6LoWPAN Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 7, 2012

J. Nieminen, Ed.
B. Patil
T. Savolainen
M. Isomaki
Nokia
Z. Shelby
Sensinode
C. Gomez
Universitat Politecnica de
Catalunya/i2CAT

March 6, 2012

Transmission of IPv6 Packets over Bluetooth Low Energy
draft-ietf-6lowpan-btle-06

Abstract

Bluetooth Low Energy is a low power air interface technology defined by the Bluetooth Special Interest Group (BT SIG). The standard Bluetooth radio has been widely implemented and available in mobile phones, notebook computers, audio headsets and many other devices. The low power version of Bluetooth is a new specification and enables the use of this air interface with devices such as sensors, smart meters, appliances, etc. The low power variant of Bluetooth is commonly specified in revision 4.0 of the Bluetooth specifications and commonly refered to as Bluetooth 4.0. This document describes how IPv6 is transported over Bluetooth Low Energy using 6LoWPAN techniques.

Table of Contents

1. Introduction 3
2. Bluetooth Low Energy 3
  2.1. Bluetooth Low Energy stack 4
  2.2. Link layer roles and topology 4
  2.3. BT-LE device addressing 5
  2.4. BT-LE packets sizes and MTU 5
3. Specification of IPv6 over Bluetooth Low Energy 6
  3.1. Protocol stack 6
  3.2. Link model 7
    3.2.1. Stateless address autoconfiguration 7
    3.2.2. Neighbor discovery 8
    3.2.3. Header compression 9
    3.2.4. Unicast and Multicast address mapping 9
  3.3. Internet connectivity scenarios 10
4. IANA Considerations 10
5. Security Considerations 11
6. Additional contributors 11
7. Acknowledgements 11
8. Normative References 11
Appendix A. Bluetooth Low Energy fragmentation and L2CAP Modes . 12
Authors' Addresses 13

1. Introduction

Bluetooth Low Energy (BT-LE) is a radio technology targeted for devices that operate with coin cell batteries or minimalistic power sources, which means that low power consumption is essential. BT-LE is an especially attractive technology for Internet of Things applications, such as health monitors, environmental sensing, proximity applications and many others.

Considering the potential for the exponential growth in the number of sensors and Internet connected devices and things, IPv6 is an ideal protocol due to the large address space it provides. In addition, IPv6 provides tools for autoconfiguration, which is particularly suitable for sensor network applications and nodes which have very limited processing power or a full-fledged operating system.

[RFC4944] specifies the transmission of IPv6 over IEEE 802.15.4. The Bluetooth Low Energy link in many respects has similar characteristics to that of IEEE 802.15.4. Many of the mechanisms defined in [RFC4944] can be applied to the transmission of IPv6 on Bluetooth Low Energy links. This document specifies the details of IPv6 transmission over Bluetooth Low Energy links.

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 RFC 2119 [RFC2119].

The terms 6LN, 6LR and 6LBR are defined as in [I-D.ietf-6lowpan-nd].

2. Bluetooth Low Energy

BT-LE is designed for transferring small amounts of data infrequently at modest data rates at a very low cost per bit. Bluetooth SIG has introduced two trademarks, Bluetooth Smart for single-mode devices (a device that only supports BT-LE) and Bluetooth Smart Ready for dual-mode devices. In the rest of the draft, the term BT-LE refers to both types of devices.

BT-LE is an integral part of the BT 4.0 specification [BTCorev4.0]. Devices such as mobile phones, notebooks, tablets and other handheld computing devices which include BT 4.0 chipsets also have the low-energy functionality of Bluetooth. BT-LE is also included in many different types of accessories that collaborate with mobile devices such as phones, tablets and notebook computers. An example of a use case for a BT-LE accessory is a heart rate monitor that sends data via the mobile phone to a server on the Internet.

