DESIGN CONSIDERATIONS FOR WIRELESS SENSOR NETWORKS IN NUCLEAR POWER APPLICATIONS*

Dwight A. Clayton, Richard A. Willems
Electrical and Electronics Systems Research Division
Oak Ridge National Laboratory
One Bethel Valley Road, Oak Ridge, TN USA 37831
claytonda@ornl.gov; willemsra@ornl.gov

Abstract

Today's nuclear power plant (NPP) instrumentation uses current loops and voltage-based communications. Copper-based communications technology also relies on insulation that could degrade after decades of exposure to power plant environments and can be flammable. Wireless technologies offer the potential for greater expansion in instrumentation in a plant that could augment human performance, provide additional data on plant equipment and component status, and facilitate online assessment of the material condition of plants. By combining wireless communications technologies with power harvesting techniques, development of truly wireless sensor nodes (WSNs) becomes a possibility. This paper discusses the design considerations and potential solutions for WSN deployment in a NPP environment.

Keywords: power harvesting, security, wireless sensor network, IPv6, IEEE 802.15.4, 6LoWPAN,

1 INTRODUCTION

In many industries, wireless sensor networks are beginning to replace conventional point-to-point wiring. The ease at which additional sensors can be added to monitor a process is often a major factor in deploying wireless sensor networks. In fact, wireless sensor networks have proven to be less expensive, more flexible, and more reliable in industrial settings than their wired counterparts [1]. To be accepted as an alternative to conventional point-to-point wiring, in many key applications these wireless sensor networks must exhibit extreme reliability and prove to be secure.

When wireless communications technologies and power harvesting techniques are ready for the nuclear power plant environment, the benefits will extend far beyond a reduction in cable installation and maintenance cost. Self-powered wireless sensor nodes (WSNs) operating in an ad hoc mesh network will provide a cost-effective way to add new or redundant measurements to existing plant instrumentation systems. Because nodes scavenging certain types of energy could continue to operate during extended station blackouts (SBOs) and during periods when operation of the plant's internal power distribution system has been disrupted, measurements identified as critical to accident management should be among the first targeted. The availability of this data would be invaluable not only to operators trying to manage an accident situation but to teams responsible for post-incident analyses as well. Self-powered WSNs and the networks that tie them together will provide an opportunity to make substantial improvements in the reliability and safety of modern nuclear power plants (NPPs). Obviously, robust digital instrumentation communication techniques and architectures are essential to address this potential.

 This work is supported by the U.S. Department of Energy Office of Nuclear Energy's Nuclear Energy Enabling Technologies (NEET) Program.

2 WIRELESS SENSOR NODES

The primary issue of using power harvesting technologies currently available (and even those under development) is the limited generation capacity. Matching a compact and efficient energy-conversion device with an adequate energy source is an engineering challenge, as well as minimizing energy consumption by other circuitry in the WSN (Figure 1). Luckily, the demand for smaller packages and longer battery life in consumer electronics has driven the development of ultra-low power circuitry for the last decade; self-powered WSN technology will benefit from these advances.

The architecture of a self-powered WSN will be largely independent of the harvesting technology employed and the wireless communications method used – assuming low power consumption is kept as a key feature. Specifically, the power management block would vary slightly according to the type of harvester used, but circuitry implementing the remaining functions would not be radically modified.

