Opportunistic Medical Monitoring Using Bluetooth P2P Networks

Dae-Ki Cho, Seung-Hoon Lee, Alexander Chang, Tammara Massey, Chia-Wei Chang, Min-Hsieh Tsai,
Majid Sarrafzadeh and Mario Gerla
Department of Computer Science
University of California, Los Angeles
{pinecho, shlee, acmchang, tmassey, orbita, chaii, majid, gerla}@cs.ucla.edu

***Abstract*—Remote medical monitoring using body sensors and wireless communications has been gaining attention recently because of the potential savings in patient care and the equally impressive enhancements of quality of care for mobile individuals. What makes remote medical monitoring feasible are the advances in the body sensor technology (non-intrusive sensors embedded in actuators to monitor vital signs); and in wireless technology (Body LAN, cellular and Wireless LAN). Currently, most medical vests and body LANs connect to the Internet in a point-to-point fashion, via the cellular system (say SMS). With the growing popularity of ubiquitous computing and opportunistic P2P personal networks, it makes sense to explore beyond the point to point health care paradigm and study new models for remote patient care that exploit P2P networking among patients and care providers (nurses, doctors, emergency personnel). In this paper we identify several medical care applications based on P2P Health Networking. We then focus on two specific scenarios with nurses and patients both equipped with Bluetooth devices: a field hospital where nurses opportunistically collect, share and upload in P2P fashion patient medical records during bedside visits, and a field trip situation with patients supervised by nurses, where a patient emergency is promptly reported to the nearest nurse using enhanced inquiry response Bluetooth techniques. Simulation and testbed experiments show that Bluetooth P2P networking is both feasible and cost-effective in remote medical monitoring.**

I. Introduction

Ubiquitous computing has been gaining popularity due to recent advances in the fabrication of powerful tiny processors. One of the emerging applications is medical monitoring. Tiny, non-intrusive computing nodes, integrating sensors, actuators and radios can be applied to the human body to monitor vital signs. An example is the medical vest [10], designed to collect medical and biological signals from patients.

In a medical vest, different sensors transmit a variety of bio data to a gateway. The gateway filters the data and sends summaries to the Health Provider in the Internet. If the gateway connects to the Internet via a cellular phone, connectivity is ubiquitous, albeit low speed. For higher data rates (as required for multimedia patient data), WiFi and Bluetooth will be more appropriate, if supported by the gateway. However, access to Bluetooth and WiFi access points may be intermittent. In the latter case, patient data dispatching to an Internet server will suffer high latency. Fortunately, in an environment where many users (patients and nurses) are equipped with WiFi and Bluetooth devices, it is possible to facilitate data delivery using opportunistic ad hoc networking. Namely, the data can propagate hop-by-hop through the peers, exploiting their forwarding capacity as well as their motion (in some cases, the patient data is mechanically transported to the Access Point (AP) by the peers using a ”data muling” technique).

One of the goals of this paper is to examine the feasibility and effectiveness of opportunistic ad hoc networking using Bluetooth and data muling of medical records from patients to the Internet medical database. Patient data is collected from body sensors and stored on a Bluetooth-enabled gateway. Once a designated caregiver (e.g. a nurse), comes within the patient range, the patient’s gateway initiates a connection to the caregiver Bluetooth gateway (typically, a Smartphone) and transfers the stored data using a Peer-to-Peer (P2P) technique called BlueTorrent [7]. Data can be transferred either on a preset schedule (every 10 minutes) or immediately upon the availability of a caregiver. Later, the caregiver, upon completing her round of patient visits, say, uploads the patient data to a central server. This delivery can occur either directly (i.e. the same caregiver receives and then delivers the data to server), or indirectly (the data has been opportunistically transferred from nurse to nurse in a P2P manner).

BlueTorrent [7] is a P2P file sharing application based on ubiquitous Bluetooth-enabled devices. Originally proposed for sharing media contents such as movie clips or music files, BlueTorrent is used here to transfer medical monitoring data. BlueTorrent works similarly to BitTorrent in that it splits files into small chunks before sending them to other nodes. One key difference from BitTorrent is that BlueTorrent is designed for single hop data transfers. This is because of the unreliability of TCP transfers over multi-hop wireless paths in general, and the difficulty of maintaining a multi-hop (e.g. scatternet type) path in Bluetooth in particular. Thus, in BlueTorrent, random pieces are transferred only between adjacent peer nodes. BlueTorrent also handles transfers of multi-block files. As in BitTorrent, each node keeps track of the pieces received so far. A node will try to complete the assembly of the file by requesting the missing pieces from available neighbors.

