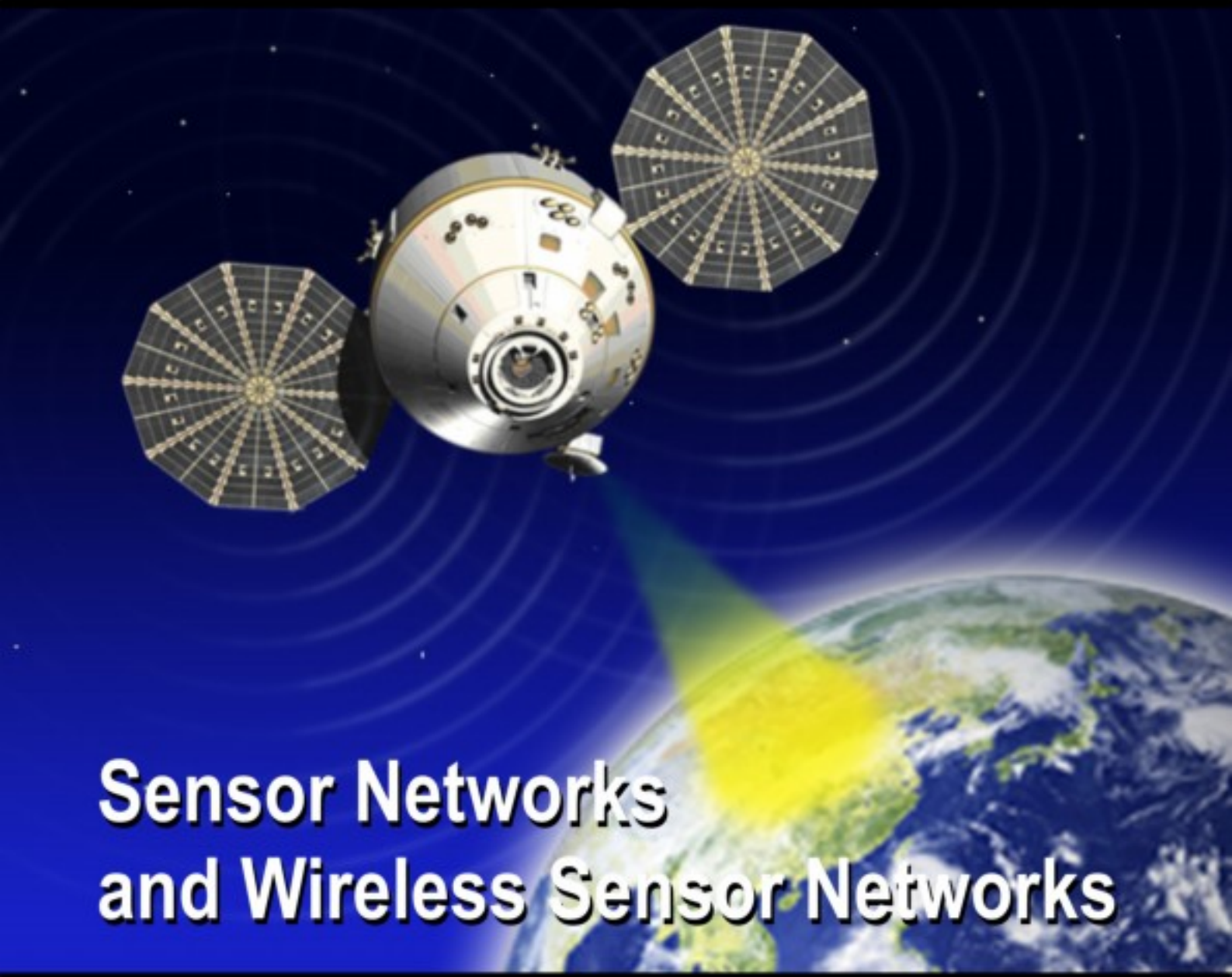
ISSN 1726-5479

SENSORS & TRANSDUCERS

vol. 94
7/08



Sensor Networks and Wireless Sensor Networks

International Frequency Sensor Association Publishing

IFSA

Sensors & Transducers

Volume 94
Issue 7
July 2008

www.sensorsportal.com

ISSN 1726-5479

Editor-in-Chief: professor Sergey Y. Yurish, phone: +34 696067716, fax: +34 93 4011989,
e-mail: editor@sensorsportal.com

Sensors & Transducers Journal (ISSN 1726-5479) is a peer review international journal published monthly online by International Frequency Sensor Association (IFSA). Available in electronic and CD-ROM.

Sensors & Transducers Journal

Contents

Volume 94
Issue 7
July 2008

www.sensorsportal.com

ISSN 1726-5479

Research Articles

Authors are encouraged to submit article in MS Word (doc) and Acrobat (pdf) formats by e-mail: editor@sensorsportal.com
Please visit journal's webpage with preparation instructions: http://www.sensorsportal.com/HTML/DIGEST/Submition.htm

Sensors & Transducers Journal, Vol. 94, Issue 7, July 2008, pp. 91-102

www.sensorsportal.com

Sensors & Transducers

ISSN 1726-5479

http://www.sensorsportal.com

A Survey of Sensor Network Security

[*1]A. VASEASHTA and [2]S. VASEASHTA

[*1] Nanomaterials Processing & Characterization Laboratories
Graduate Program in Physical Sciences, Marshall University
One John Marshall Drive, Huntington, WV 25755-2570, USA
[2] School of Computer and Information Sciences, Nova Southeastern University
3301 College Avenue, Fort Lauderdale-Davie, Florida 33314-7796, USA
E-mail: prof.vaseashta@marshall.edu, vaseasht@nova.edu

Received: 6 January 2008 /Accepted: 21 July 2008 /Published: 31 July 2008

Abstract: Sensor networks deploy sensor nodes to detect and monitor environmental events and interactions. Existing sensor networks focus on communication within the bounds of resource restrained sensor nodes at the expense of security. In this paper, a review of sensor network components, architectures, algorithms and protocols aims to increase awareness of sensor network limitations and resulting strategies to ensure information security within wireless sensor networks. Because sensor networks deployments are increasing rapidly, designers and implementers need to be aware of attacks and best practices to reduce misuse and compromise of private information. *Copyright © 2008 IFSA.*

Keywords: Sensor, Network, Protocols, Security

1. Introduction

In the 1990's, Internet usage sparked a revolution in everyday living by adding another media venue for obtaining information, goods, and services. Global networking infrastructures grew to appease user demands for easy access to information and services. In fact, users have become so accustomed to having access to communication and information tools that they demand these services beyond the boundaries of the home or office. The popularity of cellular phone services, Personal Digital Assistants, and wireless Internet access is the first glimpse of a new revolution in networking technologies characterized by being always connected. The next decade promises us a realm of everyday and specialized devices with network capabilities that seamlessly anticipate our needs,

monitor our environment, and interact with us to enhance life [1]. Micro-Electro-Mechanical Systems (MEMS) advances in semiconductor technology, digital electronics, and wireless networking are converging to create the architecture for sensor networks [1].