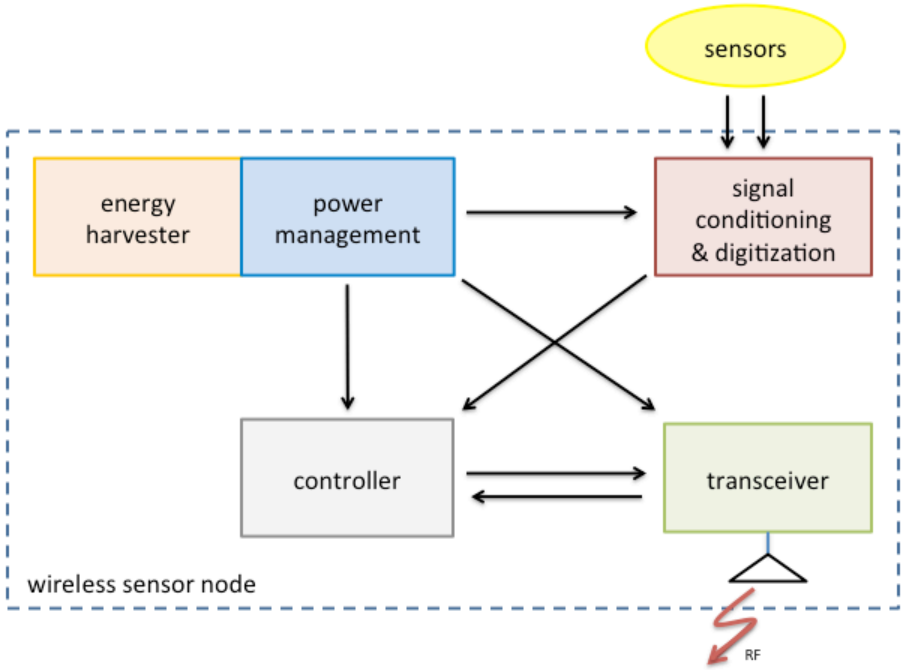

Figure 1. A functional block diagram of a WSN.

To arrive at a baseline power estimate for a hypothetical WSN (Table 1), signal conditioning and digitization electronics for four thermocouples, a small microprocessor, and a radio transceiver was considered. We assume one transmission of data from this node every 30 seconds as well as several relays of data from other nodes every second. We also assume that low-power, commercial off-the-shelf components are used and that power to the thermocouple cold-junction compensation (CJC) subcircuits can be turned off between measurements.

Table 1. Power budget for a self-powered wireless sensor node

Transceiver, including encryption	9 mW average
Microcontroller	200 μW
Four channels of CJC and amplification	1 mW average
Quad 12-bit analog-to-digital converter	18 μW
Miscellaneous circuitry	<3 mW
Power loss in 85% efficient power conversion/management circuit	2 mW
Total	**15 mW average**

A conservative power generation target would be on the order of 20 mW of continuous power. Local energy storage, probably in a supercapacitor, will allow periodic, short-duration periods of elevated power consumption. If conditions limit the amount of power that is available for prolonged periods, the frequency of data transmissions can be dynamically adjusted to reduce consumption.

3 POWER HARVESTING

Fortunately, NPP facilities are abounding with environmental energy sources having potential to power WSN. Of the harvesting technologies considered, all except thermal energy harvesting have known issues that make them unsuitable for use in the NPP environment, especially if operation through extended SBOs is desired. Thermal harvesting seems to be an attractive approach because of the abundance of waste heat at NPPs. This heat continues to be produced when the reactor is shut down and even when the fuel assemblies are removed from service and placed in spent fuel storage pools. In SBO scenarios, heat is the one form of energy most likely to persist until grid or backup power can be restored [2].

Thermal energy harvesters capture heat energy flowing from a warm surface to a cooler surface and convert it to electricity. Familiar examples are in commercially available electronic wristwatches that consume very few microwatts and can be powered by heat from the wearer's arm. However, our hypothetical WSN requires several orders of magnitude more power than these watches. The majority of thermal harvesting devices feature no moving parts and, if they are not subjected to severe environmental stresses, relatively long effective life spans.

