IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. III (Jan – Feb. 2015), PP 34-42
www.iosrjournals.org

Issues and Challenges in Distributed Sensor Networks- A Review

Sharada Y Yalavigi, Dr. Krishnamurthy G.N, Dr. NandiniSidnal

Abstract:*Distributed Sensor networks (DSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as process management, health care monitoring, environmental/earth sensing, industrial monitoring and many more scenarios. One of the major challenges distributed sensor networks face today is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future. The wireless communication technology also acquires various types of security threats. This paper discusses a wide variety of security, research, computational and design issues along with the challenges faced.*

Keywords: *Distributed Sensor Network, Design issues, Security issues, Defensive mechanisms, Challenges.*

I. Introduction

A Distributed Sensor Network can be defined as a set of spatially scattered intelligent sensors designed to obtain measurement from the environment, abstract relevant information from the data gathered, and to derive appropriate interferences from the information gained. Typical examples include temperature, light, sound, and humidity. These sensor readings are transmitted over a wireless channel to a running application that makes decisions based on these sensor readings. Many applications have been proposed for distributed sensor networks, and many of these applications have specific quality of service (QoS) requirements that offer additional challenges to the application designer.[18],[19].

We consider two aspects [8] to motivate an application-based viewpoint: First, what aspects of wireless sensors make the implementation of applications more challenging, or at least different?

One widely recognized issue is the limited power available to each wireless sensor node, but other challenges such as limited storage or processing capabilities play a significant role in constraining the application development. Second, what services are required for a wireless sensor network application toachieve its intended purpose? A number of widely applicable services, such as time synchronization andlocation determination are briefly discussed. Other services are needed to support database requirements, such as message routing, topology management, and data aggregation and storage.In this paper we discuss a wide variety of security, research, computational and design issues along with the challenges faced.

II. Design Issues And Challenges In Sensor Networks

Several design challenges [4],[5],[16],[20],[21]present themselves to designers of wireless sensor networkapplications. The limited resources available to individual sensor nodesimplies designers must develop highlydistributed, fault-tolerant, and energyefficientapplications in a small memory-footprint. For wireless sensor network applications to have reasonable longevity, an aggressiveenergy-management policy is mandatory. This is currently the greatest designchallenge in any wireless sensor network application. Several key differences between more traditional ad hoc networks and wirelesssensor networks exist. [8]

1) Individual nodes in a wireless sensor network have limited computationalpower and storage capacity. They operate on nonrenewable power sourcesand employ a short-range transceiver to send and receive messages.
2) The number of nodes in a wireless sensor network can be several orders of magnitudehigher than in an ad hoc network. Thus, algorithm scalability is animportant design criterion for sensor network applications.
3) Sensor nodes are generally densely deployed in the area of interest. This densedeployment can be leveraged by the application, since nodes in close proximitycan collaborate locally prior to relaying information back to the base station.
4) Sensor networks are prone to frequent topology changes. This is due to severalreasons, such as hardware failure, depleted batteries, intermittent radio interference,environmental factors, or the addition of sensor nodes. As a result,applications require a degree of inherent fault tolerance and the ability toreconfigure themselves as the network topology evolves over time.
5) Wireless sensor networks do not employ a point-to-point communication paradigmbecause they are usually not aware of the entire size of the network andnodes are not uniquely identifiable. Consequently, it is not possible to individuallyaddress a specific node. Paradigms, such as directed diffusion [,], employa data-

centric view of generated sensor data. They identify informationproduced by the sensor network as <attribute, value> pairs. Nodes requestdata by disseminating interests for this named data throughout the network.Data that matches the criterion are relayed back toward the querying node.

Even with the limitations individual sensor nodes possess and the designchallenges application developers face, several advantages exist for instrumentingan area with a wireless sensor network:[8]

1) Due to the dense deployment of a greater number of nodes, a higher level offault tolerance is achievable in wireless sensor networks.
2) Coverage of a large area is possible through the union of coverage of severalsmall sensors.
3) Coverage of a particular area and terrain can be shaped as needed to overcomeany potential barriers or holes in the area under observation.
4) It is possible to incrementally extend coverage of the observed area and densityby deploying additional sensor nodes within the region of interest.
5) An improvement in sensing quality is achieved by combining multiple,independent sensor readings. Local collaboration between nearby sensornodes achieves a higher level of confidence in observed phenomena.
6) Since nodes are deployed in close proximity to the sensed event, this overcomesany ambient environmental factors that might otherwise interfere withobservation of the desired phenomenon.

