Wireless Ad Hoc Sensor Networks for Port Security

Final Report

METRANS Project AR 07-10

June 2011

Principal Investigator
Tracy Bradley Maples, Ph.D.

College of Engineering/
Computer Engineering and Computer Science Department

California State University
Long Beach, California 90840

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the Department of Transportation, University Transportation Centers Program, and California Department of Transportation in the interest of information exchange. The U.S. Government and California Department of Transportation assume no liability for the contents or use thereof. The contents do not necessarily reflect the official views or policies of the State of California or the Department of Transportation. This report does not constitute a standard, specification, or regulation.

Abstract

Ad hoc wireless sensor networks (WSNs) have the potential of transforming communications in large-scale mobile workplaces. They promise ease of deployment, dynamic network configuration, swift exchange of sensor information, and real-time access to databases and other remote resources. WSNs consist of small, low cost motes (or motes) containing sensors to monitor their environment, and one or more base stations which can attach to other networks and databases. WSNs show particular promise in applications that involve complex, human-made systems. This paper seeks to identify the key issues facing the use of wireless ad hoc sensor networks for port security. A literature survey of ad hoc WSN security applications was conducted resulting in the creation of a taxonomy for WSN security applications. An annotated bibliography of the key publications describing WSN security applications can be found in Appendix A. In addition, an extensive literature survey of security issues in ad hoc WSN technologies is discussed. A summary of the key security vulnerabilities and countermeasures and of current WSN technology is presented following the TCP/IP layers model. In Appendix B, an annotated bibliography of the key publications concerning WSN security issues can be found.

Table of Contents

List of Figures and Tables

Disclosure

Project was funded in entirety under this contract to California Department of Transportation.

Acknowledgements

The Principle Investigator wishes to acknowledge the outstanding work of two Computer Engineering and Computer Science Students from California State University, Long Beach on this research project. Masters candidate Larisa Melnik provided invaluable help in researching and categorizing the security vulnerabilities of Wireless Ad Hoc Sensor Networks. Undergraduate student Victoria Ting worked diligently in gathering and sorting papers related to security applications for Wireless Ad Hoc Sensor Networks.

An additional thank you goes to Mr. Ryan Baird, General Manager of SSA Marine Terminal C60, for the helpful tour. Mr. Baird took a great deal of time out of his busy schedule to show us the terminal, explain how it functions, and answer our many questions.

Introduction

Wireless ad hoc sensor networks (ad hoc WSNs or WSNs) have become one of the hot topics in mobile computer networks. Technical conferences and publications highlighting WSN technology and applications are commonplace. Research, development, and manufacturing of these networks are thriving. Nevertheless, ad hoc WSN technology is not yet mature. Many applications for WSNs have been proposed, but few are operational. Many technical issues about WSNs remain to be solved by researchers. Of primary importance, the security issues facing WSNs are many and varied.

WSN motes (or motes) vary in size and functionality. Because they can use wireless transmission to communicate and form ad hoc networks, they hold the promise of ease of deployment, dynamic configuration, swift exchange of information, and real-time access to databases and other remote resources. They have the potential of transforming communications in large-scale mobile workplaces. In an ideal application, they would become proactive networks; that is, computer networks that not only collect and disseminate information, but also organize and process the data they carry.

Ad hoc WSNs seem particularly well suited to the domain of seaport operations and goods movement. For example, wireless motes that sense global position, temperature, or light–level can be embedded in shipping containers (much like RFID tags) as they travel from ships through the ports to distribution centers and beyond. Each of these motes can join the ad hoc (i.e., self-configuring) wireless network in its own vicinity, thus communicating with the motes in other containers in a peer-to-peer fashion. In turn, these ad hoc wireless networks can connect via gateways to other ad hoc wireless networks or other wired computer networks to form large heterogeneous networks. The data provided by these networks can then be used to provide valuable input to the management of supply chain logistics.

The aim of this research project is to identify the key issues facing the use of wireless ad hoc sensor networks for port security. To address this issue, two phases of research were conducted. In Phase I, a literature survey of ad hoc WSN security applications was conducted and a visit was made to the Port of Long Beach. The outcome of this phase was the creation of a WSN Security Application Taxonomy that allows for categorization of WSN applications. In addition, an annotated bibliography of the key publications describing WSN security applications was produced. In Phase II, an extensive literature survey of security issues in ad hoc WSN technology was completed. The outcome of this phase of the research is a summary of key the security mechanisms and vulnerabilities of current WSN technology. In addition, an annotated bibliography of the key publications relating to WSN security issues was produced. Additionally, a WSN testbed was constructed to gain insight into current WSN technologies.

Security Applications for Wireless Ad Hoc Sensor Networks

Phase I of this research project focused on identification of possible security applications for ad hoc WSN usage within the Los Angeles and Long Beach ports. For this task two sources of information were used: (1) a visit to the port of Long Beach, and (2) an extensive literature survey of current, published wireless sensor network articles. The primary outcome of Phase I is a detailed taxonomy of current ad hoc WSN security applications. Within this taxonomy we pinpoint those applications that are relevant for Port security.

Visit to Port of Long Beach

Along with a number of other METRANS researchers, a visit was made to the SSA Marine Terminal C60 at the Port of Long Beach. The purpose of this visit was to gather information from the port community that would help to understand more fully the security-related environment into which these wireless sensor networks might be integrated.

SSA Marine Terminal C60 provides service for MATSON, one of leading firms in Pacific shipping. From this terminal, MATSON primarily provides service between Long Beach and Hawaii. The MATSON ships arrive and depart following an established schedule.

FIGURE 1 SSA Marine Terminal C60: Arriving Trucks and Container Being Loaded by Crane

The terminal covers 58 acres at the Port of Long Beach and has six incoming lanes for arriving vehicles and four outgoing lanes. It has two berths with three 40-ton cranes in operation. Given its size and specialized focus on the needs of its client MATSON, SSA Marine Terminal C60 is one of the smaller, more specialized, terminals in the Ports of Long Beach and Los Angeles.

FIGURE 2 SSA Marine Terminal C60: Empty Containers Awaiting Pick-up and MATSON Ship Bound for Hawaii

The visit to SSA Marine Terminal C60 provided useful information in examining the issues of WSNs for port security. Of particular assistance was examining the physical layout of the Terminal and informally evaluating the possibility of installing ad hoc WSN that would adapt to different topologies of the containers.

Taxonomy of Ad Hoc WSN Applications

In recent years, there have been extensive publications in the field of ad hoc WSNs. For this project, we narrowed our literature survey to focus on applications that use WSNs for security purposes. Originally, many ad hoc WSNs were developed with military security applications in mind. Over the last decade, their use has expanded to include a broad range of applications including applications related to locating, tracking, monitoring, or controlling objects.

Early in the literature search it became clear that some organization needed to be imposed on the many WSN applications that were being proposed. While categorization of these applications may not always be clear-cut, we have developed a useful taxonomy of ad hoc WSN security applications. This taxonomy can be found in Figure 3. Included in Figure 3 is also a list of the key publications relating to each taxonomy category. Each of these references is also included in the **Annotated Bibliography of Wireless Ad Hoc Sensor Network Security Applications** found in Appendix A.

FIGURE 3: Taxonomy of Wireless Ad Hoc Sensor Network Applications

The following discussion relates directly to the taxonomy presented in Figure 3:

Under the umbrella heading of *Wireless Sensor Networks*, WSN security applications naturally fall into three different categories: (1) *Military Applications*, (2) personal *Health Applications*, and (3) applications involving the monitoring or protecting of an *Environmental Applications* or a specifically bounded location.

In *Military Applications,* the literature discusses WSNs usage for tracking missiles or targets or locating the source of sniper fire. [KATOP07, RAZAA05, KUCKE07] Other possibilities include using WSNs as a military monitoring network (such as the proposed MIL-MON) for surveillance purposes to monitor large areas against intruders and send alerts and information about intruders in real time. [BEKME05] Another application seeks to improve situational awareness and targeting through real-time aerial deployed WSNs. [DIAMO07]

A second major category of WSN security applications involves personal *Health Applications*. These applications include, but are not limited to, the use of WSN to monitor a patient's vital statistics and to track and monitor the patient's environment. [ZHOUH07, BAKER07, TEAWH05] These systems will often alert medical personnel in the event of life-threatening events and communicate important information and statistics.

The third major category of WSN applications, relates to the monitoring and protection of an environment or designated area. Since this category includes many types of applications, we have subdivided it into applications relating to: (a) *Natural Areas* or systems, and (b) *Human-Made Systems*. The uses of WSNs in *Natural Areas* typically involve the monitoring of environments that do not regularly depend on human interaction. Examples of these types of types of systems include, but are not limited to: volcanic hot-zones, detection of predicting risk of fires, gathering data on semi-arid regions, and detecting extreme temperature gradients in the ocean by monitoring marine microorganisms. [WERNE06, YULIA06, CHACZ05, ZHANG04, LUKEJ07, PRABH07]

The second subcategory of environmental-based applications, *Human-Made Systems*, has a wide-range of complexity in its applications. It includes relatively simple WSNs such as those used to monitor *Home and Office Space*, those used to monitor and protect more *Complex Human-Made Systems*, and then those applications relating specifically to *Goods and Objects*. *Home and Office Space* applications are typically small, simple WSNs that have a limited scope and purpose. [SONGW07, PARKB07, HWANG07] For example, these applications may be used to control the lighting or temperature within a building, or to access a defined space by controlling digital door locks.

The second subcategory of *Human-Made Systems* is *Complex Systems*. This category is further divided into those applications that focus solely on *Property Safety Only* and those that address both *Human and Property Safety*. The WSNs that are used solely to protect property include structural monitoring, railway maintenance monitoring, aircraft maintenance monitoring, and pipeline and water distribution monitoring. [KURAT06,

STOIA07, SUNGA08, LINWU08, SAMPI07, ABOEL06] Conversely, WSN applications that involve the protection of both people and property include intersection accident prevention, and coalmine (and miner) monitoring, and fire rescue applications. [SENAR08, KINGB07, SHAKH06, WANGZ07, SONGC08, CHEHR07].

The third subcategory of *Human-Made Systems* consists of applications relating to *Goods and Objects*. This subcategory includes *Transport Related* management of these objects, and applications that are *Goods and Objects Related*. For the *Transport Related* category, WSN applications that involve the railway industry, intelligent transportation, and supply chain management automation were discussed in the literature. [SHAFI07, LIBEN06, EVERS07] For the non-transportation related *Goods and Objects* category, WSN applications address monitoring the condition of and tracking containers. [MAHLK07, BUKKA07]

The shaded portion of Figure 3 shows application subcategories in which WSN security applications that relate to Port security can be found. This shaded area includes the subcategories of shipped goods and objects, the transport of such items, and human and property safety issues as they relate to the complex systems that would need to be developed. Of the thirty-four conference and journal articles we found most relevant to WSN security applications, only eleven of those had a direct application to goods movement and security in the Ports. Of those eleven, none of the articles directly addressed using WSNs for security in a Port setting. The most relevant involved container tracking and integrity and condition monitoring of goods. [MAHLK07, BUKKA07] Based on the increase in WSN publications in the last few years, there is no doubt that additional articles relating to WSN applications for security will soon become available. It is hoped that the taxonomy presented in this report will serve as an aid in assessing the applicability of the new publications to the issue of Port security.

