Mainka Saharan, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Security in Wireless Sensor Networks by using Machine Learning

Mainka Saharan, Professor Dr. Vishal Bharti
MMDU Ambala

Abstract- Wireless sensor networks (WSNs) have emerged as a vast technology in almost every fields, enabling prevalent monitoring and data collection in various environments. However, inherent characteristics of WSNs, such as resource constraints, dynamic network topology, and vulnerability to various at- tacks, pose significant security challenges. This paper provides a comprehensive review of security issues in WSNs, including authentication, confidentiality, integrity, availability, and resilience against attacks. Various security mechanisms and protocols proposed to address these challenges are analyzed, highlighting their strengths, limitations, and suitability for different applications. Addition- ally, the paper discusses future research directions and emerging trends in WSN security, aiming to provide researchers and practitioners with insights to develop robust and secure WSN solutions."

Keywords - Wireless Sensor Networks (WSNs) , Security, Confidentiality, Integrity, Availability, Attacks, Intrusion Detection , Encryption , Key Management ,Trust Establishment ,Secure Routing ,Data Aggregation , Energy Efficiency , Resilience

I. INTRODUCTION

Wireless sensor networks (WSNs) have developed as a generative technology with applications spreading environmental monitoring, healthcare, industrial automation, and smart cities. These networks consist of large small scale, resource-strained sensor nodes that collect data from their surroundings and transmit it to a central base station or lower node [1]. However, the prevalent development of WSNs in caviling infrastructure and actual environments has brought forth a host of security challenges that must be referenced to ensure the reliability, integrity, and confidentiality of the transmitted data. This paper aims to provide an extensive overview of the security issues and challenges in WSNs. We will explore the fundamental security requirements of WSNs, including authentication, confidentiality, integrity, and availability, and discuss the specific threats and vulnerabilities that intimate these requirements. Furthermore, we will analyze existing security mechanisms and protocols designed to mitigate these threats, highlighting their strengths, weaknesses, and applicability in different scenarios [2]. In addition to addressing current challenges, we will also identify emerging trends and future research directions in WSN security.

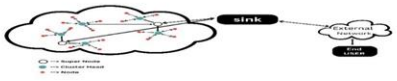


Figure 1: Wireless Sensor

This includes the inspection of novel cryptography techniques, incursion detection mechanisms, and secure routing protocols sewn to the unique characteristics of WSNs. By shedding light on the pressing security concerns and potential solutions in WSNs, this paper aims to provide researchers, practitioners, and policymakers with valuable insights to enhance the security posture of wireless sensor networks and foster their widespread adoption in critical applications.

II.LITERATURE REVIEW

Introduction to Wireless Sensor Networks and Security: W.S.Ns and their significance in various applications such as environmental inspection,

healthcare, and industrial automation. Introduce the value of security in Wireless Sensor Networks due to their sensitivity to various attacks, including eavesdropping, tampering, and node compromise. Highlight the particular characteristics of Wireless Sensor Networks, such as resource restraints, dynamic topology, and distributed nature, which challenges to implementing security mechanisms.

Security Threats and Attacks in Wireless Sensor Networks: Identify natural security hazards and attack vectors targeting W.S.N. including node capture, sinkhole attacks, wormhole attacks, and denial-of-service attacks. Discuss the potential impact of these attacks on the integrity, confidentiality, and availability of data transmitted and processed by sensor nodes.

Existing Security Mechanisms and Solutions: Review popular cryptography techniques such as asymmetric and symmetric encryption algorithms, digital signatures and key management protocols suited for Wireless Sensor Networks. Explore lightweight cryptography algorithms and protocols optimized for resource-constrained sensor nodes in terms of energy consumption and computational overhead [4]. Discuss network-layer security protocols (e.g., LEACH, TEEN) and routing algorithms designed to mitigate routing attacks and ensure data confidentiality and integrity. Examine intrusion detection and prevention systems (IDS/IPS) tailored for Wireless Sensor Networks, including distortion detection algorithms and distributed monitoring techniques.

Key Management and Secure Communication: Investigate key management schemes for secure key distribution, establishment, and revocation in Wireless Sensor Networks , considering factors such as scalability, resilience to node compromise, and energy efficiency. Discuss secure communication protocols and techniques for data transmission and aggregation, including datacenter routing, multi path routing, and data fusion strategies.

