Bluetooth Location Networks

F. J. González-Castaño, J. García-Reinoso
Departamento de Ingeniería Telemática, Universidad de Vigo,
ETSI Telecomunicación, Campus, 36200 Vigo, Spain, {javier,reinoso}@det.uvigo.es

***Abstract*—In this paper, we propose a Bluetooth Location Network (BLN) for location-aware or context-driven mobile networks, such as m-commerce networks or e-museums. We assume that, in any of those scenarios, there exist *service servers* that need to know user location in real-time, to send context-oriented information to user handhelds when necessary. The BLN transmits position information to the service servers, without user participation. It is not subject to line-of-sight constraints and is supported by existing commercial handhelds. BLN users carry either a Bluetooth-enabled handheld or any mobile data terminal and a Bluetooth *badge*. The BLN is composed by small, wireless Bluetooth nodes, which establish an spontaneous network topology at system initialization. The BLN can coexist with Bluetooth devices that are not part of the location system, such as printers or headphones.**

I. Introduction

A. Motivation

In this paper, we propose a Bluetooth Location Network (BLN) for location-aware or context-driven mobile networks.

For instance, m-commerce (mobile e-commerce) for cell phones or PDAs [1], [2] has a promising future. In a typical m-commerce scenario, customers walk around a large commercial area or mall carrying wireless PDAs. A PDA client allows its user not only to purchase items, make reservations or request information, but also to receive (possibly context-driven) store coupons, advertisements, advice and guidance.

Another interesting application field is electronic guidance. Exhibition visitors receive specific information associated to their current location. See [3] for a review of current initiatives.

In any of those scenarios, there exist service servers that need to know user location in real-time, and send context-oriented information to user handhelds when necessary.

The BLN transmits position information to the service servers, without user participation. It is not subject to line-of-sight constraints and its base technology is supported by existing commercial handhelds. As a fully operational data network, the BLN admits alternative uses as a security network when the target area is closed to the public, or as a spare network for emergencies.

BLN users carry either a Bluetooth-enabled handheld or any mobile data terminal and a Bluetooth badge (thus, the BLN may provide location services to *any* mobile data terminal). The BLN is composed by small, wireless Bluetooth nodes, which establish an spontaneous network topology at system initialization. The BLN can coexist with Bluetooth devices that are not part of the location system, such as printers or headphones. We analyze BLN performance with IBM's BlueHoc simulator.

B. Background

Many user-positioning solutions have been proposed in previous research, but they are based on specialized devices that are not supported by commercially available data terminals [4], [5], [6], [7]. If we review positioning systems supported by commercial terminals, we find the following:

- Cell phone location services [8] and GPS are quite effective for outdoor applications (specially GPS), and possibly the best choice. However, they are useless indoors.
- HP's Cooltown [9] is based on IR *beacons*, which push position-dependent URLs into handheld IR ports (included in most state-of-the-art PDAs and WAP phones). Cooltown is user-dependent, because the user must aim the infrared port to location beacons. It could be argued that this is not a drawback, since automatic detection of location information (without user participation) may have severe consequences in terms of nuisance value. For example, when users are annoyed because the Web page they are viewing is suddenly supplanted by one advertising frozen peas from a grocery store nearby. Cooltown is one of the key technologies in the Electronic Guidebook Research Project [3]. Other examples of IR-based systems are described in [10], [11].

User-independence is only a disadvantage in *aggressive* systems, which is not a desirable scenario. Consider, for example, a museum, where updates could only take place when users enter new halls, and imagine that the update shows the previous page with a tiny flashing icon at its bottom meaning "do you want to update context information?" Also, asking the user to locate IR beacons each time he enters a room full of visual distractions may be tiring, and signaling beacons with large red arrows unsightly.

We can conclude that, depending on the specific application, user-dependent line-of-sight IR systems may be more advantageous than user-independent RF ones or vice versa. *In fact, they are complementary.* For example, in a museum, an iPAQ H3870 could use Cooltown to retrieve information on a single object (e.g. "Celtic *fibula*"), and Bluetooth-assisted context awareness to retrieve information on the surrounding hall (e.g. "Iron Age").