2.1 Data Aggregation:

Redundancy exists in sensordata in both the temporal and spatial domains. That is, readings collected by asingle sensor at different times or among neighboring sensors may be highlycorrelated, and contain redundant information. Instead of transmitting all thehighly correlated information to subscribers, it may be more effective forsome intermediate sensor node(s) to digest the information received andcome up with a concise digest, in order to reduce the amount of raw data tobe transmitted (and hence the power incurred, and bandwidth consumed, intransmission). This technique is termed as dataaggregation (also called data fusion).Data fusion can also be integrated with routing. Compared withtraditional address-centric routing, which finds the shortest paths betweenpairs of end nodes, data-fusion–centric routing aims to locate routes thatlead to the largest degree of data aggregation [41].

Theaggregation typically follows a tree topology rooted at thesink. Each leaf node would deliver its collected data to itsparent node. Intermediate sensor nodes of the tree mayoptionally perform certain operations (e.g., sum, maximum, minimum, mean, etc.) on the received data and forward theresult. Because the wireless medium is shared, transmissionsto forward the data need to be coordinated in orderto reduce interference and avoid collision. The fundamentalchallenge can be stated as: How can the aggregation transmissionsbe scheduled in a wireless sensor network suchthat no collision may occur and the total number of timeslots used (referred to as aggregation latency) is minimized?This is known as the Minimum-Latency Aggregation Scheduling(MLAS) problem in the literature.The MLAS problem is typically approached in two steps:(i) data aggregation tree construction and (ii) link transmissionscheduling. For (ii), we assume the simplest modein which every non-leaf node in the tree will make onlyone transmission, after all the data from its child nodeshave been received. A correct solution to the MLAS problemrequires that no concurrent transmissions interfering witheach other should take place. If steps (i) and (ii) are carriedout simultaneously in a solution, we have a ‘‘joint’’ design.

2.2 Time Synchronization

Sensor networks are used to monitor real-world phenomena. For such monitoringapplications, physical time often plays a crucial role. For example,the times of occurrence of physical events are often crucial for the observer to associate event reports with the originating physical events. Also, methods for localization of sensor nodes based on the measurement of time of flight or difference of arrival time of certain signals also require synchronized time. Providing synchronized physical time is a complex task dueto various challenging characteristics of sensor networks like energy and other resources, network dynamics, infrastructure and configuration.[17],[37].

Different applications like beam- forming array, data aggregation, recognition of duplicate detection of same event from different sensors, ordering of logged events have different synchronization requirements and also any single synchronization mechanism is not appropriate for all circumstances sensors should have multiple methods available to them so that they can dynamically trade precision for energy, or scope for convergence time. Existing time synchronization methods like NTP conserve use of bandwidth and try to keep the clock synchronization at all times but are not aware of the stringent energy constraints and the heterogeneity of the hardware that may be deployed in sensornets.

2.3 Localization

In emerging sensor network applications it is necessary to accurately orient the nodes with respect to a global coordinate system in order to report data that is geographically meaningful. Furthermore, basic middle ware services such as routing often rely on location information (e.g., geographic routing). Application contexts and potential massive scale make it unrealistic to rely on careful placement or uniform arrangement of sensors. Rather than use globally accessible beacons or expensive GPS to localize each sensor, we would like the sensors to self-organize a coordinate system.

Some of the design goals of localization in wireless sensor networks are:

- RF-based: Normally, the sensors have some kind of short-range radio transceivers for communication. By leveraging this radio for localization the high cost and size requirements of GPS can be avoided.
- Receiver-based: For greater scalability, the responsibility for localization must lie with the receiving node that needs to be localized and not with the reference points.
- Ad Hoc: For easy deployment, the solution should not require preplanning or extensive infrastructure.
- Low Energy: Since the sensors have modest processing capabilities, the mechanisms should minimize computation and message costs to reduce power consumption.
- Adaptive Fidelity: The accuracy of the localization algorithms should be adaptive to the granularity of available reference points.

