A Real-time Fault Tolerant Intra-body Network

Sanjeev Baskiyar, Ph.D.
Assistant Professor
Dept. of Comp. Sci. & Soft. Eng.
Auburn University
Auburn, AL 36849
baskiyar@eng.auburn.edu

Abstract

This paper designs an intra-body network (IBN) of nodes, consisting of small sensors and processing elements (SPEs) placed at different locations within the body and a Personal Digital Assistant placed externally but in close proximity to the body. The sensors measure specific physiological attributes such as electrophysiological and biochemical changes in the myocardium (action potentials of cells), glucose level, blood viscosity etc. and forward them to the processing element. Communication protocols for configuration and data access protocols are proposed. The privacy of the IBN data, fault tolerance and real-time data acquisition are addressed.

Keywords: Intra-body, implant, sensor, bio-sensor, wireless, network.

1 Introduction

The design of an intra-body network (IBN) of nodes, consisting of small SPEs (sensors and processing elements) placed at different locations within the body and a Personal Digital Assistant placed externally but in close proximity to the body has been addressed. The sensors measure specific physiological attributes such as electrophysiological and biochemical changes in the myocardium (action potentials of cells), glucose level, blood viscosity etc. and forward them to the processing element. The processing element communicates the data to the PDA. The data is evaluated at the PDA and can be relayed to nearby hospitals for urgent medical assistance. With the availability of small sized, low priced chips, we foresee the commercial viability of such systems. Also, it is projected that with the advent of nano-technology lightweight, low power, macro intelligent sensors with reasonable processing power will be available in the near future. Such intelligent sensors can aid in the prediction of the onset of (a) heart attacks via electrophysiological and biochemical changes in the myocardium (e.g. via signature waveforms of the action potentials measured using a laser) (b) stroke via measurements of blood viscosity (c) abnormal glucose levels (*real-time* insulin treatment control loop) (d) preeclampsia etc. An intra-body network can also provide computational support for artificial limb responses, hearing and vision for the impaired, and imaging for diagnosis and surgery. An embedded multiprocessor system that can be used to interface with a motor to aid paraplegics walk has been visualized [5]. Because of distributed weight, it is easier to use a multiprocessor system for intra-body applications rather than a single processor system. We anticipate that this work will lead to products that will enable senior citizens receive emergency help via automatic monitoring of their physiological system. Such distributed intelligent sensors can also be employed in the exploration of seismic sites, caves, tunnels, deep oceans and surveillance. The Berkeley smart sensor dust [8] project visualizes intelligent sensors mounted on micro-helicopters that can be used for the above purposes. Figure 2 shows a sensor that was actually implanted in a human body [17] (Dr. K. Warwick, Director of Cybernetics, University of Reading) with implanted chip in body; it is expected that in the near future the size will be much smaller than shown.

The organization of this paper is as follows. Section 2 surveys background work, Section 3 discusses the design of the network and in Section 4 the results are summarized and future work is discussed.

2. Background

The BodyLan [6] project obtained body parameters such as temperature and oximetric data from probes

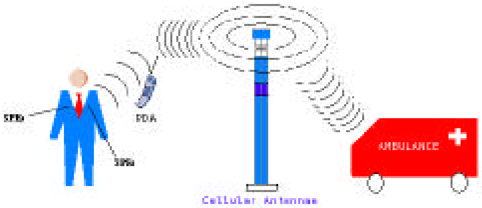


Fig. 1. An application of intra-body networks

external to the body and transmitted them to a control station. However, this paper deals with the measurement of parameters, such as action potential of heart cells, glucose/insulin levels and blood viscosity for which currently accurate external measurement techniques are unavailable and *transmission through tissue* is required. Communication within the intra-body network may be via use of the Personal Area Network (PAN) or very low power Bluetooth standards within the safe RF guidelines as per FCC/FDA. FCC limits RF exposure to the general population to $1mw/cm^2$ of tissue for 30 minutes (FCC OET Bulletin 56, Aug 1999) limiting the RF power transmitted by an embedded transmitter. The maximum traversal needed for intra-body communication is less than 2.8m, the upper limit on human height. Also, data rate will be in bursts shorter than a second rather than in minutes, allowing a flexible range of safe operation.

