Network Working Group
Internet-Draft
Expires: August 28, 2006

N. Kushalnagar
Intel Corp
G. Montenegro
Microsoft Corporation

February 24, 2006

6LoWPAN: Overview, Assumptions, Problem Statement and Goals

draft-ietf-6lowpan-problem-02.txt

Status of this Memo

Copyright Notice

Abstract

This document describes the assumptions, problem statement and goals for transmitting IP over IEEE 802.15.4 networks. The set of goals enumerated in this document form an initial set only. Additional goals may be found necessary over time and may be added to this document.

Table of Contents

1. Introduction

Low-power wireless personal area networks (LoWPANs) comprise devices that conform to the IEEE 802.15.4-2003 standard by the IEEE [ieee802.15.4]. The IEEE 802.15.4 devices are characterized by short range, low bit rate, low power and low cost.

This document gives an overview of LoWPANs and describes how they benefit from IP and IPv6 networking. It describes the requirements of LoWPANs with regards to IP layer and above. It spells out the underlying assumptions of IP for LoWPANs. Finally, it describes problems associated with enabling IP communication between devices in LoWPAN, and defines goals to address these in a prioritized manner. Admittedly, not all items on this list are necessarily appropriate tasks for the IETF. Nevertheless, they are documented here to give a general overview of the larger problem. This is useful both to structure work within the IETF as well as to understand better how to coordinate with external organizations.

1.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Overview

A LoWPAN is a simple low cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. A LoWPAN typically includes devices that work together to connect the physical environment to real-world applications, e.g., wireless sensors. LoWPANs conform to the IEEE 802.15.4-2003 standard. [ieee802.15.4].

Some of the characteristics of LoWPANs are:

1. Small packet size. Given that the maximum physical layer packet is 127 bytes, the resulting maximum frame size at the media access control layer is 102 octets. Link-layer security imposes further overhead, which in the maximum case (21 octets of overhead in the AES-CCM-128 case, versus 9 and 13 for AES-CCM-32 and AES-CCM-64, respectively) leaves 81 octets for data packets.

2. Support for both 16-bit short or IEEE 64-bit extended media access control addresses.

3. Low bandwidth. Data rates of 250 kbps, 40 kbps and 20 kbps for each of the currently defined physical layers (2.4 GHz, 915 MHz and 868 MHz, respectively).

4. Topologies include star and mesh operation.

5. Low power, typically some or all devices are battery operated.

6. Low cost, typically associated with sensors, switches, etc. These drive some of the other characteristics such as low processing, low memory, etc. Numerical values for "low" have not been explicitly mentioned here as historically the costs tend to change over time.

7. Large number of devices expected to be deployed during the life-time of the technology. This number is expected to dwarf the number of deployed personal computers, for example.

8. Location of the devices are typically not predefined, thus these devices are deployed in an adhoc fashion. Furthermore, sometimes the location of these devices may not be easily accessible. Additionally these devices may move to new locations.

9. Devices within LoWPANs have a higher possibility of being unreliable due to variety of reasons: uncertain radio connectivity, battery drain, device lockups, physical tampering, etc.

10. Devices within LoWPANs have a higher possibility of being unavailable because often these devices are in sleep mode or in a power down mode to conserve power.

The following sections take into account these characteristics in describing the assumptions, problems statement and goals for LoWPANs.

3. Assumptions

Given the small packet size of LoWPANs, this document presumes applications typically send small amounts of data. However, the protocols themselves do not restrict bulk data transfers.

LoWPANs as described in this document are based on IEEE 802.15.4-2003. It is possible that the specification may undergo changes in the future and may change some of the requirements mentioned above.

Some of these assumptions are based on the limited capabilities of devices within LoWPANs. As devices become more powerful, and consume

less power, some of the requirements mentioned above may be somewhat relaxed.

Nevertheless, not all devices in a LoWPAN are expected to be extremely limited. This is true of so-called "Reduced Function Devices" (RFDs), but not necessarily of "Full Function Devices" (FFDs). These will also be present albeit in much smaller numbers, and will typically have more resources and be mains powered. Accordingly, FFDs will aid RFDs by providing functions such as network coordination, packet forwarding, interfacing with other types of networks, etc.

IP technology is assumed to provide the following benefits:

1. The pervasive nature of IP networks allows use of existing infrastructure.
2. IP based technologies already exist, are well known and proven to be working.
3. An admittedly non-technical but important consideration is that intellectual property conditions for IP networking technology are either more favorable or at least better understood than proprietary and newer solutions.
4. Tools for diagnostics, management and commissioning of IP networks already exists.
5. IP based devices can more easily be connected to other IP based networks, without the need for translation gateways and the like.

4. Problems

Based on the characteristics defined in the overview section, the following sections elaborate on the main problems with IP for LoWPANs Note that a common underlying goal is to reduce packet overhead, bandwidth consumption, and processing requirements.

4.1. IP Connectivity

The requirement for IP connectivity within a LoWPAN is driven by the following:

1. The many devices in a LoWPAN make network auto configuration and statelessness highly desirable. And for this, IPv6 has ready solutions.
2. The large number of devices poses the need for a large address space, well met by IPv6.
3. Given the limited packet size of LoWPANs, the IPv6 address format allows subsuming of IEEE 802.15.4 addresses if so desired.