Wireless Ad Hoc Sensor Network Security Issues

Phase II of this research project focused on investigating the current level of security in wireless ad hoc sensor networks, and whether these levels meet the standards required by the Ports of Los Angeles and Long Beach. We surveyed the current literature on WSN security and looked at existing standards. The outcome of this research is a discussion of the primary security concerns in wireless sensor networks and the proposed security solutions. Security threats, the effects of these threats, and possible recovery methods are discussed layer-by-layer of the TCP/IP Protocol Stack.

Wherever WSNs are used for sensitive applications, they should be adequately protected. Network security should provide confidentiality, integrity, authenticity, and data availability (freshness). In respect to security, WSNs differ from most other networks in a number of important ways. First, motes of a WSN have limited processing capability and memory; therefore, computation-intensive, public-key cryptography is unavailable for their use. Second, the inability to secure the wireless medium (an issue common to all wireless networking devices) leaves WSNs vulnerable to the eavesdropping of traffic, the leaking of data to neighbor networks, the injection of spurious data into the network, and jamming of the network. Third, because of deployment of WSNs is often in unsecured, publicly accessible areas, there exists the possibility of physical tampering and destruction of the devices. Finally, WSN motes are powered by batteries so power (or energy) conservation is critical. WSN motes can run at full power for approximately two weeks only. Such an energy-dependent nature imposes threats in the form of resource-consumption attacks to WSN security.

In order to discuss WSN security problems in general, some further clarification is necessary. Throughout this section, we will assume that the trust requirements of the WSNs are as follows:

- Base stations (which act as a gateways to the outside world) are assumed to be trustworthy and correctly operating.
- Individual sensors inside of motes are assumed to be trustless since each sensor has the potential to be compromised.
- Each sensor in a mote trusts itself.

In order to discuss the issue of WSN security in a structured fashion, we will consider security at each of five layers of TCP/IP Protocol Stack (i.e., Physical Layer, Link Layer, Internet Layer, Transport Layer, and Application Layer) (see Figure 4). Such an approach will help with layer localization of the existing security problems, and consequently, with the creation of a more precise classification of the threats and countermeasures.

Layer 5	Application	Specifies how a particular application uses a network.
Layer 4	Transport	Specifies reliable transport of data.
Layer 3	Internet	Specifies packet format and routing.
Layer 2	Link	Specifies frame organization and transmittal.
Layer 1	Physical	Specifies the basic network hardware.

TABLE 1: TCP/IP Protocol Layers

Physical Layer

The easiest type of attack to perform on the Physical Layer is a jamming attack. [XUW05] In this attack, no knowledge is needed of the WSN that is being attacked, except for the frequency at which the motes are sending. In a jamming attack, the mote that performs the jamming will try to prevent, or interfere with, the reception of signals at the motes in the surrounding WSN. It will do this by sending out a continuous random signal on the frequency that is used by the WSN. Affected motes will not be able to receive messages from other motes and will therefore be completely isolated until the jamming stops.

Jamming attacks can be prevented with frequency hopping, where motes change frequencies in a predetermined sequence and the mote that performs the jamming is ignorant of the specific sequence. [SUNHS07] Frequency hopping in WSN requires extra complexity in terms of processing and calibration it requires. The other way to withstand a jamming attack is to use a radio communication technique that is virtually impossible to jam. Ultra Wide-band (UWB) is based on the transmission of very short pulses in the order of nanoseconds, on a large part of a frequency band simultaneously. [AIELL03] UWB is well suited for WSN because of its low energy requirements and is therefore a worthwhile jamming countermeasure.

Because WSN motes function unattended, they are vulnerable to the threat of physical tampering or destruction. Such attacks can be prevented or their negative results minimized by hiding or camouflaging the motes or using some type of tamper-proof packaging for motes. [WOODS02]

Link Layer

The Link Layer is most susceptible to the following types of attacks: collision attacks, exhaustion attacks, and denial-of-sleep attacks.

In a collision attack, the attacker uses its radio to listen to the frequency on which a WSN is transmitting. [BROWN05] When it hears the start of a message, it sends out its own signal that interferes with the message. This is called a collision and causes the message to be received incorrectly at the receiver. It is difficult to detect this type of attack because the only evidence of a collision attack is the reception of incorrect messages. If a frame fails the cyclic redundancy code (CRC) check, the packet is discarded. This attack causes the network to waste its bandwidth and motes to exhaust their power supplies. The countermeasures that can be applied to collision attacks are the same as those used against jamming attacks. Use of error-correcting codes provides for fair mitigation of collisions.

In an exhaustion attack a malicious mote continuously transmits a large number of request-to-send (RTS) packets to generate clear-to-send (CTS) responses from a targeted mote. [BROWN05] The targeted mote remains awake, waits for the expected forthcoming messages, which never arrive, and eventually exhausts its power source. This attack also leads to multiple collisions of the packets, starvation of other motes, and a waste of bandwidth. The other motes also unproductively expend their power resources. The effects of these attacks can be lessened using the rate limiting technique. In this approach, the rate limit cannot drop below the expected maximum data rate the network supports, or the network will ignore all excessive requests. This prevents motes from extreme power consumption.

Another link-layer threat to WSNs is the denial-of-sleep attack. This attach prevents the mote from going into sleep mode. [BROWN05, STAJA99, RAYMO06] At full power, the battery-powered motes can run for only about two weeks before exhausting their batteries. Most mote power consumption happens when a mote is transmitting or listening. Therefore, it is crucial that motes are active (awake) as little as possible (usually at around 1% of the time) and remain in sleep mode for the remainder of the time. An attacker can exhaust a mote's resources by repeatedly sending RTS messages triggering CTS responses from a targeted mote. In this case, all the motes within the radio range of the sender will be receiving those (RTS) control packets, thus draining their power supplies. The attacker may also send a constant stream of unauthenticated or replayed broadcast packets causing the motes to remain awake.

Various contention-based MAC protocols such as Sensor MAC (S-MAC), Berkeley MAC (B-MAC) or Timeout MAC (T-MAC) were designed with the goal of extending the network life cycle by minimizing the number of collisions, idle listening periods, and message overhearing. These protocols synchronize the transmitting activities and sleep of motes, thus saving battery power. An attacker can also determine which protocol a particular WSN is using by analyzing the network traffic. Using this information, an attacker can gather the information necessary to mount a denial-of-sleep attack. As the way to lessen the effect of these attacks, anti-replay protection, strong link-layer authentication, and broadcast attack protection are proposed. [RAYMO06]

Internet Layer

At the Internet Layer, attacks target routing protocols. A WSN is a wireless ad-hoc network, thus each sensor mote supports a multi-hop routing algorithm where motes forward packets to the base station.

The most general attacks to sensor network routing are spoofing, replaying, or altering routing-control information. In these attacks the adversary injects bogus routing information into the network. This leads to routing inconsistencies, and, as a consequence increases end-to-end delays and packet loss in the network. Fortunately, these types of attacks can be effectively prevented using link-layer authentication and anti-replay techniques.

In an Internet Layer selective forwarding attack, a malicious mote joins the routing and makes itself a part of many routes. [KARLO03] The mote then drops all packets or (if it wishes to stay undetected) suppresses or modify packets from a few selected motes while properly forward the remaining traffic.

There are different ways to combat selective forwarding attacks. One of them is to use implicit acknowledgements to ensure that packets are forwarded as they were sent. This technique is considered unattractive for sensor networks because of the extensive consumption of the power by sensor motes' radios. Another way to combat selective forwarding attacks is a multipath routing. [KARLO03, YUGOV01] The same data is sent over multiple paths to give it a higher probability of reaching its destination. This technique is far from satisfactory because it wastes power on redundant paths and consumes additional network bandwidth. Moreover, there might not be so many routing options in particular network.

HELLO flooding is an attack that exploits WSN protocols that require motes to broadcast HELLO packets to announce their presence to their neighbors. [KARLO03] An attacker using a large transmission power can replay a previously recorded HELLO packet and advertise to neighbor motes misleading routing information. Because the network motes' radio range does not allow the motes to communicate with the originating mote, this attack can lead to the inability of legitimate network motes to reliably forward traffic.

Motes can be instructed to authenticate each other by verifying bidirectional links before constructing their routes. This preventative measure can combat HELLO flooding attacks. [SUNK06, KARLO03] Also, geographic routing protocols, which require each mote to know its own location and be able to communicate that location to other motes, can be employed against HELLO flooding attacks. [YUGOV01]

The wormhole attack consists of recording traffic from one region of the network and replaying it in a different region [KARLO03]. Wormholes are very likely to be chosen as routes because they provide a seemingly shorter path to the destination. Thus, an adversary performing this kind of attack supplies the legitimate motes with bogus routing information and lures their traffic into a sinkhole. As a result, the communication

between sensor motes and the base station may be disrupted. Wormholes use a private low-latency channel invisible to the rest of a WSN in order to tunnel recorded information. Defense for these attacks may be found in carefully designed routing protocols (e.g., geographic routing protocols). In these specialized protocols, sensor motes interact locally with their neighbors with no involvement from base station thus constructing the ad hoc topology on demand and limiting vulnerabilities. [YUGOV01, KARLO03].

In homing attacks, an adversary may perform network traffic analysis to determine the geographic location of critical motes, such as neighbors of the base station or base station itself. [DENGH05, WOODS02] The attacker can then physically disable these motes (i.e., by jamming). The adversary may even be able to attack the base station thus disabling the entire network. In order to prevent the geographic location of critical motes from being revealed, packet header encryption can be used. Unfortunately, this does not completely prevent traffic analysis since the asymmetry of traffic, when most data flows are directed toward base station, can reveal the location of a base station. To address this issue, the authors in [DENGH04] suggest that uniform sending rates over the entire network should be used. These can be achieved by dynamically setting the sending rate between motes. "Dummy packets" are sent to equalize the traffic volume. This preventive technique, however, taxes the sensor motes' energy resources, and can be considered useful only when preventing traffic analysis is of supreme importance.

The attack countermeasures at the network layer are highly dependent on authentication; thus, it is worth mentioning the newly proposed lightweight message authentication mechanism in [ZHANG08]. The authors suggest that use of a public key for message authentication may impose too high an overhead in terms of computational cost and network bandwidth consumption. Use of symmetric keys and hash functions is effective, but when the sensor mote is compromised, the keys can become known to the adversary. Therefore, the authors offer message authentication and verification via polynomials with independent and random factors for the perturbation of polynomial shares preloaded to individual motes. While keeping the computational overhead low, this method increases the complexity of breaking the secret polynomial for an adversary thus making the authentication more resilient to mote compromises.

Transport Layer

If all motes on the WSN are running TCP, attacks become possible at the Transport and Application Layer. At the Transport Layer attacks target the protocols that provide transfer of data between end systems. When explicit connections between identifiable motes are used, either end of the connection maintains some form of connection control block. An attacker can issue a large number of connection setup requests that result in the exhaustion of memory at the end motes. This is called a TCP SYN flood attack. [WOODS02] Traditional defense against this attack is done using SYN cookies. In order to prevent memory exhaustion, SYN cookies do not store any state on the machine; thus, keeping all state information about the initial TCP connection in the network itself. All this is done with an extensive use of cryptographic functions. It is not clear if this

approach will suitable for WSNs due to its computational and message-size overhead. [BERNS08]

Another kind of Transport Layer attack is the desynchronization attack. [WOODS02] This attack targets the transport protocols that rely on sequence numbers. An attacker issues forged packets with wrong sequence numbers and, as a result, causes retransmissions, which waste both energy and bandwidth. Participants may even end the connection without performing any useful exchange of information. Use of a header or even full packet authentication is good defense measure against such an attack. It is not possible for an adversary to forge authenticated packets, thus the end points of communication can detect and reject malicious packets.

