Bluetooth 2.1 based Emergency Data Delivery System in HealthNet

Seung-Hoon Lee, [†]Sewook Jung, Alexander Chang, Dae-Ki Cho, Mario Gerla
Department of Computer Science [†]Wireless Connectivity Group
University of California, Los Angeles Broadcom Corporation
{shlee,acmchang,pinecho,gerla}@cs.ucla.edu, [†]sewookj@broadcom.com

***Abstract*—The interests in health care have considerably increased these days as the aging population becomes larger. Health care has grown to the one of most active research areas especially in the area of wireless, mobile health monitoring systems. The wireless network technologies have advanced to the point where they can enable and help deploy a very broad gamut of systems suitable for medical applications. Several researches have proposed to replace the wired connections among medical devices with wireless connections. Wireless network technologies interwork with sensor equipped Body LANs. Wireless Personal Area Networks (WPANs) are well positioned to support Health Care applications in limited geographic areas. In particular, the characteristics of Bluetooth and its popularity make it the preferred network infrastructure for HealthNet environments. However, Bluetooth has the "bad reputation" of long connection delays, which may be disastrous in some health applications. In this paper we address the connection delay and propose a new data transfer protocol based on Bluetooth version 2.1. The 2.1 version was published very recently and offers new features that are interest to our application. Among the new features we leverage EIR and SSP to solve the delay problem. Extensive simulation results show that the proposed system significantly improves data delivery as well as power consumption. It solves a well known problem in Bluetooth based wireless networks. Using our proposed scheme, Bluetooth devices are now adequate to support sophisticated scenarios such as emergencies and urgent data dissemination requirements.**

I. Introduction

The expenditure in US health care was a $1,280B industry in 2003 [10], [6]. Health care has emerged to be one of the most active research areas in the field of mobile sensing, communications, and computing. It exploits two technologies, Embedded Computing Systems and Wireless Personal Area Networks (WPAN). The embedded technologies make medical devices smaller, cheaper, and more power-efficient. The wireless network technology makes systems more easily deployable in medical environments. These two technologies form the infrastructure of modern HealthNet applications.

The medical sensors have become more accurate and richer in features, allowing us to improve the quality of health care. The sensors are able to delicately and non-intrusively monitor body status such as blood pressure, heart rate, etc. The sensors continuously observe changes in body status because the nature of physiological data is unpredictable. Today, doctors and nurses manually record and track patients' status [13]. Unfortunately, the traditional processes to monitor patients' status can no longer guarantee high accuracy and efficiency due to the increased sophistication of the sensed data [5]. [14] and [15] propose BodyLan based wireless sensor platforms to monitor body status without human intervention. Lo *et al.* have designed a system where tiny medical sensors are attached to the body and are connected to a local wireless device that serves as the gateway to two small wireless networks [15]. The BodyLAN interconnects body sensors to the data collection gateway(Intra-Networking). In turn, the gateway connects to external networks to propagate the data for further processing(Inter-Networking). Related to these efforts, Gao *et al.* have proposed AID-N, an ad-hoc health information system which overcomes the difficulties of patient monitoring [5]. This system features electronic triage for efficient and accurate management of large patient populations.

Along with the development of ever more sophisticated sensing devices, several researches are now proposing to replace wired connections among sensors with wireless. Wireless Personal Area Networks (WPANs) are a natural match due low cost, broad availability, low power consumption and limited range. Bluetooth, ZigBee, and 802.11 standards are widely used for WPAN. Jung *et al.* evaluate ZigBee based wireless interconnection methods for HealthNet environments. The intrinsic characteristics of ZigBee – low power consumption, built-in security – are also well suited to medical sensor networks [7]. In [3], [12], and [11], Bluetooth based wireless sensor networks are proposed. Bluetooth devices are popular for medical applications because they are power-efficient, small enough to work on medical devices and are present in virtually all cellphones and laptops. Moreover, Bluetooth devices can network with other devices. Self-organized interworking is of prime importance in mobile wireless sensor networks. Recently, Bluetooth has gained more attention than ZigBee because of its widepread availability.

From the above it is clear that radio characteristics and popularity make Bluetooth the network of choice for HealthNet. However, Bluetooth does suffer from one problem – connection set up latency. Bluetooth devices must establish a connection in order to communicate each other. On average, it takes about 5 seconds to establish the connection (the minimum is 0.00375s and the maximum is 12.8s-33.28s) [11]. This delay can cause severe problems in medical environments. For example, when a body sensor detects symptoms of heart attack, the emergency situation must be reported immediately. These kinds of emergencies are very common in medical environment. Unfortunately, the current Bluetooth based wireless networks do not have any special mechanisms to deal with emergency circumstances.

