HCTL Open International Journal of Technology Innovations and Research (IJTIR)
http://ijtir.hctl.org
Volume 14, April 2015
e-ISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3

Wireless Sensor Networks: Introduction, Advantages, Applications and Research Challenges

Prashant Tiwari[1], Varun Prakash Saxena[2], Raj Gaurav Mishra[3], Devendra Bhavsar[4]

prashantcuj@gmail.com

Abstract

This paper presents introduction, advantages and disadvantages, possible applications and research challenges of Wireless Sensor Networks (WSN).

Keywords

WSN, Self-Positioning Algorithm, Localization Algorithm

Introduction to Wireless Networks

A wireless network is any sort of computer network that uses wireless data connections to plug network nodes. Wireless networks are computer networks who are not connected by cables regardless of the sort. The use of a wireless network enables enterprises to prevent the costly means of introducing cables into buildings or as a connection between different equipment locations. The cornerstone of wireless systems is radio waves, an implementation that occurs at the physical higher level of network structure.

Wireless technologies differ in a number of dimensions, most notably in just how much bandwidth they provide and how far apart communicating nodes can be. Other important differences include which perhaps the electromagnetic spectrums they choose (including whether or not this has a license) and exactly how much power them consume (very important to mobile nodes). In this section we discuss four prominent wireless technologies: Bluetooth (802.15.1), Wi-Fi (more formally generally known as 802.11), Wi-MAX (802.16), and third-generation or 3G cellular wireless. In the following sections we present them as a way from shortest range to longest range. Table 2.1 gives an introduction to these technologies and the way they connect with one another [1].

[1]M.Tech Scholar, Central University of Jharkhand, India.
[2]Assistant Professor, Govt. Women Engineering College, Ajmer, Rajasthan, India.
[3]Faculty Member, FST, The ICFAI University, Dehradun, India.
[4]Assistant Professor, J.K. Lakshmipati University, Jaipur, Rajasthan, India.

e-ISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3

One of the most traditionally used wireless links today are usually asymmetric, i.e., both endpoints are usually kinds of nodes. One endpoint, sometimes termed the base-station, normally has no mobility, but has a wired (or at best high bandwidth) link to the internet or other networks as shown in Figure 1. The node in the opposite end from the link shown because a “client node” can often be mobile and utilizes its link to the base station for those its communication with other nodes [2].

Types of Wireless Networks

Basically, there are five types of wireless networks:

1. Wireless PAN
2. Wireless LAN
3. Wireless MAN
4. Wireless WAN
5. Global Area Network [1]

Ad-hoc Networks

An advert hoc network is usually a network that is certainly composed of individual devices communicating jointly directly. The idea of implies spontaneous or impromptu construction because networks often bypass the gate keeping hardware or central access point for example a router. Many random networks are neighborhood networks where computers or other products are enabled to send data on to each other rather than dealing with a centralized access point [3].

Ad-hoc networks are multi-hop wireless networks that can operate minus the services of the established backbone infrastructure. While such networks have obvious applications from the military and disaster relief environments, more modern works that contain motivated their use even in regular wireless packet data networks have raised their significance. The main objective on this paper should be to study the performance with the TCP transport layer protocol over ad-hoc networks [4].

Thinking about an ad hoc network is normally unfamiliar to finish users with only seen small residential or business networks that use a standard router to send wireless signals to individual computers. However, the ad hoc network will be used a great deal in new sorts of wireless engineering, although until recently it turned out a rather esoteric idea. One example is a mobile random network involves mobile devices communicating directly with each other. A different type of random network, the vehicular random network, involves placing communication devices in cars. Both these are examples of ad hoc networks designed to use a large variety of individual devices to freely communicate with no sort of top-down or hierarchical communication structure [3].

Ad-hoc Networks Characteristics

1. Mobility: the truth that nodes can be rapidly repositioned and/or move could be the raison d ‘etre of random networks. Rapid deployment in areas without the need of infrastructure often means that a gamers must explore a place along with perhaps form teams/swarms that in turn coordinate among themselves to generate a taskforce or a mission. You can have individual random mobility, group mobility,

e-ISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3

motion along preplanned routes, etc. The mobility model might have major effect on the selection of a routing scheme and can thus influence performance.

2. Multihopping: a multihop network is a network the spot that the path from source to destination traverses other nodes. Random nets often exhibit multiple hops for obstacle negotiation, spectrum reuse, and conservation. Battlefield covert operations also favour a sequence of short hops to scale back detection by the enemy.