2.1. Bluetooth Low Energy stack

The lower layer of the BT-LE stack consists of the Physical (PHY) and the Link Layer (LL). The Physical Layer transmits and receives the actual packets. The Link Layer is responsible for providing medium access, connection establishment, error control and flow control. The upper layer consists of the Logical Link Control and Adaptation Protocol (L2CAP), Generic Attribute protocol (GATT) and Generic Access Profile (GAP) as shown in Figure 1. GATT and BT-LE profiles together enable the creation of applications in a standardized way without using IP. L2CAP provides multiplexing capability by multiplexing the data channels from the above layers. L2CAP also provides fragmentation and reassembly for large data packets.

```
+-----------------------------------------+-------------------+
|              Applications                                   |
+-----------------------------------------+-------------------+
|        Generic Attribute Profile        |  Generic Access   |
+-----------------------------------------+     Profile       |
| Attribute Protocol |Security Manager    |                   |
+--------------------+--------------------+-------------------+
|              Logical Link Control and Adaptation            |
+--------------------+--------------------+-------------------+
|              Host Controller Interface                      |
+--------------------+--------------------+-------------------+
|           Link Layer        |      Direct Test Mode         |
+--------------------+--------------------+-------------------+
|              Physical Layer                                 |
+--------------------+--------------------+-------------------+
```

Figure 1: BT-LE Protocol Stack

2.2. Link layer roles and topology

BT-LE defines two Link Layer roles: the Master Role and the Slave Role. A device in the Master Role, which is called master, can manage multiple simultaneous connections with a number of devices in the Slave Role, called slaves. A slave can only be connected to a single master. Hence, a BT-LE network (i.e. a BT-LE piconet) follows a star topology.

```
                 [BTLE-Slave]-----\                /-----[BTLE-Slave]
                                   \              /
                  [BTLE-Slave]-----/[BTLE-Master]/-----[BTLE-Slave]
                                   /              \
                 [BTLE-Slave]-----/                \-----[BTLE-Slave]
```

Figure 2: BT-LE Star Topology

A master is assumed to be less constrained than a slave. Hence, master and slave can correspond with 6LoWPAN Border Router (6LBR) and host, respectively.

In BT-LE, communication only takes place between a master and a slave. Hence, in a BT-LE network using IP, a radio hop is equivalent to an IP link and vice versa.

2.3. BT-LE device addressing

Every BT-LE device is identified by a unique 48 bit Bluetooth Device Address (BD_ADDR). A Bluetooth Smart device such as a sensor may use a public (obtained from IEEE Registration Authority) or a random device address (generated internally). The public address is created according to the IEEE 802-2001 standard [IEEE802-2001] and using a valid Organizationally Unique Identifier (OUI) obtained from the IEEE Registration Authority. This specification mandates that the Bluetooth Device Address MUST be a public address.

2.4. BT-LE packets sizes and MTU

Maximum size of the payload in the BT-LE data channel PDU is 27 bytes. Depending on the L2CAP mode in use, the amount of data available for transporting IP bytes in the single BT-LE data channel PDU ranges between 19 and 27 octets. For power efficient communication between two BT-LE devices, data and its header should fit in a single BT-LE data channel PDU. MTU larger than 27 bytes can be supported by the L2CAP specification. The Basic L2CAP Mode allows a maximum payload size (i.e. IP datagram size) of 65535 bytes per L2CAP PDU. The rest of the L2CAP modes allow a maximum payload size that ranges between 65527 and 65533 bytes per L2CAP PDU.

The maximum payload size of a BT-LE data channel PDU is 27 bytes, from which L2CAP headers may consume additional bytes. However, data packets may be much larger (e.g. IPv6 requires support for an MTU of 1280 bytes). Fragmentation and Recombination (FAR) functionality is an inherent function of the BT-LE L2CAP layer. Larger L2CAP packets can be transferred with the assistance of the FAR functionality.

Appendix A describes FAR operation and five L2CAP Modes. This specification requires that FAR functionality MUST be provided in the L2CAP layer up to the IPv6 minimum MTU of 1280 bytes. The corresponding L2CAP Mode MUST be Basic Mode. Since FAR in BT-LE is a function of the L2CAP layer, fragmentation functionality as defined in [RFC4944] MUST NOT be used in BT-LE networks.