Localization methods typically rely on some form of communication between reference points with known positions and the receiver node that needs to be located. Various localization techniques can be classified into two broad categories based on the granularity of information inferred during the communication. Fine-grained localization systems (e.g., GPS) provide high precision location information, typically estimated ranges or angles relative to beacons (reference points) and compute location of the unknown node using trilateration (position estimation from distance to three points) or triangulation (position estimation from angles to three points). Coarse-grained localization systems estimate unknown node location from proximity to beacons or landmarks

2.4 Node Deployment

Node deployment[11][45] in WSNs is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation. Intersensor communication is normally within short transmission ranges due to energy and bandwidth limitations. Therefore, it is most likely that a route will consist of multiple wireless hops.

2.5 Network Dynamics

Most of the network architectures assume that sensor nodes are stationary. However, mobility of both BS's and sensor nodes is sometimes necessary in many applications. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, in addition to energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application, e.g., it is dynamic in a target detection/tracking application, while it is static in forest monitoring for early fire prevention. Monitoring static events allows the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting and consequently generate significant traffic to be routed to the BS [12].

2.6 Energy Efficiency

Once the WSN is functional it becomes difficultto replace or recharge the battery of sensor nodes. This further posesthe challenge to maintain sensors in hostile and harsh environmentand scaling of sensor network to hundreds or thousands of nodes.Therefore, an energy-efficient mechanism is required to save energyand prolong the network lifetime [12].

2.7 Node/Link Heterogeneity

In many studies, all sensor nodes wereassumed to be homogeneous, i.e., having equal capacity in terms ofcomputation, communication, and power. However, depending onthe application a sensor node can have different role or capability.The existence of heterogeneous set of sensors raises many technicalissues related to data routing. These special sensors can be eitherdeployed independently or the different functionalities can beincluded in the same sensor nodes. Even data reading and reportingcan be generated from these sensors at different rates, subject todiverse quality of service constraints, and can follow multiple datareporting models.

For example, hierarchical protocols designate acluster-head (CH) node different from the normal sensors. Thesecluster heads can be chosen from the deployed sensors or can bemore powerful than other sensor nodes in terms of energy, bandwidth,and memory. Hence, the burden of transmission to the BS is handledby the set of cluster-heads [12].

2.8 Fault tolerance and reliability

For many WSN applications, datamust be delivered reliably over the noisy, error-prone, and timevaryingwireless channel. In such cases, data verification andcorrection on each layer of the network are critical to provide accurate results. Additionally, sensor nodes are expected to performself-testing, self-calibrating, self-repair and self-recovery proceduresduring their lifetime.

2.9 Scalability

Sensor networks should be scalable or flexible. Sensor networks dynamically adopt changes in node density and topology. Sometimes few nodes are added to the sensor networks existed nodes for the purpose of coverage issue. So sensor network is flexible to adapt these changes.

2.10 Data Centric Routing

In data-centric routing protocol, whenever a sink requires any data it sends a query message to the different part of the sensor network field. After receiving this query message sensors node replies and sends data to the sink. In data-centric protocol attribute based naming is used which specifies the properties of the data.

III. Security Issues And Challenges In Dsn

3.1 Security Requirements [2]-[6],[13][14][42]:

1) Availability

Availability determines whether a node has the ability touse the resources and whether the network is available forthe messages to communicate. However, failure of thebase station will eventuallythreaten the entire sensor network. Thus availability is ofprimary importance for maintaining an operationalnetwork.

2) Authentication

Authentication ensures the reliability of the message byidentifying its origin. Attacks in sensor networks do notjust involve the alteration of packets; adversaries can alsoinject additional false packets []. Data authenticationverifies the identity of the senders and receivers. Dataauthentication is achieved through symmetric orasymmetric mechanisms where sending and receivingnodes share secret keys. Due to the wireless nature of themedia and the unattended nature of sensor networks, it isextremely challenging to ensure authentication.

3) Confidentiality

Confidentiality is the ability to conceal messages froma passive attacker so that any message communicated viathe sensor network remains confidential. This is the mostimportant issue in network security. A sensor node shouldnot reveal its data to the neighbors.

