Distance Bounded Energy Detecting Ultra-wideband Impulse Radio Secure Protocol

Daniel S. Hedin, *Senior Member, IEEE*, Daniel T. Kollmann, *Member, IEEE*, Paul L. Gibson, *Member, IEEE,* Timothy H. Riehle, *Member, IEEE*, and Gregory J. Seifert, *Member, IEEE*

***Abstract*— We present a demonstration of a novel protocol for secure transmissions on a Ultra-wideband impulse radio that includes distance bounding. Distance bounding requires radios to be within a certain radius to communicate. This new protocol can be used in body area networks for medical devices where security is imperative. Many current wireless medical devices were not designed with security as a priority including devices that can be life threatening if controlled by a hacker. This protocol provides multiple levels of security including encryption and a distance bounding test to prevent long distance attacks.**

I. Introduction

There is an increased desire for body area sensor networks due to an aging population. According to the administration of aging, the older population numbered 39.6 million in 2009 and is estimated to be about 72.1 million in 2030 in the United States. They are seeking benefits such as improved health, lower health care costs, and improved quality of life.[1] The use of sensor technologies can be used to replace human monitoring in some cases, manage chronic disease therapies, and help identify problems before they become emergencies in other cases. The end result is fewer trips to the emergency room, better overall health since problems can be found earlier, and improved quality of life since elderly can live at home longer.[1] Increased use of body sensor networks is driving the need for improved wireless technologies. In order to satisfy the needs of non-invasive sensors, very low power wireless technologies are needed. While there are many different wireless technologies for body area networks such as Bluetooth and Zigbee, the wireless industry for medical applications is not mature.[2] An important aspect of medical sensors and electronic health data is privacy and security.[2–8] For example, there have been demonstrations of the ability of an adversary to control a popular insulin pump from a long distance through its wireless link.[9–11]

Ultra-wideband impulse radio (UWB-IR) technology has only been recently made available by the Federal Communications Commission (FCC) and can provide novel solutions for body area networks. UWB-IR technology has unique ranging aspects that are exploited to improve security in this protocol.[12] It can also be used in frequency bands not allowed by narrowband solutions. The technology for low power radios and microprocessors, due to improved silicon technologies, has dramatically increased the capabilities and miniaturization of sensors for health monitoring. These technologies have been used primarily for their ubiquity as opposed to being the optimum solution. The use of these technologies and more specifically the frequency spectrum that they occupy is increasing dramatically with smartphones and other mobile devices, wireless home networks, etc. causing increasing levels of interference. Another issue with utilizing standard wireless technologies in their current state is privacy and security. The radio technology proposed in this study provides a layer approach to security including encryption and distance bounding. The new design also offers a unique interference detection scheme that allows for real time pauses and resumption during interference in the middle of packet transfers. A secure link is necessary for patient protection for applications where the sensor is being used to directly provide therapy decisions such as a wireless link between a glucose sensor and an insulin pump in an artificial pancreas.

*Research supported by the National Institute of Diabetes and Digestive and Kidney Diseases grant: Application Number: 1 R43 DK096810-01A1.

D. S. Hedin, is with Advanced Medical Electronics, Maple Grove, MN55369 USA.

P. L. Gibson is with Advanced Medical Electronics, Maple Grove, MN55369 USA.

G. J. Seifert are with Advanced Medical Electronics, Maple Grove, MN55369 USA.

D. T. Kollmann is with Koronis Biomedical Technologies, Inc. Maple Grove, MN, 55369, USA.

T. H. Riehle is with Koronis Biomedical Technologies, Inc. Maple Grove, MN, 55369, USA.

II. Protocol And Radio Architecture

This paper demonstrates a protocol for a distance bounded UWB radio for body area networks. This protocol is designed for a particular type of ultra-wide band radio called an impulse radio and based on work from M Kuhn *et al*.[12]. Impulse radios send pulses of energy to transmit data. The transmitter and receiver are time synchronized so the receiving radio can know when to expect pulses. Impulse radios are advantageous because of their simplicity and ability to achieve very low powers. There are multiple steps in the protocol to authenticate a slave node such as a glucose sensor to the master node such as a glucose pump. One of the key aspects to the distance bounding is a rapid response circuit. This circuit provides a high-speed response to an incoming code that can only be performed within a short distance due to limitations on the speed of RF signals in air. The rapid bit response circuit is discussed first followed by the entire protocol.