The maximum achievable efficiency for any thermodynamic device is limited to its theoretical Carnot efficiency, which is determined by the difference in temperatures of the heat source and the heat sink (T_h is the hot side temperature, and T_c is the cold side temperature). Greater temperature differentials yield greater theoretical efficiencies.

$$\eta_{carnot} = \frac{T_h - T_c}{T_h} .$$

Thermoelectric generators (TEGs) utilize the Seebeck effect to extract electrical energy from a temperature difference between two surfaces. Semiconductor thermocouples, consisting of one p-type material and one n-type material, are usually used in thermoelectric harvesters. Bismuth telluride (Bi_2Te_3) is the most often used material, but recent research has produced significant efficiency increase with the use of silicon nanowires. A typical arrangement of a thermoelectric generator is to place a pair of p-type and n-type semiconductors electrically in series and thermally in parallel as depicted in Figure 2.

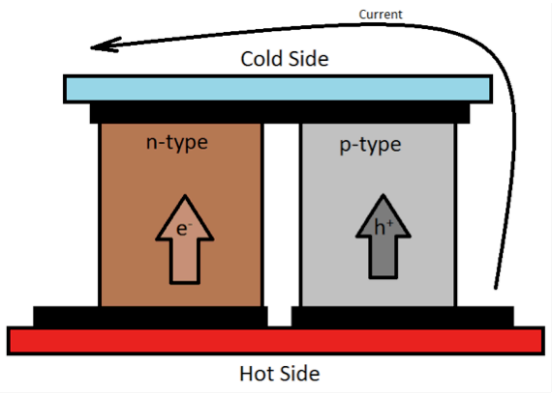

Figure 2. A semiconductor thermocouple consists of both p-type and n-type material.

The charge carriers (electrons, or e^-, for the n-type and holes, or h^+, for the p-type) in each semiconductor tend to migrate away from the warm side of the thermocouple. This results in a current. A single TEG can consist of hundreds of thermocouples connected in series. Using commercially available technology (25% of the theoretical maximum efficiency), a thermoelectric generator approximately the size of a blackboard eraser could power the hypothetical WSN if mounted on a warm surface at least 50°C above ambient temperature. No penetration of reactor pipes or vessels would be required.

4 IPv6

It is important to note that ad-hoc mesh networks generally do not operate in a stand-alone mode, i.e. they usually have to interact with one or more other mesh networks (mesh clouds) and with wired infrastructure. Typical security concerns for mesh networks include both passive and active attacks. In a passive attack, the attacker does not insert any information into the network, but listens and attempts to retrieve vulnerable information. In active attacks, messages are inserted and as a result the operation is disrupted or some nodes may be harmed – impersonation and spoofing are examples of active attacks. An attacker may also attempt to disrupt the operation of the network by causing a large amount of control packets that can cause overloading of wireless links and render the network unavailable.

In 1998 the Internet Engineering Task Force (IETF) introduced IPv6. It was primarily designed to replace IPv4 as the network protocol of the Internet. With an increasing number of networked devices, one of the key driving forces for developing IPv6 was the realization that the current Internet protocol IPv4 was rapidly running out of unique IP addresses. To avert the threat of address space exhaustion, IPv6 expands the address space of IPv4 from 32-bits to 128-bits giving a total of 2^{128} or 3.4×10^{38} unique network addresses [3].

In addition to a large address space, IPv6 supports network-layer encryption and authentication. Through the use of header extensions, IPv6 implements L2 encryption and authentication with IPSec to ensure both data confidentiality and authenticity [4].

An IPv6 data packet is comprised of two main parts: the header and the payload. The IPv6 header format is streamlined to keep packet header overhead to a minimum by moving both non-essential fields and optional fields to extension headers that are placed after the IPv6 header. The first 40 bytes/octets of an IPv6 packet comprise the header (Figure 3) that contains the following fields [5]:

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination address			

Figure 3. IPv6 Header Packet Composition

- The first four bits of the header packet represent the Internet Protocol version number and is set to 0110b or 6.
- The traffic class field is an 8-bit field and is used to implement Quality of Service (QoS) markings based on data loss, latency and/or bandwidth.
- The 20-bit flow label field allows the marking of packets so that they belong to a particular traffic flow for which the sender requires special handling, i.e., real-time.
- The payload length is a 16-bit unsigned integer and represents the number of bytes/octets following the packet header. As noted earlier, any header extensions are treated as part of the payload.
- The next header field represents an 8-bit selector that identifies the header type immediately following the IPv6 packet header.
- The hop limit field is an 8-bit field that is decremented by one each time the packet is forwarded. When the hop limit reaches zero the packet is discarded.
- The source address is the 128-bit address of the originator of the packet.
- The destination address is the 128-bit address of the intended recipient of the packet.