Application Layer

At the Application Layer, an adversary with only minimal effort can launch a severe and effective attack known as the path-based Denial-of-Service (DoS) attack. A DoS attack can disable a large portion of a WSN. [DENGH05] This type of attack is based on the attackers ability to inject incorrect or replayed packets into the network at leaf motes. As a result, motes along the path will exhaust their power supply. Because of the tree-structured topology of a WSN, motes that are located downstream from motes along the main path will be unable to communicate with the base station.

One proposed countermeasure to the path-based DoS attack is the one-way hash chain (OHC) mechanism. [DENGH05] Using this mechanism, motes along the path can detect a path-based DoS attack and prevent the propagation of incorrect packets. Each time a mote sends a packet, it includes within the packet newly generated one-way hash chain number. When an intermediate mote receives the packet, it verifies (against its own maintained verifier) that the OCH number is a new one. If OCH in the received packet is new, the intermediate mote forwards the packet; otherwise, it discards this packet. An adversary cannot deduce a valid next OHC number from the current and earlier OHCs. Thus, this mechanism effectively protects the network from flooding with bogus packets or replayed packets.

The TinyOS proposed for use in WSNs contains the convenient yet vulnerable feature of remote reprogramming of motes. A Deluge (reprogramming) attack can be waged on the system. An adversary can hijack the reprogramming session, and, as a consequence, gain control over some portion of a network or the entire network. A method for securing of the reprogramming process is offered in [DUTTA06]. The authors underscore the fact that traditional, cryptographically strong, public key-based systems for source authentication and integrity verification cannot be implemented in resource-constrained sensor motes. They propose instead the idea of dividing program binary into series of messages, each message containing hash of the next message. It becomes impossible for an adversary to construct the message that matches hash contained in previous message. The secure initiation of a legitimate reprogramming process is provided by a digitally signed advertisement, which contains the program name, version number, and hash of the first message.

Summary of Security Issues

In the previous sections of this paper, the main issues in wireless sensor network security have been presented. For each of the five protocol layers of the TCP/IP stack, the requirements, threats and possible countermeasures were discussed. A diagram summarizing the "Security Threats and Their Effects" and the "Methods of Recovery (or Countermeasures)" can be found in Figure 4. Table 2 provides a complete list of the security issues identified with references. Each of these references is also included in the **Annotated Bibliography of Wireless Ad Hoc Sensor Network Security Issues** found in Appendix B.

FIGURE 4: Wireless Ad Hoc Sensor Network Security Threats, Effects, and Recovery Methods

TCP/IP Layer	Types of Attacks and Key References	Countermeasures and Key References
Physical	Jamming attacks **[XUTRA05]**	Frequency hopping [**SUNHS07]** Ultra Wide-band (UWB) **[AIELL03]**
	Mote tampering or destruction **[WOOD02]**	Hide or camouflage motes **[WOOD02]** Tamper-proof packaging **[WOOD02]**
Link	Collisions attacks **[BROWN05]** Exhaustion attack **[BROWN05]**	Rate limiting **[BROWN05]**
	Denial of Sleep **[BROWN05], [STAJA05], [RAYMO06]** Error correcting codes **[LIUMA97]**	Contention-Based Sensor MAC Protocols **[STAJA05]**
Internet	Selective forwarding **[KARLO05]**	Redundancy **[NGAIL06], [YUGOV01]** Acknowledgements **[YUXIA06]**
	Sinkhole Attacks **[KARLO05]**	Authorization **[NGAIL06]**
	HELLO Flood **[KARLO05]**	Authentication **[SUNPE06]** Link verification **[Karlo05]** Routing checks **[KARLO05], [YUGOV01]**
	Sybil Attack **[KARLO05]**	Authentication **[ZHANG08]**
	Routing cycles **[KARLO05]**	Link verification **[KARLO05]** Routing checks **[KARLO05], [YUGOV01]**
	Bogus routing information **[KARLO05]**	One-way hash chains **[DENGH05}]**
	Wormholes **[KARLO05]**	Geographic Routing **[YUGOV01]** Secure cluster formation **[KARLO05]**
	Spoofing, replaying, or altering routing-control traffic or clustering messages **[KARLO05]**	Secure cluster formation **[SUNPE06]**, **[KARLO05]**
	Homing **[WOODS02]**	Uniform sending rate **[DENGH04]**
Transport	SYN (synchronize) flood **[WOODS02]**	SYN **[BERNS08]**
	Desynchronization attack **[WOODS02]**	Packet authentication **[WOODS02]**
Application	Path-based DoS **[DENGH05]**	One-way hash chains **[DENGH05]**
	Deluge (reprogramming) attack **[DUTTA06]**	Streams Authentication **[DUTTA06]**

TABLE 2: Wireless Ad Hoc Sensor Network Security Threats and Countermeasures by Layer

Wireless Ad Hoc Sensor Network Testbed

In order to gain insight into the current state-of-the-art in ad hoc WSNs, a testbed was created. The basic design of the WSN testbed is shown in Figure 5. The testbed was implemented using multiple, off-the-shelf wireless motes with sensor capabilities forming wireless mesh network. A wireless sensor network base station was installed on a workstation to act as gateway for the wireless sensor network. The gateway connected the testbed to the existing IP (Internet Protocol) network and the Internet.

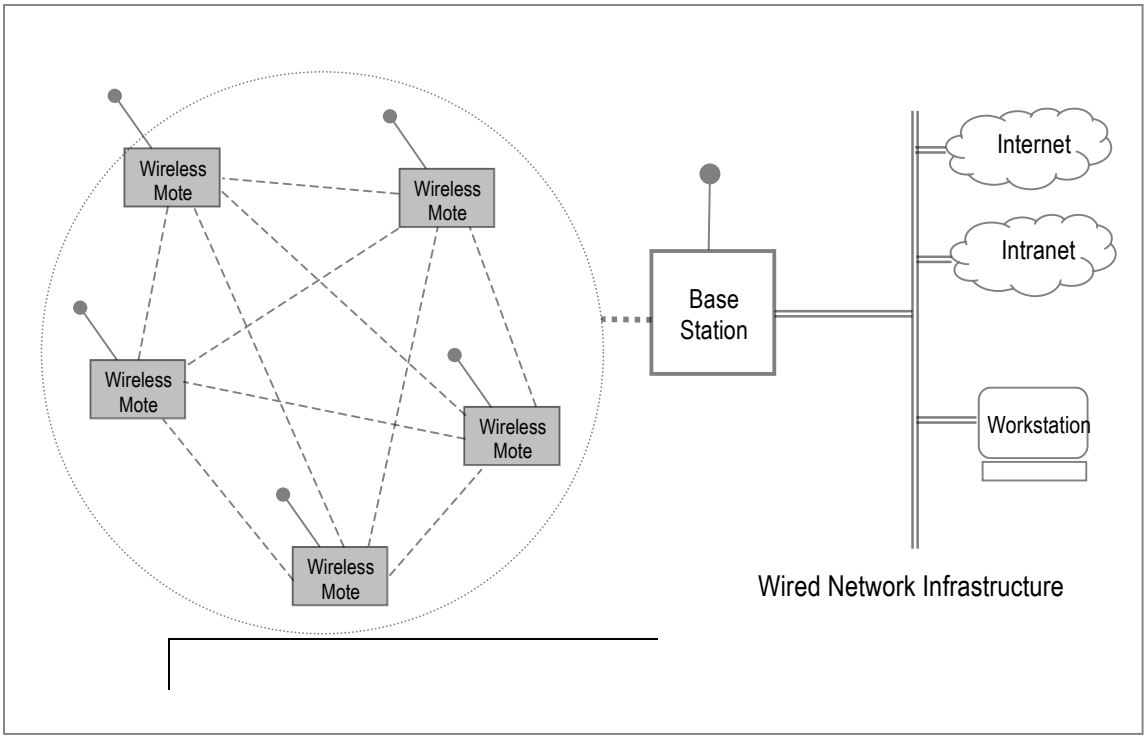


FIGURE 5: Wireless Ad Hoc Sensor Network Testbed with Mesh Topology

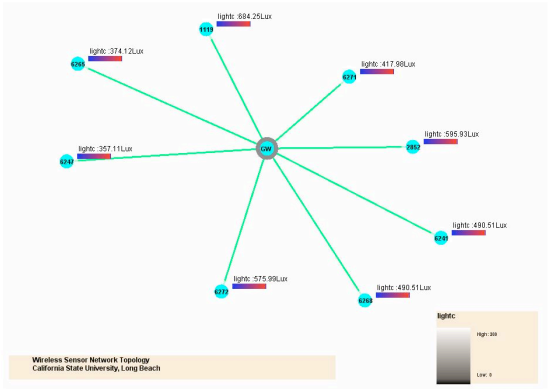
The Crossbow Technologies Professional Kit for Wireless Technologies was used to implement the WSN testbed. The kit contains six wireless sensor motes (motes) (see Figure 6), a base station, data acquisition board, and USB programming board. It allows for Microsoft Windows™-based control and observation of the wireless sensor network. The WSN testbed was constructed in the Computer Engineering and Computer Science Department's Computer Networking and Security Laboratory.

The experimentation performed on this WSN testbed was straightforward. The general aim was to evaluate the maturity of current, state-of-the-art WSN technology with respect to its application to port security. One primary concern was the ad hoc routing functionality of the WSN equipment. Figure 7 shows two screen captures taken from the Crossbow WSN monitoring software. In (a), the WSN topology and routing is shown to be a star. In this example all motes were located in the same lab within 15 feet of the base station. In (b), the topology and routing of the ad hoc WSN is changing as the motes were moved farther away from the base station in a semi-linear fashion. The motes were

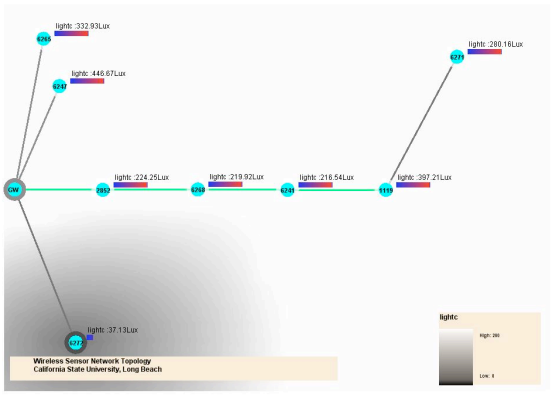
spaced approximately 20 feet apart down a long corridor. As you can see from the figure, Mote 6271 routes information to the base station via the path 6271 → 1119 → 6241 → 6268 → 2852 → GW (gateway or base station). This topology change occurred without human intervention and seemingly instantaneously. This simple test replicates the type of reconfiguration a WSN would need to make if motes attached to shipping containers were moved from a general storage facility where they are all in range of the base station, to a train with one base station and a linear topology.

FIGURE 6 Crossbow Technologies Wireless Motes Used in Testbed

Another area of interest for the WSN testbed was examining the functionality of the sensors on the motes. The Crossbow motes each contain four sensors. These sensors measure (and report to the base station through routing protocols) the environmental characteristics of temperature, barometric pressure, humidity, and ambient light.