In this paper, we propose a new protocol in Wireless Personal Area Networks using Bluetooth version 2.1. This recently published version includes many new features [1]. Among the features, we customize EIR and SSP to our system for a fast and secure data distribution, enabling better response to health emergency situations.

- EIR (Extended Inquiry Response): By manipulating EIR, we make a device send data without connection establishment stages and pull data from multiple slave devices.
- SSP (Secure Simple Pairing): By employing SSP, we protect EIR based data delivery against potential attackers. Public Key Infrastructure (PKI) based security method is deployed.

In Section II, we overview Bluetooth based Wireless Personal Area Networks (WPANs). Section III presents the details of the new features in Bluetooth version 2.1. The proposed EIR based data delivery system is introduced in Section IV. In Section V and VI, the new system is evaluated. We conclude in Section VII.

II. Bluetooth Overview

In this section, we overview the procedures that Bluetooth devices undergo to establish connections. Then we discuss the synchronization problem inherent in these procedures, which causes severe data delivery delay.

Bluetooth divides its bandwidth into 79 channels and a device moves from one channel to another channel by Frequency Hopping. Frequency changes 1600 hops per second and a frequency lasts a time slot = $625\mu s$. The *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. *Piconet* is a networking unit in Bluetooth networks. In one *Piconet*, one master device is able to have connections with up to seven slave devices. To make a connection with slave devices, the master device invokes two procedures – *Inquiry Procedure* and *Paging Procedure*.

A. Inquiry Prodecure: Peer Discovery

A device has to find other Bluetooth devices to make connections. The step to discover other devices in communication range is *Inquiry Procedure* or *Peer Discovery*. Fig. 1 shows the overall procedure of the *Inquiry Procedure*. A master device dedicates T_{w_inq} for connection establishment. The slots within T_{w_inq} are categorized into *Tx slots* and *Rx slots*, taking place in an alternating manner. The master device broadcasts an ID packet in *Tx slot* and waits for a response packet from other devices in a *Rx slot*. Other Bluetooth devices within the communication range of the master device receive the ID packet when they are in *Inquiry Scan State*.

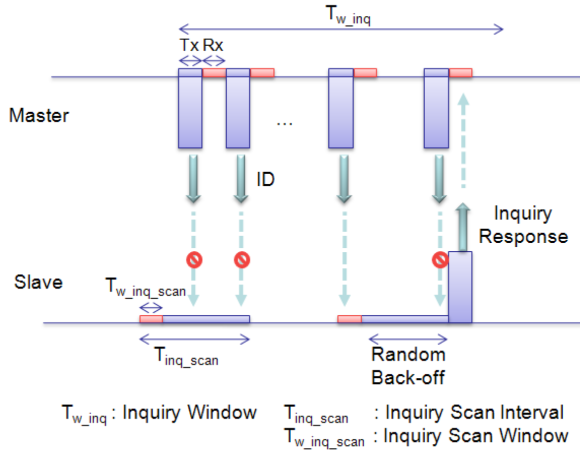


Fig. 1. Inquiry Procedure

A potential slave device periodically enters $T_{w\_inq\_scan}$ in each T_{inq_scan}. The device is only able to listen to the ID packet from the master device during $T_{w\_inq\_scan}$. The intervals, T_{inq_scan} and $T_{w\_inq\_scan}$, are manually controllable parameters. After receiving the ID packet, a device sends an *Inquiry Response* packet if the device wants to make a connection with the master device. The response packet contains the address and clock information required for the next step. To minimize collision with other potential slave devices, the response packet is sent after a random back-off interval. The range of back-off time is dependent on the T_{inq_scan}. If the scan interval is longer than or equal to 1.28 seconds, the range of back-off time is [0, 1023] slots. Otherwise the range is [0, 127] slots. The device changes its state to *Inquiry Response State* and moves to *Paging Procedure*.