Energy-Efficient Security Solutions: Explore energy aware security mechanisms and protocols designed to minimize the impact of security operations on sensor node energy consumption. Discuss sleep/wake scheduling algorithms, duty cycling techniques, and energy-efficient cryptography primitives for proving network lifetime while maintaining security.

Privacy and Trust Management: Discuss privacy-preserving techniques and anonymity protocols to protect sensitive information collected and transmitted by sensor nodes. Examine trust management models and reputation-based mechanisms for evaluating the trustworthiness of sensor nodes and mitigating insider threats and malicious behaviors.

Case Studies and Practical Implementations: Analyze real-world deployments and case studies of security solutions in Wireless Sensor Networks across various application domains [5]. Evaluate the effectiveness, scalability, and performance overhead of security mechanisms in practical Wireless Sensor Networks deployments.

III. FUTURE DIRECTIONS AND RESEARCH CHALLENGES

Identify emerging trends and research gaps in security for Wireless Sensor Networks , such as securing Internet of Things integration, blockchain-based solutions, and quantum-resistant cryptography. Propose directions for future research, including interdisciplinary approaches, standardization efforts, and cross-layer security optimizations for Wireless Sensor Networks.

IV. FEASIBILITY OF BASIC SECURITY SCHEMES IN WIRELESS

Sensor Networks Security is a largely used term encircling the attributes of authentication, integrity, privacy, non reputation, and anti playback . The more trust on the information provided by the networks has been enlarged, the more the risk of secure transportation of information over the networks has enlarged. For the secure transportation of many types of information over networks, various

cryptography, stenographic and other techniques are used which are known.

Cryptography this is study of techniques for securing communication and data from third party. Here are some key concepts :

Encryption: Converting plain text into cipher text is called Encryption.

Decryption: Converting cipher text back into plain text by using secret key is known as decryption.

Symmetric Key Cryptography: Sender and receiver use the same key for encryption and decryption.

Asymmetric Key Cryptography: A public key for encryption and a private key for decryption.

Hash Functions: This take an input and produce a fixed-length string of characters, which is typically a digest that is unique to each individual input.

Digital Signatures: This method for verifying the authenticity and integrity of a message, software, or digital document.

V. CONSTRAINTS

Constraints in wireless sensor networks (WSNs) refer to various limitations and challenges inherent in the design, deployment, and operation of these networks. These constraints can significantly impact the performance, scalability, and security of WSNs. Here are some key constraints commonly observed in WSNs:

Limited Resources: Sensor nodes in WSNs are typically equipped with conditioned resources such as computational power, memory, and energy [7]. These constraints challenges in executing complex algorithms, storing large amounts of data, and maintaining continuous operation over extended periods.

Energy Constraints: Energy capability is a captious concern in WSNs due to the trust on battery-powered sensor nodes. The limited energy budget restricts the transmission range, data processing capabilities, and overall lifetime of sensor nodes. Energy-efficient protocols and mechanisms are necessary to prolong network longevity.

Bandwidth Limitations: WSNs often operate in bandwidth-constrained environments, especially in wireless communication spectrum allocated for low-power devices. Limited bandwidth imposes restrictions on the rate of data transmission and the size of messages exchanged between sensor nodes, requiring efficient data aggregation and compression techniques.

Communication Range: The communication range of sensor nodes determines the topology and connectivity of the network. However, the low transmission power of sensor nodes and the presence of obstacles can limit the effective communication range, leading to connectivity issues and network partitioning.

Deployment Challenges: WSNs are deployed in diverse and often harsh environments, ranging from remote locations to indoor settings. Deployment challenges include ensuring adequate coverage, managing node placement, addressing environmental factors (e.g., temperature, humidity), and dealing with physical obstacles that obstruct communication.

Fault Tolerance: Sensor nodes in WSNs are susceptible to failures due to hardware malfunctions, environmental factors, or malicious attacks [8]. Ensuring fault tolerance and resilience in the face of node failures is crucial for maintaining network connectivity and data reliability.

VI. SECURITY REQUIREMENTS (WSNS)

Confidentiality: Confidentiality ensures that sensitive information transmitted over the network remains private and inaccessible to unauthorized entities. [9] Encryption techniques such as symmetric and asymmetric cryptography are used to secure data transmission and prevent eavesdropping.