3. Specification of IPv6 over Bluetooth Low Energy

BT-LE technology sets strict requirements for low power consumption and thus limits the allowed protocol overhead. 6LoWPAN standard [RFC4944], [I-D.ietf-6lowpan-nd] and [RFC6282] provides useful generic functionality like header compression, link-local IPv6 addresses, Neighbor Discovery and stateless IP-address autoconfiguration for reducing the overhead in 802.15.4 networks. This functionality can be partly applied to BT-LE.

A significant difference between IEEE 802.15.4 and BT-LE is that the former supports both star and mesh topology (and requires a routing protocol), whereas BT-LE does not currently support the formation of multihop networks. In consequence, the mesh header defined in [RFC4944] for mesh under routing MUST NOT be used in BT-LE networks. In addition, a BT-LE device MUST NOT play the role of a 6LoWPAN Router (6LR).

3.1. Protocol stack

In order to enable transmission of IPv6 packets over BT-LE, a new fixed L2CAP channel ID MUST be reserved for IPv6 traffic by the BT-SIG. A request for allocation of a new fixed channel ID for IPv6 traffic by the BT-SIG should be submitted through the liaison process or formal communique from the 6lowpan chairs and respective area directors. Until a channel ID is allocated by BT-SIG, the channel ID 0x0007 is recommended for experimentation. Once the channel ID is allocated, the allocated value MUST be used. Figure 3 illustrates IPv6 over BT-LE stack.

```
                  +-------------------+
                  |    UDP/TCP        |
                  +-------------------+
                  |      IPv6         |
                  +-------------------+
                  | 6LoWPAN adapted   |
                  |     to BT-LE      |
                  +-------------------+
                  |  BT-LE L2CAP      |
                  +-------------------+
                  |  BT-LE Link Layer |
                  +-------------------+
                  |  BT-LE Physical   |
                  +-------------------+
```

Figure 3: IPv6 over BT-LE Stack

3.2. Link model

The concept of IP link (layer 3) and the physical link (combination of PHY and MAC) needs to be clear and the relationship has to be well understood in order to specify the addressing scheme for transmitting IPv6 packets over the BT-LE link. [RFC4861] defines a link as "a communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IP."

In the case of BT-LE, L2CAP is an adaptation layer that supports the transmission of IPv6 packets. L2CAP also provides multiplexing capability in addition to FAR functionality. This draft assumes the same common IPv6 header values as those assumed in [RFC 6282]. It is also assumed that the IPv6 payload length can be inferred from the L2CAP header length and also assumes that IPv6 addresses assigned to 6LoWPAN interfaces are formed with an IID derived directly from the 48-bit Bluetooth device addresses, as described in subsection 3.2.1.

The BT-LE link between two communicating nodes can be considered to be a point-to-point or point-to-multipoint link. When one of the communicating nodes is in the role of a master, then the link can be viewed as a point-to-multipoint link.

When a host connects to another BT-LE device the link is up and IP address configuration and transmission can occur.

3.2.1. Stateless address autoconfiguration

A BT-LE 6LN performs stateless address autoconfiguration as per [RFC4862]. The 64 bit Interface Identifier (IID) for a BT-LE

interface is formed from the 48-bit unique public Bluetooth device address [REF Sec 2.3] as per the "IPv6 over Ethernet" specification [RFC2464]. A BT-LE 6LN SHOULD utilize this EUI-64 address for stateless address autoconfiguration. The 48-bit public bluetooth address is globally unique and provided by the IEEE registration authority. Hence the "Universal/Local" (U/L) bit MUST be set to 0.

The IPv6 link-local address [RFC4291] for a BT-LE node is formed by appending the IID, as defined above, to the prefix FE80::/64, as depicted in Figure 4.

The tool for a gateway to obtain an IPv6 prefix for numbering the BT-LE network is out of scope of this document, but can for example be accomplished via DHCPv6 Prefix Delegation. The used IPv6 prefix may change due to the gateway^1s movement.

3.2.2. Neighbor discovery

[I-D.draft-ietf-6lowpan-nd] describes the neighbor discovery approach for 6loWPAN nodes. BT-LE does not support mesh networks and hence only those aspects of the [I-D.draft-ietf-6lowpan-nd] that apply to a star topology are considered.

