BLUETOOTH PAN AND EXTERNAL IP NETWORKS

Tore E. Jønvik
Unik – University of Oslo
Snaroyveien 30 –1331 Fornebu
Norway
tlf: +47 90199176
torejoen@ifi.uio.no

Paal Engelstad
Telenor R&D
Snaroyveien 30 – 1331 Fornebu
Norway
tlf: +47 416 33 776
Paal.Engelstad@telenor.com

Do van Thanh
Telenor R&D
Snaroyveien 30 – 1331 Fornebu
Norway
tlf: +47 909 77 10 2
thanh-van.do@telenor.c

Abstract

This paper discusses how ad-hoc Personal Area Network (PAN) based on Bluetooth technology may connect to external networks. We assume that the Bluetooth network (piconet) is formed by the automatic SAPIFO procedure [4], that one or more piconet devices have access to external networks, and that IPv4 is used for external communication.

Bluetooth have specified a PAN profile[2] for IP over Bluetooth, which uses BNEP[3] (Bluetooth Network Encapsulation Protocol) to emulate an Ethernet segments between master and slave. If the master has an additional Ethernet connection to an external network, it uses the NAP (Network Access Point) role to interconnect the Ethernet segments and form a piconet. If the master has no external Ethernet connections, on the other hand, it uses the GN (Group ad-hoc Network) role. The Ethernet segments are connected using functions from 802.1d [10].

This paper proposes definition of a new role, which accommodates more than one network access points by combining NAP and GN.

Keywords: Bluetooth, Ad-hoc Networking, PAN Personal Area Network, BNEP Bluetooth Network Encapsulation Protocol, IP.

Motivation

Bluetooth was initially designed as an efficient cable replacement technology primarily for handheld devices. With the forecasted abundance of Bluetooth-enabled devices, however, it is reasonable to assume that Bluetooth will evolve from being a cable replacement to become a network infrastructure connecting multiple devices together into a piconet. Indeed, all the devices belonging to one person can form a PAN (Personal Area Network) using Bluetooth.

The Bluetooth specification does not determine how a piconet is formed. One way to set up a piconet is to do it manually with the involvement of the users. The piconet is first established with two devices and successively extended with more devices. This procedure is complex, cumbersome, and time consuming. To improve user-friendliness the SAPIFO procedure for automatic piconet formation was proposed in [4].

After the piconet is formed, some devices that have external access to the Internet may provide Internet access to other piconet devices that are not directly connected to an external network.

Bluetooth have specified a PAN profile for IP over Bluetooth, which uses BNEP (Bluetooth Network Encapsulation Protocol) to emulate an Ethernet segments between master and slave. If the master has an additional Ethernet connection to an external network, it uses the NAP (Network Access Point) role to interconnect the Ethernet segments and form a piconet. If the master has no external Ethernet connections,

on the other hand, it uses the GN (Group ad-hoc Network) role. The Ethernet segments are connected using functions from 802.1d.

This paper outlines a new role, which accommodates more than one network access points by combining NAP and GN. The new role also allows a slave to serve as an access point.

Overview over Bluetooth technology

Establishing an L2CAP connection
Bluetooth is a wireless technology communicating in the 2,45 GHz ISM band and is based on a frequency hopping spread spectrum. Bluetooth has a Master/Slave architecture where one master can control up to 7 active slaves. Each Bluetooth transceiver is allocated a unique 48-bit Bluetooth Device Address (BD_ADDR) based on the IEEE 802 Standard.

Two Bluetooth devices that want to communicate with each other must use the same frequency hopping sequence, and the Master's BD_ADDR is one of the parameters used in the generation of the hopping sequence.

The link manager (LMP) is responsible for establishing, supervising and tearing down connections and logical links.