Integrity: Integrity ensures that data don't change and uncorrupted during transportation and processing. message authentication codes (MACs) and digital signatures are worked to detect and restrict unauthorized conversion to data.

Availability: Availability ensures that sensor nodes and network services are available and operational when needed. Denial-of-service (DoS) attacks and network failures can rupture the availability of WSNs. Therefore, measures such as repetition, load balancing, and intrusion detection systems are implemented to mitigate the impact of such attacks and failures.

Authentication: Authentication ensures the identity verification of sensor nodes and network users, preventing unauthorized access and malicious activities. Techniques such as already shared keys, digital certificates, and biometric authentication are used to authenticate nodes and users in WSNs.

Data Freshness: It ensures that sensor data is up-to-date and not replied from previous transmissions [10]. Timestamps and sequence numbers are commonly used to verify the freshness of data and prevent replay attacks.

Resilience: Resilience assure that WSNs can withstand and recover from many security threats and attacks. This includes the ability to detect, isolate, and mitigate security breaches, as well as the capability to adaptively reconfigure network resources to maintain functionality in the presence of interruption.

Energy Efficiency: Energy efficiency is a crucial security requirement in WSNs due to the limited energy resources of sensor nodes. Security structure and protocols should be designed to minimize energy expenditure while providing enough protection against security threats.

VII. SECURITY ALGORITHMS IN WIRELESS SENSOR NETWORKS (WSNS)

These algorithms play a critical role in alleviating various security threats and assuring the secure operation of WSNs. Here are some commonly used security algorithms in WSNs:

Symmetric Encryption Algorithms: This algorithms use a pair of key for both encryption and decryption.[11] This is computationally efficient and suitable for resource constrained sensor nodes. Common symmetric encryption algorithms used in WSNs include:

Advanced Encryption Standard (AES): A broadly prevalent symmetric encryption algorithm known for its security and efficiency.

Data Encryption Standard (DES): An eldest symmetric encryption algorithm that is less commonly used due to its relatively frail security.

Asymmetric Encryption Algorithms: Asymmetric encryption algorithms use a combination of public and private keys for encryption and decryption, respectively. They provide stronger security guarantees but are computationally more intensive compared to symmetric encryption algorithms. Common asymmetric encryption algorithms used in WSNs include:

Rivest-Shamir-Adleman (RSA): A very famous asymmetric encryption algorithm widely used for secure communication and digital signatures.

Elliptic Curve Cryptography (ECC): A very current asymmetric encryption algorithm known for its efficiency in terms of key size and computational complexity.

Hash Functions: This is used to generate strong hash values from input data. They are generally worked for data integrity verification and authentication in WSNs.

VIII. COMMON HASH FUNCTIONS USED IN WSNS

Secure Hash Algorithm (SHA): A group of cryptographic hash functions designed by the National Security Agency (NSA). SHA-1, SHA-256, and SHA-3 are mainly used variants.

Message Digest Algorithm (MD): A family of cryptographic hash functions, including MD5 and MD4, although MD5 is now considered insecure for many applications due to vulnerabilities.

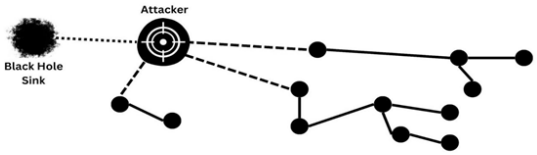


Figure 2: Black Hole

Attacks Information in transit: In this , sensors guide the modify exact parameters and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished.[12] As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks.

Black-hole : In this attack, a malignant node acts as a black-hole to engage all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. [13] Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations. Figure 2 shows the conceptual view of a black hole/sinkhole attack.