B. Paging Procedure: Connection Setup

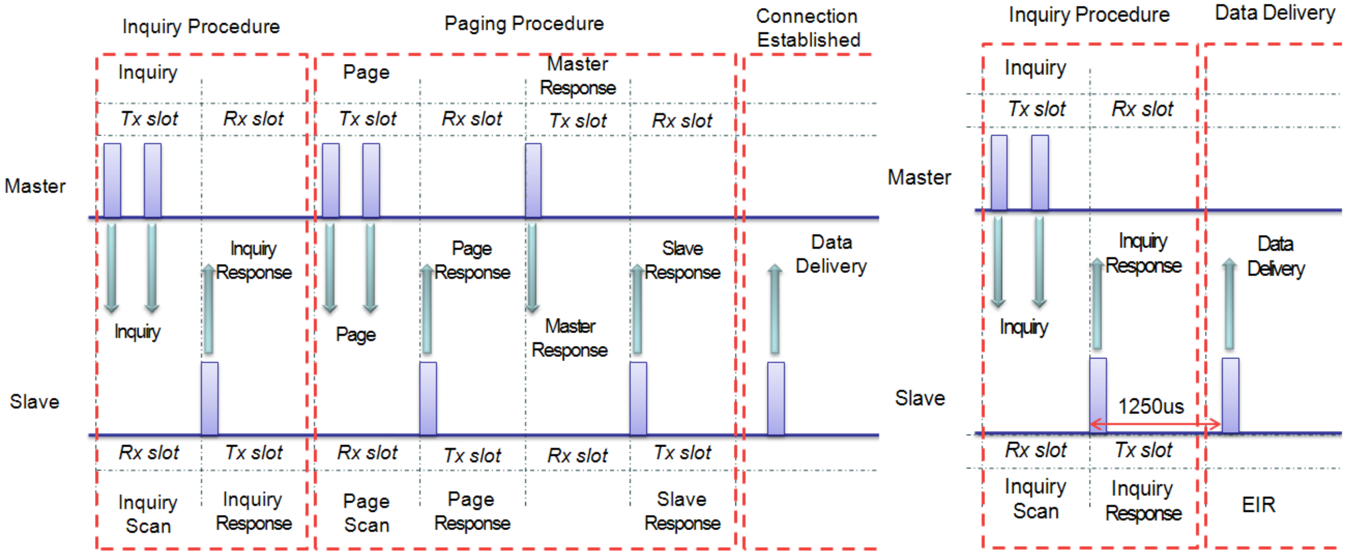
After discovering a potential slave device, the master device tries to establish a connection with the device and this procedure is called *Paging Procedure* or *Connection Setup*.

The master device starts *Paging Procedure* as a response to *Inquiry Response* from the slave device. The same timing slots are used in *Inquiry Procedures*. The master device sends a *Paging* packet in a *Tx slot* and listens to a *Paging Response* packet in a *Rx slot*.

After successfully receiving the *Paging Response* packet in a *Rx slot* from the slave device, the master device sends *Master Paging Response* packet in a *Tx slot*. The *Paging* packets are for timing and frequency synchronization between the two devices. The slave device adjusts its *Rx* and *Tx* timing to master's timing according to the *Master Paging* packet. Then a connection between two devices is established and they are ready to exchange data packets. The overall procedures of connection establishment are presented in Fig. 2.

C. Connection Delay Problem

As explained in Section II-B, connection oriented data delivery systems need four more steps to establish a connection between two devices after peer discovery. The additional steps have a timing issue which causes long connection delay. For example, based on the *Inquiry Response* packet from a potential slave device, a master device sends a *Paging* packet



(a) Connection based Data Delivery

(b) EIR based Data Delivery

Fig. 2. Overall Procedure

as the first step of the *Paging Procedure*. The *Paging* packet is sent by the master node in a *Tx slot*. The slave device must be using a *Rx slot* to receive the *Paging* packet. If the slave device is using a *Tx slot* when the master device's *Paging* packet arrives, the device cannot receive the packet. Thus it has to wait for another *Paging* packet from the master device so that it is in a *Rx slot*. Similarly the master node cannot receive *Paging Response* packet when it is using *Tx slot*. Because of these syncronization issues, devices have to wait extra time to send or receive a packet. Fig. 2(a) shows master and slave device sending two packets, *Paging* and *Master Paging Response* each during the *Probing Procedure*. This syncronization problem affects every packet transmission, resulting in a significant delay in connection establishment. The connection delay is critical in real time applications such as medical and emergency sensor networks.

III. New Features of Bluetooth version 2.1

The new version has a number of novel features to improve Bluetooth based wireless networks. Among them we leverage two features to resolve the critical problem of Bluetooth based wireless networks in HealthNet environments.