Wireless networking designs fall into two categories: wireless connections to wired infrastructures and ad-hoc networks requiring no wired infrastructure [2]. Sensor networks are a hybrid between the two. Nodes within a sensor network can communicate with each other without a fixed infrastructure, but are wirelessly linked to monitoring centers that collect data from the sensor network for processing within a wired infrastructure [3]. Sensors monitor events that occur within an environment from forces of nature, mechanical, or human intervention [1]. A system design that connects sensor networks to an Internet infrastructure with web based services promises a host of applications meeting residential, commercial, industrial, scientific, and governmental needs [1]. Accordingly, networking professionals must be able to design, implement, and maintain sensor networks offering high integrity and security. The purpose of this report is to investigate common sensor network components, architectures, algorithms and protocols to increase awareness of the sensor network limitations and resulting strategies to ensure information security within wireless sensor networks.

2. Sensor Network Components

Martinez, Hart, and Ong [4] report that a generic architecture of a sensor network includes sensor nodes, base stations, a sensor network server, and World Wide Web connectivity. Satyanarayanan [5] notes that sensors capable of generating signals have been used in computing applications for years. Sensors used in sensor networks are often referred to as smart sensors or smart dust because of their processing, power, and memory capabilities [5]. The small size of sensors allows them to be easily embedded into materials [5] or deployed in a mobile environment such as floats over water [2]. Sensor nodes often work with each other to decide what data will be transmitted throughout the ad-hoc sensor network onto the base station [4]. Raw data originating from sensor networks is processed by scientists and systems personnel for different applications [4].

Within a sensor network, sensor nodes are the hardware components that define network capabilities and implementations. The semiconductor industry giant, Intel and the University of California at Berkeley partnered to support Kris Pister's Smart Dust ubiquitous computing research that led to the development of the first Berkeley mote [6]. With a goal of designing a cubic-millimeter computer, the Smart Dust project explored emerging miniaturized components, integrated system on a chip designs, and methods for providing and conserving power to such systems [7]. Micro-electro-mechanical-systems (MEMS) make up the essential components of sensors, radio frequency and optical communication components, and power supplies [7]. Microelectronics is used for the smallest components [7]. Both solar cells and batteries provide a power source [7]. Data transmission involves use of a retroreflector for external light sources, or a laser diode with mirrors for internal light sources. Optical data reception is supported by a photodiode [7]. Processing, communications, control, storage, and energy management occur on integrated circuits [7]. A centimeter long antenna can support radio frequency communications; whereas an antenna or steering lens can support optical communications [7]. Sensor nodes have hardened enclosures suitable for different environmental conditions [6].

Measuring 1.5 inches in diameter, the first Berkeley mote was able to power itself, perform processing, transmit signals, and sense environmental factors on a cubic millimeter silicon chip [6]. As of 2003, a commercially available AA battery powered Berkeley mote uses an ". . . 8 bit, 7Mhz processor, a ChipCon CC1000 radio with a range of about 100 feet, 4KB of RAM, 128KB of program memory, 512 KB of off-chip non-volatile EEPROM, and a serial peripheral interface port" [8]. From the interface port, the user can connect a MEMS sensor board capable of detecting levels of ". . . magnetic fields, acceleration, vibration, movement, pressure, temperature, light, heat, and humidity" [8]. A mote

measures approximately 1.25 X 2.5 inches and will operate for about two years [6]. Within the mote; limited processing speed, memory, transmission capabilities, and power define operating systems, communications, computation, and querying capabilities.

According to Hamilton [6], the mote operating system, TinyOS developed by the University of California at Berkeley is a ". . . multithreaded, event-based OS designed precisely to explore new interfaces for this embedded realm". The modular design of the operating system allows customization according to developer needs [6]. Computation within a sensor node varies from traditional computing platforms. Sensor nodes must maximize processing while minimizing power consumption as opposed to computing platforms that seek to maximize processing while minimizing execution time [7]. Extremely fast, miniature transistors alleviate capacitor needs thus reducing power requirements [7]. Reducing the 3-micron fabrication process to a 0.18-micron fabrication process allows the mote processor core to fit within a scant 0.12-square millimeter space [7]. Low speed operations allow for reduced supply voltages needing only .3 volts for processing [7].

The purpose for deploying a sensor network will define the data to be acquired and when data acquisition takes place. Two models of database designs are emerging for sensor networks. A directed diffusion model queries each node individually and combines the responses to derive the output [9]. A collective model broadcasts a query to the entire sensor network simultaneously [8]. The Tiny Database (TinyDB) model, a collective model provides a simpler interface than programming the TinyOS [8]. Before responding to user queries, data must be accumulated by the sensors. Data sampling occurs in three methods: over a given time period, upon a certain event, or constantly over the life of the node or network [8]. Each method requires innovative design to overcome hardware constraints of nodes within the sensor network. Gehrke and Madden [10] advocate optimizing queries to minimize power consumption by distributing interactive queries to target sensor nodes that in turn can push the query to other nodes or pull the query from other nodes, and aggregating queries and responses to limit the amount of data crossing the sensor network.

3. Sensor Network Architecture

The topology of a sensor network must provide adequate coverage of the area being examined while minimizing power consumption [11]. The model for data acquisition and transmission within Wireless Integrated Network Sensor (WINS) architecture can be summarized in three steps: sensor nodes process sensor data locally, sensor nodes route data in multihop fashion to a WINS gateway server, a WINS gateway server routes data to a conventional network [12]. In some instances, designers can't control node placement; thus a system must be designed to help nodes organize themselves in a manner conducive to power efficiency [13]. The WINs architecture lends itself to broadcast or self-organizing topologies [13]. A broadcast topology floods the network with communications thus causing every sensor node to respond [13]. A self-organizing topology uses an algorithm to select sensors that must be involved in the communication path, evaluates and selects optimal communication paths, and repeats the process to maximize communications coverage [13].