The *Inquiry* procedure is the first step in setting up a connection. Devices in the Inquiry state send short ID packages with a predetermined hopping pattern and with a high repetition rate, once every 312 μs. It is only possible to detect devices in Inquiry Scan State. A device in this state wants to be detected and is set in discoverable mode. The device will hop in the same manner as a device in Inquiry State, but the repetition rate is much slower, once in every 1.28 s. When the device detects an ID packet, it waits a random back-off period (0 – 2047 time slots) before it responds with a FHS package (Frequency Hop Synchronisation). FHS reveals the inquired device's BD_ADDR and clock.

The *Page* procedure is the second step in setting up a connection. At this point, a device has determined to take on the master role and tries to connect to one of the devices (in a slave role). The master transmits the slave's device access code (DAC) in different hop channels and listens in between until it receives response from the slave. The response is the slave's DAC that is based on the slaves LAP. The slave's BD-ADDR determines the hopping sequence. When the master detects the DAC, it sends its own FHS. The slave sends an ACK packet, the master sends a POLL packet, and the slave answers again with a new ACK packet. Finally the master sets up an ACL link, as illustrated in fig 6.

The Link Manager will then establish a L2CAP [1] connection. On this connection the Service Discovery Protocol (SDP) [1] will unveil the devices' capabilities.

BNEP
The Bluetooth Network Encapsulation Protocol, BNEP, emulates an Ethernet on a broadcast network segment, hiding the underlying master-slave based piconet topology. BNEP runs over L2CAP, as illustrated in figure 1.

BNEP reuses the Ethernet packet format commonly used for local area networking technology. The 48 bits Bluetooth addresses are used as IEEE source and destination addresses. The format of the BNEP header is shown in Figure 2. The BNEP header may be extended with one or more extension headers that allows for additional capabilities.

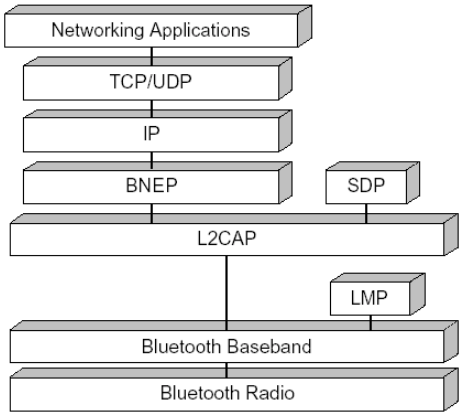

Figure 1. The networking reference stack for the PAN profile, with the Bluetooth radio (as OSI layer 1) Baseband and L2CAP as OSI layer 2) and BNEP (as the network adaptation between Bluetooth layer 2 and the IP

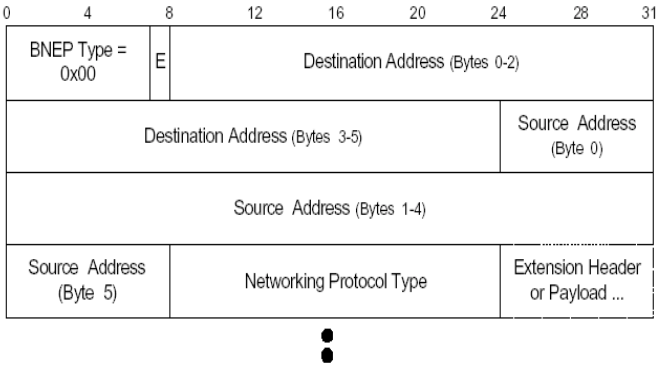

Figure 2. *BNEP with an Ethernet packet payload sent using L2CAP*

BNEP also defines connection control messages. Before completion of the BNEP connection setup, the initiator has to indicate the roles of both end-points. For bandwidth saving purposes, protocol and multicast filter commands have been defined to indicate which protocol types and multicast addresses a device wants to receive. All these control messages have to be confirmed before the new configuration applies.