A. Rapid Bit Response Circuit and Radio Architecture

The rapid bit circuit is necessary to respond to incoming pulses very quickly. Figure 1 shows a block diagram of how the rapid bit response circuit ties into the radio design. The

radio shares an antenna for both the transmitter and receiver with a switch to control the mode. The receiver has a low noise amplifier (LNA) and super-regenerative amplifier (SRA) combined with an envelope detector or integrator followed by sample and hold and fast compare comparator circuits. The transmitter is simply a timed pulse generator. In order to support the rapid bit response, an exclusive-or gate and latch are added. The exclusive-or gate encrypts the received data with a secret code without adding significant delay. The latch uses a delayed clock from the Sample Hold (S&H) clock. This provides a way to not only rapidly respond to an incoming pulse but also include the incoming bit in the response. If the incoming bit is unknown prior to reception, and the correct response depends on its value and must be returned within some minimum duration, then there is no way for an attacker to impersonate the responder from a distance without blind guessing.

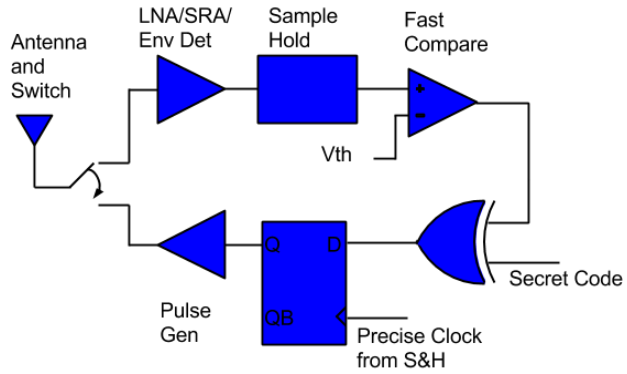

Figure 1. Circuit to provide a very fast response to an incoming bit that is also based on the incoming bit value. The receiver has a low noise amplifier (LNA) and super-regenerative amplifier (SRA) combined with an envelope detector or integrator followed by sample and hold and fast compare comparator circuits. The transmitter is simply a timed pulse generator. In order to support the rapid bit response, an exclusive-or gate and latch are added. The exclusive-or gate encrypts the received data with a secret code without adding significant delay. The latch uses a delayed clock from the Sample Hold (S&H) clock.

The rapid bit response circuit is key to the distance bounding in this design. The faster and more accurate the circuits are, the tighter the distance bounding capability. There is also a requirement of tight clock management to time the response. In this paper, we focus on the protocol design as shown in Figure 2. Note that all communication from the sensor radio to the pump radio is done using the rapid response method. In [12], the modulation scheme used is a variation of Binary Pulse Position Modulation (BPPM) called Security Enhanced Modulation (SEM). This was developed since BPPM would give a significant timing advantage for distance bounding. In the proposed design, an on-off keying (OOK) modulation is used. One of the advantages of using OOK in combination with the rapid bit response circuit is a simplification in synchronization. Once the slave node is synchronized to the master node, no further synchronization is necessary to transmit data from the slave node to the master node. This reduces the overhead of time synchronization, which is a significant portion of the packet duration, and which in turn saves power. This design also allows for the implementation of simple clear channel assessment during the rapid bit exchanges. The slave node can check for interference during the time just before the expected master pulse and the master can check for interference in the time just after the expected receive pulse. If the measured expected time pulse is a binary 1 and the time before and time after for the slave and master respectively is binary 1 interference can be assumed. In this case, the master and slave can simply ignore that time slot and continue trying on the next time slot. Once the interference has passed, the protocol will continue. If one of the nodes senses interference and the other doesn't, the packet will fail. The protocol includes cyclic redundancy check (CRC) and acknowledgements so the data can be re-sent if the interference mitigation fails during times of interference. One of the disadvantages of OOK versus BPPM or SEM is the complexity of determining threshold. It has been shown that BPPM may be 2-4dB better at BER levels of 10^{-4}, however as much 3dB is lost using SEM vs BPPM. [12,13]