4. Sensor Network Algorithms and Protocols

A review of sensor network devices, communications, computations, and querying technologies reveals that no standard suites of algorithms and protocols have emerged relevant to sensor networks [14]. Traditionally, the OSI model is the de-facto standard for designing network technologies. Bein and Datta [15] list the following five layers within the protocol stack for a sensor node based on the OSI model: Physical Layer, Data Link Layer, Network Layer, Transport Layer, and Application Layer.

The authors of this survey will review emerging sensor network algorithms and protocols according to processes, existing security measures, known vulnerabilities, and suggested countermeasures applicable to each layer.

4.1. Physical Layer Protocols, Vulnerabilities and Countermeasures

At the physical layer, a review of common protocols reveals that energy conservation is the overriding concern for sensor node and sensor network designers. Shih, Cho, Ickes, Min, Sinha, Wang, and Chandrakasan [16] advocate active, ready, monitor, observe, and deep sleep states for sensor nodes that allow physical layer voltage to be scaled according to task requirements. Hsin and Liu [17] propose a physical layer Role-Alternating, Coverage-Preserving Coordinated Sleep Algorithm (RACP) that seeks to optimize sensor network area coverage and power conservation according to a sleep schedule and stored energy. Physical layer signal modulation schemes include binary modulation (sending 1 bit at a time) and M-ary modulation (sending multiple bits per symbol) [16]. The M-ary modulation scheme increases circuitry but lowers transmission time to meet the ultimate goal of reduced power consumption. None of the above algorithms include security measures to prevent attacks that reduce power consumption. Because sensor networks communicate with radio frequency signals, they are subject to physical layer attacks from external devices capable of jamming node RF signals that constitutes a denial of service attack [18]. Radio jamming constitutes a denial of service attack within sensor networks because it can prevent nodes from communicating with other, or force nodes to attempt to communicate thus depleting node batteries [18]. Wood et al. [18] propose a Jammed-Area Mapping Service that allows affected nodes to detect and notify neighboring nodes of the jamming attack. Accordingly, neighboring nodes map the jammed area to bypass it while monitoring the area to determine if affected nodes are able to communicate normally again, and thus rejoin the network [18].

Realizing that sensor networks may be deployed in environments that are open to public access or perhaps even within a hostile attacker's environment prevents the first line of secure defense: controlled physical access to a node. At the Physical Layer, tamper resistant enclosures aren't conducive to sensor node design goals requiring low cost, lightweight, disposable products [19]. As noted by Uppuluri and Basu [20], physical access allows an attacker to read, alter, or erase any data within the node including security keys, algorithms, sensed data, the TinyOS, and other application code. Uppuluri and Basu [20] propose software based tamper resistant technique that specifies legitimate sequences of events that invoke reading the secret key and illegitimate sequences of events that cause command termination or key erasure.

Open physical access to the sensor network invites the placement of rogue nodes into the network or node capture and redeployment by smart attackers intent on eavesdropping or causing malicious behavior that redirects or interrupts communication and service [19]. In most deployments, establishing authenticated communication between sensor nodes involves symmetric key sharing. Accordingly, secure and efficient key distribution remains a research challenge. Most sensor node key exchange models require key distribution prior to deployment. According to Di Pietro, Mancini, and Mei [21], the easiest key distribution method is to equip all nodes with the same key for establishing communications prior to deployment. In the event of node capture, a system wide shared key compromises the entire sensor network [21]. In [22], Eschenauer and Gligor proposed a random-key predistribution scheme that allots several keys to nodes during initialization allowing secure communication to be established in the field when neighboring nodes discover one common shared key. Chan, Perrig, and Song [23] improve upon the security of Eschenauer and Gligor's [22] design by requiring at least two common shared keys for authenticated communication and updating communication keys for subsequent communications. The communication is authenticated with a key in these schemes but node identities are uncertain; thus Chan et al. [23] further advocate a random

pairwise key scheme that allows only two nodes to share the value of a particular key and supports key revocation by either a base station or neighboring nodes.

Watro, Kong, Cuit, Gardiner, Lynn, and Kruus [24] developed the TinyPK system that requires each node to be preloaded with a static Diffie-Hellman key pair and a text node identity string processed by a Certificate Authority's private key allowing node authentication. Huang, Mehta, Medhi, and Harn [25] advocate dividing sensor networks into zones that establish keys within and between zones that improves detection of malicious captured nodes to bypass infected areas. Wadaa, Olariu, Wilson, and Eltoweissy [26] propose a similar system that supports location awareness, group keys, session keys, revocation and re-keying, and member eviction within the group and network. Perrig, Szewczyk, Wen, Culler, and Tygar [27] propose the SPINS Secure Network Encryption Protocol (SNEP) and the µTimed, Efficient, Streaming, Loss-tolerant Authentication (µTESLA) components as building blocks for securing sensor networks. The SNEP component offers semantic security with an incremented counter that causes a different encryption result for the same message content, a Message Authentication Code (MAC) for verification of sending and receiving nodes, replay protection and weak assurance of data freshness via use of the encrypted counter [27]. The µTESLA component associates symmetric key release to a particular time interval; thus allowing recognition and denial of a spoofed packet using a key after time interval expires [27].

At the physical layer, sensor node processors limit computation of robust encryption algorithms that protect data from unauthorized disclosure during transmission. Venugopalan, Ganesan, Peddabachagari, Dean, Mueller, and Sichitiu [28] compared the computational requirements of the MD5 message digest hash, SHA-1 secure hash, RC5 symmetric key block cipher, RC4 symmetric key stream cipher, and IDEA International Data Encryption Algorithm symmetric key block cipher on several processing platforms common to sensor nodes. On a 4MHz Atmega 103 processor, the MD5 hash executed on 1-26 bytes of plaintext took 5,890 microseconds to process and the SHA-1 hash executed on 3 bytes of plaintext took 15,781 microseconds to process [28]. On the same processor, the RC5 cipher executed on 16 bytes of plaintext took 9,641 microseconds, 1,651 microseconds, and 1,636 microseconds to initialize, encrypt, and decrypt respectively and the RC4 cipher took 1,886 microseconds and 344 microseconds to initialize and encrypt respectively [28]. Finally, the IDEA cipher executed on 16 bytes of plaintext took 1,523 microseconds, 9,417 microseconds, 2,555 microseconds, and 2,614 microseconds to perform initialization of encryption, initialization of decryption, encryption, and decryption respectively [28]. For a frame of reference, on a Sparc 440 MHz platform, the same MD5 hash took 23 microseconds, the same SHA-1 hash took 27 microseconds, the same RC5 cipher took 28 microseconds for the initialization, 2 microseconds for the encryption, and 2 microseconds for the decryption, the same RC4 cipher took 96 microseconds for the initialization and 4 microseconds for the encryption, and the same IDEA cipher took 11 microseconds, 36 microseconds, 9 microseconds, and 9 microseconds for the initialization of encryption, initialization of decryption, encryption, and decryption, respectively [28].