Hello Flood Attack : This attack uses HELLO packets as a baton to satisfy the sensors in WSN. In this sort of attack an attacker with a high speed radio transmission (termed as a laptop-class attacker) in range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor.[14] As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

Wormhole Attack: This is a type of network layer attack in wireless communication networks, particularly in ad hoc networks like mobile ad hoc networks (MANETs), wireless sensor networks (WSNs), and vehicular ad hoc networks (VANETs). It is a crucial security threat because it can disrupt network routing and degrade performance by creating a fake route between distant nodes, bypassing normal routing protocols.[15]

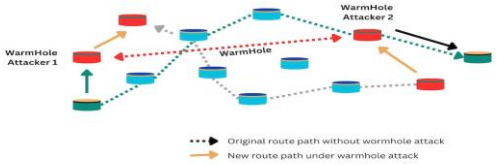


Fig. 3: Worm Hole Attack

IX. CHALLENGES IN SECURITY

Resource Constraints: Resource constraints are significant limitations that crush the overall performance, efficiency, and longevity of the network. These networks are made up of small, battery-powered sensor nodes developed in many environments to monitor and report data, such as temperature, humidity, or movement.

Limited Bandwidth: WSNs operate in bandwidth-constrained environments, which restrict the rate of data transmission and the size of messages exchanged between sensor nodes.[13.16] Efficient use of bandwidth is crucial for delivering security-related messages, such as cryptographic keys and security parameters, without overwhelming the network.

Dynamic Network Topology: WSNs exhibit dynamic and often unpredictable network topologies due to factors such as node mobility and node failures. Designing secure routing protocols and authentication mechanisms that can adapt to

changes in network topology while maintaining security is a significant challenge.

Physical Vulnerability: WSNs are deployed in open and uncontrolled environments, making them vulnerable to physical attacks such as node compromise and theft. Ensuring the physical security of sensor nodes and data transmission mediums is challenging, especially in outdoor deployments and hostile environments.

Key Management: Effective key management is important for establishing protected communication and ensuring data confidentiality and integrity in WSNs. [17] However, distributing, updating, and revoking cryptographic keys securely while considering resource constraints and network dynamics is a non-trivial task.

Authentication and Access Control: Authenticating sensor nodes and controlling access to network resources are critical for preventing unauthorized access and malicious activities.

Data Aggregation and Fusion: Data aggregation and fusion are commonly used techniques in WSNs to reduce redundant transmissions and conserve energy. However, these techniques introduce security challenges, such as ensuring the integrity and authenticity of aggregated data and detecting malicious data injection attacks.

Secure Localization: Localization is essential for many WSN applications, but it can be susceptible to attacks such as node spoofing and location tampering.[17] Ensuring the integrity and authenticity of localization information while preserving energy efficiency is a challenging task.

Reliability, Availability and Serviceability (RAS)

Reliability

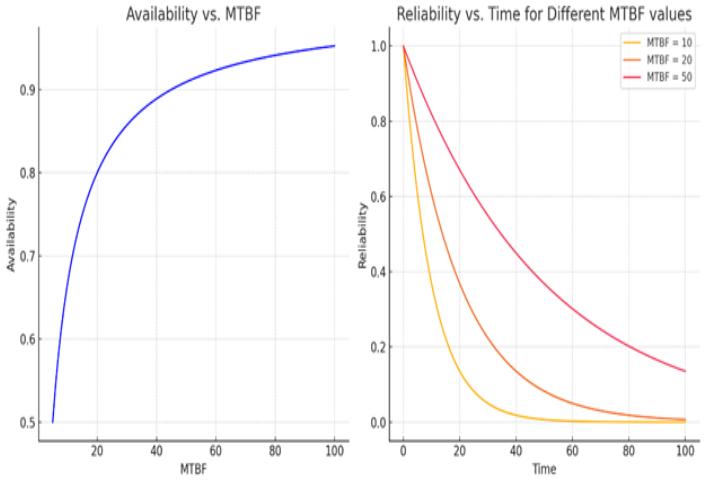
Reliability in WSNs refers to the ability of the network to consistently deliver accurate data from the sensors to the base station or CPU. Key factors impacting reliability in WSNs include:

Data accuracy: The data collected by sensors must be reliable, ensuring that transmission errors or environmental interference do not corrupt the information.

Packet loss: Minimizing packet loss, which may result from node failure, congestion, or signal interference, is vital to ensure reliable communication.[18]

PDR (Packet Delivery Ratio): The ratio of received packets to the total number of packets sent. A higher PDR indicates better reliability.

PDR= Number of packets sent/Number of packets received ×100% Mean Time Between Failures (MTBF): The average time between succesive node and network failures. A higher MTBF indicates better reliability.