4) Integrity

Data integrity in sensor networks is needed to ensurethe reliability of the data and refers to the ability toconfirm that a message has not been tampered with, altered or changed. Even if the network has confidentialitymeasures, there is still a possibility that the data integrityhas been compromised by alterations. The integrity of thenetwork will be in trouble when:

- A malicious node present in the network injectsfalse data.
- Unstable conditions due to wireless channel causedamage or loss of data. [4]

5) Data Freshness

Even if confidentiality and data integrity are assured, thereis a need to ensure the freshness of each message.Informally, data freshness [] suggests that the data isrecent, and it ensures that no old messages have beenreplayed. To solve this problem a nonce, or another time related counter, can be added into the packet to ensure data freshness

3.2 Security Attacks:

Attackers can be classified into two types: i) external attackers that are not authorized participants of the sensor network and ii) internal attackers that have compromised a legitimate sensor and use it to launch attacks in the network.Furthermore, attackers can be classified into passive and active. Passive attackers monitor network traffic without interfering with it. Their aim is to eavesdrop on the exchanged information and to acquire private data or to infer about information-sensitive applications that execute in the sensors. Active attackers disrupt network operation by launching several types of attacks that cause DoS (denial of service) in the DSN.

1) Denial of Service (DoS)

A Denial of Service attack in sensor networks in general is defined as any event that eliminates the network's capacity to perform its desired function. DoS attacks in distributed sensor networks may be carried out at different layers like the physical, link, network and transport layers. This occurs by the unintentional failure of sensor nodes. The simplest DoS attack tries to exhaust the resources available to the victim node, by transmitting additional unwanted packets and thus prevents legitimate sensor network users from tapping work or resources to which these nodes are deployed. In DSNs, several types of Denial of Service attacks in different layers might be performed, i.e. at physical layer, the Denial of Service attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and resynchronizations.

2) Spoofed, altered or replay of routing information

The most outstanding attack on routing is to alter, spoof, or just replay routing information and it is known as false routing information.Malicious nodes simply drop data packets quietly, modify the data content, generate false error messages or redirects the traffic.[17]

3) Selective forwarding

In this attack an attacker comprise itself in a data stream lane and can selectivelydrop only distinct packets. In sensor networks it is assumed that nodes faithfully forward received messages butsome compromised node might refuse to forward packets, though neighbors may start using another route.

4) Sinkhole attacks

The main goal of an adversary in sinkhole attack is to attract all the traffic toward itselfthrough an agreement node. Sinkhole attacks [10] typically work by making a compromised node look especiallyattractive to surrounding nodes.

5) Sybil attacks

In Sybil attack [10], a single node makes replicas of it and distributes it in multiple locations of thenetwork. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on thesensor network.

6) Wormhole attacks

In wormhole attack, more than two malicious colluding sensor nodes does a virtual tunnel in the sensor network, which is used to forward message packets between the tunnel edge points. This tunnel establishes shorter links in the network. In which adversary documents forwards packets at one location in the sensor network, tunnels them to different location, and re-forwards them into the sensor network. In sensor network when sender node sends a message to another receiver node in the network, then the receiving node tries to send the message to its neighboring nodes. The neighbor sensor nodes assume that the message was sent by the sender node (this is normally out of range), so they tries to forward the message to the originating node, but this message never comes because it is too far away. Wormhole attack is a great threat to sensor networks since, this type of attack will not require compromising a sensor in the network instead; it could be performed even at the starting phase during the sensors initializes to identify its neighboring information. This Wormhole attacks are very difficult to stop since routing information given by a sensor node is very difficult to check. The wormhole attack is possible even when the attacker has not compromised with any hosts nodes and even if all communication provides confidentiality and are authenticated also.

7) Hello flood attack

In this, HELLO packets will have high radio transmission range and these are used as weapons in DSN. This processing power sends HELLO packets to a number of sensor nodes, which are deployed, in a large area within a Sensor Network. The sensor devices are thus persuaded that the adversary is their neighboring node. As a result of this, while forwarding the messages to the base station, the victim sensor nodes try to go through the attacker as they are aware, that it is their neighborers and are spoofed by the attacker.[17]

8) Acknowledgement spoofing

The routing algorithm of a number of sensor networks depends on the explicit or implicit acknowledgement from the link layer. Because of this innate medium of broadcast medium, the attacker can be spoofing the acknowledgement from the link layer for sniffed packets that are meant for adjacent nodes. The aim of this attack is to make the sender nodes believe that the receiving node is in vicinity or even that a disabled/dead node is still alive.

