

A Protocol for Automatic Sensor Detection and Identification in a Wireless Biodevice Network

Kent L. Jones
Dept. of Math and CS
Whitworth College
Spokane, WA 99251
(509)-466-1000
kjones@whitworth.edu

Mark L. Manwaring, Ph.D.
School of Elect. Eng. and CS
Washington State University
Pullman, WA 99164-2752
(509)-335-5223
manwarin@eecs.wsu.edu

Kim H. Manwaring, M.D.
Phoenix Children's Hospital
Phoenix, AZ

Abstract

As transducer devices continue to shrink in size, they become increasingly suitable for implantation, enabling the creation of an exciting new class of wireless biodevice networks. A biodevice consists of sensor(s), actuator(s), and microcontroller(s) used to monitor and control biological processes. A wireless biodevice uses the principle of electromagnetic induction to receive power and data communications from an external interrogator. Multiple wireless biodevices and interrogator devices may be organized into a wireless instrumentation network (WIN). This paper starts by examining the motivations for WIN design, followed by a description of the proposed WIN architecture for subcutaneously implanted biodevices. Next, the design of a data link layer protocol for the automatic detection and identification of implanted biodevices is described and analyzed. Finally, the advantages and disadvantages of the network and protocol are discussed.

1. Introduction

The traditional way to build medical biodevice networks requires the attachment of an array of devices and sensors to a central data acquisition/control unit via a network of wires. While wires may be viewed as reliable links for the delivery of power and data, they can also pose a serious safety hazard. Transcutaneous wires limit patient mobility, provide paths for infection, and pose a logistical nightmare for medical personnel who must deal with them. Furthermore, as biodevices continue to shrink, the wires supplying power and data communications will limit the number biodevices which may be implanted thus eliminating the benefits of sensor fusion [1]. These problems are especially troublesome when measurements need to be taken over extended periods of time.

Eliminating the wires, which supply power and transmit data, solves many of these problems [2]. Wires are eliminated by direct implantation of the biodevices. This is possible because in recent years, transducer devices have appeared which are very small and thus suitable for implantation. (Some examples of sensors include pressure, temperature, chemical, and flow rate transducers. Examples of actuators include cochlear, muscular, and nerve stimulator transducers.) Transducers may be combined with tiny microcontrollers to allow for sophisticated data collection and processing. Finally an electronic circuit, used to supply power and data to the microcontroller and transducers, completes the wireless biodevice package. Many of the issues involved in supplying power and data communications to a single implanted wireless biodevice

have been described previously [2]. This paper considers the issues that arise when multiple subcutaneously implanted wireless biodevices are controlled via a network of interrogators.

2. Proposed Biodevice Network Architecture

Although many different wireless biodevice instrumentation network architectures are possible, a hierarchical network design seems to be the most suitable for a biomedical wireless instrumentation network (WIN). The hierarchical approach, inspired by the design of biological nervous systems, allows for the main controller to control biodevices via a sub-network of intermediate controllers (proxy controllers) at a high level of abstraction. A simple WIN network is shown in Figure 1.

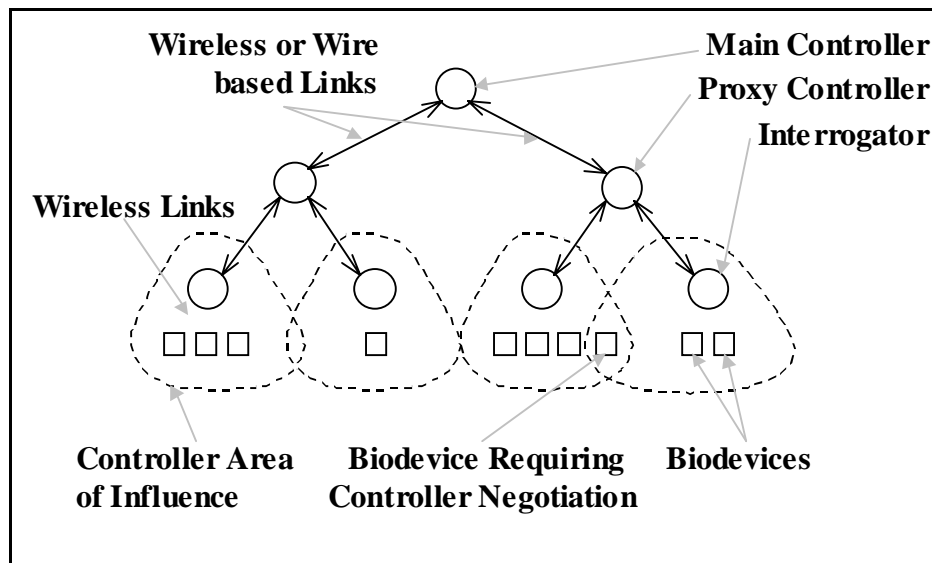


Figure 1. A Wireless Instrumentation Network (WIN)

2.1 Network Concepts

The WIN proposal calls for a single main controller capable of controlling multiple sub-controllers (i.e. proxies), in turn, each proxy must be capable of controlling sub-proxies and or interrogator devices. Higher degrees of autonomy and control belong to devices closer to the base of the WIN hierarchy tree.