In addition to relaying medical records from patients to central Internet database, the Bluetooth network may be used to alert a nurse that a patient has a medical emergency requiring

immediate attention. This application has much lower latency tolerance than the relay of patient record. To this end, we propose to disseminate the alarm across the patient community to the nurses, where the first nurse that detects the alarm responds and assists the patient. The second objective of this paper is to design an emergency propagation technique for Bluetooth. The conventional Bluetooth v2.0 protocol is too slow. We assume the availability of Bluetooth v2.1 devices (soon to be released) which implement the Enhanced Inquiry Response (EIR). As we shall see, our proposed solution reduces alarm propagation latency by orders of magnitude and can meet the most demanding applications.

As it is apparent from the two above scenarios, motion pattern has a strong impact on the performance of both medical report muling and emergency alarm relaying. In this paper we will define a few representative motion patterns that recur in assisted living situations, say, when patients and nurses move on the rest home grounds or when they take short excursions to nearby amusement parks.

In the rest of the paper we review the basic Bluetooth technology, we describe the experimental scenarios and report simulation and testbed measurements. At the end of the paper we draw some conclusions on the feasibility and limitation of Bluetooth P2P networking for patient/nurse/provider opportunistic data transfers. Our work differs from previous work in opportunistic networking with Bluetooth [11] and mobile Bluetooth Telehealth solutions [9] [12] in that it specifically addresses P2P networking with Bluetooth.

II. Bluetooth Overview

Bluetooth divides its bandwidth into 79 channels and Bluetooth devices move from one channel to another by Frequency Hopping (FH). Frequency changes 1600 hops per second. Each time slot for a given frequency lasts a time slot = $625\mu s$ (or multiple thereof in case of long packets). A *slot* is the basic time interval in Bluetooth. There are three major states and seven minor states. The minor states are temporary states between major states. The*Piconet* is the elementary network unit (cluster) in the Bluetooth network. In the *Piconet*, one master device can connect in turns with up to seven slave devices. To make a connection with slave devices, the master device invokes two procedures – *Inquiry Procedure* and *Paging Procedure*.

The high delay introduced by these two procedures has precluded in the past the use of Bluetooth in most real time applications. Fortunately, the new version Bluetooth v2.1 features a number of novel properties that help remove such limitations. We will leverage two features EIR and Secure Simple Pairing - to resolve the latency problems and launch Bluetooth in HealthNet environments.

A. Extended Inquiry Response (EIR)

Originally, devices had to build a connection prior to data exchange using the two steps *Inquiry Procedure* and *Paging Procedure*. Bluetooth v2.1, supports a new mechanism to propagate data without connection establishment. *Extended Inquiry Response (EIR)* is the method that allows each device to send data up to 240 bytes before devices make a connection. The EIR data is controlled by the user and is intended to include simple device information such as local name, service class, etc.

EIR data is propagated in the middle of *Inquiry Procedure* and the device is on *Inquiry Response State*. This removes the need for the *Paging Procedure*, which causes most of the connection delay.

In response to a master device's *Inquiry*, a potential slave device sends an *Inquiry Response* with random back-off time interval between [0,1023] slots. The response packet in the Bluetooth v2.1 includes a bit flag that announces the presence of EIR data. If the slave device must transmit EIR data, it sends the *Inquiry Response* packet with EIR flag set. EIR data is sent after 1250μs as a back-off time interval. A master device with one *Inquiry* packet can receive multiple EIR data from many slave nodes. All slave nodes listen to *Inquiry* to EIR packets. It is unlikely that collisions among EIR data happen because of the random back-off interval.

B. Secure Simple Pairing (SSP)

Bluetooth v2.1 introduces another new feature called *Secure Simple Pairing (SSP)*. SSP is designed to simplify the pairing processes and improve Bluetooth security. Its purpose is security of connection based data delivery. *Pairing* stages, as a part of SSP, take place after finishing *Paging Procedures*. SSP initiates a key generation procedure to produces a public and private key pair. Then the public keys are exchanged between two devices. *Diffie Hellman Key (DHKey)* [1] is calculated based on the exchanged public keys. The DHKey values of each device have to be the same as long as the keys are exchanged correctly.