C. Bluetooth location networks

In this paper, we define a Bluetooth Location Network (BLN) that fulfills the requirements in section I-A. We assume that the users carry a Bluetooth-enabled terminal, or any mobile data terminal and an independent Bluetooth location badge. The users must access the Web/WAP service servers from their handhelds, and enter their badge address. By doing so, the

0-7803-7632-3/02/$17.00 ©2002 IEEE

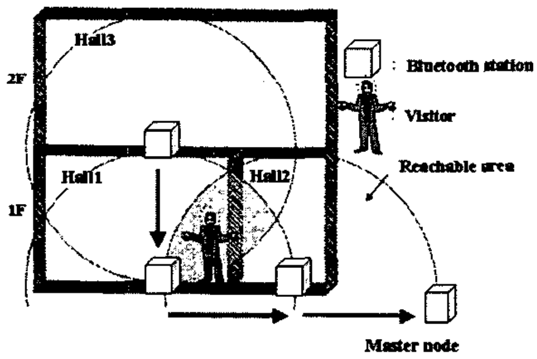

Fig. 1. Cooperative Bluetooth location

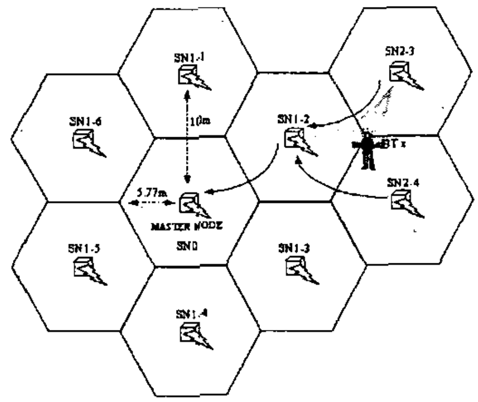

Fig. 2. Bluetooth Location Network

Bluetooth address of the badge becomes *valid* from the BLN's point of view (obviously, the location network must work even if invalid addresses are present, as we will see later). The service server associates the user' IP address or WAP session to his badge number, for all subsequent transactions. The badge (or the Bluetooth modem in the user's terminal) interacts with the BLN, which provides service servers with real-time user position. The service servers may use this information to push URLs into user terminals via TCP/IP sockets, or to update WAP cards. Thus, no client action is required to generate context-driven updates.

Bluetooth was also selected as the base technology for the information offering system in [12]. Although the authors claimed some of the advantages we enumerate in section I-A, they also stated that Bluetooth range does not provide enough location precision. Consider the example in figure 1. In principle, if the three Bluetooth stations detect the user modem, the user could be located in any hall if considering full range (even outside halls 1, 2 and 3). The key point in our philosophy is establishing a *cooperative location network*. The network transmits user modem addresses and the addresses of the Bluetooth stations that detect those modems to a *master node*. In the example in figure 1, the master node would determine that the user is located inside the grey region. Note that most of that region intersects the hall were the user is actually located. This is interesting, because this particular arrangement could not be solved by the non-cooperative system in [12]. The cooperative BLN in this paper is intended to cover 2D target areas, although it can be generalized to cover 3D ones, as we will comment later.

The rest of this paper is organized as follows: the next section describes BLN protocols. Section III analyzes BLN performance. Finally, section IV concludes.

II. BLN PROTOCOLS

A. BLN configuration

The BLN is composed by mobile badges and static Bluetooth units (located at the ceiling, for example). We will refer to the latter as *static nodes*. Static nodes (SNs) are arranged in a network that covers the whole target area. Hexagonal tiling is a typical solution in 2D cellular network planning, which we have followed in this research (figure 2). Other arrangements where any SN has at most seven closest neighbors located within its range could be used as well (approximately 10 m for class 2 Bluetooth modems). For example, meshes or k-ary 3-cubes [15] for 2D or 3D target areas, respectively.

Each cell in the ideal case in figure 2 has an area of 86.55 m^2. SN units scan their surroundings periodically, by means of Bluetooth inquiry calls [13]. All SNs are organized in a radial scatternet around a master node, SN0, connected to the service servers (not shown). The remaining SNs are arranged in "circular" layers around SN0. The notation SNX-Y is used to support the explanation and stands for the Bluetooth address of SN Y in layer X. In any layer, SNX-1 is placed right above SN0, and the remaining Y values are increased clockwise. Our example shows the six cells in the first layer, SN1-1 to SN1-6, and two cells in the second layer, SN2-3 and SN2-4. Each SN is a slave of all six surrounding neighbor SNs.