BNEP accommodates IP communication by transporting IP packets between two Ethernet-based link-layer end-points on an IP segment. It encapsulates the IP packets in BNEP headers, letting the source and destination addresses reflect the Bluetooth end-points and setting the 6-bit Networking Protocol Type field to code for an IP packet in the payload. BNEP finally encapsulates the BNEP packet in an L2CAP header and sends it over the L2CAP connection.

PAN profile

The PAN Profile identifies two configurations of a Bluetooth PAN: The Network Access Point (NAP) configuration is used when the master is connected to an external network, and the Group Ad-hoc Node (GN) configuration is used when no devices have a network connection. In both cases, the Bluetooth device that uses the NAP service or GN service is a PAN User (PANU).

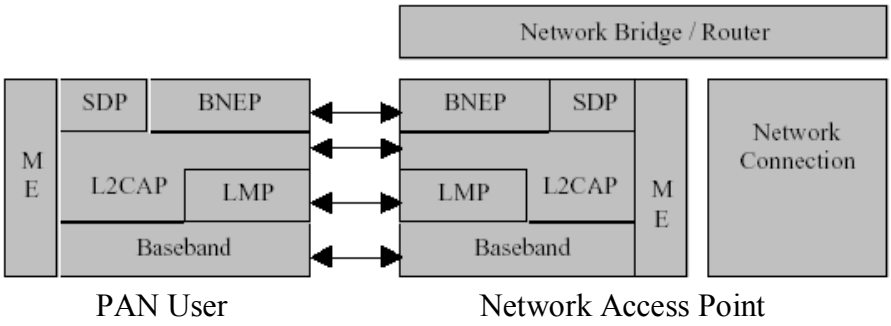

Figure 3. *The NAP configuration of the Bluetooth PAN profile.*

A Bluetooth master that supports the NAP service provides some of the features of an Ethernet bridge to support network services. It forwards BNEP packets between each of the connected Bluetooth devices (PANUs), including the Ethernet of an external network on an additional network connection. Ethernet

packets are either exchanged via Layer 2 bridging or via Layer 3 routing. These devices may require additional functionality when bridging to other networks technologies, such as GPRS. The NAP configuration is illustrated in figure 3.

A Bluetooth master that supports the GN service is able to forward Ethernet packets to each of the connected PANUs, but it does not provide access to any additional networks. GNs are intended to allow a group of devices to exchange information by forming a temporary networks. The NAP configuration is illustrated in figure 4.

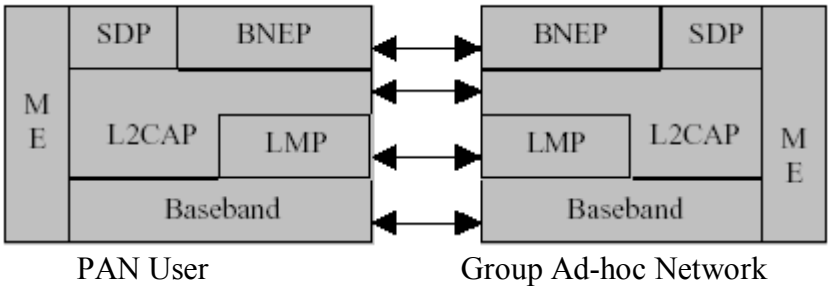

Figure 4. *The GN configuration of the Bluetooth PAN profile.*

A PANU is the Bluetooth device that uses either the NAP or the GN service. PANU supports the client role for both the NAP and GN roles. The PANU has a BNEP connection with the NAP or GN. A PANU must become a piconet slave if the NAP or GN is configured in multi-user mode.
The NAP and GN forward BNEP packets between PANUs according to the BNEP protocol, which implements parts of the IEEE 802.1D standard.

Piconet formation

Bluetooth Special Interest Group (SIG) does not indicate how to do piconet formation, and no procedure for automatic piconet formation is specified. SAPIFO [4], however, represent a suggested procedure for automatic piconet formation. This procedure is based on the assumptions of the existence of at least one possible piconet among the available Bluetooth enabled devices that
will participate in the PAN.