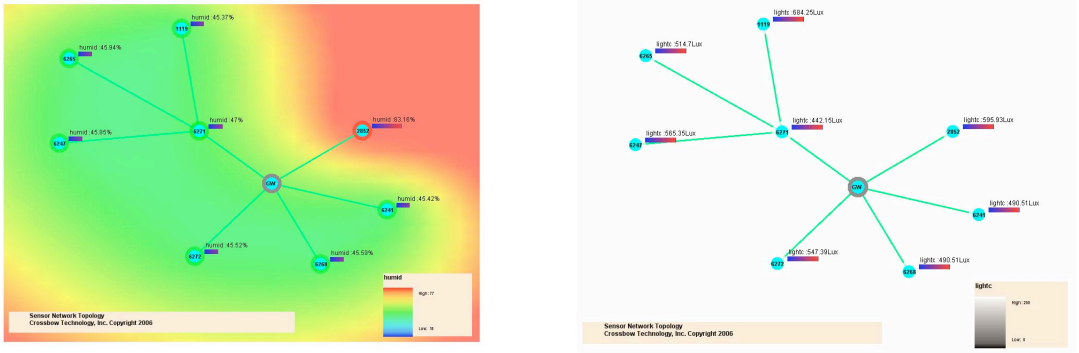
(a) WSN Testbed Motes in Star Topology



(b) WSN Testbed Motes Transitioning to a Linear Topology

FIGURE 7 Wireless Ad Hoc Sensor Network Testbed Topology Changes

In Figure 8, sensor readings from the Crossbow software are shown. In (a), the humidity readings at the sensor at each mote are shown. The green area shows humidity within the established normal range. The red area shows that mote 2852's humidity reading is considered "high". In (b), the ambient light readings for each mote are shown. In this figure, all sensors are measuring light in the "high" range. Note, at this time, the Crossbow software does not support the monitoring of more than one sensor time at a particular time, nor do sensor readings trigger any type of computer-generated response. It is expected that these functions will be incorporated into newer versions of the monitoring software.



(a) WSN Testbed Humidity Readings **(b)** WSN Testbed Ambient Light Readings

FIGURE 8 Wireless Ad Hoc Sensor Network Testbed Humidity and Ambient Light Sensor Readings

While these initial experiments with the WSN testbed were informative and provided a basic "proof of concept" for WSNs, a number of further experiments are highly desirable before in looking at WSN integration at the Ports of Long Beach and Los Angeles. Most importantly, additional focus must be placed on the security vulnerabilities discussed in the preceding section of this paper. In the testbed environment, experiments that attempting to breach security of the WSN by replicating the security attacks at each of the five TCP/IP layers, as well as, the testing of countermeasures can be explored.

Conclusions and Recommendations

Many factors contribute to the fact that security in WSNs is significantly more challenging than security in traditional networks. WSNs have inherent resource and computing constraints. WSNs operate on an insecure transmission medium. WSNs are often deployed in unattended, insecure environments. Yet, beyond these security issues there lies great promise for WSNs.

A small but useful group of security applications related to the use of WSNs in the ports currently exists. Specifically, those articles of particular interest fall into the areas of human-made systems: (a) for shipped goods and objects and the transport of such items, and (b) human and property safety issues as they relate to complex systems. It is hoped that the Taxonomy of WSN Security Applications presented in this paper will aid in the future identification of WSN applications for the ports, while the Annotated Bibliography of Wireless Security Applications in Appendix A serve as a resource for those looking examining WSN security applications.

Knowledge of the security vulnerabilities found in WSNs is certainly the first step in overcoming these limitations. The results of this research suggest that there are security vulnerabilities at every layer of the TCP/IP Protocol Stack; yet, it appears that the main reason for this widespread vulnerability is that the protocol layers were designed without considering security requirements and that traditional security solutions (like use of public-key cryptography) cannot be used due to resource constraints. Our study suggests that researchers are now actively addressing these issues. We have found that there exist some solid mechanisms for withstanding routing protocol attacks at the Internet Layer. Also, Link Layer encryption and authentication mechanisms can provide reasonable defenses and can be used for securing the higher protocol layers services.

The utilization of ad hoc WSNs to handle applications of ever-increasing complexity seems a forgone conclusion. The appeal of applying these ad hoc WSNs to port security is great. Sensor motes embedded in shipping containers with the ability to monitor temperature, ambient light, humidity, location, and many other environmental factors could be immensely useful in every phase of goods movement. The capability of these sensor networks to reconfigure their topology and routing paths on an ad hoc basis---when shipping containers move from ship to terminal or from terminal to train---makes port security an ideal environment for WSNs.

Thus, it is the security of current WSNs that must be addressed before this deployment in the ports moves ahead. The challenges facing WSN designers dictate the necessity of integrating security into every component of a WSN. Consequently, security considerations must be included at every phase of system design, and in every layer of the protocol stack.

Implementation

The results of this research project are based on literature surveys of WSN security applications and cannot be implemented directly. Rather, the results of this report are relevant whenever WSN implementation is considered at the Ports of Long Beach and Los Angeles. The most significant finding of this research is that security in WSNs is far from being mature. In every layer of the protocol stack, WSNs were found to have security vulnerabilities. And although a number of countermeasures to these vulnerabilities have been proposed, their effectiveness is not known. To further this research, additional work in a WSN testbed environment would be necessary to study the security issues in more detail, and a pilot implementation program at one of the terminals would be desirable.

Appendix A

Annotated Bibliography of Wireless Ad Hoc Sensor Network Security Applications

[ABOEL06] Aboelela, E., Edberg, W., Papakonstantinou, C., Vokkarane, V. Wireless Sensor Network Based Model for Secure Railway Operations. *25th IEEE International Performance, Computing, and Communications Conference*, 2006. IPCCC 2006 (10-12 Apr 2006): 623 – 628.

In this paper, the author introduces his approach to using wireless sensor networks to solve the issues that plague the railroad industry, including minimizing accidents and improving railroad maintenance activities. He explains the different components he's using and the architecture implemented, as well as explains and shows elementary data from the fuzzy logic-based aggregation technique he utilizes. But for all the good intentions, this system is still in its rudimentary stages and will require a lot more work, especially addressing security issues to the WSN itself, before it can begin to be reliable.

[BAKER07] Baker, C., Armijo, K., Belka, S., Benhabib, M., et al. Wireless Sensor Networks for Home Health Care. 21st International Conference on Advanced Information Networking and Applications Workshops, 2007. AINAW '07 (21-23 May 2007): Volume 2, 832-837.

This paper discusses WSNs formed using Tmote Sky (Moteiv Corp.) and SHIMMER (Intel) that are used to address specific health issues – the SleepSafe prototype addressing SIDS, the Baby Glove prototype addressing issues for premature infants, the FireLine prototype for monitoring firefighters or vital signs of patients at home, the Heart@Home prototype for blood pressure monitoring and tracking, and LISTSENse for the hearing impaired. The author does not go into details of any one of the prototypes, but rather he presents the overall usefulness and possible future applications of WSN to increase health care efficiency and reduce costs.

[BEKME05] Bekmezci, I., Alagoz, F. A New TDMA Based Sensor Network for Military Monitoring (MIL-MON). IEEE Military Communications Conference, 2005. MILCOM 2005 (17-20 Oct 2005): Volume 4, 2238-2243.

In this paper, the author proposes a new TDMA-based wireless sensor network for military monitoring of relatively large areas for intruders, called MIL-MON. He does a good job introducing the idea and assumptions made, and briefly talks through the proposed systems' theory – timing synchronization and scheduling, rescheduling, and topology. He further shares some of his elementary system performance results, but widely admits to the issues that still must be addressed – failed motes, security, etc. Overall, it does not really address security issues of the WSN being proposed, but it offers an interesting walk-thru of a real-time responding network.

[BUKKA07] Bukkapatnam, S., Komanduri, R. Container Integrity and Condition Monitoring using RF Vibration Sensor Tags. IEEE International Conference on Automation Science and Engineering, 2007. CASE 2007 (22-25 Sept 2007): 585-590.

The authors detail a very specific application using Wireless Sensor Networks to monitor container trucks – determining container integrity and condition through the monitoring and interpretation of container vibrations. In this paper, they explain the need and benefit of such a product, detail the experiment design, and explain how the results are interpreted and what they look like based off different conditions (speed, packing density, type of terrain, etc). Overall, this article presents a fairly detailed portrait of the need, functionality, and success of using container vibrations to determine container integrity and condition, but does not address threats to such a system.

[CHACZ05] Chaczko, Z., Zhmad, F. Wireless Sensor Network Based System for Fire Endangered Areas. 3rd International Conference on Information Technology and Applications, 2005. ICITA 2005 (4-7 July 2005): Volume 2, 203-207.

In this paper, the authors introduce a conceptual plan to use WSNs monitor fire-endangered areas in real time based of measuring temperature, humidity, and smoke. Although it has not fully been developed and is still in the software simulation stage, the authors talk through the hardware they would be using, the infrastructure, the issues that they had to face and deal with, and promising simulation results. General idea and promising proposal aside, this paper excluded a lot of the theory behind their design and the plethora of simulation result presented severely lacked discussion or explanations to enhance the value of the images presented.

[CHEHR07] Chehri, A., Fortier, P., Tardif, P. Security Monitoring Using Wireless Sensor Networks. 5th Annual Conference on Communication Networks and Services Research, 2007. CNSR '07 (May 2007): 13-17.

The authors of this paper propose a futuristic system for using ad-hoc wireless sensor networks to monitor the environmental, physical aspects of underground mines, to track objects in an area, and for security and emergency applications. They discuss sensor placement, topology, and give us a simplified but technical summary of the simulation model they used along with assumptions made. While there seems to be promise in this field and application, the authors admit that there are assumptions that were made that don't hold true or constant, and there is much need to form a more realistic model before one can consider this system useful.

[DIAMO07] Diamond, S.M., Ceruti, M.G. Application of Wireless Sensor Network to Military Information Integration. 5th IEEE International

Conference on Industrial Informatics, 2007 (23-27 Jun 2007): Volume 1, 317-322.

The article argues that affordable, real-time, scalable wireless sensor networks can improve normal military operations by providing another view for targeting discrepancies and countering asymmetric threats in opaque environments. The authors set out to describe the technologies needed and the importance of these systems, work that's being done now, data interoperability, system architecture, and model requirements analysis. One of the most interesting parts of the article however were the bullet points for reducing the cost of implementation, and the many topics still needing to be addressed and explored. Worthy points to note and consider.

[EVERS07] Evers, L., Havinga, P. Supply Chain Management Automation using Wireless Sensor Networks. IEEE International Conference on Mobile Adhoc and Sensor Systems, 2007. MASS 2007 (8-11 Oct 2007): 1-3.

In this article, the author describes an application of wireless sensor networks that aid in the management of the supply chain through a runtime system called SensorScheme. He starts by setting a scenario under which this system is used, giving the necessary requirements of different products that will be transported and the conditions under which they must be transported to remain undisturbed. On the journey from source to destination, different things are monitored (temperature), products nearby, location and destination, etc. If faults are found, there are a number of ways of raising an alert, depending on the present condition and location of the containers. While security is not addressed, this article shows that WSN for transportation monitoring and tracking are available for use, and useful to maintaining product integrity.

[HWANG07] Hwang, I., Baek, J. Wireless Access Monitoring and Control System based on Digital Door Lock. IEEE Transactions on Consumer Electronics. Volume 53, Issue 4, Nov 2007: 1724-1730.