The design of WIN takes into account the fact that many present and future biodevices and proxies will rely on both wire and wireless links. While transcutaneous, inductive, wireless links may pose less of a health hazard than transcutaneous wired links, unfortunately, inductive wireless links also degrade the reliability and bandwidth of the connection between the biodevices and proxies. This illustrates the need for a lightweight, fast protocol with error detection and correction. There are fewer logistical, health, and power constraints on the interrogator/proxy links, thus these links can consist of high quality wired or wireless links.

In the current research project, there is no need for network tree depths beyond 2 or 3 levels in fact, initial implementations will typically have only one main controller, one interrogator, and a few biodevices. However, it is not hard to foresee the need to add multiple proxies and multiple interrogators. WIN's hierarchical architecture avoids constraining future network designs to a limited number of biodevices and/or interrogators.

2.2 Network Operation

The proposed WIN network protocol will function in an object-oriented, inheritance based fashion. Devices higher in the network function at a higher degree of control abstraction, while devices lower in the network inherit and expand upon the capabilities of the higher level devices. This allows the network to be easily configured and adapted to different situations. The proposed WIN network architecture could provide the ability to control/query a large number of advanced biodevices, each of which may have widely varying tasks, and at the same time reduces the complexity required to route messages through the network. Complexity is reduced because proxies and interrogators can be programmed to function with a high degree of autonomy.

All devices in a WIN function in a command/response mode. The WIN forms a tree with controllers at the base of the tree, proxies at the branching nodes of the tree, and interrogators and biodevices at the leaves of the tree. Typically, commands start at a high level of abstraction at the base of a WIN tree or sub-tree. As the commands flow towards the leaves of the tree, at each level, the commands acquire the information necessary in order to be interpreted correctly by the network. Commands can originate from any controller device or proxy device. This restriction on the flow of commands results in a simpler routing mechanism for the network. Any coordination of biodevices can take place at the proxy level. Responses always flow from the leaves of the tree towards the base of the tree.

At the leaves of WIN, the interrogator devices supply power and control data communications with implanted biodevices. After the biodevices have completed their power-on cycle, the external interrogator devices automatically detect and assign a unique identification number to each biodevice within their range of control. If more than one interrogator attempts to control a given biodevice, the interrogators negotiate via their controller proxies in order to determine which interrogator will be assigned the device.

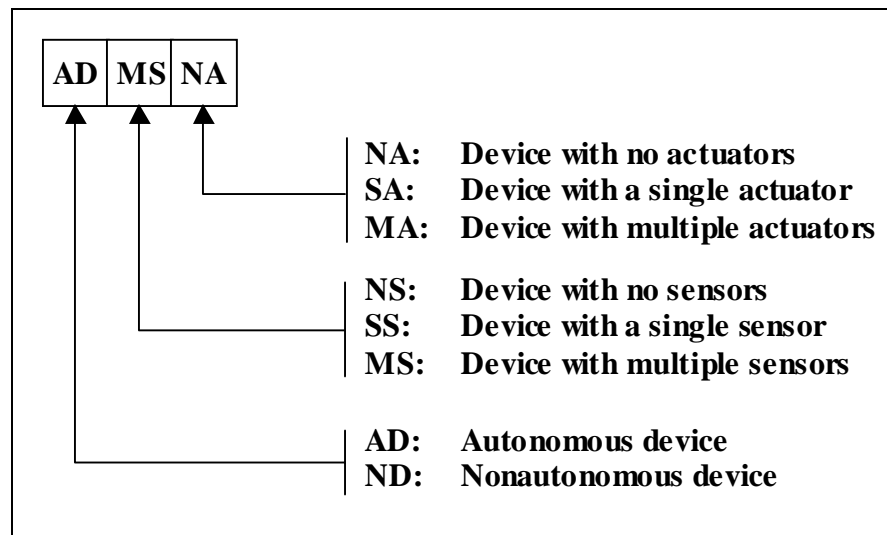


Figure 2. Example of the Biodevice Classification Scheme

After all devices have been assigned to an interrogator and given a unique identification number, the interrogators must determine the capabilities of each of the biodevices assigned to their control. The type of biodevice determines the type of communication that can take place with that biodevice. One possible biodevice classification scheme is shown in Figure 2. Biodevices are designated either as actuators, sensors or a combination of the two. The number of actuators or sensors is recorded for each biodevice. If a particular biodevice is designated as

simply a sensor, the interrogator collects the information at regular intervals and routes this information up to the appropriate proxy. If a given biodevice is designated as an actuator, then a proxy may download a control schedule to the biodevice's microcontroller via the interrogator. Such a biodevice is called an autonomous biodevice.

