Security Threats, Effects and Recovery methods on Wireless AdHoc Sensor networks

Lalita Yadav
Ph.D - Research Schloar
Dravidian University, Andhra Pradesh

Dr. P. C. Saxena
School of Computer & System Sc.
Jawaharlal Nehru University

Abstract - This paper presents a survey on Wireless Ad Hoc Sensor network security threats, effects and recovery methods. In this we discuss the security issues of Wireless Sensor network and countermeasures by Layers. 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. 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.

KeyWords : Wireless AdHoc, Network Security , Sensor , Network .

I. INTRODUCTION

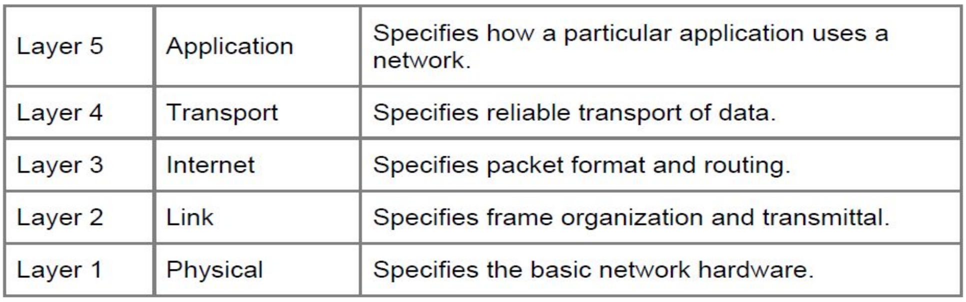
Wireless Ad Hoc Sensor Network Security Issues

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 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

II. Physical Layer -Wireless Ad Hoc Sensor Network Security Issues

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 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.

Physical Layer

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). 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 attacker's 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 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.

