事项是必要考虑的。
7. 应用层和更高层的注意事项：正因报头压缩变得越来越普遍，总体性能会更依赖于应用协议的高效性。基于 XML 的重量级协议如 SOAP[SOAP] 可能不太适合 LoWPAN。同样，更简洁的编码（或许协议）是有必要的。本文的目标是指定或建议如何修改现有协议以使它们适合用于 LoWPAN。此外，应用层的互操作性在未来可能是必需的，因此需要考虑到。
8. 安全事项：不同层的安全威胁必须仔细理解和研究。考虑到设备的安装位置、有限的显示、高度密集和点对点部署，加入安全网络是需要全面考虑的。

6 安全考虑

基于 IPv6 的 LoWPAN（6LoWPAN）应用经常需要机密性和完整性保护。安全保护可由应用层、传输层、网络层和/或链路层来提供（也就是说，在 6LoWPAN 的协议集里）。在所有这些情况下，诸多的限制会影响到一个特定协议的选择。一些更相关的限制是代码量小、低电量、低复杂度和小带宽。

考虑到这些限制，首先，为了测试当做出有意义的假设和简单化时对于减轻成本的任何风险，必需要为 6LoWPAN 设备开发一个威胁模型。一些需要考虑的威胁例子是中间人攻击和拒绝服务攻击。

一个单独的安全事项集应用于 6LoWPAN 设备加入网络的过程（即，初始密钥建立）。这通常包含应用层交换或初始密钥建立的带外技术，并可能依赖于特定应用的信任模型；因此，这不在 6LoWPAN 的范围内，所以本文不做更多描述。为了能够选择（或设计）下一项协议，这就需要由初始密钥建立的键控材料成为一个通用模型。

在初始密钥建立之外，后面的密钥管理和数据传输安全协议是在 6LoWPAN 范围内的。这里，不同的选择（TLS，IKE/IPsec 等）必须依据 6LoWPAN 的限制来评估。

在链路层上使用安全协议的一个争论是多数 IEEE 802.15.4 设备已经支持 AES 链路层安全。AES 是一个在固定块长度（128位）操作的一个块密码。为了加密更长的消息，可使用几种不同的操作方式。最早的模式是，如 ECB、CBC、OFB 和 CFB 只提供保密性，这并不能保证消息的完整性。其他已经设计出的模式可同时保证机密性和完整性，如 CCM*模式。6LoWPAN 可以使用先前的任一种模式，但使用最安全的链路层安全模式（即 CCM*）是很有必要的，并建立在这之上。

对于网络层安全，有两种可用的模型：端到端安全，即使用IPsec传输模式，或限制于网络无线部分的安全，即是使用安全网关和 IPsec 隧道模式。后一种模式的不利之处是报头太大，这对 6LoWPAN 帧的 MTU 是很重要的。为了简化 6LoWPAN 的实施，指定相关的安全模型是有好处的，并要指定一组适合于受限环境的优先密码集。

7 致谢

感谢 Geoff Mulligan、 Soohong Daniel Park、 Samita Chakrabarti、Brijesh Kumar 和 Miguel Garcia 提出的意见并帮助完成了这份文档。

8 参考文献

[RFC2460]

- Deering, S. and R. Hinden, "Internet Protocol, Version6 (IPv6) Specification", RFC 2460, December 1998.

[IEEE802.15.4]

- IEEE Computer Society, "IEEE Std. 802.15.4-2003", October 2003.

[EUI64]

- "GUIDELINES FOR 64-BIT GLOBAL IDENTIFIER (EUI-64)REGISTRATION AUTHORITY", IEEE, http://standards.ieee.org/regauth/oui/tutorials/EUI64.html.

[6LoWPAN]

- Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", Work in Progress, May 2005.

[RFC3411]

- Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[RFC3561]

- Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.

[RFC3626]

- Clausen, T. and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003.

[RFC3684]

- Ogier, R., Templin, F., and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", RFC 3684, February 2004.

[SOAP]

- "XML Protocol Working Group", W3C, http://www.w3c.org/2000/xp/Group/.

[LIAISON]

- "IETF Liaison Activities", IETF, http://www.ietf.org/liaisonActivities.html.