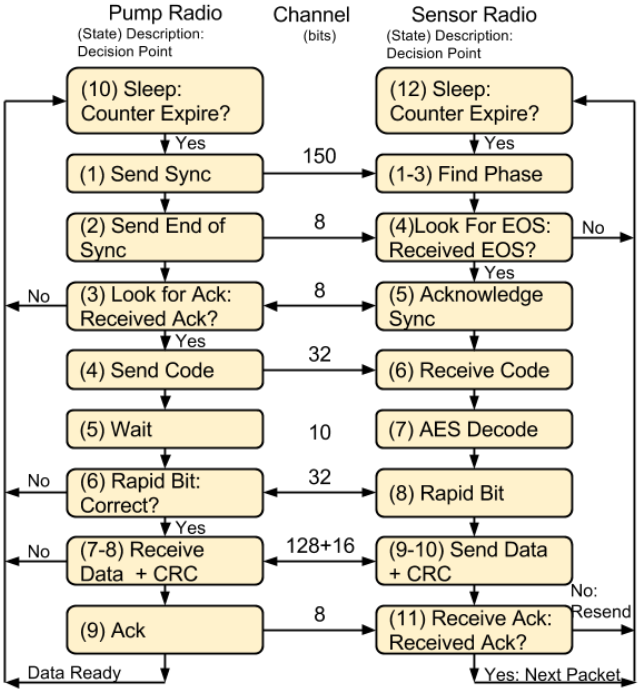

Figure 2. State machine for the protocol. In this example the left side represents a glucose pump as the master node. The right side represents a glucose sensor as the sensor node. The protocol begins with a sync phase including a end of sync (EOS) symbol. Acknowledgements (ACK) are used to verify data received and link estasblished. A rapid bit challenge is used to verify the sensor is in close proximity to the pump. The Advanced Encryption Standard (AES) is used to encrypt data sent across the link. The protocol also uses Cyclical Redundancy Check (CRC) to verify error free data transfer.

B. Protocol

The protocol presented here utilizes a master node (glucose pump) and slave node (glucose sensor) for example. The protocol provides time synchronization between the pump and the sensor, provides authentication to prevent unauthorized control of the pump, and sends the sensor data

encrypted and acknowledged. The rapid response and time synchronization design of the protocol also features a unique clear channel assessment that allows the sensor and pump to nearly simultaneously detect strong interference in the middle of a packet, pause the packet, and continue when the interference is gone.

The protocol was designed and verified using Silvaco's Silos Verilog simulator. Verilog models based on Silvaco Smartspice simulations were made for the analog portions of the transmitter and receiver to provide improved functionality and timing accuracy in the simulation. The controller implementing the protocol was designed in Verilog. For simulation purposes, a channel model was also created. This enables a simulation of the interaction between the sensor and pump and allows for the addition of noise and interference to approximate real world scenarios.

A state machine for the protocol is shown in figure 2. The state machine when operating in Pump mode is shown on the left while the Sensor mode is on the right. The middle represents the channel of data passing between the Pump and Sensor. Note that when the arrow points both directions this indicates rapid bit mode. The numbers in parenthesis represent the states used in the state machine.

The top state is a low power sleep state. In this state, the only operational components are the sleep counter and the oscillator circuit. The sleep counter is set depending on the previous state. For example, if there is an error in the packet it will set to resend the packet right away. Otherwise, it will sleep for a longer period waiting for more data.

The start of a new packet begins with a time synchronization state. There are 48 different phase selections of the receiver for the 50ns clock cycle (20MHz). The pump will transmit a series of repeated binary ones resulting in regular pulses every 50ns. The sensor will synchronize to the pump by automatically searching through its range of 48 phases seeking the optimal reception of the synchronization transmission. Once it has found the optimum phase, it will begin to look for the End-Of-Sync (EOS) signal, an 8-bit code signifying the start of a packet. This comprises states 1-4 of the sensor and 1-2 of the pump. Following transmission of the EOS symbol, the pump will look for the acknowledge sync from the sensor. The bits will be sent back to the pump using the rapid bit sequence described above. If the pump receives the acknowledgement from the sensor, it will begin the authentication phase. If not it will continue periodically repeating the synchronization state.

Next, the authentication state performs an analysis of the rapid bit exchange data that provides the critical distance bounding test on the sensor's transmission. First, the pump and sensor are given a pre-shared key in manufacturing. This key will be used for encrypting data and codes using AES-128 encryption during transmissions. This prevents a rogue agent from eavesdropping and using that information to try to perform the distance bounding test outside the bounded distance. It also prevents the rogue agent from collecting medical data by eavesdropping. The first step of the authentication stage is to send a 32-bit code from the pump to the sensor. The code is a random number generated from a Linear Feedback Shift Register (LFSR) circuit. The LFSR is initialized by the real time clock of the sensor and run for a variable amount of time between packets to ensure it cannot be guessed. This code is encrypted using the pre-shared key. Once the sensor has received the code, it will decrypt it, which takes 10 clock cycles for a typical standard cell core. The pump will wait for the sensor to decrypt the code. Then the pump will begin the rapid bit test. For the rapid bit test, the pump will generate another 32-bit random number using a second LFSR circuit. The pump will send this new 32-bit number one bit at a time. For each bit of the number, the sensor will XOR the received bit with the corresponding bit of the 32 bit decrypted code sent earlier and send it back using the rapid bit sequence circuit described above. The pump will check the received 32-bit number to authenticate the sensor. In addition, during the rapid bit sequence the sensor will encrypt the 128-bit data packet waiting to be sent. It will first encrypt the data using the 32-bit code sent previously. Following encryption by this code, the data will be encrypted again using the pre-shared key. Since each encryption takes only 10 clock cycles, this can be easily accomplished during the rapid bit sequence.