IV. Measures To Overcome Issues And Challenges In Distributed Sensor Networks:

Table1: Various design issues and challenges and their requirements

Issue/Challenge	Requirements
Data Aggregation [41]	Energy efficient and low delay
Time Synchronization [37]	Rapid flooding, keeping track of neighboring nodes, overhead in terms of computation and memory allocation.
Localization [48]	Flooding, power consumption, number of anchors required for accurate localization
Node Deployment [45]	Energy and bandwidth limitations
Network Dynamics **Node/Link Heterogeneity [12][45]**	Route stability, energy, and bandwidth. Data routing issues.
Energy Efficiency [44][47]	MAC Scheduler, Data reduction, sleep/wake-up schemes, radio optimization and energy efficient routing.
Fault tolerance and reliability [12]	Reliability requirements: Noise-free, error-free, time-invariant wireless channel, error control, error detection and error correction techniques.Sensor nodes are expected to performself-testing, self-calibrating, self-repair and self-recovery proceduresduring their lifetime. Fault tolerance can be achieved with the help of redundant nodes.
Data Centric Routing [49][50]	Energy efficiency
Scalability	Topology control mechanisms
Security Requirements [4] **Availability**	Availability of resources and base station
Authentication	Authentication techniques like MAC (Message Authentication code)
Confidentiality	Encryption techniques
Integrity	Encryption techniques
Data Freshness	a nonce, or another time-related counter, can be added into the packet to ensure data freshness.

Table2: Various security attacks and their countermeasures

Type of attack	OSI layer	Characteristic[26][28]	Countermeasures
Denial of Service (DoS)[31]	Physical layer	Jamming,Tampering	Frequency hopping [2],[15], UWB(Ultra Wide Band) transmission technique, Changing and Protecting the key.**JAM** (Avoidance of jammed region by using coalesced neighbor nodes),Wormhole based (Uses wormholes to avoid jamming) [3][32]
	Link layer	Collision, Exhaustion, Unfairness	Time diversity and CRC [2][15], protecting the Network ID along with any information required for device joining [15]. Error correction code, rate limitation,small frames [6]
	Network layer	Neglect and greed, homing, misdirection, black holes.[31]	Restricting malicious node to join the network by secure network set up phase, REWARD routing protocol(Uses geographic routing, Takes advantage of the broadcastinter-radio behavior to watch neighbor transmissions and detectblackhole attacks)[2],[36]
	Transport layer	Flooding and de-synchronization	Limit the number of connections that an entity can make. Authenticating all the packets exchanged between sensor nodes along with all the control fields in transport header. The adversary cannot spoof the packets and header and thus this attack can be prevented.[2],[17] Client puzzles, Authentication [6],[38]
Spoofed, altered or replay of routing information	Link layer	Malicious nodes simply drop data packets, modify the data content, generate false error messages or redirects the traffic.	Authentication [2][15], On Communication Security (Efficient resource management, Protects the network even if partof the network is compromised) [3]
Selective forwarding [40]	Network layer	Attackers drop packets they have to route	Multipath routing, CHEMAS (Checkpoint-based Multi-hop Acknowledgement Scheme), a lightweight security scheme for detecting selective forwarding attacks. This scheme

			randomly selects a number of intermediate nodes as checkpoints which are responsible for generating acknowledgement. According to this scheme, along a forwarding path, if a checkpoint node does not receive enough acknowledgements from the downstream checkpoint nodes it can detect abnormal packet loss and identify suspect nodes.
Sinkhole attacks	Link layer,Network layer	Attacker broadcasts false routing related information so thatneighboring nodes send them their packets and stealsinformation or drops them	Data consistency& Network flow information approach, Hop count Monitoring Scheme, RSSI based Scheme,Monitoring nodes CPU Usage, Mobile Agent based approach ,Using Message Digest Algorithm.[15][35]
Sybil attacks	Physical layer	Node replication by stealing sensors identities, that is, MAC address, IP address, and so forth	Physically Protecting the devices [15]
	Data link layer		Changing the key regularly [15], key management [9]
	Network layer		Reset the devices and change the session keys, Suspicious node detection bysignal strength
Wormhole attacks [30][31]	Link layer	Adversaries exchange packets through a long-distance andlow-latency links affecting routing making legitimate sensors believe that they are neighbors with sensors of another area	Packet leashes, directional antenna, Network Neighbor Number (NNT) Test based on Hypothesis testing which detects the increase in the number of neighbors of the sensors, All Distance Test (ADT), detects the decrease of the lengths of the shortest paths between all pairs of sensors.[15]
	Network layer		
Hello flood attack	Network layer	Use of high transmission range HELLO packets so that nodes go through attacker while transmitting packets to base station	"Identity verification protocol"[39] checks the bi-directionality of link with encrypted echo-back mechanism. A "probabilistic based" proposal, which drives some randomly chosen nodes to acknowledge to base station regarding hello requests, which then further examines the request authenticity
Acknowledgement spoofing	Link layer	Spoofs the acknowledgement for the sniffed packets and gives an illusion that receiver is in its vicinity and even disabled/dead node is alive	Good encryption techniques and proper authentication for communication.[32]