Zimmerman's [19] PAN uses the human body as a conduit of information. Electronic devices placed on and near the body modulate electric fields inducing small currents within the body. Data connections are established by touch or proximity. Communication is via near-field capacitive coupling, and negligible energy is radiated out allowing global licensed operation.

The communication range of PANs called *pico-cells* [20] is within the spatial interaction volume of humans (< 10m), which accommodates the small battery energy of small portable devices. Bluetooth uses a channel capacity of 1Mbps at 2.4-2.7 GHz—class 3 uses 1mw of power. PAN used 30V with currents in the order of picoamps, with data rate 2400bps at 430Khz. PAN transmission is well within the safety limits, demonstrating the feasibility of transmission through tissue. Recently intra-body communication with a data rate of 56 Kbps has been demonstrated [14][15][3].

Most experimental medical systems employ wireless data acquisition devices [1][4][18] and wireless data presentation devices, such as palmtop PCs, pagers, and cellular phones [2]. However, with further development of low-power digital signal processing chips and biosensor technology, it will be possible to implement *intelligent* personal health monitoring devices as part of personal mobile devices [7].

Jovanov. et. al [11] presented a prototype wireless intelligent sensor using a low-power micro-controller and a DSP-based personal server. Individual sensors monitor specific physiological signals (such as ECG, EEG^{+}, GSR^{++}), which they communicate among themselves and to a personal server. The personal server integrates information from the sensors and communicates with the outside world as a standard mobile unit. They address hardware aspects, investigating design trade-offs among processing power, battery life and storage for medical applications. *However, the protocols to configure and communicate among sensors and the personal server were not addressed.*

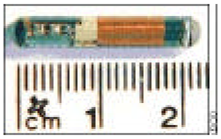


Fig. 2. An implant with sensors and chips

Real-time applications in a wireless environment have relied on existing standard wireless Media-Access Control (MAC) protocols (such as CDPD, CDMA, GSM) to transfer data. Markowski and Sethi [12] developed a MAC protocol that transmits data in a wireless environment while considering the temporal deadlines of applications. *However, there is dearth of work that support features similar to that of the IBN and provide real-time transfer of data in wireless intra-body media.* The communication of the IBN with the external world can be performed using various ad-hoc wireless routing protocols such as dynamic source routing protocol [9], cluster-based routing protocol [13], zone-based hierarchical link-state routing protocol [10], etc. However, wireless communication within the IBN is a single hop, real-time communication between fixed hosts making routing issues irrelevant. If one uses extremely low power such that the propagation distance is very small, routing may be required.

.

3. Design

All nodes (SPEs) are assigned unique-ids within the IBN. Nodes generate data, which they can communicate to other nodes or to the PDA. To facilitate fault-tolerance, two to three SPEs (also called peer nodes) are used for each measured attribute. Below we outline the protocol stack of the nodes at the

---

[+] Electro-Encephalogram

[++] Galvanic Skin Response

application layer, which supports configuration and data acquisition in the IBN.

Data layer	Bio-sensor data		
Attribute layer	Polling buffer	Data buffer	Periodic buffer
	Polling session runner	Control session runner	Periodic session runner
Node layer	Packet handler		
	Address handler		

Fig. 3: Network layers at the node

3.1 Protocol stack

For modularity, we use a *3*-layered protocol stack at the nodes and the PDA, used as an application above the network layer. The layers in the stack are named *data layer*, *attribute layer* and *node layer* as shown in Figs. 3 and 4. Encapsulation is supported at each layer and communication is on a peer-to-peer basis. A network monitor in the data layer of the PDA monitors network congestion and node failures. Actions in the network are initiated by communicating packets.

Data layer	User layer	
	Network monitor	
	Attribute DB	Faulty packet store
	Regular/Obituary packet handler	
Attribute layer	Attribute layer	
Node layer	Node runners	
	Packet handler	
	Address handler	

Fig. 4: Network layers at the PDA

3.2 Data acquisition modes

PDAs acquire data via three modes: *polling*, *periodic* and *refresh*. Nodes are set in a mode by control packets listed in Table 1. In the *polling mode*, a PDA may send a Read packet (*R-pkt*) to a node, to know the latest value of a physiological attribute. The polling mode minimizes network traffic since data is communicated only upon request. In the *periodic mode*, nodes send sensor data periodically to the PDA at a frequency that can be set by a control packet. The *refresh mode* can operate in parallel to the *polling* or the *periodic modes*. The refresh mode is simply a special case of the *polling* mode—specific node(s) are polled to send their *latest data immediately* and thereafter return to their previous mode.