Following the authentication stage, the sensor will transmit 128-bits of data to the pump. The sensor will transmit the data using the rapid bit sequence. After the data is transferred, the sensor will transmit a 16-bit CRC signal. This will guarantee that the data was transferred correctly without errors. The pump will receive the data and CRC and check the CRC to verify the data was sent correctly. If the CRC is correct for the data it has received, it will send an 8-bit acknowledgement to the sensor indicating the pump has received the data correctly. If the sensor receives the acknowledgement, it will continue to the next packet. If it does not receive the acknowledgment, it will retry sending the packet.

The protocol was designed to resist against many known attack types. The protocol protects against replay attacks where the attacker eavesdrops and resends data with modifications that will pass as new data. The protocol encrypts the data by the pre-shared key and the packet key. Encrypting additionally by the packet key prevents patterning in the encrypted data from encryption similar packets with the same key. The protocol also checks for bit flipping attacks by the CRC and double encryption. Finally, the protocol incorporates distance bounding that prevents an attacker from authenticating from a distance outside the body area network by using the rapid bit sequence. The rapid bit sequence features a challenge such that the next bit is unknown and the correct response is based on the encrypted code sent previously. The odds of guessing the received bits is one in 4.29 million based on the combinations of a 32-bit number. Furthermore, since the data is supposed to be encrypted with the packet code, the received data will be easily dismissed by the system as invalid without knowing the pre-shared encryption code. The distance bounding challenge also offers further protection if the pre-shared key is somehow compromised (known as a terrorist attack). In this case, the rapid bit sequence uses a random code each time so the attacker will have to be within the distance-bounded range.

III. Conclusion

This project has demonstrated a security protocol for ultra-wideband impulse radios based on distance bounding. Future work will be to synthesize the Verilog implementation and prototype the radio.

References

[1] A. H. Omre, "Reducing Healthcare Costs with Wireless Technology," in *Sixth International Workshop on Wearable and Implantable Body Sensor Networks, 2009. BSN 2009*, 2009, pp. 65–70.

[2] Shinyoung Lim, Tae Hwan Oh, Y. B. Choi, and T. Lakshman, "Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring," in *2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)*, 2010, pp. 327–332.

[3] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of medical systems*, vol. 36, no. 1, pp. 93–101, 2012.

[4] N. Leavitt, "Researchers fight to keep implanted medical devices safe from hackers," *Computer*, vol. 43, no. 8, pp. 11–14, 2010.

[5] C. A. Chin, G. V. Crosby, T. Ghosh, and R. Murimi, "Advances and challenges of wireless body area networks for healthcare applications," in *Computing, Networking and Communications (ICNC), 2012 International Conference on*, 2012, pp. 99–103.

[6] N. Paul, T. Kohno, and D. C. Klonoff, "A review of the security of insulin pump infusion systems," *Journal of diabetes science and technology*, vol. 5, no. 6, pp. 1557–1562, 2011.

[7] W. Burleson, S. S. Clark, B. Ransford, and K. Fu, "Design challenges for secure implantable medical devices," in *Proceedings of the 49th Annual Design Automation Conference*, 2012, pp. 12–17.

[8] A. Odeh, M. Alshowkan, and C. Bach, "Security of Wireless Sensor Networks in Biomedical," *JOURNAL OF ADVANCES IN BIOLOGY*, vol. 2, no. 2, pp. 127–134, 2013.

[9] S. Cass, "Personal Security," *MIT Technology Review*, 18-Aug-2011. .

[10] "Insulin pumps, other medical devices vulnerable to computer hackers - Washington Times." [Online]. Available: http://www.washingtontimes.com/news/2011/oct/26/insulin-pumps-other-medical-devices-vulnerable-to-/. [Accessed: 17-Nov-2011].

[11] L. Cox, "Security Experts: Hackers Could Target Pacemakers," 01-Apr-2010. .

[12] M. Kuhn, H. Luecken, and N. O. Tippenhauer, "UWB impulse radio based distance bounding," in *Positioning Navigation and Communication (WPNC), 2010 7th Workshop on*, 2010, pp. 28–37.

[13] V. Niemelä, J. Haapola, M. Hämäläinen, and J. Iinatti, "Integration interval and threshold evaluation for an energy detector receiver with PPM and OOK modulations," in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, pp. 242–248.