V. Conclusion

In this paper, we have addressed various design issues in distributed sensor networks and also challenges faced.Security requirements, attacks and countermeasures are also discussed. Drawbacks and requirements associated with countermeasures presents open research issues and researchers can work in that direction for designing secure protocols.

References

[1]. Edwin Prem, Kumar Gilbert, BaskaranKaliaperumal, and Elijah Blessing Rajsingh"Research Issues in Wireless Sensor NetworkApplications: A Survey"DOI: 10.7763/IJIEE.2012.V2.191

[2]. MahfuzulhoqChowdhury, MdFazlul Kader and Asaduzzaman" Security Issues in Wireless Sensor Networks: A Survey"International Journal of Future Generation Communication and Networking Vol.6, No.5 (2013), pp.97-116

[3]. Al-Sakib Khan Pathan, Hyung-Woo Lee, ChoongSeonHong"Security in Wireless Sensor Networks: Issues andChallenges"Feb. 20-22, 2006 ICACT2006, ISBN 89-5519-129-4

[4]. Dr. G. Padmavathi,Mrs. D. Shanmugapriya "A Survey of Attacks, Security Mechanisms andChallenges in Wireless Sensor Networks " IJCSIS Vol. 4, No. 1 & 2, 2009

[5]. Samira Kalantary, Sara Taghipour"A survey on architectures, protocols, applications, andmanagement in wireless sensor networks" Journal of Advanced Computer Science & Technology, 3 (1) (2014) 1-11, doi: 10.14419/jacst.v3i1.1583

[6]. John Paul Walters, ZhengqiangLiang,Weisong Shi, and VipinChaudhary "Wireless Sensor Network Security: A Survey"Security in Distributed, Grid, and Pervasive Computing 2006 Auerbach Publications, CRC Press

[7]. Yide Liu "Wireless Sensor Network Applications in Smart Grid:Recent Trends and Challenges" International Journal of Distributed Sensor NetworksVolume 2012, Article ID 492819, 8 pagesdoi:10.1155/2012/492819

[8]. Ivan Stojmenovic "Handbook of Sensor Networks Algorithms and Architectures" A John Wiley & Sons, Inc., Publication

[9]. Dr. Manoj Kumar Jain "Wireless Sensor Networks: Security Issues andChallenges" 2011 IJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224 (ONLINE), VOLUME 02, ISSUE 01, MANUSCRIPT CODE: 110746

[10]. Dr. Banta Singh Jangra, VijetaKumawat "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks"International Journal of Engineering and Innovative Technology (IJEIT)Volume 2, Issue 3, September 2012ISSN: 2277-3754ISO 9001:2008 Certified

[11]. HimanshuDiwan, PoojaAgrawal, A.K.Dwivedi "Current Status and Design Challenges inWireless Multimedia Sensor Networks" International Journal of Engineering Trends and Technology (IJETT) – Volume 6 number 2- Dec 2013, ISSN: 2231-5381

[12]. Anil Kumar, Preetigulia , Shikha Sharma "A Study on Power Saving and Secure WSN"International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 4 - May 2014ISSN: 2231-5381

[13]. Abdalraouf Hassan and Christian Bach "Improving Security Connection in Wireless Sensor Networks"International Journal of Innovation and Scientific ResearchISSN 2351-8014 Vol. 2 No. 2 Jun. 2014, pp. 301-307