All SNs perform inquiry cycles periodically, to publish their existence. If SN a detects an inquiry from SN b, and b is not currently listed in a's routing table, a must send its *minimum distance to the master node* in number of hops to b (in a *distance packet* with a 8-bit *control field* and a 8-bit *distance field*, which fits in a DM-1 packet [13]). All SN minimum distances are set to ∞ at power up, excepting the master node's, which is set to 0. Thus, the master node initiates the configuration by sending 0-hop distance packets to its neighbors, on demand. Later, if a SN performing an inquiry cycle does not receive an answer from one of its neighbors that was previously listed in the routing table, it deletes the corresponding entry. If this changes its minimum distance to the master node, the SN transmits a new minimum distance packet to all its slaves.

Whenever a SN receives a distance packet, it searches its routing table to check if the corresponding distance is lower than its current lowest distance to the master node. If so, the SN builds a new distance packet and transmits it to all its slave SNs, excepting those included in minimum-distance routes to the master node. This algorithm is similar to the *split horizon* algorithm [16].

Therefore, the configuration process also restarts in case of SN failures, and propagates changes from the failure neighborhood (possibly only affecting a BLN region).

If a SN receives a distance packet, it must update its routing

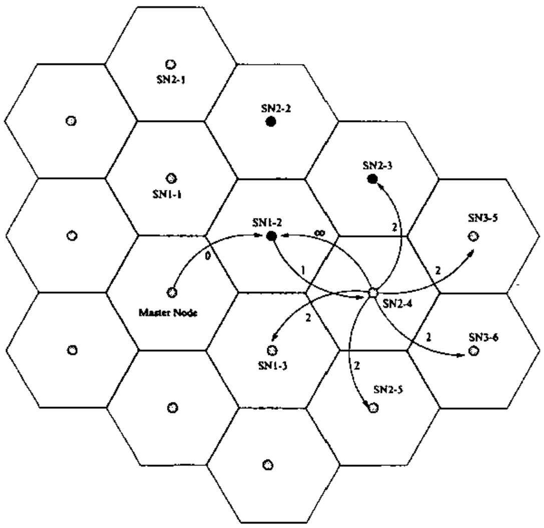

Fig. 3. BLN configuration

table. The routing table stores pairs of neighbor SN addresses and their distances to the master node, and is sorted by distance. The best path is the first entry.

Figure 3 depicts a BLN region. We describe two configuration steps to illustrate the general procedure.

1) Once the master node initiates the process, the distance from SN1-2 to the master node changes. Node SN1-2 transmits the new minimum distance (1) to all its slaves, on demand.
2) SN2-4 receives the distance packet from SN1-2. Since this distance plus 1 is lower than the current local minimum distance (∞), SN2-4 increments the received distance by 1, and updates its routing table.

As we said previously, if a SN detects that the minimum distance to the master node has changed, it builds a new distance packet with this minimum distance, and transmits it to its slaves (neighbors) except to those who are in the minimum distance path (for SN2-4, in our example, SN1-2). Those SNs receive an *infinite* distance packet, to prevent loops.

Remark 1: If a SN has less than seven neighbors within its range, it is possible to implement permanent links with them (the seven-slave transmission constraint holds). This is valid for hexagonal-tiling, mesh and k-ary 3-cube BLNs.

Remark 2: A simple authentication handshake avoids connection establishment with invalid Bluetooth modems, which are considered invalid badges for simplicity. Typically, invalid badges will answer inquiry cycles with FHS packets, which is relatively harmless (see section II-B). However, in case they answered with another kind of packet, they would be easily detected by the authentication handshake and rejected.

Remark 3: Badges do not try to establish data connections with SNs. They simply answer inquiries with FHS packets, which does not violate the seven-slave constraint.

B. BLN location protocol

The main goal of the BLN is user tracking. To meet it, all SNs have to send inquiries and collect badge responses. Every

	Before inq.		After inq.	
Bluetooth addr.	Detected	New	Detected	New
BD-3	NO	NO	YES	NO
BD-7	NO	NO	NO	NO
BD-11	NO	NO	NO	NO
BD-13	NO	NO	YES	NO
BD-17	NO	NO	YES	NO
BD-19			YES	YES

TABLE I
SN CACHE EVOLUTION

SN has a cache where it stores badge addresses. When it detects a response from a badge whose address was not in the cache, it builds a *location packet* (which fits in a DM-1 packet) with its own address, the badge address (64+64 bits) and a 8-bit control field, and transmits it to the SN on top of its routing table.

For example, table I (second and third columns) shows the current SN cache state (BD-X identifies the badge with address X) when the SN is performing an inquiry cycle. Before the cycle starts, the *detected* and *new* columns are unmarked (NO).