4.2. Data Link Layer Protocols, Vulnerabilities and Countermeasures

Within the data link layer, sensor node protocols provide controlled access to the media communications channel in accordance with energy constraints. Caccamo and Zhang [29] propose an Implicit Earliest Deadline First (EDF) medium access control protocol that distributes a conflict free transmission scheduler across all nodes within a cellular topology requiring two transceivers for intra and inter cell communications. Biaz and Barowski [30] propose the GANGS MAC protocol that divides the sensor area into clusters called gangs. Within gangs, cluster head nodes with the highest energy reserves negotiate transmission between gangs until their reserves are depleted thus shifting the communication role and necessitating network re-convergence [30]. Polastre, Hill, and Culler [31] list operational features of the Berkeley Media Access Control (B-MAC) data link layer protocol: "The

Berkeley Media Access Control (B-MAC) uses Clear Channel Assignment (CCA) and packet backoffs for channel arbitration, link layer acknowledgements for reliability, and low power listening (LPL) for low power communication". Perhaps the most innovative Media Access Control method for wireless sensor nodes is the WiseNET system on a chip developed by Enz, El-Hoiydi, Decotignie, and Peiris [32]. The WiseNET system on a chip incorporates the battery, sensor, and transmitting and receiving radio frequency antenna on the same chip [32]. The WiseNET design features the WiseMAC Layer 2 protocol customized for low power performance within the WiseNET [32]. Comparable sensor node designs use 100 times the power of the WiseNET system on a chip [32]. The data link layer protocols above are distinguished by their abilities to conserve power and dynamically re-converge as nodes become inactive or nonfunctional within the sensor network area. While sensor network availability remains an important security goal, none of the above data link layer protocols are designed with inherent security measures.

Karlof, Sastry, and Wagner [33] propose TinySec as the first data link layer protocol that optimizes security, frame size, and resource conservation. To prevent unauthorized access to a message and support integrity of its contents, TinySec supports Message Authenticated Code (MAC) encryption of the data payload [33]. The TinySec protocol also uses initialization vectors to provide semantic security that prevents accurate prediction of the values of an encrypted message [33]. Finally, Karlof et al. [33] state that the only feasible link layer technique for combating replay attacks involves sending incremental counters with messages that allow nodes to reject replayed messages with old counters. Unfortunately, this technique involves the use of a table to store counters from no more than 25 nodes due to restricted memory within sensor nodes [33]. In fact, attempts to use this technique in sensor networks exceeding 25 nodes increases vulnerability to a denial of service attack from replayed broadcasts [33]. In this scenario, replayed broadcasts quickly fill the table causing the node to deny new communications or erase the table; thus permitting the replay attack [33].

4.3. Network Layer Protocols, Vulnerabilities and Countermeasures

At the network layer, protocols define addressing schemes and optimal routing methods. The Directed Diffusion scheme will identify and route data within a sensor network according to its attribute-value pairs instead of source and destination nodes used in traditional networks [9]. A centralized sink node will distribute a task throughout the sensor network defining interesting data such as an event [9]. Sensor nodes that detect interesting data begin forwarding their events to the task originators [9]. Elson and Estrin [34] define an addressing scheme for sensor networks: the Random, Ephemeral Transaction Identifier (RETRI). Within the RETRI addressing scheme, nodes identify each transaction with a semi-random number that is used until the transaction is complete [34]. The RETRI scheme has a size advantage that results in energy conscious transmission in comparison to global addressing schemes [34]. Heidemann, Silva, Intanagonwiwat, Govindan, Estrin, and Ganesan [35] define a naming scheme for sensor network data based on attributes such as sensor type and geographic location within a sensor network. The naming scheme developed by [35] avoids the necessity to map the name through several levels of processing and supports filtering and data aggregation techniques that reduce power consumption in a sensor network. The above addressing schemes include no support for traditional address filtering methods that permit or deny communication based on source and destination address. This limitation is once again caused by resource constraints. Elson and Estrin [34] note that the life of a sensor network is expended with each transmitted bit; and a global addressing scheme comparable to IP addresses would create packets that are almost entirely made up of addresses rather than sensed data.

The second function occurring at the network layer is selecting the optimal route for traffic as it flows through the network. Heidemann et al. [35] advocate hop-by-hop routing that identifies the data being transmitted instead of the transmitting node. A key objective of their research is to process data in the

sensor network, most specifically to aggregate data thus optimizing communications for node power conservation [35]. Hu, Liu, Lee, and Saadawi [36] propose an Efficient Route Update Protocol (ERUP) to select new routes within a sensor network. ERUP addresses routing problems caused by mobile and energy depleted nodes that are part of a routing path but are no longer able to route [36]. In order to conserve power, the route rediscovery process involves sending a Route Discovery Region (RDR) packet along the previous route thus establishing a broadcast region followed by a Route Request (RRQ) packet from the source involved in the broken link [36]. The RRQ packet stays within the Route Discovery Region thus confining route rediscovery to the affected area and avoiding unnecessary communications [36].

Wadaa, Olariu, Wilson, Jones, and Xu [37] advocate training the topology of a sensor network into wedge clusters pointing towards the central sink node. Each wedge has its own virtual path [37]. The wedge-based virtual paths form a virtual tree with the sink node being the trunk [37]. Transmissions from each wedge path to the sink node can be spread out over a period of time to avoid collisions [37]. Data aggregation is a recurring theme in sensor network routing processes because summarizing data reduces overall communications thus safeguarding power reserves. Roedig, Barroso, and Sreenan [38] propose a scheme for optimizing data aggregation along the routing path. To summarize data from different nodes, the data must be delayed and summarized at certain points within the network [38]. Roedig et al. [38] define an algorithm that calculates the most resourceful data aggregation points and delays.