[14]. B.Sangeetha “Wireless Sensor Networks: Issues, Challenges and Survey of Solutions” IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 05, 2014 | ISSN (online): 2321-0613
[15]. AnserGhazaal Ali Alquraishee, AasimZafar, Syed Hamid Hasan “Security Issues in Wireless Sensor Networks” MAGNT Research Report (ISSN. 1444-8939) Vol.2(4):PP.82-91
[16]. S.Muthukarpagam, V.Niveditta, S.Neduncheliyan “Design issues, Topology issues, Quality of ServiceSupport for Wireless Sensor Networks: Survey andResearch Challenges” 2010 International Journal of Computer Applications (0975 – 8887)Volume 1 – No. 6
[17]. Pratibha, Dr. Prem Chand Vashist “A Detail Survey on Wireless SensorNetworks (WSNs) Security Issues” IJCSMC, Vol. 3, Issue. 7, July 2014, pg.111 – 118 ISSN 2320–088X
[18]. HairongQia, S. SitharamaIyengarb, KrishnenduChakrabarty “Distributed sensor networks- a review ofrecent research”H. Qi et al. / Journal of the Franklin Institute 338 (2001) 655–668
[19]. Chee-Yee Chong, and Srikanta P. Kumar “Sensor Networks: Evolution, Opportunities,and Challenges” Proceedings of the IEEE, Vol. 91, No. 8, August 2003
[20]. ArchanaBharathidasan, Vijay AnandSaiPonduru “Sensor Networks: An Overview”
[21]. S SitharamaIyengar, R.L. Kashyap and Rabinder N Madan“Distributed Sensor Networks-Introduction to the Special Section” IEEE Transactions on Systems, MAN and Cybernetics, Vol.21, No.5 September/ October 1991.
[22]. AashimaSingla, RatikaSachdeva “Review on Security Issues and Attacks in Wireless SensorNetworks” International Journal of Advanced Research inComputer Science and Software Engineering, Volume 3, Issue 4, April 2013 ISSN: 2277 128X
[23]. AmrinderKaur , Sunil Saini“Simulation of Low Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Network” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013 ISSN: 2277 128X
[24]. Gowrishankar.S ,T.G.Basavaraju , Manjaiah D.H , Subir Kumar Sarkar “Issues in Wireless Sensor Networks”Proceedings of the World Congress on Engineering 2008 Vol IWCE 2008, July 2 - 4, 2008, London, U.K.
[25]. BhaskarBhuyan, Hiren Kumar Deva Sarma, NityanandaSarma, AvijitKar, Rajib Mall“Quality of Service (QoS) Provisions in Wireless SensorNetworks and Related Challenges” Wireless Sensor Network, 2010, 2, 861-868doi:10.4236/wsn.2010.211104
[26]. AlexandrosFragkiadakis, Vangelis Angelakis and Elias Z. Tragos“Securing Cognitive Wireless Sensor Networks: A Survey” International Journal of Distributed Sensor NetworksVolume 2014, Article ID 393248, 12 pageshttp://dx.doi.org/10.1155/2014/393248
[27]. Vartika Shah, Sanjiv Sharma “A Review of Existing Security frameworks and Encryption Methods for Wireless Sensor Networks” International Journal of Innovations & Advancement in Computer ScienceIJIACSISSN 2347 – 8616Volume 3, Issue 2April 2014
[28]. RajdeepBhanot, Naveen Bilandi “Security issues and challenges in wireless sensornetworks” I JRAS ET Vol. 2 Issue IV, April 2014ISSN: 2321-9653
[29]. JijeeshBaburajan, JigneshPrajapati “A Review Paper On Watchdog Mechanism In WirelessSensor Network To Eliminate False Malicious Node Detection” IJRET: International Journal of Research in Engineering and Technology Volume: 03 Issue: 01 | Jan-2014 EISSN: 2319-1163 | PISSN: 2321-7308
[30]. SaurabhUghade, R.K. Kapoor, AnkurPandey“An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach “International Journal of Recent Development in Engineering and TechnologyWebsite: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)
[31]. JatinderSinghEr. AbhinavBhandari “A Review of Wireless Sensor Network Under the Denial Of Service Attack (DoS)”
a. IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 05, 2014 | ISSN (online): 2321-0613
[32]. ShahriarMohammadi, Reza EbrahimiAtani, HosseinJadidoleslamy “A Comparison of Link Layer Attacks onWireless Sensor Networks”Journal of Information Security, 2011, 2, 69-84doi:10.4236/jis.2011.22007