When a badge detects an inquiry, it answers with a FHS packet. The SN extracts the badge address from the FHS packet and checks it in the cache. If the address is already listed, the corresponding *detected* column is marked (set to YES). Otherwise, a new row with the address is added and both the *detected* and *new* columns are marked with YES. When the inquiry cycle ends, (i) all marked (YES) *new* columns are switched to unmarked (NO) state, and location packets for the corresponding entries are transmitted to the master node to report that new badges have entered SN range. (ii) All entries with unmarked (NO) *detected* column are deleted, and a location packet for each one of them is transmitted to the master node to report that the corresponding badges are now out of SN range.

Location packets carry two Bluetooth addresses: SN address and badge address. The packets have a bit to report if the badge arrives to or leaves the cell.

It should be understood that the SN that detects a badge is in charge of building location packets. All SNs placed along the transmission path to the master node simply forward them to the SN on top of their routing tables.

Table I, in its fourth and fifth columns, represents a possible SN cache state after the inquiry cycle. A new badge, BD-19, has been detected. Consequently, a location packet with BD-19 payload will be sent to the master node, and its *new* column will be changed to NO. Two badges, BD-7 and BD-11, have left the cell, and the corresponding location packets will be sent to the master node with the *detected* bit set to 0. Their entries will be removed. Badges BD-3, BD-13 and BD-17 are still around, but do not trigger location packet transmission.

Remark 4: SN responses to SN inquiry cycles are ignored by the location protocol, because the corresponding SNs are either listed in the routing table of the requesting SN or will be listed after establishing a master-slave link (this may happen, for example, when a dead SN is replaced).

Remark 5: Obviously, invalid badges will answer to SN inquiries, and generate location packets. However, those packets will be filtered by the master node. As we will see later, even if a large target area is crowded, the BLN can carry a large number of location packets, valid or invalid. Moreover, note that, if invalid badges correspond to static devices (e.g. printers), they will generate only *one* location packet, because their *new* column in SN location caches will be unmarked afterwards.

C. Location zones

The master node (or a service server attached to it) estimates that badge x is placed in a *location zone* that depends on the SNs that send location packets containing address x. Room-scale precision may be enough for many context-driven services in the scenarios in section I, while keeping SN complexity reasonably low. So far, we do not take signal strength nor signal delay into consideration.

Location precision depends on the number of SNs that detect a given badge, and on the range of their modems. We define different location zone *classes*, for a given network topology. A badge is said to be located in a class I zone of a hexagonal tiling topology if *only* three SNs detect the badge. For example, the class I zone depicted in figure 4 is defined by SN2-2, SN2-3 and SN3-3 detection. Note that neither SN1-2, SN3-2 nor SN3-4 detect the badges in that zone. A class I zone has an area of 16.12 m^2. A badge is said to be located in a class II zone if *only* four SNs detect it. For example, SN2-2, SN2-3, SN3-2 and SN3-3 define the class II zone in figure 4. Class II zones have an area of 18.12 m^2.

Class III zones are special cases in the neighborhood of SN failures (or at the edges of the target area). The class III zone in figure 4 has an area of 34.24 m^2. In absence of SN failures, those zones can be avoided by placing extra SNs at the walls of the target area.

Finally, a class IV zone is a single SN. When a badge is placed exactly at a SN position, it is detected by seven SNs (the closest SN and all its slaves).

D. Scalability

As the BLN grows, the number of packet transmissions per master node may become too large. It is possible to avoid this potential problem by installing additional master nodes. Due to BLN symmetry, when the configuration protocol converges to an equilibrium point, the maximum distances to the different master nodes are similar, if equally spaced. Figure 5 shows an example for four master nodes.

Note that the maximum distance route to any master node has three hops. However, even for the same network, location routes may change at the next initialization. In order to evaluate BLN symmetry, we performed simulations of several three-layer ($\sim$ 3,900 m^2) BLN initializations. We observed that, spontaneously, the area managed by each master node was inversely proportional to the number of master nodes. For a given network, the maximum distances to the different master nodes were similar.