The previously listed network layer protocols and algorithms assume that sensor nodes will gather data in a periodic or event-based fashion, thus focusing on determining the optimal paths from the nodes to the sink node to a traditional network infrastructure. Emerging research for acquiring data from sensor networks focuses on designing queries allowing the designer to specify the data to be collected and its subsequent transmission and processing within the sensor network to the sink node [10]. Sensor network designers traditionally use the C based programming language incorporated in the TinyOS to instruct each node about the data to be gathered [10]. Gehrke and Madden have designed sensor network query processors (SNQPs) called TinyDB and Cougar that operate on commercial sensor nodes. A pc base station can process the query, distribute the query into the sensor network, and gather responses from the sensor network [10]. Each node can support sensor-based software that receives queries, processes queries, performs runtime adaptation, catalogs, samples data, and communicates [10]. Transmissions are routed in a tree structure that uses the base station or storage node as the root [10]. Nodes have child and parent roles within the routing system [10]. A child node chooses one or more adjacent parent nodes based on the parent node's proximity to the root. Child nodes sharing the same parent communicate through the parent [10]. Queries flow from the base station down the parent-child hierarchy and responses flow up through the hierarchy to the base station [10].

The aforementioned network layer protocols are designed to route data through the most energy efficient means possible. In doing so, they improve the system availability goal of securing sensor networks, but none of the above protocols were designed to secure the routing process. A routing protocol that fails to authenticate and encrypt routing messages between nodes allows an adversary to spoof the routing message, alter the routing message, or replay the routing message [39]. Any of the three techniques allow the adversary to create routing loops, generate invalid control and error messages, permit unauthorized traffic or deny legitimate traffic, and delay and interrupt the entire routing process, and change routing paths [39]. The adversarial node capable of establishing itself within the optimal path can then read, alter, or drop all traffic it encounters [39]. Newsome, Shi, Song, and Perrig [40] shed insight into the Sybil attack whereby a node is capable of assuming multiple identities at once or over a time period by fabricating or stealing the identities of legitimate nodes. The Sybil attack begins when the malicious node listens to legitimate routing messages and replies directly to legitimate nodes in the absence of authentication and encryption, or a group of malicious nodes falsely advertise that they are within the optimal routing path in the absence of authentication and

encryption [40]. The Sybil attack allows adversaries to alter aggregated data, manipulate the trust factor of legitimate nodes in reputation based security schemes, and perform attacks and reinvent itself to launch new attacks [40].

4.4. Transport Layer Protocols, Vulnerabilities and Countermeasures

The transport layer is responsible for reliable delivery of data in conventional networks. Within sensor networks, research for transport layer protocols lags behind network layer protocols because there is a level of tolerance that the loss of a sensor reading is to be expected due to deployment environments [41]. However, in a directed diffusion environment, the sink node has the responsibility for defining the data to be sensed and in some cases, may define routing systems [41]. The loss of data from the sink node to sensor nodes may render the network useless for the sensing task being attempted [41]. Wan, Campbell, and Krishnamurthy [41] propose the Pump Slowly, Fetch Quickly (PSFQ) transport layer protocol that attempts reliable delivery on a hop-to-hop basis rather than source to destination basis used in traditional networks. Intermediate nodes along the path from sink to node or node to sink buffer and relay (pump) messages requesting retransmission (fetch) if a discontinuity in sequence numbers is detected. PSFQ sends a report message along with the transmission allowing each hop along the way to include feedback [41]. Sankarasubramaniam, Akan, and Akyildiz [42] propose the Event-to-Sink Reliable Transport (ESRT) protocol for use in sensor networks. The ESRT protocol supports self-configuration of the network topology, sensor node adjustment of reporting rate in instances of low power, congestion control by reducing the reporting rate, aggregated data, and sink node processing with limited sensor node processing [42]. ESRT focuses on event-to-sink reliability while PSFQ focuses on hop-to-hop reliability. The intent of these protocol designers focused on techniques to ensure available or more reliable delivery of data similar to sequencing and acknowledging techniques used in the TCP/IP transport layer. A transport layer protocol that fails to authenticate and encrypt the sequence number is open to replay attacks that can cause false data injection or denial of service attacks by forcing retransmission requests. Wagner [43] suggests that transport layer protocol designers consider that some aggregating functions are inherently more secure than others. As an example, the presence of one adversarial node that induces extremely high or extremely low readings has a substantial effect on computed averages, sums, minimums, and maximums aggregated within the TinyDB database-centric interface [43]. The count aggregate involves only the use of a 0 or a 1 value; thus the overall impact that one adversarial node can make is substantially reduced [43]. Wagner [43] suggests using the median reading as an aggregate where possible because a large number of malicious nodes must be present to significantly alter the resulting calculation. Similarly, Wagner [43] suggests trimming the highest 5% and lowest 5% of readings to combat extremely abnormal readings induced into the sensor network.

4.5. Application Layer Protocols, Vulnerabilities and Countermeasures

One function of the application layer in a sensor network is to provide an interface for managing the sensor network. Perillo and Heinzelman [44] advocate the Sensor Management Protocol (SMP) as a method of establishing a topology and controlling the quality of service by choosing sensor nodes most likely to meet application demands. Other researchers are developing java-based middleware and daemons for managing the sensor network. St. Ville and Dickman [45] propose the Garnet Java-based middleware architecture for managing data streams, deploying resource management strategies, and controlling requests. Brooks and Keiser [46] developed the Remote Execution and Action Protocol (REAP) mobile code daemons that operate on several wireless sensor networks and nodes. REAP handles message transmission between nodes, provides a method for object management, creates processes from a remote location, and supports monitoring and indexing [46]. The ability to manage a sensor network from a remote location is a necessity given that sensor networks are often deployed in

areas that are difficult or impossible for humans to enter or work in because of military or environmental factors [47, 4].