The following aspects of 6lowpan-nd are applicable to BT-LE 6LNS:

1. A BT-LE 6LN MUST register its address with the router by sending a NS message with the ARO option and process the NA accordingly. The NA with the ARO option SHOULD be sent irrespective of whether the IID is derived from the unique 48 bit BT-LE device address or the IID is a random value that is generated as per the privacy extensions for stateless address autoconfiguration [RFC4941].

2. Sending a Router solicitation (RS) and processing Router advertisements by BT-LE 6LNs MUST follow Sections 5.3 and 5.4 respectvely of [I-D.draft-ietf-6lowpan-nd].

```
  10 bits        54 bits             64 bits
+----------+-----------------+----------------------+
|1111111010|      zeros      | Interface Identifier |
+----------+-----------------+----------------------+
```

Figure 4: IPv6 link-local address in BT-LE

3.2.3. Header compression

This document assumes [RFC6282], which specifies the compression format for IPv6 datagrams on top of IEEE 802.15.4, as the basis for IPv6 header compression on top of BT-LE. It is required that all headers MUST be compressed according to HC base encoding. In BT-LE the star topology structure can be exploited in order to provide a mechanism for IID compression. The following text describes the principles of IPv6 address compression on top of BT-LE.

In a link-local communication, both the IPv6 source and destination addresses MUST be elided, since the device knows that the packet is destined for it even if the packet does not have destination IPv6 address. On the other hand, a node SHALL learn the IID of the other endpoint of each L2CAP connection it participates in. By exploiting this information, a node that receives a data channel PDU containing an IPv6 packet (or a part of it) can infer the corresponding IPv6 source address. The device MUST maintain a Neighbor Cache, in which the entries include both the IID of the neighbor and the Device Address that identifies the neighbor.

When a BT-LE slave transmits an IPv6 packet to a remote destination using global IPv6 addresses, the slave MUST elide the IPv6 source address, if a context is defined for the prefix of the IPv6 source address. In this case, the 6LBR/master can infer the elided IPv6 source address since 1) the master/6LBR has previously assigned the prefix to the slaves; and 2) the master/6LBR maintains a Neighbor Cache that relates the Device Address and the IID of the corresponding slave. If a context is defined for the IPv6 destination address, the slave MUST also elide the prefix of the destination IPv6 address. In that case, the 6LBR/master can infer the elided destination prefix by using the context.

When a master/6LBR receives an IPv6 packet sent by a remote node outside the BT-LE network, and the destination of the packet is a slave, the master/6LBR MUST elide the IPv6 destination address of the packet before forwarding it to the slave. The slave can infer that the IPv6 destination address of the packet is its own IPv6 address. If a context is defined for the prefix of the IPv6 source address, the master/6LBR MUST elide that prefix as well.

3.2.4. Unicast and Multicast address mapping

The BT-LE link layer does not support multicast. Hence traffic is always unicast between two BT-LE devices. Even in the case where a master is attached to multiple slave BT-LE devices, the master device cannot do a multicast to all the connected slave devices. If the master device needs to send a multicast packet to all its slave

devices, it has to replicate the packet and unicast it on each link. However, this may not be energy-efficient and particular care must be taken if the master is battery-powered. In the opposite direction, a slave can only transmit data to a single destination (i.e. the master). Hence, if a slave transmits an IPv6 multicast packet, the slave can unicast the corresponding BT-LE packet to the master. It is required that the master MUST provide a table for mapping different types of multicast addresses (all-nodes, all-routers and solicited-node multicast addresses) to the corresponding IIDs and Device Addresses.

3.3. Internet connectivity scenarios

In a typical scenario, BT-LE network is connected to the Internet.

```
                         h            _____________
                          \          /             \
                     h ---- 6LBR --- |  Internet   |
                          /          \_____________/
                         h
                                            h:      host
                   <-- BT-LE -->            6LBR:   6LoWPAN Border Router
```

Figure 5: BT-LE network connected to the Internet

In some scenarios, the BT-LE network may transiently or permanently be an isolated network.

```
                         h       h           h:     host
                          \     /            6LBR:  6LoWPAN Border Router
                      h --- 6LBR -- h
                          /    \
                         h      h
```

Figure 6: Isolated BT-LE network

Host-to-master and master-to-host communication MUST use the same mechanisms as would be used in global IPv6 communications. The gateway is used to route the packets to one of its slaves.