5 IEEE 802.15.4

The Institute of Electrical and Electronics Engineers (IEEE) released the 802.15.4 low power wireless personal area network (WPAN) standard in 2003 [6]. The standard attempts to achieve several goals simultaneously, two being extremely low cost and short-range wireless communication with reasonable power consumption. 802.15.4 security can be broken down into four kinds of service: access control, message integrity, message confidentiality and replay protection. Access control is accomplished through access control lists, i.e., data from unauthorized sources is not permitted. Message integrity ensures that the data received at the destination is unaltered. Data encryption provides confidentiality of the message and prevents eavesdropping on the payload. Replay protection prevents an adversary from capturing encrypted traffic and re-injecting it into the network.

There are three fields in the IEEE 802.15.4 MAC frame that are related to security: the Frame Control, the Auxiliary Security Header and the Data Payload (Figure 4).

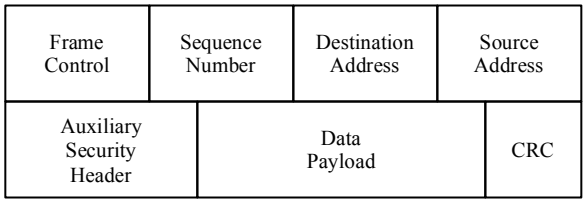

Figure 4. IEEE 802.15.4 MAC Frame Composition

To enable the Auxiliary Security Header and thereby enable link-layer security, the Security Enabled bit of the Frame Control field must be turned on. The Auxiliary Security Header shown in Figure 5 has three fields: Security Control, Frame Counter and Key Identifier.

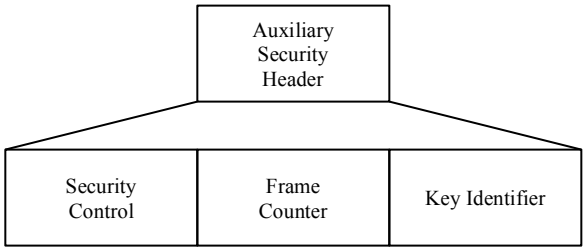

Figure 5. IEEE 802.15.4 MAC Frame Security Composition

The Security Control is a 1-byte field, specifies the global Security Policy for the frame and is comprised of two bit fields: Security Level and Key Identifier Mode (Figure 4).

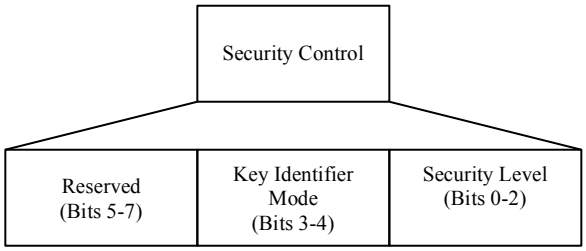

Figure 6. Security Control Field Composition

Within the Security Control field, the Security Level bits specify the encryption level and the key length. The Security Level values and their corresponding security properties are shown in Table 2 [7].