3.3 Security

Three levels of passwords *user password*, *super-user* and *privileged* are used. A *user* can query and receive attributes; a *super-user* can change the frequency of the *periodic* mode and read and reply to configuration information. The functions to change network configuration are reserved to the highest level, called the *privileged level*. All three passwords are encrypted and stored in the nodes. All packets communicated must have an encrypted password appropriate to the usage mode, which must be validated at the node or the PDA. In the *user mode*, a PDA can change user mode password, and read and modify the *data acquisition mode* and *update frequency* of the *periodic mode*. More than one PDA can be used in user mode. In the super-user mode, in addition to the user mode functions, one can also change the *super-user mode password* and reset *user mode passwords* via packets. In the *privileged mode*, a PDA can modify network configurations, including turning nodes on and off. In the privileged mode one can also reset the *super-user mode password*, and modify the *privileged user password* and read and modify *net time*. For security and correctness of operation only one PDA is allowed each in the super-user and privileged modes. Security can be enhanced by encryption and or frequency hopping. Clearly, they have an impact on performance, battery life etc. which must be studied.

3.4 Communication

Each node has a unique *id* that is a concatenation of *group-id* and *local-id*. The *group-id* refers to a peer group of nodes that measure the same attribute. For example *4*-bits can be allocated for *group-id* and *3* for *local-id* providing $2^4-2= 14$ unique attribute representations and $2^3 - 2 = 6$ local-ids per group. (As usual a pattern of all *1s* is used for multicast and all *0*'s for self-reference.) An *IBN-id*, perhaps a social security number, unique to every individual, identifies the IBN.

Group-id	Local-id

Fig. 5: *Node-id*

Ten packets configure and operate the IBN as shown in Table 1. The fields in different packets have some combination of the following: source and destination addresses, packet-id, appropriate passwords, timestamps, network time, update frequency, turn off/on flag, data and data acquisition mode.

3.5 Node functions

Time last R-pkt received

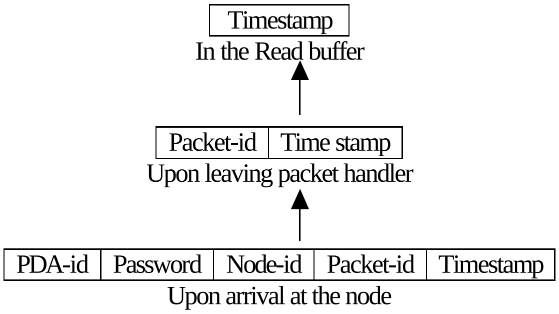
a. Read Buffer

Data	Timestamp

b. Data Buffer/*D-pkt* /Periodic Buffer

Fig 6: Attribute layer in the node

The data layer receives data from bio-sensors, time stamps and periodically forwards them to the data buffer. In addition to other considerations, the expected rate of change of the specific sensor data is considered in deciding the forwarding period. The address handler verifies the address and password of packets. After verification the address and passwords are stripped and the packet is forwarded to the packet handler.



Timestamp

In the Read buffer

Packet-id	Time stamp

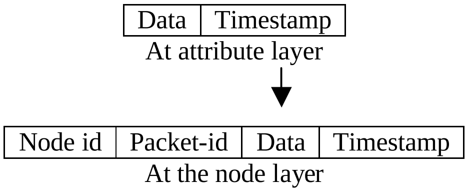
Upon leaving packet handler

PDA-id	Password	Node-id	Packet-id	Timestamp

Upon arrival at the node

Fig. 7: *R-pkt* transition at the SPE

The packet handler, depending upon the packet-id, forwards the packet to the polling, control or periodic session runner. An *R-pkt* forwarded to the polling session runner is time-stamped and the polling buffer is overwritten with it. The polling session runner responds by forwarding the data (*D-pkt)* from the data buffer to the address handler, which appends the *node-id* to the outgoing *D-pkt*. The transformations of an *R-pkt* are illustrated in Fig. 7.