Dependence availability and reliability on MTBF

Fault tolerance: Nodes in WSNs may fail due to energy depletion or environmental conditions, so the network should be designed to tolerate faults and recover quickly from them (self-healing networks).

Availability

Availability refers to the uptime of the WSN, the proportion of time the network is operational and ready to deliver services. Availability is crucial for applications like surveillance, disaster monitoring, or industrial automation, where network downtime can lead to critical issues.

Availability (A) = Uptime/(Uptime+DowntimeUptime)

In percentage terms:

Availability (A) = Uptime/(Uptime+Downtime) X 100

Where

Uptime: The period during which the network or system is functioning and available.

Downtime: The period during which the network is unavailable due to failure, maintenance, or other issues.

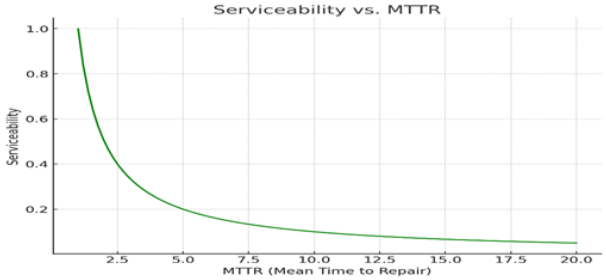
Node availability: Individual sensor nodes must remain functional and have sufficient energy to perform their tasks.

Network connectivity: The network topology must support redundancy (such as multiple communication paths) to ensure that even if a node or link fails, other routes can be used for communication.

Energy management: Since sensor nodes often rely on limited battery power, efficient energy consumption and energy harvesting techniques are essential to maintain long-term availability.

Serviceability

Serviceability relates to the ease with which the network can be managed, repaired, and maintained. In WSNs, especially those deployed in remote or harsh environments, maintaining the network can be challenging.



To find serviceability :

S= 1/MTTR

Where

MTTR is Mean Time to Repair

Node maintenance: Physical access to nodes for repair or replacement can be difficult. Therefore, remote configuration, over-the-air programming, and diagnostics are vital for serviceability.

Self-diagnosis and healing: Advanced WSNs can automatically detect faulty nodes, perform diagnostics, and sometimes reconfigure themselves (e.g., adjusting routes or task assignments) without human intervention.[30]

Scalability and adaptability: The network should support easy integration of new nodes and be adaptable to changing conditions, such as adding more sensors or altering operational parameters.

Challenges in RAS for WSNs:

Energy constraints: Wireless sensor nodes are often battery-powered, limiting their reliability and availability over long periods.

Environmental factors: Physical and environmental conditions (e.g., weather, obstacles) can affect communication reliability and node durability.

Interference and noise: Wireless communication is vulnerable to interference from other devices and noise, which can reduce reliability.

Proposed Security Schemes and Related Work

In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchers around the world. In this section we review and map various security schemes proposed or implemented so far for wireless sensor networks.

REFERENCES

Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.

Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at, http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf

Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534.

Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International

Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340.

Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets, M., and Tuan, T., "PicoRadios for wireless sensor networks: the next challenge in ultra-low power design" 2002 IEEE International Solid-State Circuits Conference (ISSCC 2002), Volume 1, 3-7 Feb. 2002, pp. 200 – 201.

Hollar, S, "COTS Dust", Master's Thesis, Electrical Engineering and Computer Science Department, UC Berkeley, 2000.

Saleh, M. and Khatib, I. A., "Throughput Analysis of WEP Security in Ad Hoc Sensor Networks", Proc. The Second International Conference on Innovations in Information Technology (IIT'05), September 26-28, Dubai, 2005.

Kurak, C and McHugh, J, "A Cautionary Note on Image Downgrading in Computer Security Applications", Proceedings of the 8th Computer Security Applications Conference, San Antonio, December, 1992, pp. 153-159.

Mokowitz, I. S., Longdon, G. E., and Chang, L., "A New Paradigm Hidden in Steganography", Proc. of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland, 2001, pp. 41 – 50.