This article proposes an application of wireless sensor networks that allows for wireless access monitoring and control through the digital door lock using Zigbee modules. The author begins by arguing the practicality and need of such a systems, and then gives us a detailed system overview and a very complete view of the modes of operation for the system. Through the use of half a dozen flow charts, he clearly presents the purpose and theory behind each mode. He also introduces the different hardware modules used in this system. Overall, it gives a good picture of the complete system that makes it seem both practical and relevant, but fails to address security concerns in the system itself.

[KATOP07] Katopodis, P., Katsis, G., Walker, O., Tummala, M., Michael, J.B. A Hybrid, Large-scale Wireless Sensor Network for Missile Defense. *IEEE International Conference on System of Systems Engineering*, 2007. SoSE '07 (16-18 Apr 2007): 1-5.

In this article, that author presents a hybrid, large-scale WSN for missile defense using terrestrial and satellite motes. He makes the interesting point of addressing the motes not as individual systems, but instead looks at the network as a system of systems. In this paper he thoroughly discusses his proposed data dissemination mechanism that merges the features of data aggregation and clustering with those of a data centric routing protocol. He also shows a simulation example of his system where we see that the data aggregation he's proposing does not introduce a significantly larger time lag.

[KING07] King, T.I., Barnes, W.J., Refai, H.H., Fagan, J.E. A Wireless Sensor Network Architecture for Highway Intersection Collision Prevention. *IEEE Intelligent Transportation System Conference*, 2007. ITSC 2007 (30 Sept – 3 Oct 2007): 178-183.

The author of this article acknowledges that many interesting models have been created to try to prevent intersection collisions. Though simulation, he looks at the limitations of those WSN collision avoidance systems that involve deploying sensors before and outside the intersection that feed information back to the base station. After giving a brief theoretical overview and explaining the details and components of the simulation, he concludes under normal driving conditions, the simulated system should perform well. However, he admits, that it is both difficult and expensive to confirm these simulation results in the physical reality.

[KUCKE07] Kuckertz, P., Ansari, J., Riihijarvi, J., Mahonen, P. Sniper Fire Localization using Wireless Sensor Networks and Genetic Algorithm based Data Fusion. *IEEE Military Communications Conference*, 2007. MILCOM 2007 (29-31 Oct 2007).

The author presents the design, implementation, and performance results of a WSN based solution to sniper fire localization using time-of-arrival (TOA) measurements and a genetic algorithm based data fusion framework. He discusses previous and related work, explains the calculation of TOA, data fusion, and trajectory estimation, and then presents and explains two large sets of results. He praises the capability of his proposed system, but admits to short-comings and issues that still need to be addressed and handled. It offers an interesting glimpse at how supersonic projectiles can be detected and tracked.

[KURAT06] Kurata, N., Saruwatari, S., Morikawa, H. Ubiquitous Structural Monitoring using Wireless Sensor Networks. *International Symposium on Intelligent Signal Processing and Communication*, 2006. ISPACS '06 (12-15 Dec 2006): 99-102.

The authors of this paper argue for the need and value of having wireless sensor network technology for ubiquitous structural monitoring – for disaster prevention, security, building control, and structural maintenance. And although they did not

mention any complete systems, the reported extensively on lab work being done in this field of study. While this system is nowhere near complete, it is interesting to read about the sensor boards used and simulation results.

[LIBEN06] Li, Benliang; Wang, H., Yan, B., Zhang, C. The Research of Applying Wireless Sensor Networks to IntelligentTransportation System (ITS) Based on IEEE 802.15.4. *6th International Conference on ITS Telecommunications Proceedings*, 2006. 939-942.

The IntelligentTransportation System that the authors present links various technological medium – computers, wireless radio communication systems, and sophisticated sensors – in a fashion that allows them to be useful in transit specifically using IEEE 802.15.4. After discussing and evaluating the IEEE 802.15.4 in this domain, the author concludes that this standard is aimed at simple, low cost and low power implementations which also enable pervasive WSN. And while that all seems attractive, the author admits that there are severe network architecture issues that need to be evaluated and addressed in order for the new IEEE 802.15.4 standard to important and useful to the IntelligentTransportation System.

[LINWU08] Lin, M., Wu, Y., Wassell, I. Wireless Sensor Network: Water Distribution Monitoring System. *IEEE Radio and Wireless Symposium,* 2008 (22-24 Jan 2008): 775-778.

In an era where water is becoming a precious resource, the authors of this paper are determined to use WSNs to help detect leakage from the pipes through a water distribution monitoring system. They discuss various aspects of their design – measurement concerns, measuring underground verses above ground channels, and gave some interesting results from field measurements. While they are pleased with their results, they admit to the need for higher resolution measurements as they move towards proposing a desirable model.

[LUKEJ07] Lu, Kejie; Qian, Y., Rodriguez, D., Rivera, W., Rodriguez, M. Wireless Sensor Networks for Environmental Monitoring Applications: A Design Framework. *IEEE Global Telecommunications Conference*, 2007. GLOBECOM '07 (26-30 Nov 2007): 1108 – 1112.

In this article, the author discusses the design needs of a WSN that is meant to monitor the environment. The author discusses acoustic monitoring at a particular WSN testbed at the Jobos Bay National Estuarine Research Reserve in Puerto Rico. The strength of this article is that it lays out the design requirements – in terms of security, quality of service, and routing requirements – as well as a framework for WSN design. To illustrate his points, he provides a case study to explain the potential of his design.

[MAHLK07] Mahlknecht, S., Madani, S. On Architecture of Low Power Wireless Sensor Networks for Container Tracking and Monitoring Applications. *5th*

IEEE International Conference on Industrial Informatics, 2007 (23-27 Jun 2007): Volume 1, 353-358.

The authors of this paper are well informed of other like-missioned products, including TREC (by Secure Trade Line) and WFSCT (by WiFi, Wireless Inc.), and thus first set out to inform us how their product idea differs from the competition. They then go into wonderful details on nine problems faced by container industry, a five-part proposed solution, and seven technical challenges they've had to address and work through. The strength of this article lies in the breadth and detail of the author's discussion – that he addresses so many traits of WSN one by one.

[PARKB07] Park, H., Burk, J., Srivastava, M. Design and Implementation of a Wireless Sensor Network for Intelligent Light Control. *6th International Symposium on Information Processing in Sensor Networks*, 2007. IPSN 2007 (25-27 Apr 2007): 370-379.

In this article, the authors begin by addressing the need for a system like their Illuminator, which not only does light sensing (like most sensor networks), but also controls lighting (like the computerized commercial control systems in theaters that rely on commands but do not sense). They address the role of the intelligent light system they are aiming to create, and the design requirements – including light sensing, user constraints, and environmentally adaptive. They then explore similar work done by others, discuss the representation of user constraints, sensor placements, and light characterization and profile generation. They then discuss their system architecture and implementation as it pertains to the Illuminator Core. And while they present some experimental results, they admit to the need for much more testing in public settings, as well as expanding from a system that only controls light intensity to one that handles color and color temperatures for the capabilities of public buildings and theaters.

[PRABH07] Prabhakar, T.V., Rao, N.V.C, Sujay, M.S., Panchard, J., Jamadagni, H.S., Pittet, A. Sensor Network Deployment for Agronomical Data Gathering in Semi-Arid Regions. *2nd International Conference on Communication Systems Software and Middleware*, 2007. COMSWARE 2007 (7-12 Jan 2007): 1-6.

The authors of this article created a WSN called COMMONSenseNet (Community Oriented Management and Monitoring of Natural Resources through Sensor Networks) that they deployed in a one square kilometer area in the semi-arid region of Karnataka, India. Their innovation is geared towards providing the locals there with important environmental data relating to soil moisture, temperature, barometric press, humidity, etc. It was interesting to see the flow of their project development, from the user surveys to gather what information the farmers thought was important, through preparing for deployment, into reading about the deployment experiences, first results, and lessons learned. The author comments that building off their experience, they have new hardware in mind to alleviate some communication issues

in bad weather, but they caution that the issue of local topography is key to the design of deployment.

[RAZAA07] Raza, H.M.M.T., Akbar, A.H, Chaudhry, S.A., Bag, G., Yoo, S., Kim, K. A Yaw Rate Aware Sensor Wakeup Protocol (YAP) for Target Prediction and Tracking in Sensor Networks. *IEEE Military Communications Conference*, 2007. MILCOM 2007 (29-31 Oct 2007).

These authors claim that one of the most important military applications for WSN is target tracking, and that the most difficult issue of target tracking is predicting the future location and behavior of the target. Thus, in their paper, the set out to address this issue of predicting future target location by first looking at related work and the various approaches taken by their peers, then by explaining their own system model and assumptions made. With respect to effective prediction of target locations, they discuss 5 major points in detail – target absence, detection, localization, prediction and stop – and then present their protocol's results. Since their work is still in the R&D phase, there are many issues, including security of the system, that need to be addressed. But it is an interesting theory none-the-less.

[SAMPI07] Sampigethaya, K., Li, M., Poovendran, R., Robinson, R., Bushnell, L., Lintelman, S. Secure Wireless Collection and Distribution of Commercial Airplane Health Data. *IEEE/AIAA 26th Digital Avionics Systems Conference*, 2007. DASC '07 (21-25 Oct 2007): 4.E.6-1 – 4.E.6-8.

In this article, that authors claim that applications of WSN involving airplane maintenance and health monitoring, as well as detection and identification of threats has the potential to significantly improve air travel safety and efficiency. The authors go into detail about the system model and trust assumptions and adversary models associated with the system. They also discuss the topics of safety and business security threats, as well as the challenges of securing data collection by WSN, within the Avionics System, and securing data distribution to Ground. As this topic is still an open and ongoing investigation, the author leaves us with a discussion of open problems. Much appreciated is all the detailing of possible security issues within the WSN.

[SENAR08] Senart, A., Karpinski, M., Wieckowski, M., Cahill, V. Using Sensor Networks for Pedestrian Detection. *5th IEEE Consumer Communications and Networking Conference*, 2008. CCNC 2008 (10-12 Jan 2008): 697-701.

The authors of this article claim that pedestrian/vehicle accidents are the 2nd largest cause of traffic-related injuries and fatalities worldwide. There are solutions now that are costly and effective only if the pedestrian is in the vehicle's line of sight. Their proposed system would make use of "cat's eyes" and communication to enhance the system and make it cheaper yet more reliable. They discuss previous work, as well as their own implementation and simulation / evaluation of their system. They claim that although their system is inexpensive and simple, it performed with precision

more than 95% of the time. But, they also admit that their future work will need to include security protocols to guard against attacks and misuse.

[SHASH06] Sha, K., Shi, W., Watkins, O. Using Wireless Sensor Networks for Fire Rescure Applications: Requirements and Challenges. *IEEE International Conference on Electro/Information Technology*, 2006 (7-10 May 2006): 239-244.

In this article, the authors first lay down the top four specific requirements that their system must address – accountability of firefighters, real-time monitoring, intelligent scheduling / resource allocation, and web-enabled service and information. They then describe how their system, FireNet, is designed to those requirements. They also include a lengthy discussion of research challenges, regarding the protocol, software, and hardware. The discussion over challenges were educating to read and much appreciated.

[SHAFI07] Shafiullah, C.M.; Gyasi-Agyei, A., Wolfs, P. Survey of Wireless Communications Applications in the Railway Industry. *2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, 2007. AusWireless 2007 (23-30 Aug 2007).