Data	Timestamp

At attribute layer

Node id	Packet-id	Data	Timestamp

At the node layer

Fig. 8: *D-pkt* transition at the SPE

In the periodic mode, the attribute layer sends *D-pkts* to the periodic session runner, which forwards them to the address handlers for dispatch in a similar fashion. The *periodic session runner* stores notification of such sends into the *periodic buffer*. The transformation of each *D-pkt* traveling from the attribute layer to the node layer is shown in Fig. 8. The *control session runner* maintains Node Configuration of the node as shown in Fig. 9.

Mode: Polling/Periodic/Refresh			
Timer	Update frequency	Time	On/Off

Fig 9: Node configuration

3.6 PDA functions

At the PDA the *address handler* rejects packets not addressed to the IBN (using social security number) for which the PDA has been configured or those with invalid node addresses. It strips addresses in incoming packets before forwarding them to packet handlers. It also inserts destination addresses in outgoing packets. The *packet handler* forwards incoming packets to appropriate node runners; it inserts *packet-id* field in outgoing packets. Concurrently executing *node runners* (for each node) allow concurrent communication with multiple nodes. The *node runner* (a) maintains configuration information and the latest *D-pkt* received from the node (b) appends *attribute id* to incoming *D-pkts* before forwarding them to the attribute layer (c) generates *R-pkts* and other configuration packets and (d) runs a watchdog timer upon sending an *R-pkt* to a node. If it does not receive a *D-pkt* from the node within a predetermined deadline, it resends the *R-pkt*. If after *x* resends, it does not receive any *D-pkt*, it surmises that either the network may be congested or the node may be faulty. It does so also when it does not receive *D-pkts* periodically from the nodes during the *periodic mode.* In such instances, it generates an obituary *D-pkt*, with *timestamp* of the last valid *D-pkt* it received from the node. The *packet validity* bit is set to *false* for obituary *D-pkts*. The node runner then appends the *node id* and *attribute id*.

Node-id1	Mode	Data	Timestamp	Update Frequency

Fig. 10: Node-Info database at PDA

The Regular/Obituary packet handler forwards *D-pkts* to the attribute database or the faulty packet-store (FPS) depending upon the *packet validity* bit. The *attribute layer* stores data for every attribute; usually the number of entries per attribute equals the number of sensors used for that attribute. The transition of a *D-pkt* is shown in Fig. 11.

The *network monitor* responds to queries from user layer for attribute values. It responds with the latest value of the attribute in the attribute database, if found. If it cannot find, any entry in the attribute database, it checks for an entry in the FPS. If in the FPS sufficient entries, later than the last entry in the attribute database are found, the corresponding node is flagged faulty; otherwise it surmises that the IBN is congested. A faulty node or network congestion is conveyed to the user layer.

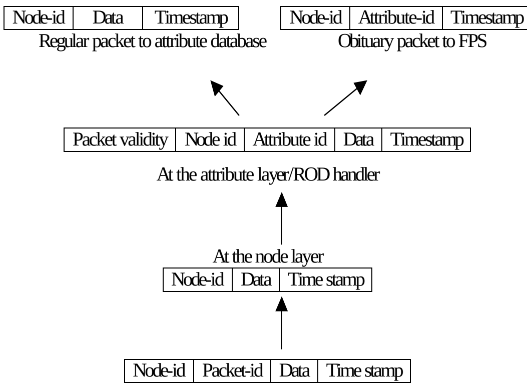


Fig. 11: *D-pkt* transition in the PDA

4. Conclusion

This paper designed an intra-body network consisting bio-sensors that can be implanted and PDAs. Communication protocols to configure and operate the network have been developed. Future work will involve software simulation of the design, performance analysis, encryption techniques for such a lightweight system and hardware prototyping.

References

[1] J.Bai, Y.Zhang, D.Shen, L.Wen, C.Ding, Z.Cui, F.Tian, B.Yu, B.Dai, J.Zhang, “A Portable ECG and Blood Pressure Telemonitoring System,” *IEEE Engineering in Medicine and Biology*, pp. 63-70, July-August, 1999.

[2] S.Barro, J.Presedo, D.Castro, M.Fernández-Delgado, S.Fraga, M.Lama and J.Vila., “Intelligent Telemonitoring of Critical Care Patients,” *IEEE Engineering in Medicine and Biology*, pp. 80-88, July-August 1999.

[3] T. Barber Jr, P. Carvey, A. Chandrakasan, “Designing for Wireless LAN communications,” *IEEE Circuits and Devices Magazine*, v 12-4, July 1996.