A. Extended Inquiry Response (EIR)

Originally, devices had to build a connection prior to data exchange using the two steps presented in Section II. Bluetooth version 2.1, supports a new mechanism to propagate data without the connection establishment procedures. *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 means that we do not need *Paging Procedure*, which causes most of the connection delay. As a 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 new version includes a bit flag which represents the availability of EIR data. If the slave device has an 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 listened to *Inquiry* packet send EIR data. It is unlikely that collisions among EIR data happen because of the random back-off interval.

B. Secure Simple Pairing (SSP)

Bluetooth 2.1 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 Prodecures*. 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.

[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 [4].

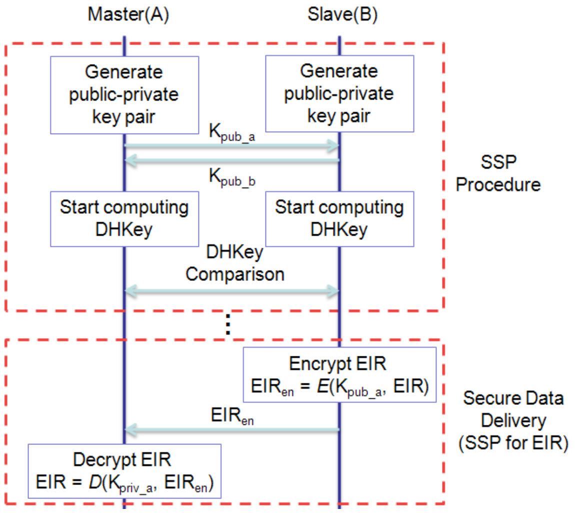

Master(A)
Slave(B)
Generate public-private key pair
Generate public-private key pair
K_{pub_a}
K_{pub_b}
SSP Procedure
Start computing DHKey
Start computing DHKey
DHKey Comparison
Encrypt EIR
$EIR_{en} = E(K_{pub\_a}, EIR)$
EIR_{en}
Secure Data Delivery (SSP for EIR)
Decrypt EIR
$EIR = D(K_{priv\_a}, EIR_{en})$

Fig. 3. Secure Data Delivery

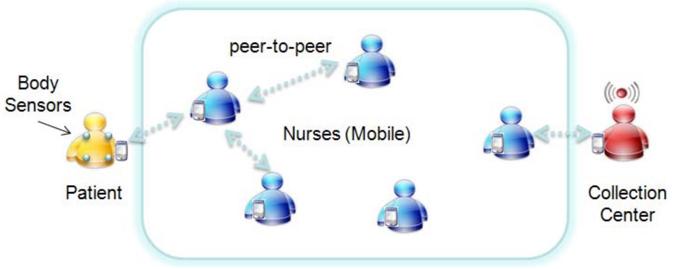


Fig. 4. Simulation Scenario

TABLE I
SIMULATION PARAMETERS

Area	[50 × 50, 100 × 100, 150 × 150] m^2
Number of Nodes	[15, 25, 30, 35, 45]
Speed of Nodes	[0.5, 0.75, 1, 1.25] m/s
Packet Type	DH5
Data Size	240 bytes

Once SSP procedures are successfully processed, data is encrypted by the public keys. If a device does not have a proper private key, decryption steps fail. It 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.

IV. FAST AND SECURE DATA DELIVERY WITH BLUETOOTH 2.1

In this section, we discuss how we reduce data delivery delay using EIR and how we ensure secure data delivery using SSP.

A. Fast Data Delivery

As discussed in Section III, EIR based data delivery improves performance compared to the connection based data transmission. We take this advantage by using EIR for our medical system, assuming EIR data field is large enough for HealthNet environments, since most of the applications in wireless sensor networks aggregate the data in order to minimize communication overhead [9]. EIR supports all packet types defined in [8] and we use DH5 as a packet type to support large enough data in medical applications. The performance is improved in two aspects: receiving multiple data responses and no connection establishment.

