Bluetooth Hotspots: Extending the reach of Bluetooth by transparently tunneling communications over IP Networks

David Mackie and Peter Clayton

Abstract—This paper presents ideas on how to extend the availability of Bluetooth by introducing the concept of Bluetooth hotspots. Currently two Bluetooth devices cannot communicate with each other unless they are within range, since Bluetooth was designed as a cable-replacement technology for wireless communication over short ranges. An investigation is being done into the feasibility of creating Bluetooth hotspots that allow distant devices to communicate with each other by tunneling their communication between hotspots via an alternative network infrastructure such as Internet Protocol (IP). Two methods are under investigation; creating a distributed service discovery database to offer alternative means for devices to locate and use each other’s services, and the spoofing of distant devices by the local hotspot to allow seamless communication.

Index Terms—Bluetooth, Piconets, Tunneling, Hotspots, Service Discovery

I. BLUETOOTH

Bluetooth [1] is a specification for a low-cost, low-power, short-range wireless communication technology that provides connectivity between mobile devices such as cell phones, personal digital assistants (PDA), and portable computers. Its main use is as a cable replacement technology for point-to-point situations, but is also used to form ad-hoc networks in a master-slave formation called piconets, allowing users to create Personal Area Networks (PAN) between devices. The specification is controlled by the Bluetooth Special Interest Group (SIG) [3], which is a trade association of over 2000 different companies comprising the leaders in the telecommunication, networking, and information technology industries, (headed by 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia, and Toshiba), who are driving the development of Bluetooth.

II. BLUETOOTH NETWORKS

The basic structure of a Bluetooth network is a master-slave relationship where a maximum of seven slave devices can connect to a single master forming a piconet. Fig. 1(a) shows a piconet with one master and one slave and Fig. 1(b) shows a network with multiple slaves. Devices can be in more than one piconet at a time, thus forming a scatternet as shown in Figure 1c, though the specification does not specify how this can be done. These networks are very temporal and are formed in an ad-hoc manner, with the device that initiates the communication becoming the master.

Bluetooth operates in the license-free 2.4GHz ISM radio-frequency band with a range of ~10 meters. This can be extended to 100 meters with improved transmission power and receiving sensitivity, but at the cost of power consumption and cost. Only device that are within range of the master are able to form part of a piconet.

III. BLUETOOTH HOTSPOTS

What we are attempting to accomplish is to allow devices that are not within range to be able to communicate with each other via an alternative means, which must act seamlessly and transparently to the devices as far as is possible. We envision setting up Bluetooth “Hotspots” that will allow devices in different hotspots to communicate with each other by tunneling the communication over an IP network joining the hotspots, thus allowing for the extension of an individual’s Personal Area Network. This is demonstrated in Fig. 2. Device B and Device C are at one location and Device A is at another, distant enough so that Device A is out of the conventional Bluetooth range of the other two devices. There are Repeater devices (X and Y) at both locations connected together by an IP network backbone. Two methods are being investigated to allow Device A to talk to Device B; using Bluetooth’s Service Discovery Protocol (SDP) to advertise and set up connections between devices and hopefully ultimately, spoofing the devices themselves by the hotspots.

A. Using Service Discovery Protocol

The Bluetooth specification defines the Bluetooth Service Discovery Application Profile (SDAP) and its associated Service Discovery Protocol (SDP) [4] as a core component of every Bluetooth device [1]. This is used by individual devices to discover what services are available from other devices, and what functionality these services offer. The protocol is used in two different ways, one where a known device is queried and requests are made to find what
specific services it offers and the other is where all local devices are searched for a particular service or service with a particular property.

An investigation is being undertaken into the possibility of leveraging SDAP to provide facilities to discover distant devices and facilitate the setting up of communication channels. The scenario as shown in Fig. 2 is that when a user (Device A) is within the range of a hotspot (Repeater X) he will be able to query that hotspot for all the services that it offers. The hotspot will then return a list (“Services Available”) of what other devices (Device B & C) are within range of the other distant hotspots (Repeater Y) and what services (“Sync”) it can offer to allow for communication with a distant device. If the user for example chooses to “Sync with Device C” a communication channel would then be set up between Device A and Device C by the hotspots that will transparently tunnel the communication via the IP network. Applications on the end devices will then seamlessly communicate with one another, unaware that the devices are not within the standard Bluetooth range. Given that these two piconets can be considered to be a scatternet, with the repeaters and IP network being the common slave device (Fig 1(c)) investigations into service discovery in scatternet such as [5,6] are being considered.

B. Using Spoofing

The ultimate goal of the project is to enable the hotspots to advertise or spoof themselves as other devices. A study into the possibility of spoofing a Bluetooth’s MAC (Medium Access Control) layer address will be done. This would allow a local hotspot to masquerade as non-local devices. This would allow for easy access and use of the hotspots, as once a pairing of devices is done, they will communicate seamlessly whether within range or via the hotspots without user intervention.

IV. GOALS OF THIS RESEARCH

A. Device Discovery

The initial focus of this research is on device discovery and a means to allow distant Bluetooth devices to interact and join up into piconets, as if they are within range. It is intended that this be done with no modification to the devices, and we are investigating to what extent can this be achieved.

B. Tunneling

The feasibility of tunneling of Bluetooth network data across an IP-based network by attempting to encapsulate the Bluetooth packets such as using Generic Routing Encapsulation (GRE) [7] is being investigated. The tunneling is to be completely transparent to the devices, and issues of latency in the tunnel and how repeater devices can listen on multiple piconets will need to be investigated.

C. Security

Several security aspects are being investigated. Of particular interest is how the security ideology of Bluetooth is affected by breaking the general assumption that Bluetooth devices only communicate within their close vicinity. Issues such as authentication and authorization for access to hotspots will also need to be looked at, and how these can be seamlessly handled, once again without modifying the devices.

D. Hand-Over

Another interesting question is whether there can be hand-over from the logical piconet, the connection being tunneled over IP, and its “physical” piconet. Could multiple repeater devices be spread throughout a building, allowing for an almost continuous coverage of the virtual piconet? Furthermore, how can this traffic be managed so as not to flood everywhere location where there is a repeater device with all repeater device traffic?

REFERENCES