Perrig, Stankovic, and Wagner [48] point out that application layer services such as secure group management, intrusion detection, and random sampling of nodes and data may hold the most promise for sensor network security. Wadaa, Olariu, Wilson, Eltoweissy, and Jones [49] describe vulnerabilities induced when the network infrastructure is revealed during setup. Realizing that the sink node is a single point of failure, the identity of the sink node should be kept secret during network convergence processes [49]. Wadaa et al. [49] propose a solution that requires nodes to generate fake message traffic over many randomized points thus making the true sink undetectable during initial network setup. Ozturk, Zhang, and Trappe [50] describe an interesting attack aimed at detecting the exact location of a protected source by backtracking the routing process from the sink node to the protected source. Ozturk et al. [50] combat this attack by using phantom routing techniques that make it difficult and time-consuming for an adversary to determine which of the available paths lead to the protected source. Deng, Han, and Mishra [51] propose two techniques for protecting the base station, one-way hash routing messages over multiple paths and dummy messages that complicate traffic analysis by adversaries.

Intrusion detection techniques focus on identifying malicious nodes and optimal placement of intrusion detection nodes within the sensor network infrastructure. Pires, Figueiredo, Wong, and Loureiro [52] describe the HELLO flood attack and Wormhole attack both of which capitalize on physical layer RF signaling vulnerabilities. A HELLO flood attack is executed from a malicious node broadcasting an extremely powerful RF signal to fool many other nodes into thinking that this node is a neighbor [52]. The simplest method for combating this attack is to require receiving nodes to broadcast echoes back to transmitting nodes before establishing neighbor relationships [52]. While the malicious node may be capable of transmitting an abnormally strong signal, it may not be close enough to receive the normal echo reply required for neighbor establishment [52]. A Wormhole attack occurs when an adversary in one part of the network transmits a message to an adversary in a distant part of a network over a low-band channel [52]. The receiving adversary then can transmit packets to immediate neighbors that lead them to believe that they are closer to the originating adversary than they really are thus inducing traffic latency and incorrect routing [52]. Pires et al. [52] propose a technique that combines echoing, signal strength, and geographic location awareness that reveals malicious nodes transmitting from far distances. Both techniques proposed by Pires et al. [52] are indicative of anomaly based intrusion detection systems. Pirzada and McDonald [53] and Ganeriwal and Srivastava [54] advocate trust based intrusion detection systems for detecting and blacklisting nodes exhibiting anomalous behavior. Anjum, Subhadrabandhu, Sarkar, and Shetty [55] recommend that signature based IDS modules be placed on cluster heads within sensor network cluster topology schemes. Similar to signature based IDS systems, Qin and Lee [56] propose an application layer security management system that attempts to recognize attacks from low-level alerts, predict whether an attack is aimed at higher level processes, and predict future attacks based on known attacks.

5. Conclusion and Future Directions

Each component and data transmission within a sensor network offers challenges for reaching security goals. Culler et al. [1] state that sensor nodes must be small and inexpensive to be useful thus leading to limited power, processing, memory, and communication capacity. Easily installable components and easily usable interfaces and software systems must be developed for mainstream deployment [4]. Increased deployment of sensor networks creates an urgent need for solutions that secure sensor network infrastructure and communications [19]. Lax security raises the possibility of sensor network technology misuse [57]. Embedded sensors may track information about our personal lives that we consider private [57]. Data that seems harmless to an ethical person may present an opportunity for

criminal activity to an unethical person [57]. Very few researchers are exploring database techniques to protect private information gathered from sensor networks when national defense is the overriding concern [57]. Carman, Coffin, Dutertre, Swarup, and Watro [58] advocate the following research directions to improve existing sensor network security: improving cryptographic efficiencies within protocols, designing asymmetric algorithms that integrate outside resources, tight design of security features within applications, and recognizing levels of vulnerability appropriate for a wide variety of sensor node implementations. The outcomes of the author's investigation into sensor network security illustrate that sensor node hardware constraints require new architectures, identification schemes, algorithms and protocols that address security assurance within the physical, media access control, network, transport, and application layers. The academic and semiconductor research communities are actively deploying sensor networks to improve and develop off-the-shelf sensor hardware components, infrastructure guidelines, and protocols and systems for implementing and maintaining a sensor network [6]. The number of sensor network deployments increase daily and remarkably, initiatives are in place to interconnect isolated sensor networks. The ability to interconnect sensor networks to form a global sensor web creates a new source of data for widespread use and at present, a vulnerable target for compromise.

References

[1]. D. Culler, D. Estrin, M. Srivastava, Overview of sensor networks, *Computer*, 37, 8, 2004, pp. 41-49.

[2]. P. Mohapatra, Panel discussion: Wireless ad hoc networks for internet applications: real or hype, In *Proceedings of the 3rd IEEE Workshop on Internet Application*, San Jose, CA, USA, 23-24 June 2003, p. 72.

[3]. J. Wu, I. Stojmenovic. Ad hoc networks, *Computer*, 37, 2, 2004, pp. 29-31.

[4]. K. Martinez, J. Hart, R. Ong, Environmental sensor networks, *Computer*, 37, 8, 2004, pp. 50-56.

[5]. M. Satyanarayanan, Of smart dust and brilliant rocks, *Pervasive Computing*, 2, 4, 2003, pp. 2-4.

[6]. S. Hamilton, Intel research expands Moore's law, *Computer*, 36, 1, 2003, pp. 31-40.

[7]. B. Warneke, M. Last, B. Liebowitz, K. Pister, Smart dust: Communicating with a cubic-millimeter computer, *Computer*, 34, 1, 2001, pp. 44-51.

[8]. J. Hellerstein, W. Hong, S. Madden, The sensor spectrum: technology, trends, and requirements, *ACM SIGMOD Record*, 32, 4, 2003, pp. 22-27.

[9]. C. Intanagonwiwat, R. Govindan, D. Estrin, Directed diffusion: A scalable and robust communication paradigm for sensor networks, In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, Boston, MA, USA, 6-11 August 2000, pp. 56-67.

[10]. J. Gehrke, S. Madden, Query processing in sensor networks, *Pervasive Computing*, 3, 1, 2004, pp. 46-55.

[11]. K. Dasgupta, M. Kukreja, K. Kalpakis, Topology-aware placement and role assignment for energy-efficient information gathering in sensor networks, In *Proceedings of the IEEE International Symposium on Computers and Communication*, Kiris-Kemer, Turkey, 30 June–3 July 2003, pp. 341-348.

[12]. G. Pottie, W. Kaiser, Wireless integrated sensor networks, *Communications of the ACM*, 43, 5, 2000, pp. 51-58.

[13]. H. Gupta, S. Das, Q. Gu, Connected sensor cover: Self-organization of sensor networks for efficient query execution, In *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Annapolis, MD, USA, 1-3 June 2003, pp. 189-200.