4. IANA Considerations

While there are no actions for IANA, we do expect BT SIG to allocate

an L2CAP channel ID (see Section 3.1).

5. Security Considerations

The transmission of IPv6 over BT-LE links has similar requirements and concerns for security as for IEEE 802.15.4. IPv6 over BT-LE SHOULD be protected by using BT-LE Link Layer security.

BT-LE Link Layer supports encryption and authentication by using the Counter with CBC-MAC (CCM) mechanism [RFC3610] and a 128-bit AES block cipher. Upper layer security mechanisms may exploit this functionality when it is available. (Note: CCM does not consume bytes from the maximum per-packet L2CAP data size, since the link layer data unit has a specific field for them when they are used.)

Key management in BT-LE is provided by the Security Manager Protocol (SMP).

6. Additional contributors

Kanji Kerai, Jari Mutikainen, David Canfeng-Chen and Minjun Xi from Nokia have contributed significantly to this document.

7. Acknowledgements

Samita Chakrabarti and Erik Nordmark have provided valuable feedback for this draft.

8. Normative References

[BTCorev4.0]
"Bluetooth Core Specification v4.0, http://www.bluetooth.org/Technical/Specifications/adopted.htm".

[I-D.ietf-6lowpan-nd]
Shelby, Z., Chakrabarti, S., and E. Nordmark, "Neighbor Discovery Optimization for Low Power and Lossy Networks (6LoWPAN)", draft-ietf-6lowpan-nd-18 (work in progress), October 2011.

[IEEE802-2001]
"IEEE 802-2001 standard, http://standards.ieee.org/findstds/standard/802-2001.html".

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

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[RFC3610] Whiting, D., Housley, R., and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, September 2003.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC6282] Hui, J. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, September 2011.

Appendix A. Bluetooth Low Energy fragmentation and L2CAP Modes

This section provides an overview of Fragmentation and Recombination (FAR) method and L2CAP modes in Bluetooth Low Energy. FAR is an L2CAP mechanism, in which an L2CAP entity can take the (large) upper layer PDU, prepend the L2CAP header (4 bytes in the Basic L2CAP mode) and break the resulting L2CAP PDU into fragments which can then be directly encapsulated into Data channel PDUs. There are bits in the Data channel PDUs which identify whether the payload is a complete L2CAP PDU or the first of a set of fragments, or one of the rest of the fragments.

There are five L2CAP modes defined in the BT 4.0 spec. These modes are: Retransmission Mode (a Go-Back-N mechanism is used), Enhanced Retransmission Mode (includes selective NAK among others), Flow Control Mode (PDUs are numbered, but there are no retransmissions), Streaming Mode (PDUs are numbered, but there are no ACKs of any kind) and Basic L2CAP Mode.

Authors' Addresses

Johanna Nieminen (editor)
Nokia
Itaemerenkatu 11-13
FI-00180 Helsinki
Finland

Email: johanna.1.nieminen@nokia.com

Basavaraj Patil
Nokia
6021 Connection drive
Irving, TX 75039
USA

Email: basavaraj.patil@nokia.com

Teemu Savolainen
Nokia
Hermiankatu 12 D
FI-33720 Tampere
Finland

Email: teemu.savolainen@nokia.com

Markus Isomaki
Nokia
Keilalahdentie 2-4
FI-02150 Espoo
Finland

Email: markus.isomaki@nokia.com

Zach Shelby
Sensinode
Hallituskatu 13-17D
FI-90100 Oulu
Finland

Email: zach.shelby@sensinode.com

Carles Gomez
Universitat Politecnica de Catalunya/i2CAT
C/Esteve Terradas, 7
Castelldefels 08860
Spain

Email: carlesgo@entel.upc.edu