4. Simple interconnectivity to other IP networks including the Internet.

However, given the limited packet size, headers for IPv6 and above layers must be compressed whenever possible.

4.2. Topologies

LoWPANs must support various topologies including mesh and star.

Mesh topologies imply multi-hop routing, to a desired destination. In this case, intermediate devices act as packet forwarders at the link layer (akin to routers at the network layer). Typically these are "full function devices" that has more capabilities in terms of power, computation, etc. The requirements that apply on the chosen routing protocol are:

1. Given the minimal packet size of LoWPANs, the routing protocol must impose low (or no) overhead on data packets, hopefully independently of the number of hops.
2. The routing protocols should have low routing overhead (less chatty) balanced with topology changes and power conservation.
3. The computation and memory requirements in the routing protocol should be minimal to satisfy low cost and low power characteristics. Thus storage and maintaining of large routing tables may be detrimental.

As with mesh topologies, star topologies include provisioning a subset of devices with packet forwarding functionality. If, in addition to IEEE 802.15.4, these devices use other kinds of network interfaces such as ethernet, IEEE 802.11, etc., the goal is to seamlessly integrate the networks built over those different technologies. This, or course, is a primary motivation to use IP to begin with.

4.3. Limited Packet Size

Applications within LoWPANs are expected to originate small packets. Adding all layers for IP connectivity should still allow transmission in one frame without incurring excessive fragmentation and reassembly. Furthermore, protocols must be designed or chosen so that the individual "control/protocol packets" fit within a single 802.15.4 frame.

4.4. Limited configuration and management

As alluded to above, devices within LoWPANs are expected to be deployed in exceedingly large numbers. Additionally, they are

expected to have limited display and input capabilities. Furthermore, the location of some of these devices may be hard to access. As such, protocols designed for LoWPANs should have minimal configuration, preferably work "out of the box", provide easy bootstrapping, and the network should be able to self heal given the inherent unreliable characteristic of these devices. The network management should have less overhead yet be powerful to control dense deployment of devices.

4.5. Service discovery

LoWPANs require simple service discovery network protocols to discover, control and maintain services provided by devices. In some cases, especially in dense deployments, abstraction of several nodes to provide a service may be beneficial. In order to enable such features, new protocols may have to be designed.

4.6. Security

Security for LoWPAN devices must be carefully considered depending upon the application needs. IEEE 802.15.4 provides AES link layer security. Due to the nature of 6LoWPAN devices, security solutions that need excessive computing, or bandwidth may not be suitable for LoWPAN devices. Please refer to security consideration section below for an in depth requirements for security.

5. Goals

Goals mentioned here may point at relevant work that can be done within the IETF (e.g., specification required to transmit IP, profile of best practices for transmitting IP packets, and associated upper level protocols, etc). It may also point at work to be done in other standards bodies that exist or may exist in the future (e.g., desirable changes or profiles relevant to IEEE 802.15.4, W3C, etc). When the goals fall under the IETF's purview, they serve to point out what those efforts should strive to accomplish. Regardless of whether they are pursued within one (or more) new (or existing) working groups. When the goals do not fall under the purview of the IETF, documenting them here serves as input to those other organizations [liaison].

The following are the goals according to priority for LoWPANs:

1. As mentioned in the overview, the protocol data units may be as small 81 bytes. This is obviously far below the minimum IPv6 packet size of 1280 octets, and in keeping with section 5 of the IPv6 specification [RFC2460], a fragmentation and reassembly

adaptation layer must be provided at the layer below IP.

2. Given that in the worst case the maximum size available for transmitting IP packets over IEEE 802.15.4 frame is 81 octets, and that the IPv6 header is 40 octets long, (without optional headers), this leaves only 41 octets for upper-layer protocols, like UDP and TCP. UDP uses 8 octets in the header and TCP uses 20 octets. This leaves 33 octets for data over UDP and 21 octets for data over TCP. Additionally, as pointed above, there is also a need for a fragmentation and reassembly layer, which will use even more octets leaving very few octets for data. Thus if one were to use the protocols as is, it would lead to excessive fragmentation and reassembly even when data packets are just 10s of octets long. This points to the need for header compression As there is much published and in-progress standardization work on header compression, this goal needs to investigate using existing header compression techniques and if necessary specify new ones.

3. [I-D.ietf-ipv6-rfc2462bis] specify methods for creating IPv6 stateless address auto configuration. Stateless auto configuration has an advantage over stateful by having less configuration overhead on the hosts suitable for LoWPANs. The goal should specify a method to generate an "interface identifier" from the EUI-64 [EUI64] assigned to the IEEE 802.15.4 device.

4. A routing protocol to support a multi-hop mesh network is necessary. There is much published work on adhoc multi hop routing for devices. Some examples include [RFC3561], [RFC3626], [RFC3684], all experimental. Also, these protocols are designed to use IP based addresses that have large overheads. For example, the AODV [RFC3561] routing protocol uses 48 octets for a route request based on IPv6 addressing. Given the packet size constraints, transmitting this packet without fragmentation and reassembly may be difficult. Thus care should be taken when using existing protocols or designing new protocols for routing so that the routing packets fit within a single IEEE 802.15.4 frame.