Biodevices can run programs/schedules autonomously only if requested and authenticated periodically by their interrogator. Proxies and interrogators communicate via reliable, dedicated links. Proxies and biodevices typically communicate via unreliable wireless links.

Because the network architecture provides for autonomous proxies, not all commands need to travel from the top of the network clear to the bottom (and vice versa). Proxies higher up in the network tree can connect to and control lower level autonomous proxies with a higher level of abstraction than possible otherwise. In some ways this approach is similar in concept to a layered network architecture, where each layer expands upon the information supplied by the previous layer [3].

Periodically each interrogator device polls its assigned biodevices in order to determine if they are still functional. During the same polling period, any new biodevices are detected, assigned a unique identification number, interrogated to determine their functionality, and finally assigned an interrogator device. These newly detected biodevices are then added to property list of the appropriate proxy devices. If an interrogator determines a given biodevice is no longer functional (i.e. not responding) then, the interrogator relays this information to the appropriate proxy and the device is removed from the property list of the proxy device. The main controller device communicates with a user interface device, which communicates with a human. The human can access the property lists of any specific proxy devices as well as specify control programs for actuators, data collection schedules for sensors, and data logging activities.

The data collected from the WIN system must be highly reliable. Medical personnel assess the status of patients based on the data collected by the WIN system. Because of this fact, the interrogator devices should only accept data if the probability of error is extremely low. If a biodevice is not working properly this information must be made available to the human responsible for the operation of the WIN system.

3. Biodevice Identification Protocol

In standard biodevice networks, each biodevice is easily located and identified due to the fact it is connected to the controller via a wire. In WINs, the biodevices are completely implanted, making it much more difficult to ascertain the number of devices that have been placed in a given patient. In WINs, the communication process must be carefully orchestrated so the devices do not interfere with one another, thus, each device must be assigned a unique identifier so that the interrogator can tell it apart from the other biodevices, and ascertain what capabilities the given biodevice has.

There are a number of systems, commonly in use, which have some of the features or limitations similar to those described. For example, new computers have bus architectures that allow the operating system to automatically detect the addition or removal of hardware devices. Cellular phone networks use protocols that can automatically detect and identify individual telephones. On the Internet, computers are identified by unique IP addresses. Because biodevices must be very small, they have serious power and computational restrictions, furthermore, the use of induction as the medium for the exchange of power and data, places wireless biodevices in a completely different category. First of all the wireless portion of WINs are inherently more unreliable than typical wire or wireless networks. Secondly, the wide variety of medical sensors and actuators available makes it less feasible to reliably assign each sensor and actuator a unique id at the time of manufacture. Allowing the interrogator/controller to dynamically assign

biodevice ids seems like a more flexible approach. This would allow devices to be implanted and removed without changing the configuration of the software controlling the devices.

3.1 Protocol Concepts

This section describes and analyzes one of a number of data link protocols that are currently under investigation as potential device identification protocols. This particular protocol was chosen as a starting point because of its simplicity. Because the current generation of inductive wireless biodevices cannot listen to their own data transmissions, it is not possible to use standard collision detection protocols. Furthermore, because of the nature of WINs, the interrogators will control all conversations between biodevices and interrogators (i.e. the biodevices operate in command/response mode). Thus, the job of detecting collisions is shifted to the interrogator.

In this particular scheme, (which is similar to slotted aloha)[4,5], an interrogator will periodically attempt to identify all biodevices under its control. At the start of this period (device identification), the interrogator will command all of its biodevices to self-identify. This period consists of a number of time slots, and each biodevice waits a random number of slots before replying. Assuming that all biodevices reply with the same response code, after a single id period, the interrogator will not know exactly how many biodevices are under its control. This is because it does not know which replies were actually multiple devices replying in the same time slot. Thus, the id period must be repeated multiple times in order for the interrogator to have a high degree of confidence that it has actually detected the correct number of biodevices. Every time the interrogator detects a new maximum number of biodevices, it can instruct the biodevices to remember which slot they replied in. Once the interrogator has a high degree of confidence that the maximum number of biodevices have been detected, it can use these slot numbers as identification numbers for future command/response based communications. The interrogator can then query each of the biodevices in turn to determine their properties, and it can classify each identified biodevice according to capability. The command/response mode of the protocol is controlled either with a simple alternating bit protocol or with a more complex ARQ protocol.