Two possible security issues, passive eavesdropping and man-in-the-middle (MITM) attacks, can be resolved by SSP. By the nature of wireless networks, an unwanted user can overhear the data transmissions between devices. Especially in medical environments, the sensed data should not be exposed. Once SSP procedures are successfully processed, data is encrypted by the public keys. If a device does not have a proper private key, the decryption steps fail. SSP prevents the passive overhearing attacks because there is no way attackers can have the correct key. In addition, if data is altered by an attacker in the middle of the two devices, the original data cannot be recovered by the private key, preventing the MITM attacks.

III. Patient monitoring and record management

In this section, we review monitoring and data recording applications using Bluetooth. We identify two scenarios and propose two techniques NurseNet and BlueAlert - to support them.

[1]Diffie-Hellman (D-H) key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel [2].

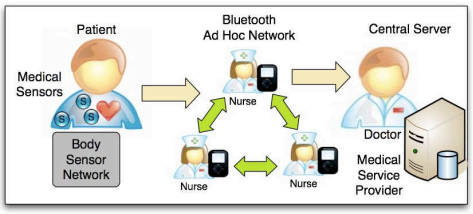

Fig. 1. NurseNet Architecture

A. NurseNet: Patient data uploading to the Central Database

The data collected by body sensors can be dispatched to the provider host via several techniques such as 3G, 802.15.4, WiFi and Bluetooth. In some environments these techniques are not adequate or not allowed. For example, in hospitals, the use of cellphones is prohibited [3]. WiFi is note desirable because of high energy consumption and interference with medical instrumentation. ZigBee (more generally IEEE 802.15.4) is problematic because of scarce commercial penetration and significant interference vulnerability to wifi interference [1]. This leaves us with Bluetooth as the option of choice for P2P data exchanges (patient to patient; patient to nurse; nurse to nurse).

With this motivation we review a few Bluetooth-based architectures. We start with NurseNet (see Figure 1). The NurseNet architecture consists of three components – patient, nurse, and AP/Central Database/Doctor – all equipped with a Bluetooth device. Patients have sensors attached to their body, and the data collected from sensors is stored on a Bluetooth-enabled mobile device. The patients device passes the medical data to a caregiver (say, nurse) device that then transfers the stored data over Bluetooth P2P to the database. This delivery can occur either directly (i.e. the same caregiver receives and then delivers the data to server), or indirectly, (two or more nurses help each other transfer the data to the server).

To offer a more concrete scenario of NurseNet, consider a Field Hospital, i.e. a large tent with several beds organized in rows, and 20-40 patients per row, 5 to 10 meter apart. Military patients come already equipped with medical vests; nurses make the rounds and spend a variable amount of time at each patient bed. While visiting the patients, the nurses opportunistically download their records. Periodically, nurses return to the office, 50 meters away from the patients. They upload the patient data to the medical database. Nurses can share data among themselves in a P2P manner. A patient cannot share data with other patients because of privacy and security reasons. There are also nurse aids, to assist the nurses with various chores, including going back and forth to the office to fetch medications or instruments. Nurse aids also participate in P2P transfers of patient data to the AP.

The above field hospital model has characteristics common to many nurse/patient scenarios, such as a nursing home where elderly patients stroll on the grounds (several acres) adjacent to the main building. Nurses roam around the patients, monitoring, assisting and entertaining them. Nurse aids interact as before. Again, the patient data eventually gets transferred to the main database.

B. BlueAlert: An emergency alarm protocol with Bluetooth v2.1

The conventional Bluetooth-based patient monitoring system is not suitable for emergencies. Bluetooth connection establishment takes 5 to 10 seconds and this delay can cause severe problems in medical environments. Thus we need a special mechanism to deal with urgent message propagation [8], If the data stream detected by body sensors exceeds a certain threshold, the Bluetooth device changes its data propagation mode from BlueTorrent to emergency mode (BlueAlert). The device keeps disseminating the emergency message to other peers around. Since the situation is urgent, all nodes cooperate in the dissemination.