Iyer, R., Kleinrock, L.: QoS control for sensor networks. In: IEEE International Conference onCommunications, vol. 1, pp. 517–521 (2003) Pottie, G., Kaiser, W.: Wireless integrated network sensors. Commun. ACM 43(5), 51–58 (2000) Estrin, D., Girod, L., Pottie, G., Srivastava, M.: MIT Technology Review: 10 emerging technologies that will change the world. MITTechnology Review, Cambridge (2003)

Rey, R.F.: Engineering and Operations in the Bell System. Bell Labs, New Jersy (1977)

Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Commun. ACM47(6), 53–57 (2004)Crawley, E., Nair, R., Rajagopalan, B., Sandick, H.: A framework for QoS-based routing inthe Internet. Internet informational RFC 2386, 37. http://wUHHUww.ietf.org/rfc/rfc2386.txt (1998)

Chen, S.: Routing support for providing guaranteed end-to-end quality-of-service. Ph.D.thesis, UIUC, 207.

http://cairo.cs.uiuc.edu/publications/papers/SCthesis.ps (1999)

Min, R., Bhardwaj, M., Cho, S.H., Shih, E., Sinha, A.: Low power wireless sensor networks.In: Proceedings of International Conference on VLSI Design, pp. 205–210 (2001)

Stallings, W.: Network security essentials. Applications and standards. Prentice Hall, UpperSaddle River (2000)

Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's Ad hoc Netw. J. Spec. Issue Sens. Netw. Appl. Protoc. 1(2–3), 293–315 (2003)

Kargl, F., Schlott, S., Klenk, A., Geiss, A.: Michael weber. Securing ad hoc routing protocols.In: IEEE EUROMICRO, pp. 514–519 (2004) Undercoffer, J., Avancha, S., Joshi, A., Pinkston, J.: Security for sensor networks, wireless sensor networks, pp. 253–275 (2004) Chiang, M.W., Zilic, Z., Radecka, K., Chenard, J.S.: Architectures of increased availability wireless sensor network nodes. In: ITC International Test Conference, vol. 43(2), pp. 1232– 124 (2004)

Knight, J.C.: An introduction to computing system dependability. In: Proceedings of the 26thInternational Conference on Software Engineering. IEEE Computer Society, pp. 730–731 (2004)

Callaway, E.H.: Wireless sensor networks architectures and protocols. Auerbach Publications, UK (2004)

Headquarters, Department of the Army, TM-5-698-1: Reliability/Availability of Electrical &Mechanical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance Facilities (2003)

Huang, C., Tseng, Y.: The coverage problem in a wireless sensor network. In: ACM International Workshop on Wireless Sensor Networks and Applications (WSNA), pp. 115– 121 (2003)

Kumar, S., Lai, T.H., Balogh, J.: On k-coverage in a mostly sleeping sensor network. In: International Conference on Mobile Computing and Networking, pp. 144–158 (2004) 7. Zhang, H., Hou, J.: On deriving the upper bound of α-lifetime for large sensor networks. In:

International Symposium on Mobile Ad Hoc Networking and Computing, pp. 121–132 (2004)

Gui, C., Mohapatra, P.: Power conservation and quality of surveillance in target tracking sensor

networks. In: International Conference on Mobile Computing and Networking, pp. 129–143 (2004)
Gage, D.W.: Command control for many-robot systems. In: Nineteenth Annual AUVSTechnical Symposium, vol. 10(4), pp. 28–34 (1992)
Hynes, S.: Multi-agent simulations (mas) for assessing massive sensor coverage anddeployment. Technical Report, Master's Thesis, Naval Postgraduate School (2003)
Gay, D., Levis, P., Culler, D.: Software design patterns for TinyOs. In: Proceedings of theACM SIGPLAN/SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems, pp. 40–49 (2005)
Kumar, S., Lai, T.H., Arora, A.: Barrier coverage with wireless sensors. In: MobiCom,pp. 284–298 (2005)
Niculescu, D., Nath, B.: Ad hoc positioning system (APS). In: INFOCOM 2003. IEEETwenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, pp. 1734–1743
Intanagonwiwat, C., Govindan, R., Estrin, D.: Directed diffusion: A scalable and robustcommunication paradigm for sensor networks. In: Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pp. 56–67 (2003)
Newsome, J., Song, D.: GEM: Graph embedding for routing and data-centric storage in sensornetworks without geographical information. In: Proceedings of the First ACM Conference on Embedded.