All devices will start a procedure to detect Bluetooth enabled devices within radio range and their Bluetooth address (BD-ADDR). SAPIFO presupposes the use of a Dedicated Access Code (DIAC) in the Inquiry phase that is reserved for certain computing class of devices. It is therefore not necessary to set up a L2CAP connection and use the SDP protocol to search for devices with computing capabilities.

When all devices have detected all other devices within radio range, they will inform their neighbours about the detected devices. After this is finished, all devices will have a table of all devices and their possible connections in the future piconet. This table will be basis for the distributed procedure to select possible Master candidates for the piconet. All devices with the highest number of detected devices will be candidates. If more than one is device is candidate, the one with highest BD-ADDR will be selected master.

The selected master will now page the other devices and form the piconet. If there is more than one master candidate, the others can be used as backup master(s). SAPIFO also contains procedures for piconet maintenance taking care for devices entering or leaving. A consequence of the maintenance procedure is that a new master can be selected.

Using IP for Internet access

The new role presented in this paper and illustrated in Fig 5 assumes a mobile piconet that is able to connect to different access technologies including WLAN, GSM GPRS or GSM HSCD. IP is a technology that allows such inter-technology communication, and the ubiquitous IPv4 protocol is therefore assumed [5].

Since the network may be mobile, access points may gain and lose Internet connectivity in a non-deterministic manner as the Bluetooth network moves, and the network must reconfigure itself automatically to changing Internet connectivity conditions. Due to the dynamic nature of our scenario, one or more access points may pop up on slaves as well as on the piconet master, which is the situation that the new role must cope with (Fig. 5). In comparison, access points on slaves cannot be fully utilized as a resource if the existing Bluetooth NAP profile is being uses. NAP only allow the master to connect to one external Ethernet-like network by means of BNEP-based bridging.

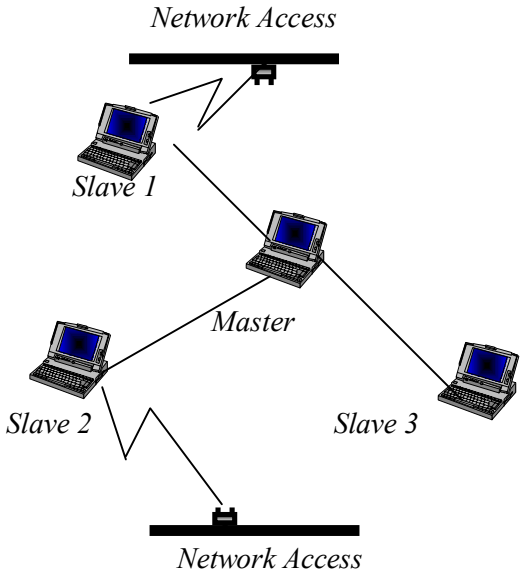

Fig 5 *The new role proposed in this paper allows one or more slaves to serve as access points to external networks*

The most limiting factor for IPv4 is the scarcity of IP addresses. ISPs are often reluctant to allocate global IP addresses to roaming nodes, which often have limited access privileges. This means that an access point is likely to receive one external IP-address at most - probably a private IP-address (i.e. the ISP is implementing a NAT solution) or a global IP address at best.

The way an access point acquires the external IP-address - assuming automatic address allocation - is dependent on the link-layer technology used for the external access. If the external network is Ethernet based [11], it will likely use DHCP [9], or it may receive the address from a Mobile IP foreign agent through an ICMP Router Advertisement [10]. On PPP-enabled links, however, the access point will likely be authorized an IP-address after successful PPP authentication [14]. On 2G and 3G cellular networks, other techniques may apply.
Different nodes in the Bluetooth piconet must share the external IP-address that the access point acquires. The easiest way to accommodate this is to allocate private IP addresses [7] or IPv4 link-local addresses [8] to hosts and routers on the piconet, and use Network Address and Port Translation (NAPT) for Internet Access [13]. A NAPT is a router that replaces a private or link-local IP source address and port number for outgoing IP packets with a global IP address and a unique port number before forwarding them towards the Internet. It performs the reverse translation with the destination addresses of incoming packets before forwarding them into the internal network.