We use the new Bluetooth feature called EIR. EIR travels across a Bluetooth overlay much faster than the regular Inquiry Response (IR). While it can carry a limited payload, it is still sufficient to carry the name of the patient, the geo-coordinates and the gravity of the emergency (from the need to find a toilet to the symptoms of an imminent stroke). The EIR message, as opposed to the IR message in BlueTorrent that seeks nurses only, can travel from patient to patient and can alert any nurse.

IV. Testbed Experiments

In this section, we describe preliminary field test results. The key performance measure is the delay to deliver data from patients to the Bluetooth Access Point (BT-AP). In the experiment, we logged the path of patient data and measured data delivery time over several hops.

A. Experiment Environment

To reproduce the most general conditions from hospital to battlefield and disaster area, we decided to include open space environments (as opposed to a lab). Thus, our experiment takes place at the second level of the UCLA parking garage. The size of the parking structure is roughly 75×75 meters. The experiments were performed late at night to avoid interference with pedestrian and vehicular traffic.

B. Experiment Setting

In the experiment as shown in Figure 2, our system consists of three components. The first component is the patient. The patient moves inside a designated area of 10×10 meters. The patient is equipped with two different body sensors – ECG and Purse Oximeter. Both medical sensors are from Alive Technology [4]. Each sensor continuously transmits a 143-Byte sensor packet every $240ms$ on the Bluetooth channel to the patient's gateway (a laptop in our experiment). Thus, the gateway roughly generates 70 KBytes of medical data per minute. A patient node continually performs inquiry to discover nurses. Upon discovering a nurse, the gateway starts sending the list of its data blocks. It then proceeds to push the missing blocks (pieces) to the mobile nurse gateway.

The second component is the BT-AP. In our scenario, only the BT-AP provides Internet access. Cellphones are disabled in

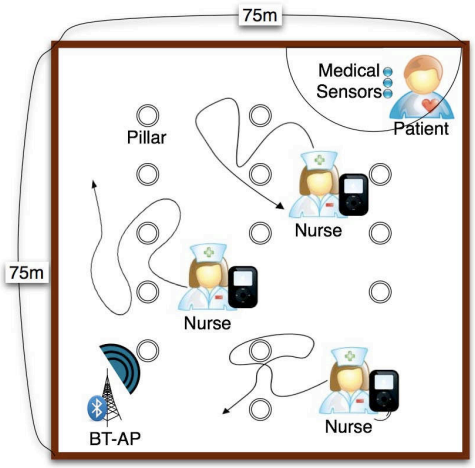

Fig. 2. Experiment Scenario (Parking Lot 4, UCLA)

Average	334.89 (sec)
Minimum	115.10 (sec)
Maximum	631.45 (sec)
Standard Deviation	137.29 (sec)
Data size	100 KBytes

TABLE I
PACKET DELIVERY TIME

the hospital area. WiFi, while available on the nurse gateway, is not used because of energy saving considerations. The BT-AP delivers patient data to the doctor stations via the Internet. The BT-AP periodically performs inquiries to discover nurse gateways. Upon discovering a nurse gateway, the BT-AP requests the missing pieces from its patient files.

The last component is the nurse. There are three nurses, interconnected in a P2P network. The main role of the nurses in this experiment is to collect and deliver patient data to the BT-AP. As we mentioned in Section III, we use a P2P scheme to propagate the data via multi-hopping to the BT-AP, to improve performance. We implemented the P2P system using Python. We use PyBluez, a Python library that enables access to BlueZ functions in Linux. Each mobile node alternates between inquiry and inquiry scan mode to discover other nodes. If multiple peers are detected, a node selects the peer with the highest RSSI value. In the experiment, three members of the measurement team play the nurses role. They randomly walk holding a laptop around the testing area at a speed from 0.5 to $1m$/s.

We used Kensington 33348 Bluetooth dongles (v2.0 EDR, Class 2, and Broadcom chipset) for nurse nodes, patient node and BT-AP node. As mentioned earlier, the patient node generates a 70 KBytes file every minute. We set piece size to 500-Bytes (thus, total of 140 pieces/file). We ran each test for 20 minutes and performed a total of 5 tests.