[33]. ParamjitKour, Lal Chand Panwar“A Review on Security Challenges and Attacks inWireless Sensor NetworksInternational Journal of Science and Research (IJSR)ISSN (Online): 2319-7064
[34]. SachinLalar“Security in Wireless Sensor Networks: Issues and Security Mechanisms” International Journal of Current Engineering and TechnologyE-ISSN 2277 – 4106, P-ISSN 2347 – 5161
[35]. JunaidAhsenaliChaudhry, Usman Tariq, Mohammed Arif Amin and Robert G. Rittenhouse “Sinkhole Vulnerabilities in Wireless Sensor Networks” International Journal of Security and Its ApplicationsVol.8, No.1 (2014), pp.401-410
[36]. ZdravkoKarakehayov “Using REWARD to detect team black-hole attacks inwireless sensor networks”
[37]. KasımSinanYıldırım and ÖnderGürcan “Efficient Time Synchronization in a Wireless SensorNetwork by Adaptive Value Tracking” IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 13, NO. 7, JULY 2014
[38]. UshamRobinchandra Singh, Sudipta Roy, HerojitMutum “A Survey on Wireless Sensor Network Security and its Countermeasures: An Overview” International Journal of Engineering Science InventionISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726www.ijesi.org Volume 2 Issue 9‖ September. 2013 ‖ PP.19-37
[39]. J.SteffiAginoPriyanka, S.Tephillah and A.M.Balamurugan “Attacks And Countermeasures In WSN” IIJEC, Volume 2, Issue 1, January 2014
[40]. WazirZadaKhana, Yang Xiangb, Mohammed Y Aalsalema, QuratulainArshada “The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures” I.J. Wireless and Microwave Technologies, 2012, 2, 33-44, DOI: 10.5815/ijwmt.2012.02.06
[41]. PrakashgoudPatil,UmakantKulkarni “Delay Efficient Distributed Data Aggregation Algorithm in Wireless Sensor Networks” International Journal of Computer Applications (0975 – 8887)Volume 69– No.1, May 2013
[42]. Kai Xing, ShyaamSundharRajamadamSrinivasan , Manny Rivera ,Jiang Li, Xiuzhen Cheng “Attacks and Countermeasures in Sensor Networks: ASurvey”NETWORKSECURITYScott Huang, David MacCallum, and Ding Zhu Du(Eds.) 2005 Springer.
[43]. Ivanovitch Silva , LuizAffonsoGuedes , Paulo Portugal and Francisco Vasques “Reliability and Availability Evaluation ofWireless SensorNetworks for Industrial Applications” Sensors 2012, 12, 806-838; doi:10.3390/s120100806
[44]. Luca Anchora , Antonio Capone , Vincenzo Mighali , Luigi Patrono , Francesco Simone “A novel MAC scheduler to minimize the energy consumptionin a Wireless Sensor Network” Ad Hoc Networks 16 (2014) 88–104
[45]. M. EmreKeskin ,I. Kuban Altınel, Necati Aras , CemErsoy “Wireless sensor network lifetime maximization by optimalsensor deployment, activity scheduling, data routing and sinkmobility” Ad Hoc Networks 17 (2014) 18–36
[46]. Hongxing Li , ChuanWua, Qiang-Sheng Hua , Francis C.M. Lau “Latency-minimizing data aggregation in wireless sensornetworks under physical interference model” Ad Hoc Networks 12 (2014) 52–68
[47]. TifennRault , AbdelmadjidBouabdallah, YacineChallal “Energy efficiency in wireless sensor networks: A top-downsurvey” Computer Networks 67 (2014) 104–122
[48]. HaidarSafa “A novel localization algorithm for large scale wireless sensor networks” Computer Communications 45 (2014) 32–46
[49]. B. P. S. Sahoo, Deepak Puthal “DRUG: An Energy-Efficient Data-Centric RoutingProtocol for Wireless Sensor Networks”

arXiv:1404.4685v3 [cs.NI] 18 Jun 2014
[50]. Nitika Vats Doohan, SanjivTokekar "A Survey on Routing Techniques of Data-CentricWireless Sensor Networks"International Journal of Computer Applications (0975 – 8887)Volume 53– No.16, September 2012
[51]. Prof. SachinDeshpande, Dr. J. W. Bakal, Prof. MritunjaykumarOjha "Simulation of Target Tracking in Wireless Sensor Network" Volume 4, Issue 2, February 2014 IJARCSSE ISSN: 2277 128X .