[14]. R. Poor, C. Bowman, C. Auburn, Self-healing networks, *Queue*, 1, 3, 2003, pp. 52-59.

[15]. D. Bein, A. Datta, A self-stabilizing directed diffusion protocol for sensor networks, In *Proceedings of 2004 International Conference on Parallel Processing Workshops*, Montreal, Quebec, Canada, 15-18 August 2004, pp. 69-76.

[16]. E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, A. Chandrakasan, Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks, In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, Rome, Italy, 16-21 July 2001, pp. 272-287.

[17]. C. Hsin, M. Liu, Network coverage using low duty-cycled sensors: Random & coordinated sleep algorithms, In *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, Berkeley, CA, USA, 16-21 July 2004, pp. 433-442.

[18].A. Wood, J. Stankovic, S. Son, JAM: A jammed-area mapping service for sensor networks, In *Proceedings of the 24th IEEE International Real-Time Systems Symposium*, Cancun, Mexico, 3-5 December 2003, pp. 286-297.
[19].H. Chan, A. Perrig, Security and privacy in sensor networks, *Computer*, 36, 10, 2003, pp. 103-105.
[20].P. Uppuluri, S. Basu, LASE: Layered approach for sensor security and efficiency, In *Proceedings of the 2004 IEEE International Conference on Parallel Processing Workshops*, Montreal, Quebec, Canada, 15-18 August 2004, pp. 346-353.
[21].R. Di Pietro, L. Mancini, A. Mei, Efficient and resilient key discovery based on pseudo-random key pre-deployment, In *Proceedings of the 18th International Parallel and Distributed Processing Symposium*, Santa Fe, NM, USA, 26-30 April 2004, pp. 186-196.
[22].L. Eschenauer, V. Gligor, A key-management scheme for distributed sensor networks, In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, Washington, D. C. , USA, 18-22 November 2002, pp. 41-47.
[23].H. Chan, A. Perrig, T. Song, Random key predistribution schemes for sensor networks, In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 11-14 May 2003, pp. 197-215.
[24].R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, P. Kruss, TinyPK: Securing sensor networks with public key technology, In *Proceedings of the 2nd ACM workshop on Security of Ad Hoc and Sensor Networks*, Washington, D. C. , USA, 25 October 2004, pp. 59-64.
[25].D. Huang, M. Mehta, D. Medhi, L. Harn, Location-aware key management scheme for wireless sensor networks, In *Proceedings of the 2nd ACM workshop on Security of Ad Hoc and Sensor Networks*, Washington, D. C. , USA, 25 October 2004, pp. 29-42.
[26].A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, Scalable cryptographic key management in wireless sensor networks, In *Proceedings of the 24th International Conference on Distributed Computing Systems Workshops*, Tokyo, Japan, 23-26 March 2004, pp. 796-802.
[27].A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, SPINS: Security protocols for sensor networks, *Wireless Networks*, 8, 5, 2001, pp. 521-534.
[28].R. Venugopalan, P. Ganesan, P. Peddabachagari, A. Dean, F. Mueller, M. Sichitiu, Encryption overhead in embedded systems and sensor network nodes: modeling and analysis, In *Proceedings of the 2003 International Conference on Compilers, Architectures and Synthesis for Embedded Systems*, San Jose, CA, USA, October 29 – November 1 2003, pp. 188-197.
[29].M. Caccamo, L. Zhang, The capacity of implicit EDF in wireless sensor networks, In *Proceedings of the 15th European Conference on Real-Time Systems*, Porto, Portugal, 2-4 July 2003, pp. 267-278.
[30].S. Biaz, Y. Barowski, "GANGS": An energy efficient MAC protocol for sensor networks, In *Proceedings of the 42nd Annual ACM Southeast Regional Conference*, Huntsville, AL, USA, April 2-3, 2004, pp. 82-87.
[31].J. Polastre, J. Hill, D. Culler, Versatile low power media access for wireless sensor networks, In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, Baltimore, MD, USA, 3-5 November 2004, pp. 95-107.
[32].C. Enz, A. El-Hoiydi, J. Decotignie, V. Peiris, WiseNET: An ultralow-power wireless sensor network solution, *Computer*, 37, 8, 2004, pp. 62-69.
[33].C. Karlof, N. Sastry, D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, Baltimore, MD, USA, 3-5 November 2004, pp. 162-175.
[34].J. Elson, D. Estrin, Random, ephemeral transaction identifiers in dynamic sensor networks, In *Proceedings of the 21st International Conference on Distributed Computing Systems*, Phoenix, AZ, USA, 16-19 April 2001, pp. 459-468.
[35].J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, D. Ganesan, Building efficient wireless sensor networks with low-level naming, In *Proceedings of the 18th ACM Symposium on Operating Systems Principles*, Banff, Canada, 21-24 October 2001, pp. 146-159.
[36].X. Hu, Y. Liu, M. Lee, T. Saadawi, A novel route update design for wireless sensor networks, *Mobile Computing and Communications Review*, 8, 1, 2004, pp. 18-26.
[37].A. Wadaa, S. Olariu, L. Wilson, K. Jones, Q. Xu, On training a sensor network, In *Proceedings of the International Conference on Parallel and Distributed Processing Symposium*, Nice, France, 22-26 April 2003, p. 220b.
[38].U. Roedig, A. Barroso, C. Sreenan, Determination of aggregation points in wireless sensor networks, In *Proceedings of the 30th EUROMICRO Conference*, Rennes, France, 31 August – 3 September 2004, pp. 503-510.

[39].C. Karlof, D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, In *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, Anchorage, AL, USA, 11 May 2003, pp. *113-127*.

[40].J. Newsome, E. Shi, D. Song, A. Perrig, The sybil attack in sensor networks: Analysis & defenses, In *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, Berkeley, CA, USA, 26-27 April 2004, pp. 259-268.

[41].C. Wan, A. Campbell, L. Krishnamurthy, PSFQ: A reliable transport protocol for wireless sensor networks, In *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*, Atlanta, GA, USA, 28 September 2002, pp. 1-11.

[42].Y. Sankarasubramaniam, O. Akan, I. Akyildiz, ESRT: Event-to-sink reliable transport in wireless sensor networks, In *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Annapolis, MD, USA, 1-3 June 2003, pp. 177-188.

[43].D. Wagner, Resilient aggregation in sensor networks, In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, Washington, DC, USA, 24 October 2004, pp. 78-87.