C. Evaluation

Figure 3 shows that all nodes contributed to the delivery of data from the patient to the BT-AP. Nurse nodes exchanged their packets with neighbors to decrease packet delivery latency. Figure 4 shows the fraction of hop lengths it took to deliver each file. We notice that data delivery time can be reduced if we have more hops between sources (patients) and destination (BT-AP). Figure 5 shows average file delivery time over number of hops. Due to the limitation of our equipment, we could consider only one patient. In the next section, we will show simulation results with several patients in a similar environment. Table I shows the average time to deliver the patients data: 300 seconds is fine for background data, but it is unacceptable if a patient has an emergency. Our answer to emergency support is the EIR feature offered in Bluetooth v2.1. Since Bluetooth v2.1 devices are not yet available, we will show the performance of the proposed emergency protocol EIR through simulation in the next section.

Our preliminary test shows that there is still room for improvements. For example, a Bluetooth connection to a BT-AP or peer should be closed as soon as the mobile peer goes out of range; however, the mobile keeps the connection. Throughout the experiments, we observed that a node wastes time attempting to use the failed connection; instead, it should attempt connections with other Peers. Another desirable design choice would be to install multiple Bluetooth interfaces in the BT-AP to alleviate the persistent connection problem. Moreover, we noticed that peer selection should be assisted by motion prediction, to prevent unnecessary connection attempts to a node that is moving away from the source.

V. SIMULATION

In this section, we investigate via simulation two scenarios: patient to nurse and nurse to AP transfer of patient records (NurseNet) and; propagation of emergency messages using a Bluetooth overlay (BlueAlert). In our simulation experiments we have leverage the testbed, by selecting the key parameters to be consistent with measured data. Our simulation platform is ns-version 2.9 [6] with UCBT [5], a Bluetooth simulator. UCBT is public, opened and it implements the major Bluetooth protocols such as baseband, LMP, L2CAP, and BNEP. Bluetooth v2.1 features such as EIR and SSP are not yet available in UCBT [8]. They have been implemented by our team.

A. Simulation Scenario I: NurseNet

The setting is a Field Hospital. Each patient has body sensors and a Bluetooth-enabled gateway. The sensors keep generating medical data. The Bluetooth-enabled gateway periodically gathers the data from the sensors. Each nurse also has a Bluetooth device and collects patient data through it. There are 50 patients (modeled as static nodes) and 5 nurses who move around visiting patients (Table II). Each visiting nurse has a list of patients to visit. We model the nurse itinerary as a random walk. The nurse walks for 20 seconds on average (at a speed of 1m/s) from one patient to the next. She stays with a patient for 5 minutes on average. The nurse collects data from near by patient while walking until it pauses to visit a patient. While the nurse is walking, a full 100 Kbytes record

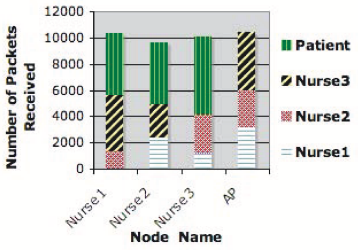

Fig. 3. Num of packet received by different entities

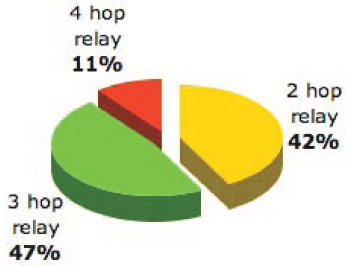

Fig. 4. Num of hops traveled by patients file

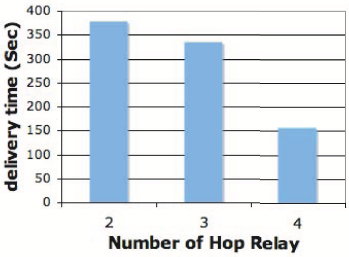

Fig. 5. Avg delivery time vs Number of hops

can be downloaded in a 10 seconds, 10 meters contact window. Once a patient record is read by the nurse, a new record is immediately created by the patient Body LAN (we assume there is room only for one record in each patient memory). During the 5minute visit, the nurse does not collect data from surrounding patients. The rationale is that the nurse has already downloaded the record of the patient that is being visited, and is using her PDA for other tasks, such as processing the patient data. Upon completing the visit, the nurse with probability *1-P* resumes the round; or, with probability *P* returns to the main office. In our experiment, P = .2. At the office, the nurse uploads the data collected so far at one of the BT-APs. It then resumes the visits.

In this scenario, we experiment with two different Bluetooth overlay mechanisms.