[4] Cleveland Medical Devices, http://www.clevemed.com

[5] S. Crowe, “Study to help paraplegics walk,” University of Sydney News, http://www.usyd.edu.au/publications/news/2K0406News/0604_walk.html

[6] M.B. Debski, *The Snap! Toolkit for Developing Sensor Networks and its Applications to Cross-Country Skiing*, BS/ME-EECS thesis, http://www.media.mit.edu/pia/Research/ESP

[7] K.A.Delin and S.P.Jackson, “Sensor Web for In-Situ Exploration of Gaseous Bio-signatures,” *Proceedings of the 2000 IEEE Aerospace Conference*, Big Sky, Montana, March 1999.

[8] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, “System Architecture Directions for Networked Sensors,” 2000, http://www.cs.berkeley.edu/~awoo/smartdust

[9] B.D.Johnson, D.A. Maltz, “Dynamic Source Routing in Ad-hoc Networks,” *Mobile Computing*, pp. 152-81, 1996.

[10] M.Joa-Ng and I.T.Lu, “A Peer-to-Peer zone-based two-level link state routing for mobile Ad Hoc Networks,” *IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks*, pp.1415-25, Aug. 1999.

[11] E.Jovanove, P.John, R.Dejan, K.Krishna, M.Thomas and A.Reza, “Wireless Personal Area Networks in Telemedical Environment,” *Proceedings of the 2000 IEEE-EMBS International Conference on Information Technology Applications in Biomedicine*, pp.22-27, 2000.

[12] M.J.Markowski and A.S.Sethi, “Fully Distributed Wireless Transmission of Heterogeneous Real-Time Data,” *48th IEEE Vehicular Technology Conference*, v 2, pp. 1439-1442, 1998.

[13] J.Mingliang, L.Jinyang, Y.C.Tay, “Cluster Based Routing Protocol,” *IETF Draft*, August 1999.

[14] K. Partridge, L. Arnstein, G. Borriello and T. Whitted, “ Fast Intra-body Signaling,” *Wireless and Mobile Computer Systems and Applications*, Monterey, CA, Dec 2000.

[15] K. Partridge, B. Dahlquist, A. Veiseh, A. Cain, J. Goldberg, A. Foreman and G. Borriello, "Empirical Measurements of Intrabody Communication Performance under Varied Physical Configurations," *User Interface Software & Technology*, 2001.

[16] RFC: 2002, Network Working Group, IBM, 1996.

[17] K. Warwick, *CNN Interview*, http://www.cnn.com/TECH/computing/9901/14/chipman.idg/

[18] Wearable Polysomnograph, Advanced Medical Electronics Corporation, http://www.ame-corp.com/Wearable_Polysomnograph.htm

[19] T.G.Zimmerman, "Personal Area Networks: Near-field intrabody communication," *IBM Systems Journal*, v 35, n 3-4, pp. 609-617, 1996.

[20] T.G.Zimmerman, "Wireless Networked Digital Devices: A New Paradigm for Computing and Communication," *IBM Systems Journal*, v 38, n 4, pp.566-574, 1999.

Acknowledgements

The author wishes to thank Dr. S. Fickas, Department of Computer Science, University of Oregon, group faculty meetings with whom at Auburn University initiated the ideas in this paper. Special thanks are due to Dr. W. E. Smith, Department of Bio-medical Engineering at the University of Alabama, Birmingham for informative discussions. The author would like to acknowledge and thank research assistant N. Meghanathan who participated in the initial phase of this study. A part of this work was supported by an internal grant from the Department of Computer Science and Software Engineering, Auburn University.

Packet-id	Packet name	Mode;minm. password level for access	Function
0	Read pkt (*R-pkt*)	Polling; User	Request data of nodes
1	Data pkt (*D-pkt*)	Any; User	Used by nodes to send data
2	Read/Set time pkt	Any; User/Privileged	Read/Set network time
3	Read mode pkt	Any; User	Read mode
4	Set user password pkt	Any; User	Set user password
5	Set super-user password pkt	Any; Super-user	Set super-user password
6	Read Configuration pkt	Any; Super-user	Request/Send configuration
7	Set configuration pkt	Any; Privileged	Set privileged password, configuration/mode
8	Read/Set update-frequency pkt	Any; User/Super-user	Read/Set update frequency
9	Refresh pkt	Any; User	Send latest data immediately

Table 1. Communicating packets