[44].M. Perillo, W. Heinzelman, Wireless sensor networks, *Kluwer Academic Publishers*, Norwell, MA.

[45].L. St. Ville, P. Dickman, Garnet: A middleware architecture for distributing data streams originating in wireless sensor networks, In *Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops*, Providence, RI, USA, 19-22 May 2003, pp. 235-241.

[46].R. Brooks, T. Keiser, Mobile code daemons for networks of embedded systems, *IEEE Internet Computing*, 8, 4, 2004, pp. 72-79.

[47].M. Maroti, G. Simon, A. Ledeczi, J. Szitpanovits, Shooter localization in urban terrain, *Computer*, 37, 8, 2004, pp. 60-61.

[48].A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, *Communications of the ACM*, 47, 6, 2004, pp. 53-57.

[49].A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, K. Jones, On providing anonymity in wireless sensor networks, In *Proceedings of the 10th International Conference on Parallel and Distributed Systems*, Newport Beach, CA, USA, 7-9 July 2004, pp. 411-418.

[50].C. Ozturk, Y. Zhang, W. Trappe, Source-location privacy in energy-constrained sensor network routing, In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, Washington, DC, USA, 24 October 2004, pp. 88-93.

[51].J. Deng, R. Han, S. Mishra, Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks, In *Proceedings of the 2004 International Conference on Dependable Systems and Networks*, Florence, Italy, 28 June - 1July 2004, pp. 637-650.

[52].W. Pires, T. Figueiredo, H. Wong, A. Loureiro, Malicious node detection in wireless sensor networks, In *Proceedings of the 18th International Parallel and Distributed Processing Symposium*, Santa Fe, NM, USA, 26-30 April 2004, pp. 24b-25b.

[53].A. Pirzada, C. McDonald, Establishing trust in pure ad-hoc networks, In *Proceedings of the 27th Australasian Computer Science Conference*, Dunedin, New Zealand, 18-22 January 2004, pp. 47-54.

[54].S. Ganeriwal, M. Srivastava, Reputation-based framework for high integrity sensor networks, In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, Washington, DC, USA, 24 October 2004, pp. 66-77.

[55].F. Anjum, D. Subhadrabandhu, S. Sarkar, R. Shetty, On optimal placement of intrusion detection modules in sensor networks, In *Proceedings of the 1st International Conference on Broadband Networks*, San Jose, CA, USA, 25-29 October 2004, pp. 690-699.

[56].X. Qin, W. Lee, Attack plan recognition and prediction using causal networks, In *Proceedings of the 20th Annual Computer Security Applications Conference*, Tucson, AZ, USA, 6-10 December 2004, pp. 370-379.

[57].J. Kumagi, S. Cherry, Sensors & sensibility, *IEEE Spectrum*, 41, 7, 2004, pp. 22-28.

[58].D. Carman, D. Coffin, B. Dutertre, V. Swarup, R. Watro, Forum session: Security for wireless sensor networks, In *Proceedings of the 19th Annual Computer Security Applications Conference*, Las Vegas, NV, USA, 8-12 December 2003, pp. 106-107.

Guide for Contributors

Aims and Scope

Sensors & Transducers Journal (ISSN 1726-5479) provides an advanced forum for the science and technology of physical, chemical sensors and biosensors. It publishes state-of-the-art reviews, regular research and application specific papers, short notes, letters to Editor and sensors related books reviews as well as academic, practical and commercial information of interest to its readership. Because it is an open access, peer review international journal, papers rapidly published in *Sensors & Transducers Journal* will receive a very high publicity. The journal is published monthly as twelve issues per annual by International Frequency Association (IFSA). In additional, some special sponsored and conference issues published annually.

Topics Covered

Contributions are invited on all aspects of research, development and application of the science and technology of sensors, transducers and sensor instrumentations. Topics include, but are not restricted to:

- Physical, chemical and biosensors;
- Digital, frequency, period, duty-cycle, time interval, PWM, pulse number output sensors and transducers;
- Theory, principles, effects, design, standardization and modeling;
- Smart sensors and systems;
- Sensor instrumentation;
- Virtual instruments;
- Sensors interfaces, buses and networks;
- Signal processing;
- Frequency (period, duty-cycle)-to-digital converters, ADC;
- Technologies and materials;
- Nanosensors;
- Microsystems;
- Applications.

Submission of papers

Articles should be written in English. Authors are invited to submit by e-mail editor@sensorsportal.com 6-14 pages article (including abstract, illustrations (color or grayscale), photos and references) in both: MS Word (doc) and Acrobat (pdf) formats. Detailed preparation instructions, paper example and template of manuscript are available from the journal's webpage: http://www.sensorsportal.com/HTML/DIGEST/Submition.htm Authors must follow the instructions strictly when submitting their manuscripts.

Advertising Information

Advertising orders and enquires may be sent to sales@sensorsportal.com Please download also our media kit: http://www.sensorsportal.com/DOWNLOADS/Media_Kit_2008.pdf

Smart Sensors Systems Design

A five-day advanced engineering course

10-14 November 2008, Barcelona, Spain

SMARTSES
Marie Curie Chair (ERC) project

General Information

This course is suitable for engineers who design different digital and intelligent sensors, data acquisition, and measurement systems. It is also useful for researchers, graduate and post graduate students. Course will be taught in English.

Course Description

An advanced engineering course describes modern developments and trends in the field of smart sensor systems and digital sensors design.

After a general overview of data acquisition methods, modern smart, digital and quasi-digital sensors, smart systems details are discussed. A systematic approach towards the design of low-cost high-performance smart sensors systems with self-adaptation and self-identification possibilities is presented.

Contact Person

Susana Escriche
Fundació UPC. Edifici Vèrtex
Plaça Eusebi Güell, 6, 08034 Barcelona
Tel.: +34 93 401 08 94
E-mail: susana.escriche@fundacio.upc.edu

Course Instructor

Prof. Sergey Y. Yurish,
Centre de Disseny d'Equips Industrials (CDEI),
Universitat Politecnica de Catalunya (UPC-Barcelona)
Tel.: + 34 93 401 74 37, fax: + 34 93 401 19 89
E-mail: syurish@sensorsportal.com

Online Registration:

http://www.sensorsportal.com/HTML/SSSD_Course_2008.htm

Deadline for Registration:

31 October, 2008

Fundació UPC

MARIE CURIE ACTIONS

IFSA

www.sensorsportal.com