The authors of this article spend the majority of the article discussing a plethora of existing WSN applications for the railway industry that help with communication and signaling systems for rail control, monitoring systems for reliable operations of railway vehicles, and WSN techniques and applications in the railway industry. They then very briefly present their work-in-progress which would be a low-cost low-power WSN to monitor conditions of railway trains. The value of this article lies in it's survey of WSN applications in the railway industry today.

[SONGC08] Song, B., Choi, H., Lee, H. Surveillance Tracking System using Passive Infrared Motion Sensors in Wireless Sensor Network. *International Conference on Information Networking*, 2008. ICOIN 2008 (23-25 Jan 2008): 1-5.

In this article, the authors aim to prove that the passive infrared motion sensors (PIR sensors) are ideal for surveillance system applications. They first discuss the background and related work, and discuss the suitability and performance of the PIR sensors. Then they propose a deployment scheme and tracking algorithm, and describe the implementation of their surveillance system along with it's performance results. The authors admit that more work needs to be done to track multiple humans / intruders, and also on the security issues relating to the system itself.

[SONGW07] Song, G., Wei, Z., Zhang, W., Song, A. A Hybrid Sensor Network System for Home Monitoring Applications. *IEEE Transactions on Consumer Electronics*. Volume 53, Issue 4, Nov 2007: 1434 – 1439.

The authors of this article present their concept of a hybrid home monitoring system that allows for remote home environment monitoring using both static and mobile modes to measure such factors as temperature, humidity, light, motion, etc. The impressive thing about this article was all the images – as descriptions of the hardware used, the flow of the system, the architecture of the board, testbed setups and experiment setups and results – which definitely helped to clarify and augment the descriptions present. The disappointing factor of this article was it's lack of future work or issues to be addressed which would point towards a vision and promising application, and the lack of discussion on any security issues, or even issues addressed in general.

[STOIA07] Stoianov, I., Nachman, L., Madden, S. PIPENET: A Wireless Sensor Network for Pipeline Monitoring. *6th International Symposium on Information Processing in Sensor Networks*, 2007. IPSN 2007 (25-27 Apr 2007): 264-273.

These authors detail their experiences developing PipeNet, a wireless sensor created for monitoring pipeline infrastructure through collecting and processing hydraulic, acoustic, and vibration data at high sampling speeds to detect and locate leaks. The article is well written and detailed, and provides a plethora of validation and test results, based of laboratory work and a deployment in collaboration with Boston Water and Sewer Commission. It also goes into depth on the algorithm used for data analysis. Also useful and appreciated was the summary of lessons learned. In this impressively complete paper, the only topic missing may have been the security issues addressed in the design of the system to protect against intrusion, data manipulation, etc.

[SUNGA08] Sung, J., Ahn, S., Park, T., Jang, S., Yun, D., Kang, J., Yoo, S., Chong, P., Kim, D. Wireless Sensor Networks for Cultural Property Protection. *22nd International Conference on Advanced Information Networking and Applications – Workshops*, 2008. AINAW 2008 (25-28 Mar 2008): 615-620.

In this article, the authors describe the use of wireless sensor networks to monitor buildings that are cultural relics - they detail their experiences with monitoring Dul-guk-sa Temple in Korea. They argue that their system of property protection has to fulfill several requirements – environmental information monitoring (such as temperature and humidity), automatic fire detection that will send an alarm to remote uses, implementation with minimal infrastructure so as to appear invisible, system reliability and battery lifetime. They go on to disclose the hardware and software design of their system, and the development and evaluation of the system. The one downside to the article is that they don't adequately discuss the steps they take to ensure system reliability and security from outside attacks.

[TEAWH05] Teaw, E., Hou, G., Gouzman, M., Tang, K.W., Kesluk, A., Kane, M., Farrell, J. A Wireless Health Monitoring System. *IEEE International Conference on Information Acquisition*, 2005 (27 Jun – 3 Jul 2005).

The authors of this article present their system, the Health Tracker 2000, which addresses the concerns of a booming senior population in the next thirty years. Their system monitors the user's vital signs and can notify the user's relatives and medical professionals of their location in the event of life threatening situations. Although the authors discuss the many attributes that their system has to offer, they do very little to present their test results or validation of the system. And they fail to mention how they verify data integrity and correctness or provide security in their system at all.

[WANGZ07] Wang, X., Zhao, X., Liang, Z., Tan, M. Deploying a Wireless Sensor Network on the Coal Mines. *IEEE International Conference on Networking, Sensing and Control*, 2007 (15-17 Apr 2007): 324-328.

These authors describe their usage of WSN to form a system that monitors coal mines – the conditions within the coal mine and the localization of miners. They discuss the topology of such a system, and the hardware, software, and algorithm designs of their system. They do a poor job of discussing their simulation or experiments and reporting results of any system validation that may have been performed. Instead, they choose just to say that they were satisfied with the system's performance and list the reasons why. They then mention issues to consider in perfecting their system – evaluation and deployment of the system to evaluate performance and reliability, optimization of data collection and processing capabilities, and improving localization precision and tracking of minors through wireless sensors.

[WERNE06] Werner-Allen, G., Lorincz, K., Ruiz, M., Marcillo, O., Johnson, J., Lees, J., Welsh, M. Deploying a Wireless Sensor Network on an Active Volcano. *IEEE Internet Computing*, Volume 10, Issue 2, March-April 2006: 18-25.

In this article, the authors detail the work they've done thus far in using wireless sensor networks to aid in the study of active volcanoes. While they don't discuss much of they theory of their system, their attention to certain system attributes – overcoming high data rate with event detection and buffering, reliable data transmission and time synchronization, and command and control are all appreciated. They also discuss their experiences of deploying on Volcan Reventador in Ecuador and early results they collected. While their work seems promising and grounded in much physical implementation and deployment, they admit to lacking more ambitious research of implementing sophisticated data processing within the wireless sensor network itself.

[YULIA05] Yu, Liyang., Wang, N., Meng, X. Real-Time Forest Fire Detection with Wireless Sensor Networks. *2005 International Conference on Wireless*

Communications, Networking and Mobile Computing, 2005 (23-26 Sept 2005): Volume 2, 1214-1217.

The authors of this article claim that they have developed a WSN that can detect and forecast forest fires more quickly and accurately than the traditional detection approach using satellites. This paper details their neural-network method of processing data, and the evaluation of their system. They conclude by comparing their system with other related works, and claiming that the simulation results show the efficiency of their network. Their lack of future goals or improvement work to the system is a bit disappointing. They also fail to mention or address security of their system, and they offer no solid trial deployment of their system for validation purposes.

[ZHANG04] Zhang, B., Sukhatme, G.S., Requicha, A.A. Adaptive Sampling for Marine Microorganism Monitoring. *IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2004. IROS 2004 Proceedings (28 Sept – 2 Oct 2004): Volume 2, 1115-1122.

In this article, the authors detail their design and construction of a network of underwater sensors that monitor for marine microorganisms by detecting extreme temperature gradients. They discuss their adaptive sampling algorithm, which uses a distributed binary search. Then they prove the validity of their algorithm using simulation and experiments on their mote test bed, and even seek to improve the energy efficiency of their system through the introduction of a submarine robot to be used as a data mule. This is an interesting application of WSN, but as discussed in the article, there are limitations and assumptions that they are working to overcome. Also, no mention of wireless security is made or discussed.

[ZHOUH07] Zhou, B., Hu, C., Wang, H., Guo, R., Meng, M.Q.-H. A Wireless Sensor Network for Pervasive Medical Supervision. *IEEE International Conference on Integration Technology*, 2007. ICIT '07 (20-24 Mar 2007): 740-744.

The authors of this article start by setting their product apart from other systems developed to address real time medical supervision of at-risk patients. They make it a defining point to highlight their more commercially feasible design, and their product's strength of not only reporting bio-information on a patient, but also the surrounding environment's parameters and patient's video or picture in emergencies. They claim that this additional information can be useful to medical professionals when they are looking to make judgments about an illness. They discuss the system architecture as well as implementation issues faced, and to a fairly complete job of presenting an overview of their system. But they also readily admit that there are still some challenging issues that they face, including cross-layer security management in the network to protect patient's private information from being modified or eavesdropped on.

Appendix B

Annotated Bibliography of Wireless Ad Hoc Sensor Network Security Issues

[BROWN05] Michael Brownfield. Wireless Sensor Network Denial of Sleep Attack. In: Proceedings of the IEEE Workshop on Information Assurance and Security United States Military Academy, 2005

The paper analyzes the energy resource vulnerabilities of WSNs, which are targeted by attacks known as denial-of-sleep attacks. At full power the buttery-powered motes can run for only about two weeks before exhausting their batteries. Most mote power consumption happens when mote is transmitting or listening. Therefore, it is crucial that motes are active (awake) at around 1% duty cycle and remain in sleep mode for the rest of the time. An attacker can exhaust a mote's resources by repeatedly sending RTS messages to get CTS responses from a targeted mote. In this case all the motes within the radio range of the sender will be receiving those control packets, thus draining their power supplies. The attacker may also send a constant stream of unauthenticated or replayed broadcast packets causing the motes to remain awake.

The various contention-based MAC protocols such as Sensor MAC (S-MAC), Berkeley MAC (B-MAC) or Timeout MAC (T-MAC) were designed with the goal of extending the network life cycle by minimizing number of collisions, idle listening, or message overhearing. These protocols synchronize the transmitting activities and sleep of motes, thus providing for saving of battery power. The article describes the denial of sleep vulnerabilities of previously mentioned WSN MAC protocols and presents a new WSN MAC protocol (G-MAC), which has been proven to dramatically mitigate effects of denial-of-sleep attacks.

[CHATZ07] Chatzigiannakis I., Strikos A. A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks. In: Proceedings of IEEE Conference on Emerging Technologies & Factory Automation, ETFA., September, 2007.

This paper summarizes existing security threats in WSN and points out the major attacks against large-scale wireless sensor networks used for monitoring/surveillance purposes. The authors stress the importance of protection from both inside and outside intruders and propose the decentralized and energy-efficient intrusion detection systems to deal with security threats in WSN. The authors suggest that an effective intrusion detection system should be hierarchical pointing out that such structure helps to overcome limited energy sources available to sensor motes. They show that the hierarchical routing method presented in the article is more resilient to attacks from malicious participants (i.e., internal adversaries) even though it might

not be the best energy path to base station. The authors admit that there is a tradeoff of energy efficiency in favor of increased security.

[DENGH04] J. J. Deng, R. Han, and S. Mishra. Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks. In: Proceedings of International Conference on Dependable Systems and Networks, IEEE CS Press, 2004, pp. 637–656.

An adversary may perform network traffic analysis to determine the geographic location of critical motes, such as neighbors of the base station or base station itself. The attacker can then physically disable these motes or may even be able to attack the base station thus disabling the entire network. The asymmetry of traffic, when most data flows directed toward base station would reveal the location of a base station. Thus the authors suggest that uniform sending rate over the entire network should be created. This can be achieved by dynamically setting the sending rate between motes, when "dummy packets" are sent to equalize the traffic volume. Thus, the location of the base station would be disguised from an adversary. In order not to allow the isolation of base station by disabling its neighbor motes, the authors propose secure set up of multiple paths to base station.

[DENGH05] J. Deng, R. Han, and S. Mishra. Defending against Path-Based DoS Attacks in Wireless Sensor Networks. In: Proceedings of 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM Press, 2005, pp. 89–96.