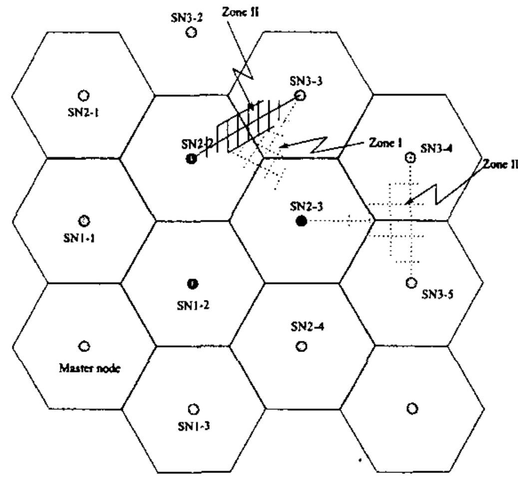

Fig. 4. Location zones

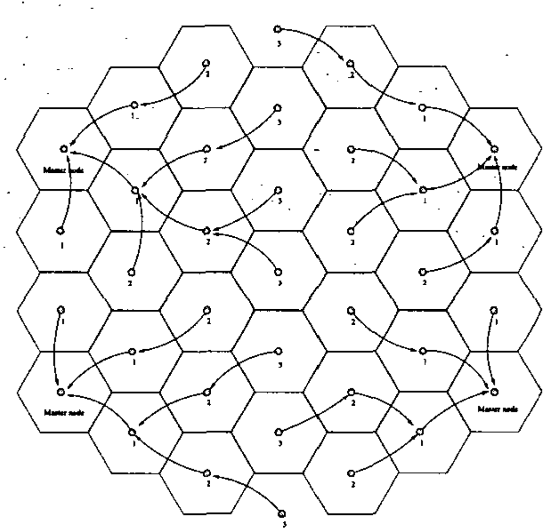

Fig. 5. Location packet routes (sample), four master nodes

III. Performance Evaluation

In this section, we analyze BLN protocol timings. The inquiry cycle scans all frequencies, and it is recommended that it should last for 10.24 s at most ([13], pag. 110).

We used the IBM BlueHoc simulator [17] to estimate the worst individual badge response time to SN inquiries, as the number of badges grow. Figure 6 shows the results. Ideally, all badges must be detected during the inquiry cycles of the surrounding SNs. Therefore, the number of badges per SN should be less than 50 (we see that some badges are not detected when we approach that limit). If we consider that SN range is a circle of radius 10 m, for 50 badges, there are only $\sim$ 6 m^2 per user, which represents a crowded scenario. The average worst response time for 50 users is less than T_W =8 sec, with an average of $\sim$ 6 sec, which is coherent with the results in [18]. Of course, we could detect more badges if we allowed several inquiry cycles for badge detection, but it does not seem necessary,

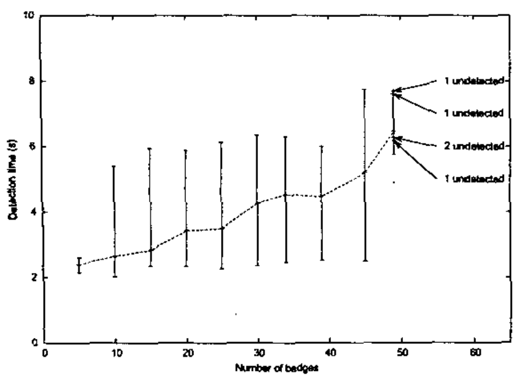

Fig. 6. Inquiry response time vs. number of badges

since we are already supporting a crowded area.

Next, and also using the BlueHoc simulator, we calculated location packet hop transfer timings. Instead of DM-1 packets, we used 210-byte DM-5 packets [13], which is the default for BlueHoc. Therefore, in a real implementation, hop transfer times would be much lower.

If we analyze the sample in figure 5, we see that there are three *basic subnets*, according to the number of incoming branches. We evaluated them with BlueHoc. Let T_L be the transfer time of a DM-5 packet in ms, in case of simultaneous incoming transmissions. Then:

- Three-branch subnet: three incoming links to a SN with an outgoing link (unless the SN is the master node). $\overline{T}_L$=4.22, σ_{T_L}=1.01.
- Two-branch subnet: same as above, with two incoming links. $\overline{T}_L$=4.12, σ_{T_L}=0.83.
- One-branch subnet: same as above, with a single incoming link. $\overline{T}_L$=3.59, σ_{T_L}=0.37.

The target area has $\sim$ 3,900 m^2 and is covered by 37 SN. In the crowded scenario, there are $\sim$ 650 badges (6 m^2 per badge). Since each SN will detect up to 50 badges (the number of badges that fit into SN range, $\sim$ 300 m^2), there are up to 1,850 location packets to be transferred as a consequence of an inquiry cycle. Taking average T_L values as a reference, we simulated the average worst-case location packet transfer time in figure 5 (required to forward the *last* location packet to its master node), as a consequence of a single inquiry cycle. The result is 3.66 s, for the upper left master node.