Table 2. IEEE 802.15.4 Security Properties

Security Level	**Security Property**	**Description**
0x00	No security	Data unencrypted Data not authenticated
0x01	AES-CBC-MAC-32	Data unencrypted Data authenticated
0x02	AES-CBC-MAC-64	Data unencrypted Data authenticated
0x03	AES-CBC-MAC-128	Data unencrypted Data authenticated
0x04	AES-CTR	Data encrypted Data not authenticated
0x05	AES-CCM-32	Data encrypted Data authenticated
0x06	AES-CCM-64	Data encrypted Data authenticated
0x07	AES-CCM-128	Data encrypted Data authenticated

The value of 0x00 specifies no data encryption and no data authentication. Values 0x01-0x03 specify the data are authenticated using the encrypted Message Authenticated Code (MAC) but the payload content is transmitted in plaintext. The MAC can be 32, 64 or 128-bits. The 0x04 value specifies the packet is encrypted but not authenticated. Values in the range of 0x05-0x07 specify that the data are encrypted and authenticated.

The Key Identifier Mode bits specify the kind of key to be used (implicit or explicit) by the sender and receiver. Table 3 lists the possible values.

Table 3. Key Identifier Modes

Key Identifier Mode	**Description**
0	The sender and receiver know the Key ID implicitly. Key ID is not sent in the message.
1	The Key ID is determined explicitly by the Key Index subfield of Key Identifier.
2	The Key ID is determined explicitly by the Key Index and 4-bytes of the Key Source.
3	The Key ID is determined explicitly by the Key Index and 8-bytes of the Key Source.

The Frame Counter is a 4-byte counter given by the source of the current frame and is used to guard against message replay.

The Key Identifier field is used if the Key Identifier Mode value is non-zero. The Key Identifier is a 10-byte field that is further divided into the Key Source subfield (9-bytes) and the Key Index subfield (1-byte), and is shown in Figure 7.

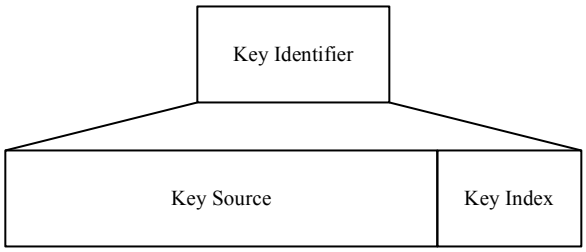

Figure 7. Key Identifier Field Composition

For non-zero values, the Key Source specifies the group key originator and the Key Index specifies different keys from a particular Key Source. Although IEEE 802.15.4 supports encryption keys, the standard does not specify how the keys are managed nor how authentication policies should be applied. It is assumed that the high layer protocols handle the key management.

The encryption algorithm used in IEEE 802.15.4 is the Advanced Encryption Standard (AES) with a 128-bit key length. Not only is AES used to encrypt the payload but also to authenticate it. For authentication, a 128-bit key is used but the resulting MAC is appended to the payload as 32, 64 or 128-bits. Figure 6 shows the formatting of the data payload for the three main security suites [8].

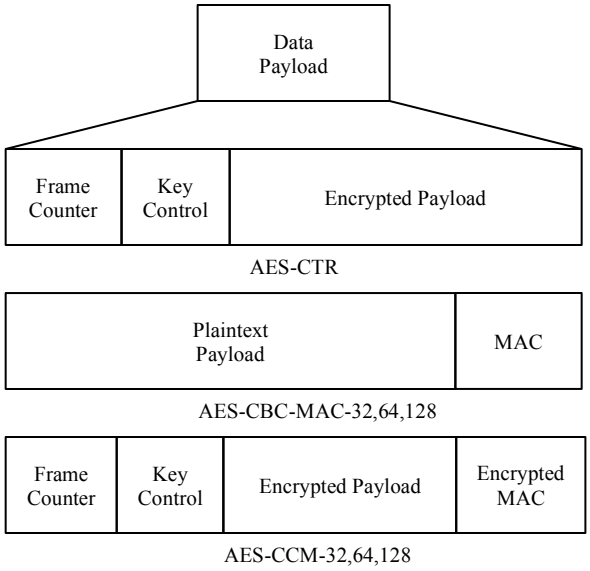

Figure 8. IEEE 802.15.4 MAC Frame Data Payload for three main security suites.