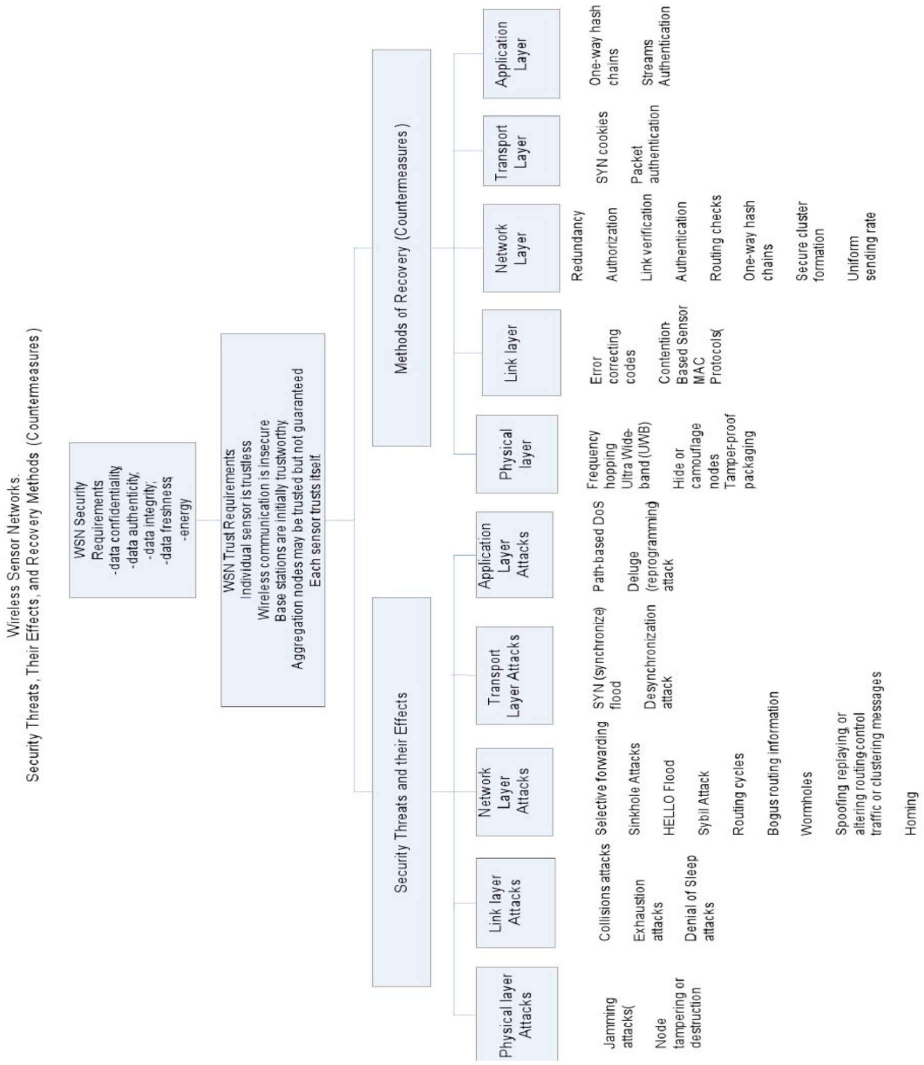
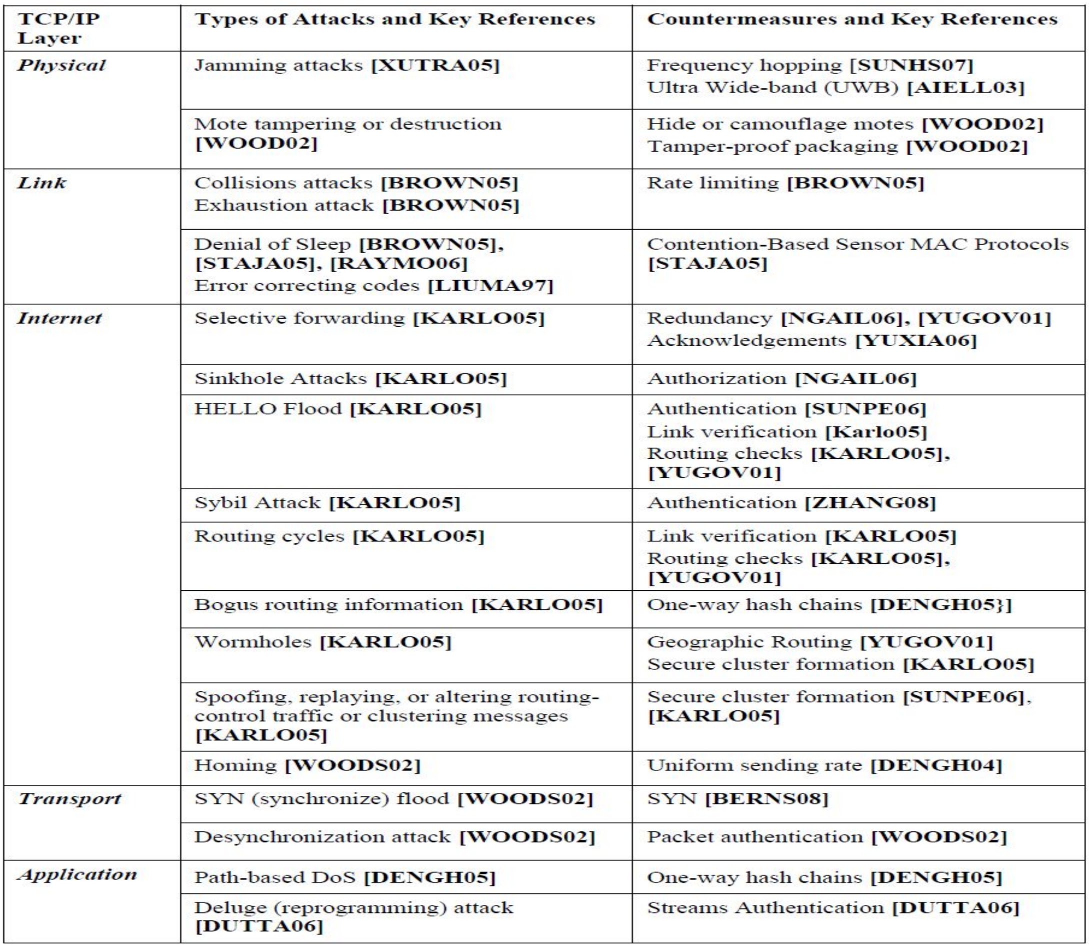


FIGURE 4: Wireless Ad Hoc Sensor Network Security Threats, Effects, and Recovery Methods



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

III. 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.

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.

REFERENCES

[1] [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.

[2] [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).

[3] [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).

[4] [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.

[5] [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.

[6] [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.

[7] [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.

[8] [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).

[9] [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.

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

[11] and Mobile Computing, 2005 (23-26 Sept 2005): Volume 2, 1214-1217.

[12] [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.

[13] [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, 1115-1122.12.

[14] [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. 39

[15] [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.

[16] [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.

[17] [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.

[18] [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.

[19] [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.

[20] [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.

[21] 19 .[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.

[22] [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.

[23] [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.

[24] [ABOEL06] Aboelela, E., Edberg, W., Papakonstantinou, C., Vokkarane, V. Wireless SensorNetwork Based Model for Secure Railway Operations. 25th IEEE International Performance,

[25] Computing, and Communications Conference, 2006. IPCCC 2006 (10-12 Apr 2006): 623 – 628.