5. One of the points of transmitting IPv6 packets, is to reuse existing protocols as much as possible. Network management functionality is critical for LoWPANs. [RFC3411] specifies SNMPv3 protocol operations. SNMP functionality may be translated "as is" to LoWPANs. However, further investigation is required. SNMPv3 may be found to be not suitable, or it may be only suitable after adapting it appropriately. This adaptation could include limiting the data types and simplifying the Basic

Encoding Rules so as to reduce the size and complexity of the ASN.1 parser, thereby reducing the memory and processing needs to better fit into the limited memory and power of LoWPAN devices.

6. It may be the case that transmitting IP over IEEE 802.15.4 would become more beneficial if implemented in a "certain" way. Accordingly, implementation considerations are to be documented.

7. As header compression becomes more prevalent, overall performance will depend even more on efficiency of application protocols. Heavyweight protocols based on XML such as SOAP [SOAP], may not be suitable for LoWPANs. As such, more compact encodings (and perhaps protocols) may become necessary. The goal here is to specify or suggest modifications to existing protocols so that it is suitable for LoWPANs. Furthermore, application level interoperability specifications may also become necessary in the future and may thus be specified.

8. Security threats at different layers must be clearly understood and documented. Bootstrapping of devices into a secure network could also be considered given the location, limited display, high density and ad hoc deployment of devices.

6. IANA Considerations

This document contains no IANA considerations.

7. Security Considerations

6lowpan applications often require confidentiality and integrity protection. This can be provided at the application or transport level, at the network layer, and/or at the link layer, i.e. within the 6lowpan set of specifications. In all these cases, 6LoWPAN constraints will influence the choice of a particular protocol. Some of the more relevant constraints are small code size, low power operation, low complexity, and small bandwidth requirements.

It is understandable that these constraints have associated tradeoffs. Thus a threat model for 6LoWPAN devices needs to be first developed in order to weight any risks against the cost of security and at the same time make meaningful assumptions and simplifications. Some examples for threats that would be considered are man in the middle attacks, denial of service attacks.

A separate set of security considerations might apply to bootstrapping a 6lowpan device into the network, in particular

initial key establishment processes. This is generally involved with other application level transactions and may rely on an application-specific trust model; thus it will not be part of 6LoWPAN. Some choices may be to use out of band communication techniques such as USB, infrared or NFC (Near Field Communication) for the initial key establishment.

After the initial key establishment, subsequent key management protocols would fall under the purview of 6LoWPAN. In order to be able to select (or design) this next set of protocols, there needs to be a common model of the keying material created by the initial key establishment. There are a few cryptographic protocols to choose from. It is to be seen if the protocols available as part of IPsec meet the constraints of 6LoWPAN.

One argument for using link layer security is that most IEEE 802.15.4 chips already have support for AES link layer security. AES is a block cipher operating on blocks of fixed length, i.e., 128 bits. To encrypt longer messages, several modes of operation may be used. The earliest modes described, such as ECB, CBC, OFB and CFB provide only confidentiality, and this does not ensure message integrity. Other modes have been designed which ensure both confidentiality and message integrity, such as CCM* mode. 6LoWPAN could choose to operate in one of the modes of operation, but it is desirable to utilize as much of link level security as possible and build upon it.

For network layer security, two models are applicable: end-to-end security, e.g. using IPsec transport mode, or security that is limited to the wireless portion of the network, e.g. using a security gateway and IPsec tunnel mode. The disadvantage of the latter is the larger header size, which is significant at the 6lowpan frame MTUs. To simplify 6lowpan implementations, it would be beneficial to consider security model needed and identify a preferred set of cipher suites that are appropriate given the 6lowpan constraints.

8. Acknowledgements

Thanks to :

Geoff Mulligan

Soohong Daniel Park

Samita Chakrabarti

Brijesh Kumar

for their comments and help shaping this document.

9. References

9.1. Normative References

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

[I-D.ietf-ipv6-2461bis] Narten, T., "Neighbor Discovery for IP version 6 (IPv6)", draft-ietf-ipv6-2461bis-05 (work in progress), October 2005.

[I-D.ietf-ipv6-rfc2462bis] Thomson, S., "IPv6 Stateless Address Autoconfiguration", draft-ietf-ipv6-rfc2462bis-08 (work in progress), May 2005.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[ieee802.15.4] IEEE Computer Society, "IEEE Std. 802.15.4-2003", October 2003.

9.2. Informative References

[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.

[RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[SOAP] "SOAP", W3C http://www.w3c.org/2000/xp/Group/.

[liaison] "LIASONS", IETF http://www.ietf.org/liaisonActivities.html.

Authors' Addresses

Nandakishore Kushalnagar
Intel Corp

Email: nandakishore.kushalnagar@intel.com

Gabriel Montenegro
Microsoft Corporation

Email: gabriel_montenegro_2000@yahoo.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.