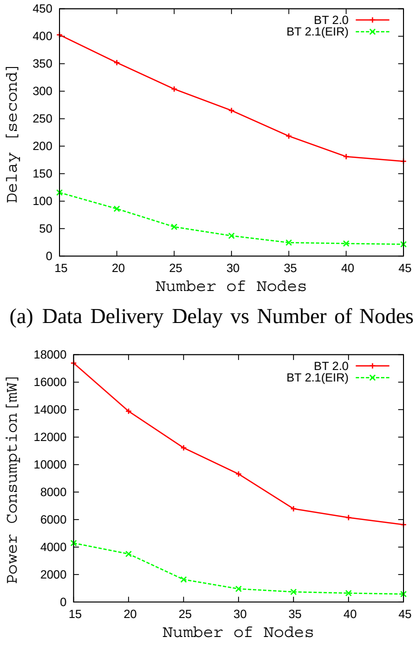
First, a master device in *Inquiry Interval* is able to receive multiple EIR data packets from potential slave nodes in *Inquiry Scan Interval*. This significantly improves data delivery performance. In [8], Bluetooth devices in peer-to-peer networks only receive one data packet at a time because they make a one-to-one connection between master and slave devices. In contrast, with EIR, the querying node does not make a connection; rather, it collects all EIR data from slaves that receive the *Inquiry* packet.

Second, EIR data is sent when the device is in *Inquiry Response State* which is the state before making a connection.EIR uses the same procedure to discover other peers. After that, however, EIR avoids the need for additional steps which cause delay. As in Fig. 2(b), EIR data is sent without *Paging Procedure*. After *Inquiry Response* is sent, the data is delivered with the back-off time of 1250μs. Hence, it does not have any timing problems presented in Section II-C.

B. Secure Data Delivery

Bluetooth has security mechanisms that protect data delivery once a Bluetooth connection is set up between two devices. However, our EIR based data delivery does not set up a connection in order to reduce the delay. Hence, we must develop an additional security system and we leverage SSP to protect EIR data. We *customize* the SSP procedure for our purpose since SSP was not designed for EIR.

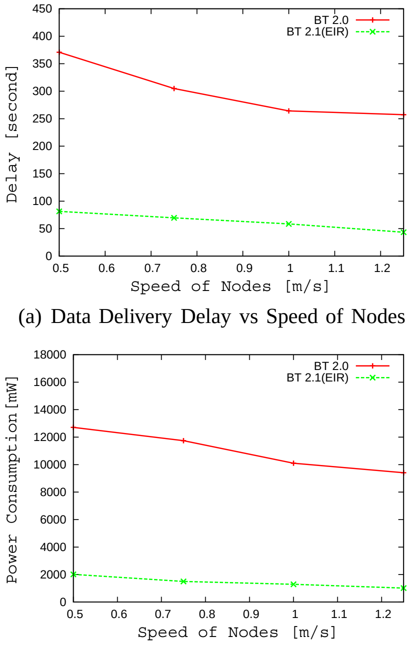
We use the security keys generated by SSP. First a master device checks whether it has the public key of the potential slave device. If it does not have the key, the master device *pretends* to make a connection with the slave device. The actual connection is not established. We only need to generate the security keys to encrypt and decrypt EIR data. After public and private keys are generated in each device and public keys are exchanged, the devices stop the SSP procedures. Now the master device has a public key of the slave device. No additional connection procedure is required. The slave device can instantaneously send an encrypted EIR to the master device. Then the master device sends *Inquiry* packet again to solicit an EIR from the slave device. The EIR data is encrypted by the slave with the public key of master and the master device recovers the original data with its private key. It is unlikely that an unintended user overhears or manipulates the EIR data in the middle of two devices on account of SSP. The overall data protection procedure is presented in Fig. 3.