3. Self-organization: the ad hoc network must autonomously determine its very own configuration parameters including: addressing, routing, clustering, position identification, power control, etc. Sometimes, special nodes (e.g., mobile backbone nodes) can coordinate their motion and dynamically distribute from the geographic area to supply coverage of disconnected islands.

4. Energy conservation: most ad hoc nodes (e.g., laptops, PDAs, sensors, etc.) have limited power supply no power to generate their particular power (e.g., solar power systems). High efficiency protocol design (e.g., MAC, routing, resource discovery, etc) is important for longevity with the mission.

5. Scalability: in certain applications (e.g., large environmental sensor fabrics, battlefield deployments, urban vehicle grids, etc) the random network can grow to thousand nodes. For wireless “infrastructure” networks scalability is actually handled by a hierarchical construction [3].

Vehicular Ad-hoc Networks

Vehicular Ad Hoc Networks (VANETs) have cultivated out of the have to support the growing quantity of wireless items that very easily employed in the vehicles. These products include remote keyless entry devices, personal digital assistants (PDAs), laptops and mobile telephones. As mobile wireless devices and networks become increasingly important, the need for Vehicle-to-Vehicle (V2V) and Vehicle to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I) Communication will continue to develop. VANETs can be utilized to get a broad range of safety and non-safety applications, leave useful services like vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services for example choosing the closest fuel station, restaurant or travel lodge and infotainment applications including providing access to the online world [6].

Fixed Wireless Networks

Fixed wireless will be the operation of wireless devices or systems accustomed to connect two fixed locations (e.g., building to building or tower to building) using a radio or other wireless link, like laser bridge Usually, fixed wireless is part of a wireless LAN infrastructure. The objective of a limited wireless link would be to enable data communications between the two sites or buildings. Fixed wireless data (FWD) links will often be a price-effective alternative to popular leasing fiber or installing cables between your buildings.

e-ISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3

The idea-to-point signal transmissions occur throughout the air over the terrestrial microwave platform rather than through copper or optical fiber therefore, fixed wireless does not require satellite feeds or local phone service. Some great benefits of fixed wireless add the ability to connect with users in remote areas with the necessity for laying new cables and also the capacity for broad bandwidth that isn't impeded by fiber or cable capacities. Fixed wireless devices usually derives their electrical energy from the public-service corporation mains, unlike mobile wireless or portable wireless devices which are generally battery powered [7].

Wireless Sensor Networks

A Wireless Sensor Network (WSN) is by hundreds of small, low-cost nodes that are fitted with limitations in memory, energy, and processing capacity. In this particular form of networks, several problems is to learn each node. Recent advances in wireless communications and electronics have enabled the roll-out of low-cost, low-power and multi-functional sensors that are small in dimensions and communicate in a nutshell distances. Cheap, smart sensors, networked through wireless links and deployed in vast quantities, provide unprecedented opportunities for monitoring and controlling homes, cities, along with the environment. Furthermore, networked sensors use a broad spectrum of applications within the defense area, generating new capabilities for reconnaissance and surveillance and various Tactical applications. Self-localization capability can be a highly desirable sign of wireless sensor networks. In environmental monitoring applications for example bush fire surveillance, water quality monitoring and precision agriculture, the measurement data are meaningless lacking the knowledge of the placement from the location where the data are obtained. Moreover, location estimation may enable many applications for example inventory management, transport, intrusion detection, road traffic monitoring, health monitoring, reconnaissance and surveillance.

With all the advances inside the miniaturization and integration of sensing and communication Technologies, large-scale wireless sensor networks using a large number of low-cost and low-power sensors are already developed. Within a wireless sensor network, lots of money of tiny, battery-powered sensor nodes are scattered throughout a physical area. Each sensor in the sensor network collects data, as an example, sensing vibration, temperature, radiation along with other environmental factors [5].

A wireless sensor network (WSN) includes hundreds to a large number of low-power multi-functional sensor nodes, operating within the unattended environment, and having sensing, computation and communication capabilities. The essential the different parts of a node undoubtedly are a sensor unit, an ADC (Analog to Digital Converter), a CPU (C.P.U.), an electrical unit as well as a communication unit. Sensor nodes are micro-electro-mechanical systems (MEMS) that develop a measurable a reaction to a general change in some fitness like temperature and pressure. Sensor nodes sense or measure physical data in the area being monitored. The continual analog signal sensed through the sensors is digitized by an analog-to-digital converter and sent to controllers for more processing. Sensor nodes are of small size, consume extremely low energy, are operated in high volumetric densities, and will be autonomous and adaptive towards the environment.