Inherent limitations of WSNs such as insecure medium, limited processing capability, and energy-deprived nature of the network path-based Denial of Service attacks make them vulnerable to path-based Denial of Service attack. These attacks can disable large portion of a WSN. The path-based Denial of Service attack is based on an attacker activity of injecting spurious or replayed packets into the network at leaf motes. As a result, motes along the path will exhaust their power supply. Because of the tree-structured topology of a WSN, motes that are located downstream from motes along the main path will be unable to communicate with base station. Eventually, path-based Denial of Service attack disables a big portion of a WSN. The paper focuses on defending against such path-based Denial of Service attack with the use of one-way hash chain (OHC) mechanism. The authors prove that this mechanism impose almost no burden on computational power and energy expenditure and, yet, provides efficient way to defend against path-based Denial of Service attacks.

[DUTTA06] P.K. Dutta et al., Securing the Deluge Network Programming System. In: Proceedings of 5th International Conference on Information Processing in Sensor Networks, ACM Press, 2006, pp. 326–333.

Such effective and convenient feature of TinyOS's Deluge network-programming system as remote reprogramming of the motes holds the possibility of Deluge (reprogramming) attack. An adversary can hijack the reprogramming session, and, as

a consequence, to get control over either some portion of a network or over entire network. The article presents the method of securing of the reprogramming process. The authors underline the fact that traditional cryptographically-strong, public key-based system for source authentication and integrity verification cannot be implemented in resource-constrained sensor motes. They proposed the idea of dividing program binary into series of messages, each message containing hash of next message. It becomes impossible for an adversary to construct the message that matches hash contained in previous message. Secure initiation of legitimate reprogramming process is provided by digitally signed advertisement, which contains the program name, version number, and hash of the first message.

[KARLO03] C. Karlof and D. Wagner. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. In: Proceedings of 1st IEEE International Workshop on Sensor Network Protocols and Applications, IEEE Press, 2003, pp. 113–127.

The article presents a comprehensive overview on attacks on routing protocols in WSNs and proposed countermeasures. Vulnerabilities of WSNs in respect to routing protocols are analyzed. The authors prove that sensor network routing protocols must be designed with security as a goal. The authors present countermeasures and design considerations for secure routing protocols in sensor networks.

[NGAIL06] E.C.H. Ngai, J. Liu, and M. R. Lyu .On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks. In: Proceedings of IEEE International Conference on Communications (ICC '06.), June 2006.

The paper presents the novel approach to defend a WSN from a sinkhole attack. In a wireless sensor network, multiple motes send sensor readings to a base station for further processing. Such a many-to-one communication is highly vulnerable to the sinkhole attack, where an intruder attracts surrounding motes with unfaithful routing information, and then performs selective forwarding or alters the data passing through it. A sinkhole attack forms a serious threat to sensor networks, especially because of their limited computation and energy sources. The algorithm, presented in the paper, first finds a list of suspected motes, and then effectively identifies the intruder in the list through a network flow graph. The algorithm is also robust to deal with cooperative malicious motes that attempt to hide the real intruder. The authors evaluate the performance of the proposed algorithm through both numerical analysis and simulations and make a conclusion about effectiveness and accuracy of the algorithm. They also found out that the algorithm's communication and computation overheads are reasonably low for wireless sensor networks.

[PERRI04] A. Perrig, J. Stankovic, and D. Wagner. Security in Wireless Sensor Networks. In: Communications of. ACM, Vol. 47(6), Jun 2004, pp. 53-57.

The paper highlights the challenges to providing security in WSN. The authors stress the necessity of integrating of the security into every component, since components designed without security can become a point of attack. The authors give a deep

analysis of WSNs security challenges including key establishment, secrecy, authentication, privacy, robustness to denial-of-service attacks, secure routing, and mote capture. The paper contains a rich set of ideas about future research in the area of WSN security.

[RAYMO06] D. Raymond et al., Effects of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols. In: Proceedings of 7th Annual IEEE Systems, Man, and Cybernetics (SMC) Information Assurance Workshop (IAW), IEEE Press, 2006, pp. 297–304.

The paper presents another exploration of denial-of-sleep attack. Impacts of the attacks toward S-MAC, T-MAC, and G-MAC protocols are classified in this paper. The authors found out that full protocol knowledge and ability to penetrate link-layer encryption enables an adversary to lunch full domination denial-of-sleep attack and, consequently, reduce network lifetime to the minimum possible. The authors suggest a framework for defending against denial-of-sleep attacks in WSN, which includes five key components: strong link-layer authentication, anti-replay protection, jamming identification and mitigation, broadcast attack defense, and resilience to compromised motes. The authors analyze the state-of-the-art of those components and offer the ways of improvement.

[SABBA06] Sabbah E., Majeed A., Kang K., Liu K., and AbuGhazaleh, N. An Application Driven Perspective on Wireless Sensor Network Security. In: Proceedings of Q2SWinet'06, October 2, 2006, Torremolinos, Malaga, Spain.

The authors stress the challenging nature of WSN security due to their unique nature as an application and a network, and due to their limited capabilities. The authors claim that in order to be effective, security solution for WSN must be sensitive to the application and infrastructure of the WSN. The authors underline the necessity of application-specific security context as the combination of a potential attacker's motivation and the WSN vulnerability. The authors support their argument by two example applications, analyze security issues for each one, and describe application-specific security attacks and countermeasures in each case.

[SUNHS07] Hung-Min Sun, Shih-Pu Hsu, and Chien-Ming Chen. Mobile Jamming Attack and its Countermeasure in Wireless Sensor Networks. In: Proceedings of 2nd International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) 2007.

The article addresses the countermeasures mechanisms to the jamming attacks on WSNs. The authors classify a jamming attack as a denial-of-service attack in respect to such resource constrained property of WSNs as limited power supply. The authors present the novel type of jamming attack, namely, a mobile jamming attack. This attack not only threatens the link layer or physical layer, but also breaks the routing on WSN. The novel multi-data topologies defense scheme is proposed to withstand the mobile jamming attack. It has been proven that the proposed scheme successfully

mitigates the damage caused by mobile jammer while having light overhead in terms of energy consumption and computational power.

[WOODS02] A.D. Wood and J.A. Stankovic. Denial of Service in Sensor Networks, Computer, vol. 35, no. 10, 2002, pp. 54–62.

This article addresses the issue of incorporating security considerations into the process of system design. The article lays the ground for a layer-based approach to security in WSNs. The authors analyze the security threats at each of five layers and describe the adopted defense mechanisms. They stress the necessity of applying the defense strategies on a system level rather than trying to mitigate particular problems at particular layers.

[XUTRA05] W. Xu et al., The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In: Proceedings of 11th Annual International Conference on Mobile Computing and Networking, ACM Press, 2005, pp. 46–57.

The article addresses the most feasible and easy to perform attack on the physical layer, namely, a jamming attack. In this attack no knowledge is needed of the WSN that is being attacked, except for the frequency the motes are sending at. In jamming attack, the mote that performs the jamming will try to prevent, or interfere with, the reception of signals at motes in the surrounding WSN. It will do this by sending out a continuous random signal on the frequency that is used by the WSN. Affected motes will not be able to receive messages from other motes and will therefore be completely isolated until the jamming stops. The authors evaluate the effect of four different jamming attacks on sensor network availability, discuss the schemes for detecting the jamming attacks, and introduce two enhanced detection algorithms that enable reliable detection of jamming attacks.

[YUGOV01] Y. Yu, R. Govindan, and D. Estrin. Geograhical and Energy Aware Routing:A Recursive Data Dissemination Protocol for Wireless Sensor Networks, tech. report UCLA/CSD-tr-01-0023, Computer Science Dept., Univ. of California, Los Angeles, 2001.

One of the attacks that exploits WSNs's routing protocols vulnerabilities is aselective forwarding attack where a malicious mote can make itself a part of many routes and then drop all packets or, in order to be undetected, suppress or modify packets from a selected few motes while properly forward the remaining traffic. The way to combat selective forwarding attacks is a multipath routing. The same data is sent over multiple paths to give it a higher probability of reaching its destination. The paper discusses the Geographic and Energy Aware Routing (GEAR) algorithm which requires each mote to know its location and be able to communicate this location to other motes thus preventing malicious motes from becoming a part of legitimate routes and, consequently, disabling the selective forwarding attack. Also, the GEAR

algorithm has been proven to provide defense against HELLO flooding attacks because the algorithm allows motes to discount hello messages from motes not within communication range. This article can be considered as an example of successful adaptation of carefully thought out design approach to secure WSN development.

[YUXIA06] B. Yu and B. Xiao. Detecting Selective Forwarding Attacks in Wireless Sensor Networks. In: Proceedings of Symposium on Parallel and Distributed Processing, IPDPS 2006.

The paper presents another approach to defend WSNs from selective forwarding attacks. In such attacks, a malicious mote selectively drops sensitive packets. The authors argue that countering selective forwarding by using multipath forwarding suffers from several drawbacks. First, communication overheads increase dramatically as the number of paths increases. Second, multiple paths ultimately join up in the area neighboring the base station, so if motes around the base stations are compromised, selective forwarding is still applicable. Finally, the multipath forwarding shows poor security resilience. To compromise the system, an adversary only needs to ensure the presence of one compromised mote in each path. The authors propose lightweight security scheme that detects selective forwarding attacks by using a multihop acknowledgement technique that increases detection accuracy yet lowers overhead. The scheme allows both the base station and source motes to collect attack alarm information from intermediate motes. Thus even when the base station is temporarily deafened by adversaries, attacks can still be detected.

[ZHANG08] W. Zhang, N. Subramanian, and G. Wang. Lightweight and Compromise-Resilient Message Authentication in Sensor Networks. In: Proceedings of IEEE 27th Conference on Computer Communications INFOCOM, 2008.

The attack countermeasures at network layer are highly dependable on authentication. The authors suggest that use of public key for message authentication may impose high overhead in terms of computational cost and network bandwidth consumption. Use of symmetric keys and hash functions is effective, but when the sensor mote is compromised, its key material becomes known by an adversary. Therefore, the authors offer message authentication and verification via polynomials with independent and random factors for perturbation of preloaded to individual motes polynomial shares. While keeping the computational overhead low, this method increases the complexity for an adversary to break the secret polynomial thus making the authentication to be resilient to mote compromises.

References

[KATOP07] Katopodis, P., Katsis, G., Walker, O., Tummala, M., Michael, J.B. A Hybrid, Large-scale Wireless Sensor Network for Missile Defense. *IEEE International Conference on System of Systems Engineering*, 2007. SoSE '07 (16-18 Apr 2007): 1-5.

[RAZAA07] Raza, H.M.M.T., Akbar, A.H, Chaudhry, S.A., Bag, G., Yoo, S., Kim, K. A Yaw Rate Aware Sensor Wakeup Protocol (YAP) for Target Prediction and Tracking in Sensor Networks. *IEEE Military Communications Conference*, 2007. MILCOM 2007 (29-31 Oct 2007).

[KUCKE07] Kuckertz, P., Ansari, J., Riihijarvi, J., Mahonen, P. Sniper Fire Localization using Wireless Sensor Networks and Genetic Algorithm based Data Fusion. *IEEE Military Communications Conference*, 2007. MILCOM 2007 (29-31 Oct 2007).

[BEKME05] Bekmezci, I., Alagoz, F. A New TDMA Based Sensor Network for Military Monitoring (MIL-MON). IEEE Military Communications Conference, 2005. MILCOM 2005 (17-20 Oct 2005): Volume 4, 2238-2243.

[DIAMO07] Diamond, S.M., Ceruti, M.G. Application of Wireless Sensor Network to Military Information Integration. 5th IEEE International Conference on Industrial Informatics, 2007 (23-27 Jun 2007): Volume 1, 317-322.