(a) Data Delivery Delay vs Number of Nodes

(b) Power Consumption vs Number of Nodes

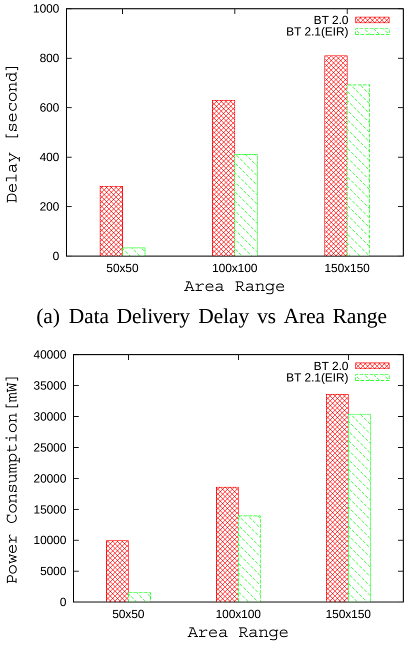
Fig. 5. Impacts of Number of Nodes



(a) Data Delivery Delay vs Speed of Nodes

(b) Power Consumption vs Speed of Nodes

Fig. 6. Impacts of Speed of Nodes



(a) Data Delivery Delay vs Area Range

(b) Power Consumption vs Area Range

Fig. 7. Impacts of Area Range

V. Simulation

A. Simulation Environment

We use the NS-2 version 2.9[2] with UCBT[3] to evaluate our new system. UCBT is a public, open Bluetooth Simulator and implements the major Bluetooth protocols such as baseband, LMP, L2CAP, and BNEP. The specification of Bluetooth version 2.1 has been published lately; therefore, UCBT does not yet have EIR and SSP. We implemented these features into UCBT so that it supports the new features.

B. Simulation Scenario

The purpose of our new scheme is to quickly deliver urgent and small data. We do not address the dissemination of large amounts of data as medical monitoring applications only involve short data packets. There are three kinds of nodes: patient, collection center, and nurses. The patient node is the source of the emergency data. The collection center is the destination; it collects the emergency data. In our scenario, these two nodes are static and positioned on each side of the simulation area. Other nodes are randomly placed and mobile. They emulate intermediate data carrying and forwarding agents such as nurse nodes. There are two types of nurse nodes. A master nurse tries to receive EIR data from slave nurses. A slave nurse keeps propagating EIR data to master nurses. Initially every nurse is a master and keeps performing *Inquiry Procedure* until receiving EIR data. Once a master nurse obtains EIR data, the node becomes a slave and spreads EIR data over the network.

Sensors on a human body keep monitoring patient's status and collecting data. A Bluetooth equipped device (*gateway*) on the patient gathers all of the data from sensors. If one of the sensed values is over a predefined threshold, it means the patient needs emergency care. The emergency is propagated by peer-to-peer forwarding. Nurses participate in the P2P transfer by continuously monitoring patients with a Bluetooth equipped device. Fig. 4 presents the scenario.

The simulation area is bounded. If a mobile node reaches the border, it inverts direction. We measure two metrics, data delivery delay and power consumption. The delay measurement starts as a patient node turns on the emergency alarm and put its physiological data in an EIR packet. The measurement ends when a data collection node receives the emergency data. Power consumption is the total consumed power (by all nodes during the emergency delivery). We calculate the energy consumption in mW by counting the number of packet transmissions and considering each state of nodes. According to [2], the power consumption for each action and state are $C_{inq} = 231mW$, $C_{idle} = 6.6mW$, $C_{scan} = 139mW$, $C_{data} = 181mW$. We make 30 simulation runs for each experiment and calculate the average for each result.

VI. Evaluation

In this section, we evaluate our system with three sets of experiments. Each experiment corresponds to different number of nodes, speed, and coverage area.

A. Impacts of Number of Nodes

In this simulation, we change the number of nodes to examine its effects on overall delay and power consumption. The speed of a node is fixed to $1m/s$ and the simulation

[2] http://wwwisi.edu/nsnam/ns/

[3] http://www.ececs.uc.edu/c̃dmc/ucbt/

area is $50 \times 50m^2$. Fig. 5 shows that as the number of nodes increases, delivery delay decreases in both cases. This is because more nodes cooperate to deliver the data, accelerating data propagation. Bluetooth version 2.0 takes a lot more time to deliver a packet than the new Bluetooth version 2.1, mainly due to connection set up delays. Every time a device sends data, the two connection procedures, *Inquiry* and *Paging Procedure*, are required. The new version tries to make a connection only when a device does not have a public key for a potential slave device. Once a master device has exchanged its public key, it immediately downloads the data using EIR. That is why the EIR based data delivery results in shorter delay. For this reason, as Fig. 5(b) shows, EIR consumes a much smaller amount of energy compared to Bluetooth 2.0. Nodes using Bluetooth 2.0 send *Paging* packets and *Paging Response* packet during the *Paging Procedure*. Power consumption decreases as the population of nodes grows. It is because when the number of nodes goes up, the total time spent for data delivery is reduced, which is why less power is consumed.