Therefore, if we consider that location packet transfer windows are interspersed with 8-s (T_W) inquiry cycles, we need 11.66 s to update the position of all users in the sample network in figure 5. In the application scenarios in section I, typical users make frequent stops at displays and stands. If we suppose that an interested person stays at a particular spot for a minute, location packet flush times meet real-time constraints. Moreover, since user badges only generate location packets when they enter or leave the range of a new SN, the number of location packets per inquiry cycle in figure 5 will normally be much less than 1,850.

We are not considering user data transmissions, which could also be supported by the BLN. Nevertheless, note that the use of DM-1 instead of DM-5 packets (as previously described) would free most of the transmission time in the analysis above.

With additional master nodes, the BLN may cover larger target areas, for a given performance (or may have a better performance, for a given target area size).

IV. Conclusions

In this paper, we have proposed a Bluetooth Location Network for context-driven services, BLN. The location network has the following characteristics:

- The BLN transmits position information to the service servers without user participation.
- The BLN is based on a RF technology available in existing handhelds.
- The BLN can be used as a general-purpose data network.
- The BLN infrastructure consists of small, completely independent Bluetooth nodes (no wires).
- The spontaneous topology configuration is scalable, by placing as many master nodes as necessary.
- The BLN can coexist with Bluetooth devices that are not part of the location system, such as printers or headphones.

Note that the spontaneous BLN configuration allows SNs to find alternative routes to the master node in case of SN failures. Forthcoming work will study BLN survivability, as well as new BLN topologies: mesh and k-ary 3-cube BLNs.

References

[1] U. Varshney, R. J. Vetter, and R. Kalakota. Mobile commerce: A new frontier. *Computer*, 10:32–38, 2000.

[2] A. Darling. Waiting for the m-commerce explosion. *Telecommunication International*, 3:34–39, 2001.

[3] Electronic Guidebook Project. WWW. http://www.exploratorium.edu/guidebook.

[4] J. Werb and C. Lanzl. A positioning system for finding things indoors. *IEEE Spectrum*, 35(9):71–78, 1998.

[5] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The Cricket location-support system. In *Proc. of the Sixth Annual ACM Intl. Conf. on Mobile Computing and Networking*, 2000.

[6] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster. The anatomy of a context-aware application. In *Proc. of the Fifth Annual ACM/IEEE Intl. Conf. on Mobile Computing and Networking*, 59–68, 1999.

[7] Texas Instruments TIRIS RFID systems. WWW. http://www.ti.com/tiris/default.htm.

[8] ETSI document TS 122 071 V3.2.0.

[9] T. Kindberg and J. Barton. A web-based nomadic computing system. *Computer Networks*, 35(4):443–456, 2001.

[10] G. D. Abowd, C. G. Atkeson, J. Hong, S. Long, R. Kooper, and M. Pinkerton. Cyberguide: a mobile context-aware tour guide. *Wireless Networks*, 3(5):421–433, 1997.

[11] R. Want, W. N. Schilit, N. I. Adams, R. Gold, K. Peterson, D. Goldberg, J. R. Ellis, and M. Weiser. *The ParcTab Ubiquitous Computing Experience*. In *Mobile Computing*. Kluwer Academic Publishers, 1996.

[12] T. Yamasaki, M. Kishimoto, N. Komoda and H. Oiso. An information offering system for exhibition explanation by Bluetooth Technology. In *SSGRR 2001, Advances in Infrastructure for Electronic Business, Science, and Education on the Internet*, L'Aquila, Italy, Aug. 2001.

[13] Bluetooth SIG. Specification of the Bluetooth system-core v1.0b. Technical report, December 1999.

[14] J. Lansford and P. Bahl. The design and implementation of HomeRF: A radio frequency wireless networking standard for the connected home. *Proceedings of the IEEE*, 88:1662–1676, 2000.

[15] W. Mao and D. M. Nicol. On k-ary n-cubes: theory and applications. NASA CR-194996 ICASE report # 94-88, 1994.

[16] A. Tanenbaum. *Computer Networks*. Prentice Hall, 1996.

[17] BlueHoc. WWW. http://www-124.ibm.com/developerworks/opensource/bluehoc/.

[18] C. Law, A. K. Mehta, and K. Y. Siu. Performance of a new Bluetooth scatternet formation protocol. In *Proc. of the ACM Symposium on Mobile Ad Hoc Networking and Computing*, 2001.