Proposed IP solution

The new role proposed in this paper attempts to locate all essential state information centrally on the master. The piconet is then more easily maintained, and there is far less fate sharing, i.e. the piconet does not depend on a slave being present in addition to the master. The back-up masters assigned during the SAPIFO procedure may also easily replicate the state information directly from the master, and services take over network based on existing state information without disruption.

As a result of this design choice, the new role mandates that:

- The master serves as a network router, which intercepts and forwards IP packets, and maintains IP state information about the slaves on the piconet. Slaves, on the other hand, can be IP hosts.
- A slave acquires a private or link-local IP address for its own from the master. Thus, the master implements DHCP-server for allocation of private IP addresses, and answer DHCP request from slaves [8].
- The master serves as the default gateway of hosts on the piconet.
- Since the master has full control with all local IP-addresses, it answers ARP requests directly without broadcasting the request to other slaves. The master also answers requests from slaves trying to claim a link-local IP address [8], and ensures that all link-local addresses are unique.

One problem with using NAPTs and multiple access points is that all outgoing packet of a stateful session (e.g. a TCP session) must pass through the same address translator where the state information about the address translation is stored. Otherwise, the IP-packet will be assigned a new global source IP-address and the session will break. Furthermore, since Internet Service Providers (ISPs) are probable to implement ingress filtering, the packet should be sent over the access point corresponding to the IP-address that the private IP-address is translated into.

The new role therefore mandates that the master assigns an access point to each communicating host, and that this information is stored on the master. When the master-router receives an IP-packet bound for an external network, it checks the table to find which access point to forward the packet to. If the master has a connection to an external network, it may naturally serve as an access point for some of the slaves.

Some access points may implement a NATP-router. It these cases, the master forwards packets unaltered to the access point, which in turn translates the packet. A host residing on the access point itself uses the private IP-address as source address, and outgoing packets destined for the Internet may be sent directly from the access point, without being sent via the master. The packets must however be passed through the NAPT module to ensure correct and consistent address and port translation of all hosts residing on the piconet.

However, it is anticipated that some access points may not be able to implement NAPT or serve as a router. In these cases the master should do the translation on behalf of the access points. All incoming packets carrying an IP payload from the external network, is sent directly to the master by copying the IP-payload into a BNEP packet. All outgoing IP-packets are sent from the master, and the access point uses copies the payloads from a BNEP packet into a header corresponding to access technology for external access.

The master needs a method to acquire the external IP address from the access point, while the access point acquires a private IP address from the master as described above. In this mode of operation, the access point must send all packets originated from itself to the master, using its private address as a source address.

Packets destined for the access point is only accepted from the master, and the IP-header must carry its private IP-address as a destination address. The access point needs a method to distinguish IP-packets that are to be blindly forwarded to the access network from those destined for the access point itself. We propose to introduce a BNEP extension header type for this purpose: All packets carrying the specific extension header type will be blindly forwarded to the external network. Some additional filtering rules may be specified to optimize the solution.

Proposed Bluetooth solution

It should be clear that the proposed IP solution requires support from the underlying Bluetooth technology. We propose that the piconet is formed automatically using the SAPIFO procedure. The procedure allows a master to be elected, while other candidate masters serve as back-up masters of the piconet. It also mandates how the piconet is set up.

After the L2CAP connections have been established, the master uses SDP to check the capabilities of different slaves, and determines which slaves are willing to and capable of servicing as access point. A service class for Internet Access Points with a predefined UUID[1] should be defined for this purpose.