- P2N (Patient-to-Nurse): A nurse collects data only from patients.
- P2N (Patient-to-Nurse) + N2N (Nurse-to-Nurse): A nurse can collect data directly from both a patient or indirectly from another nurse. When two nurses encounter, they exchange patient data. The encounter of two nurses happens opportunistically, when they cross each other.

1) Evaluation: We define two delay measures in this experiment: data collection delay (from data creation to nurse download time) and data uploading delay (from download from patient to upload to hospital). Figure 6 and Figure 7 show collection and uploading delay, respectively. The P2N case refers to peer exchange between patient and nurse only. There is no exchange of patient data between nurses. The case P2N + N2N implies that there is subsequent exchange between nurses, in order to speed up the delivery of patient data to the hospital database. From the results in Figure 6, we note that it takes on average 3,000 seconds from the time data is created and posted by the patient on its gateway to the time the data is collected by a nurse. Figure 6 shows no difference between P2N and P2N+N2N, as expected, since N2N plays no role in the collection phase. The collection delay is quite high. This is in part due to the assumption that the nurse does not collect data during the pause. Relaxing this constraint reduces the collection time from 3000 to 100 seconds (as estimated using a simple analytic model). Further reduction can be obtained with patient-to-patient (and eventually nurse) exchanges. These tradeoffs will be investigated in future extensions of this work.

Turning now to upload time, Figure 7 shows that the time required to upload the data from nurse to the hospital database is indeed influenced by the N2N exchange. Without N2N it takes on average 1,000 seconds to upload a patient record. With N2N the delay is reduced to 700 seconds. In the N2N case, when two nurses encounter each other, they exchange some of the data collected so far (the actual amount exchanged depends on Bluetooth channel speed and contact time). As a result, patient data is replicated among nurses. Each nurse has a data uploading probability P after a round of patient visits. With N2N exchange, data upload rate to the hospital increases (and latency decreases) with number of nurses and with P. With the current parameter settings, the latency is clearly dominated by the collection time, thus N2N has minor impact on overall latency. The N2N exchange would have more impact, if the collection time were reduced (in the limit, to 100 seconds by allowing nurses to collect patient data during the pause intervals).

TABLE II
SIMULATION I PARAMETERS

Area	(100×50)meters
Number of Nodes	50 Patients and 5 Nurses
Speed of Nurse nodes	1 m/s

B. Simulation Scenario II: BlueAlert

The previous patient monitoring protocols based on BlueTorrent are not suitable to handle multi-hop propagation of alarms. In fact, the connection establishment between two Bluetooth devices alone takes 5 seconds. This delay, amplified by several hops, can cause excessive latency in emergencies. Lee *et al* proposed an emergency data delivery system exploiting a new version of the IR protocol available in the Bluetooth v2.1 release[8]. We apply this new version to our medical monitoring system for emergency situations.

We assume patients move in a $100 \times 100m^2$ area. They are escorted by nurses. Suddenly, one of the patients needs urgent attention from the nurses. The Bluetooth gateway on the patient body LAN detects the emergency and propagates the emergency alarm message to all neighbors. In our experiment we have a variable number of patients and five nurses. We measure the number of hops and the delay until the emergency message reaches one of the nurses. Figure 8 illustrates the scenario. The simulation setup parameters are reported in Table III. We assume that patients move at s $0.5m/s$ speed.

1) Evaluation: Figure 9 and Figure 10 show the results. As the number of patients increases, the number of hops increases.