6 6LoWPAN

An IEEE 802.15.4 MAC frame is 127 octets; however, after adding the MAC frame header overhead and including the AES-CCM-128 security feature, only 81 octets remain for the upper network layers. Given that the minimum transmission unit (MTU) size of IPv6 is 1280 bytes/octets, a translation layer is required.

In order to accommodate IPv6 packets over IEEE 802.15.4 wireless networks, an adaptation layer needed to be developed to translate the larger IPv6 packet sizes to the smaller 802.15.4 frame sizes. In 2007, the IETF developed the 6LoWPAN standard for mapping IPv6 over low-power IEEE 802.15.4 wireless networks. The standard deals primarily with the frame format as well as the link-local addresses and stateless auto configured addresses of IPv6 packets over IEEE 802.15.4 networks. No additional security layers are added, however a section on security considerations is included [9]. It is expected that these frames can be transmitted within the targeted 20 mW of continuous power discussed in Section 2.

7 Conclusion

Many industries are beginning to utilize mesh networks to replace conventional point-to-point wiring, reaping the cost savings associated with eliminating the communications cabling. In addition to these cost savings, these mesh networks open the potential for greater expansion in instrumentation in the plant that could augment human performance, provide additional data on plant equipment and component status, and facilitate online assessment of the material condition of plants.

The combination of wireless communications and power harvesting enables the implementation of truly wireless sensor nodes (WSNs). Development of methods to couple low-drift, high-accuracy, low-power transducers with ambient power harvesting to produce a transducer that is capable of being installed during construction of the plant and operating reliably for many years and possibly until the plant is decommissioned is possible.

6LoWPAN represents a melding of two technologies: IPv6 and IEEE 802.15.4. IPv6 nodes are geared towards attaining high speeds and tend to have large resources, whereas for IEEE 802.15.4-compliant devices, energy conservation and code-size optimization are the top priorities. Both IPv6 and IEEE 802.15.4 provide built-in security. Using IPSec, IPv6 ensures both message confidentiality and authentication. IEEE 802.15.4 devices provide link-layer security; however, key management must be implemented at a high layer. Because of dissimilar domains, an

adaptation mechanism is required to allow interoperability between the two domains that could potentially lead to security risks. As Kim [10] has shown, the adaptation layer is vulnerable to potential threats through packet fragmentation attacks. When deploying WSNs, security considerations must be taken into account. Clearly with 6LoWPAN, security threats at different layers must be thoroughly understood to ensure proper levels of confidentiality are maintained.

8 REFERENCES

[1] R. Allan, "Energy Harvesting Powers Industrial Wireless Sensor Networks", Electronic Design, pp. 22-29, 20 September 2012.

[2] Clayton, Dwight A., William H. Andrews Jr and Roberto Lenarduzzi. *Power Harvesting Practices and Technology Gaps for Sensor Networks*. ORNL/TM-2012/442. Oak Ridge, TN: Oak Ridge National Laboratory.2012.

[3] RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden, December 1998, p. 1.

[4] RFC 2401, Security Architecture for the Internet Protocol, S. Kent, R. Atkinson, 1998.

[5] RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden, December 1998, pp. 3-4

[6] Wireless medium access control and phyical layer specifications for low-rate wireless personal area networks. IEEE Standard, 802.15.4-2003, May 2003. ISBN 0-7381-3677-5

[7] Security in 802.15.4 and ZigBee networks. http://www.sensor-networks.org/index.php?page=0903503549, D. Gascon, February 5, 2009.

[8] Security Considerations for IEEE 802.15.4 Networks, N. Sastry, D. Wagner, WSE '04, October 1, 2004.

[9] RFC 4944, Transmission of IPv6 Packages over IEEE 802.15.4 Networks, G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, Septmember 2007.

[10] Protection against Packet Fragmentation Attacks at the 6LoWPAN Adaption Layer, HyunGon Kim, IEEE 2008.