The master reads the mode of operation and status of the access point from appropriately defined SDP attributes. It finds whether the access point is capable of dynamically allocating of external IP-addresses and port-numbers to Bluetooth hosts (i.e. by implementing NAPT on the access point) , or if this functionality shall be managed by the master. This mandates the behavior of the access point and how the master forward packets over the access point, as outline above.

If the master is to allocate external IP-addresses (e.g. by performing NATP-translation) on behalf the access point, it may find the external IP address or prefix of the access point through an SDP attribute. It should be noted that the number external IP-address managed by the master may exceed the number of Bluetooth hosts requiring Internet access, especially if some access points have acquired an IP-prefix from the external network. In this case, the master may not need to do port translation. Each Bluetooth host may even be assigned an external IP-address directly through DHCP, instead of using private address, and not even address translation will be required.

Another SDP attribute that gives the status of the external access should also be defined. Hence, the master may use SDP periodically to check if an access point have gained or lost Internet access over the external network, or if the external IP-address or prefix of the access point has changed.

Back-up masters should be ready to take over the network if the master goes down. A potential back-up master should therefore periodically download the state information cached at the master. SNMP [12] is an example of an IP-based protocol that may be used for this purpose. However, a Bluetooth specific solution is preferable, since the back-up mechanism should not mandate that the Bluetooth nodes run IP - some devices may not even be configured with an IP stack.

The already existing Bluetooth protocol, SDP, might be used for replicating state information. Backup-masters would poll the SDP-server on the master periodically and download (i.e. pull) status information from the master. Alternatively, new Bluetooth protocol functions may be defined for this purpose. The master may for example use some new LMP commands to upload (i.e. push) state information onto the backup-masters. Another approach would be to introduce an entirely new protocol over L2CAP with a new reserved Protocol Service Multiplexor (PSM).

The proposed solution will be detailed in a subsequent paper.

Conclusion

This paper proposed a new Bluetooth role, which allows ad-hoc Personal Area Network (PAN) based on Bluetooth technology to connect to external networks. Unlike for the NAP and GN roles, a slave may provide access to the Internet and multiple Internet access points may be used simultaneously. The proposal assumes that the Bluetooth network (piconet) is formed by the automatic SAPIFO procedure [4], and that IPv4 is used for external communication.

The new role will be detailed in a subsequent paper.

References

[1] Specification of the Bluetooth System http://www.bluetooth.com/dev/specifications.asp

[2] Personal Area Networking Profile http://www.bluetooth.com/pdf/PAN_Profile_0_95a.pdf

[3] Bluetooth Network Encapsulation Protocol (BNEP) Specification
http://www.bluetooth.com/pdf/Bluetooth_11_Specifications_Book.pdf

[4] Tore Jønvik, and Do Van Thanh "Ad-hoc formation of Bluetooth Piconet for data communication"
3Gwireless and Beyond. San Francisco May 2002

[5] Internet Protocol http://www.ietf.org/rfc/rfc791.txt

[6] IP Mobility Support for IPv4 http://www.ietf.org/rfc/rfc3220.txt

[7] Address Allocation for Private Internets http://www.ietf.org/rfc/rfc1918.txt

[8] Dynamic Configuration of IPv4 Link-Local Addresses http://files.zeroconf.org/draft-ietf-zeroconf-ipv4-linklocal.txt

[9] Dynamic Host Configuration Protocol http://www.ietf.org/rfc/rfc2131.txt

[10] 802.1d http://www.ieee802.org/1/pages/802.1D.html

[11] Ethernet http://standards.ieee.org/getieee802/

[12] A Simple Network Management Protocol (SNMP) http://www.ietf.org/rfc/rfc1157.txt

[13] Traditional IP Network Address Translator (Traditional NAT) http://www.ietf.org/rfc/rfc3022.txt

[14] The Point-to-Point Protocol (PPP) http://www.ietf.org/rfc/rfc1661.html