B. Impacts of Node Speed

In this section we vary the speed of mobile nodes. We have 30 nodes in this experiment and the area is $50 \times 50m^2$. Fig. 6 shows that as the node speed increases, data delivery delay decreases. It is likely that a mobile node makes contacts with more nodes with high mobility. It means that the emergency data is quickly propagated on the area and it reduces the data delivery delay in the end. In Bluetooth 2.0 networks, the delivery delay is decreased from 370.92 seconds to 257.28 seconds with node speed 0.5 and $1.25m/s$ respectively. EIR reduces the delay from 81.41 to 43.52 seconds – almost by half. The direction of node movement is random and the fast mobility pattern helps the data propagation over the entire networks. Power consumption is reduced as overall delay is diminished.

C. Impacts of Area Range

We change the simulation area range. The number of nodes is 30 and node speed is fixed at $1m/s$. Fig. 7 shows that again EIR based data delivery reduces the data delivery delay in each case. The difference of delay and power consumption becomes smaller as the simulation range increases. The differences are 249.85, 218.58, 118.32 seconds with 50×50, 100×100, $150 \times 150m^2$, respectively. In a large area, it is more likely that data is delivered by the node's movement instead of peer-to-peer forwarding. However, if node density is sufficiently high, EIR significantly decreases the data delivery delay by fast peer-to-peer communication.

VII. Conclusion

In this paper, we have proposed a new data dissemination system using the new Bluetooth version 2.1. We use two new features of the version. *Extended Inquiry Response (EIR)* allows us to send data without connection establishment stages and it considerably mitigates the latency problem of Bluetooth based wireless networks. *Secure Simple Paring (SSP)* gives us a secure data protection mechanism for EIR. Extensive simulation results show that the new version significantly improves data delivery and power consumption. Using the proposed mechanism, Bluetooth becomes practical also in emergency and urgent data dissemination environments. In the future, we plan to test Bluetooth 2.1 based data delivery system in a real testbed once dongles and smart phones equipped with Bluetooth 2.1 are available.

References

[1] Bluetooth SIG Bluetooth Specification 2.1.

[2] Juan-Carlos Cano, Jose-Manuel Cano Eva Gonzalez, and Carlos Calafate Pietro Manzoni. Evaluation of the energetic impact of bluetooth low-power modes for ubiquitous computing applications. *PE-WASUN '06*, Oct. 2006.

[3] Chandrashekhar Dethe, Digambar Wakde, and Chandrakant Jaybhaye. Bluetooth based sensor networks issues and techniques. *AMS '07*, March 2007.

[4] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22:644–654, Nov. 1976.

[5] Tia Gao, Mammara Massey, Leo Selavo, Matt Welsh, and Majid Sarrafzadeh. Participatory user centered design techniques for a large scale ad-hoc health information system. *HealthNet '07*, June 2007.

[6] US Census Bureau. 2003 Service Annual Survey. Health-Care and Social Assistance Services. http://www.census.gov/svsd/www/sas62-1.pdf.

[7] Sewook Jung, Alexander Chang, and Mario Gerla. Comparisons of zigbee personal area network interconnection methods. *The IEEE International Symposium on Wireless Communication Systems(ISWCS)*, Oct. 2007.

[8] Sewook Jung, Uichin Lee, Alexander Chang, Daeki Cho, and Mario Gerla. Bluetorrent: Cooperative content sharing for bluetooth users. *Percom 2007*, March 2007.

[9] Naoto Kimura and Shahram Latifi. A survey on data compression in wireless sensor networks. *ITCC '05*, April 2005.

[10] Darok Kirovski, Nuria Oliver, Mike Sinclair, and Desney Tan. Health-os: A position paper. *HealthNet '07*, June 2007.

[11] Srdjan Krco. Bluetooth based wireless sensor networks-implementation issues and solutions. *10th TELECOMUNICATIONS FORUM(TELEFOR2002)*, Nov. 2002.

[12] Martin Leopold, Mads Bondo DydensBorg, and Philippe Bonnet. Bluetooth and sensor networks: A reality check. *SenSys '03*, Nov. 2003.

[13] Lena Mamykina and Elizabeth D. Mynatt. Invstigating and supporting health management practices of individuals with diabetes. *HealthNet '07*, June 2007.

[14] Anirudh Natarajan, Mehul Motani, Buddhika de Silva, Kok-Kiong Yap, and K. C. Chua. Investigating network architectures for body sensor networks. *HealthNet '07*, June 2007.

[15] Benny P.L.Lo, Surapa Thiemjarus, Rachel King, and Guang-Zhong Yang. Body sensor network - a wireless sensor platform for pervasive healthcare monitoring. *PERVASIVE 2005*, May 2005.