3.2 Protocol Analysis

In order to simplify the first stage of protocol analysis, assume that the noise level on the link is negligible during the device identification period.

Assume that a particular interrogator has d biodevices assigned to it,

Let the device identification period consist of s time slots, and

Let r denote the number of slots in which the interrogator detects some response. A response could consist of a single biodevice's response, or a collision between multiple biodevices.

Let B equal the event that exactly r slots are detected.

To calculate $P(B)$, (i.e. the probability of event B), note that the number of ways to distribute d devices into exactly r slots is given by Stirling's numbers of the second kind [6, 7]:

$$\text{Number of } r\text{-partitions of } d = \left\{ \begin{matrix} d \\ r \end{matrix} \right\}$$

The number of ways to distribute r groups to s slots is given by:

$$\text{Number of } r\text{-permutations of } s \text{ distinct possible slot positions} = \left[\begin{matrix} s \\ r \end{matrix} \right] = \frac{s!}{(s-r)!}$$

Finally, the total number of possible outcomes for any given detection period is simply:

$$\text{Number of possible outcomes} = s^d$$

Thus, $P(B)$ is given by:

$$\text{Probability that exactly } r \text{ slots contain biodevice replies} = P(B) = \binom{d}{r} \binom{s}{r} \frac{1}{s^d}$$

In order to calculate the probability of event C , that is exactly d devices are observed, (i.e. $d = r$), note that the formula simplifies to:

$$P(C) = \binom{d}{d} \left(\frac{s^d}{(s-d)!} \right) \frac{1}{s^d} = \frac{s(s-1)(s-2)\dots(s-d+1)}{s^d}$$

Let N , $N \geq 1$, be the number of times the device identification protocol is re-run. Since the probability of not seeing all d devices on any given trial is $(1-P(C))$, the probability of actually seeing the exact number of devices at least one time out of N trials is $1-(1-P(C))^N$ thus, we can calculate how many times we must re-run the detection period in order to be as certain as we wish that we have seen the correct number of devices.

Although fairly simplistic, the analysis of this protocol forms the groundwork for a more advanced analysis of the protocol. For example, given the maximum number of devices (d) that an interrogator will ever control, and a function which measures the cost of re-running the protocol, (e.g. $\text{cost} = (s)(N)$), it is possible to determine the optimal ratio of slots (s) to retries (N) which will maximize the probability of seeing all of the devices (d) at least one time.

4. Conclusions

This paper described a network architecture for wireless instrumentation networks (WIN) and a protocol for dynamic biodevice detection and identification. The dynamic biodevice detection scheme was analyzed and a formula was determined which allows the calculation of confidence level that the correct number of biodevices are detected.

Future research topics include the analysis of alternate detection protocols – re-running the complete protocol each time seems wasteful. This is because after every detection period useful information is gained, (i.e. the interrogator at least will know that the actual number of biodevices is no less than the number of slots in which it received replies). The current analysis assumes that the noise levels are negligible during the device identification period. Future research will address noise levels during the device identification process.

The WIN architecture is unique in that it is designed to be scalable, adaptable and hierarchical. As biodevices continue to shrink in size, new methods for networking and controlling biodevices will need to be found.

-
- [1] Iyengar, S. S., L. Prasad, H. Min, *Advances in Distributed Sensor Technology*, Prentice Hall, 1995
 - [2] Mark L. Manwaring, Jones, Kent L., *Issues in Developing a Communication Protocol for Wireless (Implanted) Biodevices*, *Proceedings of the Ninth Annual IEEE Symp. Computer-Based Medical Systems*, IEEE CS Press, California, Jun. 1996
 - [3] Andrew S. Tanenbaum, *Computer Networks*, 3rd ed., Prentice Hall, Upper Saddle River, New Jersey, 1996
 - [4] Dimitri Bertsekas, Gallager, Robert, *Data Networks*, 2nd ed., Prentice Hall, Englewood Cliffs, New Jersey, 1992
 - [5] Gerard J. Holzmann, *Design and Validation of Computer Protocols*, Englewood Cliffs, New Jersey, 1991
 - [6] Martin Eisen, *Elementary Combinatorial Analysis*, Gordon and Breach, New York, New York 1969
 - [7] Bradley W. Jackson, Thoro, Dmitri, *Applied Combinatorics with Problem Solving*, Addison-Wesley, Reading Massachusetts, 1989