[ZHOUH07] Zhou, B., Hu, C., Wang, H., Guo, R., Meng, M.Q.-H. A Wireless Sensor Network for Pervasive Medical Supervision. *IEEE International Conference on Integration Technology*, 2007. ICIT '07 (20-24 Mar 2007): 740-744.

[BAKER07] Baker, C., Armijo, K., Belka, S., Benhabib, M., et al. Wireless Sensor Networks for Home Health Care. 21st International Conference on Advanced Information Networking and Applications Workshops, 2007. AINAW '07 (21-23 May 2007): Volume 2, 832-837.

[TEAWH05] Teaw, E., Hou, G., Gouzman, M., Tang, K.W., Kesluk, A., Kane, M., Farrell, J. A Wireless Health Monitoring System. *IEEE International Conference on Information Acquisition*, 2005 (27 Jun – 3 Jul 2005).

[WERNE06] Werner-Allen, G., Lorincz, K., Ruiz, M., Marcillo, O., Johnson, J., Lees, J., Welsh, M. Deploying a Wireless Sensor Network on an Active Volcano. *IEEE Internet Computing*, Volume 10, Issue 2, March-April 2006: 18-25.

[YULIA05] Yu, Liyang., Wang, N., Meng, X. Real-Time Forest Fire Detection with Wireless Sensor Networks. *2005 International Conference on Wireless Communications, Networking and Mobile Computing*, 2005 (23-26 Sept 2005): Volume 2, 1214-1217.

[CHACZ05] Chaczko, Z., Zhmad, F. Wireless Sensor Network Based System for Fire Endangered Areas. 3rd International Conference on Information Technology and Applications, 2005. ICITA 2005 (4-7 July 2005): Volume 2, 203-207.

[ZHANG04] Zhang, B., Sukhatme, G.S., Requicha, A.A. Adaptive Sampling for Marine Microorganism Monitoring. *IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2004. IROS 2004 Proceedings (28 Sept – 2 Oct 2004): Volume 2, 1115-1122.

[LUKEJ07] Lu, Kejie; Qian, Y., Rodriguez, D., Rivera, W., Rodriguez, M. Wireless Sensor Networks for Environmental Monitoring Applications: A Design Framework. *IEEE Global Telecommunications Conference*, 2007. GLOBECOM '07 (26-30 Nov 2007): 1108 – 1112.

[PRABH07] Prabhakar, T.V., Rao, N.V.C, Sujay, M.S., Panchard, J., Jamadagni, H.S., Pittet, A. Sensor Network Deployment for Agronomical Data Gathering in Semi-Arid Regions. *2nd International Conference on Communication Systems Software and Middleware*, 2007. COMSWARE 2007 (7-12 Jan 2007): 1-6.

[SONGW07] Song, G., Wei, Z., Zhang, W., Song, A. A Hybrid Sensor Network System for Home Monitoring Applications. *IEEE Transactions on Consumer Electronics*. Volume 53, Issue 4, Nov 2007: 1434 – 1439.

[PARKB07] Park, H., Burk, J., Srivastava, M. Design and Implementation of a Wireless Sensor Network for Intelligent Light Control. *6th International Symposium on Information Processing in Sensor Networks*, 2007. IPSN 2007 (25-27 Apr 2007): 370-379.

[HWANG07] Hwang, I., Baek, J. Wireless Access Monitoring and Control System based on Digital Door Lock. IEEE Transactions on Consumer Electronics. Volume 53, Issue 4, Nov 2007: 1724-1730.

[KURAT06] Kurata, N., Saruwatari, S., Morikawa, H. Ubiquitous Structural Monitoring using Wireless Sensor Networks. *International Symposium on Intelligent Signal Processing and Communication*, 2006. ISPACS '06 (12-15 Dec 2006): 99-102.

[STOIA07] Stoianov, I., Nachman, L., Madden, S. PIPENET: A Wireless Sensor Network for Pipeline Monitoring. *6th International Symposium on Information Processing in Sensor Networks*, 2007. IPSN 2007 (25-27 Apr 2007): 264-273.

[SUNGA08] Sung, J., Ahn, S., Park, T., Jang, S., Yun, D., Kang, J., Yoo, S., Chong, P., Kim, D. Wireless Sensor Networks for Cultural Property Protection. *22nd International Conference on Advanced Information Networking and Applications – Workshops*, 2008. AINAW 2008 (25-28 Mar 2008): 615-620.

[LINWU08] Lin, M., Wu, Y., Wassell, I. Wireless Sensor Network: Water Distribution Monitoring System. *IEEE Radio and Wireless Symposium,* 2008 (22-24 Jan 2008): 775-778.

[SAMPI07] Sampigethaya, K., Li, M., Poovendran, R., Robinson, R., Bushnell, L., Lintelman, S. Secure Wireless Collection and Distribution of Commercial Airplane Health Data. *IEEE/AIAA 26th Digital Avionics Systems Conference*, 2007. DASC '07 (21-25 Oct 2007): 4.E.6-1 – 4.E.6-8.

[ABOEL06] Aboelela, E., Edberg, W., Papakonstantinou, C., Vokkarane, V. Wireless Sensor Network Based Model for Secure Railway Operations. *25th IEEE International Performance, Computing, and Communications Conference*, 2006. IPCCC 2006 (10-12 Apr 2006): 623 – 628.

[SENAR08] Senart, A., Karpinski, M., Wieckowski, M., Cahill, V. Using Sensor Networks for Pedestrian Detection. *5th IEEE Consumer Communications and Networking Conference*, 2008. CCNC 2008 (10-12 Jan 2008): 697-701.

[KINGB07] King, T.I., Barnes, W.J., Refai, H.H., Fagan, J.E. A Wireless Sensor Network Architecture for Highway Intersection Collision Prevention. *IEEE Intelligent Transportation System Conference*, 2007. ITSC 2007 (30 Sept – 3 Oct 2007): 178-183.

[SHASH06] Sha, K., Shi, W., Watkins, O. Using Wireless Sensor Networks for Fire Rescure Applications: Requirements and Challenges. *IEEE International Conference on Electro/Information Technology*, 2006 (7-10 May 2006): 239-244.

[WANGZ07] Wang, X., Zhao, X., Liang, Z., Tan, M. Deploying a Wireless Sensor Network on the Coal Mines. *IEEE International Conference on Networking, Sensing and Control*, 2007 (15-17 Apr 2007): 324-328.

[SONGC08] Song, B., Choi, H., Lee, H. Surveillance Tracking System using Passive Infrared Motion Sensors in Wireless Sensor Network. *International Conference on Information Networking*, 2008. ICOIN 2008 (23-25 Jan 2008): 1-5.

[CHEHR07] Chehri, A., Fortier, P., Tardif, P. Security Monitoring Using Wireless Sensor Networks. 5th Annual Conference on Communication Networks and Services Research, 2007. CNSR '07 (May 2007): 13-17.

[MAHLK07] Mahlknecht, S., Madani, S. On Architecture of Low Power Wireless Sensor Networks for Container Tracking and Monitoring Applications. *5th IEEE International Conference on Industrial Informatics*, 2007 (23-27 Jun 2007): Volume 1, 353-358.

[BUKKA07] Bukkapatnam, S., Komanduri, R. Container Integrity and Condition Monitoring using RF Vibration Sensor Tags. IEEE International Conference on Automation Science and Engineering, 2007. CASE 2007 (22-25 Sept 2007): 585-590.

[SHAFI07] Shafiullah, C.M.; Gyasi-Agyei, A., Wolfs, P. Survey of Wireless Communications Applications in the Railway Industry. *2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, 2007. AusWireless 2007 (23-30 Aug 2007).

[LIBEN06] Li, Benliang; Wang, H.; Yan, B.; Zhang, C. The Research of Applying Wireless Sensor Networks to IntelligentTransportation System (ITS) Based on IEEE 802.15.4. *6th International Conference on ITS Telecommunications Proceedings*, 2006. 939-942.

[EVERS07] Evers, L., Havinga, P. Supply Chain Management Automation using Wireless Sensor Networks. IEEE International Conference on Mobile Adhoc and Sensor Systems, 2007. MASS 2007 (8-11 Oct 2007): 1-3.

1[XUW05] Xu, W., et al. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. Proceedings of 11th Annual International Conference on Mobile Computing and Networking, ACM Press, 2005, 46–57.

2[SUNHS07] Sun, Hung-Min; Hsu, Shih-Pu; Chen, Chien-Ming. Mobile Jamming Attack and its Countermeasure in Wireless Sensor Networks. Proceedings of 2nd International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007.

[AIELL03] Aiello, G.R.; Rogerson, G.D.; "Ultra-wideband wireless systems", Microwave Magazine, IEEE , vol. 4, no. 2 , June 2003, 36-47.

[WOODS02] Wood, A.D., Stankovic, J.A. Denial of Service in Sensor Networks, Computer Magazine, vol. 35, no. 10, 2002, 54–62.

[BROWN05] Brownfield, Michael. Wireless Sensor Network Denial of Sleep Attack. Proceedings of the IEEE Workshop on Information Assurance and Security, United States Military Academy, 2005.

[STAJA99] Stajano, F.; Anderson, R. The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks. Proceedings of 7th International Workshop on Security Protocols, Springer, 1999, 172–194.

[RAYMO06] Raymond, D., et al. Effects of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols. Proceedings of 7th Annual IEEE Systems, Man, and Cybernetics (SMC) Information Assurance Workshop (IAW), IEEE, 2006, 297–304.

[KARLO03] Karlof, C.; Wagner, D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Proceedings of 1st IEEE Inernational Workshop on Sensor Network Protocols and Applications, IEEE, 2003, 113–127.

[YUGOV01] Yu, Y.; Govindan, R.; Estrin, D.. Geograhical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks, tech. report UCLA/CSD-TR-01-0023, Computer Science Dept., Univ. of California, Los Angeles, 2001.

[SUNK06] Sun, K., et al., Secure Distributed Cluster Formation in Wireless Sensor Networks. Proceedings of 22nd Annual Computer Security Applications Conference, IEEE, 2006, 131–140.

[DENGH05] Deng, J.; Han, R,; Mishra, S. Defending against Path-Based DoS Attacks in Wireless Sensor Networks. Proceedings of 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM Press, 2005, 89–96.

[DENGH04] Deng, J. J.; Han, R.; Mishra S. Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks. In: Proceedings of International Conference on Dependable Systems and Networks, IEEE CS Press, 2004, pp. 637–656.

[ZHANG08] Zhang, W.; Subramanian, N.; Wang, G. Lightweight and Compromise-Resilient Message Authentication in Sensor Networks. Proceedings of IEEE INFOCOM, 2008.

[BERNS08] Bernstein, D.J., "SYN Cookies." Website: http://cr.yp.to/syncookies, Accessed: August 20, 2008.

[DUTTA06] Dutta, P.K., et al., Securing the Deluge Network Programming System. Proceedings of 5th International Conference on Information Processing in Sensor Networks, ACM Press, 2006, 326–333

[LIUMA97] Liu,H.; Ma, H.; El Zarki, M.; Gupta, S. Error Control Schemes for Networks: An Overview. Mobile Network Applications, 2(2), 1997, 167-182.

[SUNPE06] Sun, K; Peng, P.; Ning, P.; C.Wang. Secure Distributed Cluster Formation in Wireless Sensor Networks. Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC 22), 2006.