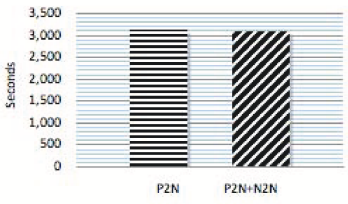

Fig. 6. Simulation Result I: Collection delay

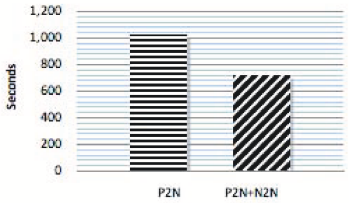

Fig. 7. Simulation Result II: Uploading delay

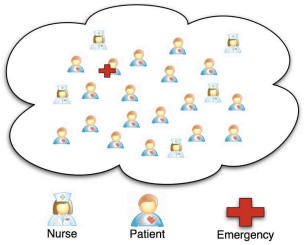

Fig. 8. Simulation Scenario II

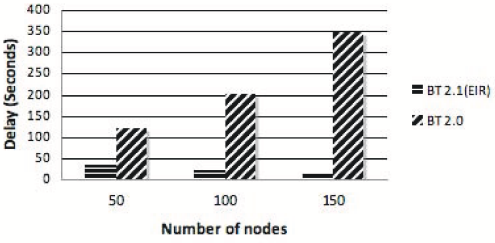

Fig. 9. Number of Nodes vs Delay

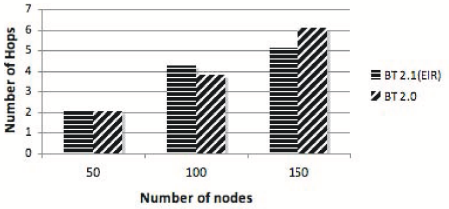

Fig. 10. Number of Nodes vs Number of hops

TABLE III
SIMULATION II PARAMETERS

Area	(100x100)meters
Number of Nodes	50,100,150 Patients + 5 Nurses
Speed of Nurse nodes	$0.5m/s$

When a patient tries to make a connection, it broadcasts *Inquiry*. Then the patient communicates with a randomly selected neighbor. Because of the randomness of the peer selection, there may be quite a large number of hops between patient and nurses. In spite of this, the newly proposed system [8] propagates the emergency message very rapidly over the entire network, reducing delay by more than a factor of 10 (for 100 nodes) and clearly demonstrating the ability of Bluetooth v2.1 to handle also emergency situation.

VI. CONCLUSION

In this paper, we have proposed a Bluetooth-based HealthNet architecture for patient monitoring, data recording and alarm dissemination. One important contribution was to show that opportunistic, delay tolerant networking using Bluetooth P2P overlay techniques (more precisely, BlueTorrent) is feasible and cost-effective in patient/nurse monitoring and data transfer scenarios. We proved this both in a simulation setting as well as in a small-scale testbed experiment.

Another contribution of this paper was to show that the traditional high latency caused by Bluetooth's slow connection time can be mitigated by exploiting EIR, a new feature that will be available in Bluetooth v2.1. The proposed EIR based dissemination technique – BlueAlert – allows us to broadcast data in the Bluetooth overlay without establishing connections, thus enabling emergency applications over Bluetooth. This second contribution was demonstrated only via simulation, since Bluetooth v2.1 devices are not yet available. Future work in the Bluetooth-based HealthNet will include: integrated Bluetooth and ZigBee support in the Body LAN; development of a gateway to interface Body LAN and radio access to the Internet and to Peers, and; integrated Bluetooth, WiFi and 3G access from Body LAN to internet.

REFERENCES

[1] BGR. Wlan interference with ieee 802.15.4. *Technical report*, March 2007.
[2] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22:644–654, Nov. 1976.
[3] The Blonde Geek. Cell phones and medical equipment interference. Dec 2007.
[4] http://www.alivetec.com.
[5] http://www.ececs.uc.edu/ cdmc/ucbt/.
[6] http://www.isi.edu/nsnam/ns/.
[7] Sewook Jung, Uichin Lee, Alexander Chang, Daeki Cho, and Mario Gerla. Bluetorrent: Cooperative content sharing for bluetooth users. *Percom 2007*, March 2007.
[8] Seung-Hoon Lee, Sewook Jung, Alexander Chang, Dea-Ki Cho, and Mario Gerla. Bluetooth 2.1 based emergency data delivery system in healthnet. *WCNC 2008*, April 2008.
[9] Xuanwen Luo. Unconfined mobile bluetooth nursing and daily collection. In *Consumer Communications and Networking Conference*, pages 693–696. IEEE, 2004.
[10] Majid Sarrafzadeh Roozbeh Jafari, Foad Dabiri. Customed: A power optimized customizable and mobile medical monitoring and analysis system. *ACM HCI Challenges in Health Assessment Workshop in conjunction with CHI 2005*, April 2005.
[11] James Scott, Pan Hui, Jon Crowcroft, and Christophe Diot. Haggle: A networking architecture designed around mobile users. In *The Third Annual IFIP Conference on Wireless On-demand Network Systems and Services*. IEEE, 2006.
[12] Lin Zhong Mike Sinclair and Ray Bittner. A phone-centered body sensor network platform: Cost, energy efficiency & user interface. In *IEEE International Workshop of Body Sensor Networks*. IEEE, 2006.