Wireless sensor networks are particularly interesting in hazardous or remote environments, or every time a multitude of sensor nodes have to be deployed. The localization concern is important where it has an uncertainty about some positioning.

e-ISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3

Should the sensor network is used for monitoring the temperature within a building, it's quite possible that we can are aware of the exact position of node. However, in the event the sensor network is utilized for monitoring the temperature inside a remote forest, nodes can be deployed from an airplane as well as the precise location coming from all sensor might be unknown. An effective localization algorithm may then make use of all the disposable information through the motes to compute each of the positions [8].

The key characteristic of any Wireless Sensor Network includes:

1. Power consumption constraints for nodes using batteries or energy harvesting
2. Chance to cope with node failures (resilience)
3. Mobility of nodes
4. Heterogeneity of nodes
5. Scalability to large scale of deployment
6. Capability to withstand harsh environmental conditions
7. Simplicity of use
8. Cross layer design [8]

Advantages and Disadvantages of WSN

Why people love wireless sensor networks might be summarized as the following [9]:

1. Network setups can be carried out without fixed infrastructure.
2. Suitable for the non-reachable places such as over the sea, mountains, rural areas or deep forests.
3. Flexible if there is random situation when additional workstation is needed.
4. Implementation pricing is cheap.
5. It avoids plenty of wiring.
6. It might accommodate new devices at any time.
7. It's flexible to undergo physical partitions.
8. It can be accessed by using a centralized monitor.

The disadvantages of wireless sensor networks can be summarized as follows [9]:

1. Less secure because hackers can enter the access point and obtain all the information.
2. Lower speed as compared to a wired network.
3. More complicated to configure compared to a wired network.
4. Easily troubled by surroundings (walls, microwave, large distances due to signal attenuation, etc).
5. It is easy for hackers to hack it we couldn't control propagation of waves.
6. Comparatively low speed of communication.
7. Gets distracted by various elements like Blue-tooth.
8. Still Costly (most importantly).

Applications of Wireless Sensor Networks

The applications for WSNs involve tracking, monitoring and controlling. WSNs are mainly utilized for habitat monitoring, object tracking, nuclear reactor control, fire detection, and traffic monitoring. Area monitoring is a very common application of WSNs, in which the WSN is deployed over a region where some incident might be monitored. E.g., a substantial variety of sensor nodes may very well be deployed over the battlefield to detect enemy intrusions rather than using landmines. When the sensors detect case

being monitored (heat, pressure, sound, light, electro-magnetic flux, vibration, etc.), the big event needs to be reported to at least one in the base stations, which often can than take some appropriate action (e.g., send some text online or even a satellite). Wireless sensor networks are utilized extensively within the water/wastewater industries. Facilities not wired for power or data transmission can be monitored using industrial wireless I/O devices and sensor nodes powered by solar panels or battery packs. Wireless sensor networks are able to use numerous sensors to detect the existence of vehicles for vehicles detection. Wireless sensor networks may also be employed to control the temperature and humidity levels inside commercial greenhouses. If the temperature and humidity drops below specific levels, the greenhouse manager might be notified via e-mail or a cellular telephone text, or host systems can trigger misting systems, open vents, first turn on fans, or control a multitude of system responses. Because some wireless sensor networks are super easy to install, they've also been simple move if the needs with the application change [2].

There are lots of applications of WSN:

1. Process Management: Area monitoring is a very common using WSNs. In area monitoring, the WSN is deployed spanning a region where some phenomenon is usually to be monitored. A military example may be the use of sensors detect enemy intrusion; a civilian example would be the geo-fencing of gas or oil pipelines. Area monitoring is most important part.

2. Healthcare monitoring: The medical applications might be of two sorts: wearable and implanted. Wearable devices are applied to the body surface of the human or maybe at close proximity from the user. The implantable medical devices are the ones that are inserted inside your body. There are numerous other applications too e.g. body position measurement and of the person, overall monitoring of ill patients in hospitals and also at homes.

3. Environmental/Earth sensing: There are numerous applications in monitoring environmental parameters samples of which are given below. They share any additional challenges of harsh environments and reduced power supply.

4. Polluting of the environment monitoring: Wireless sensor networks have been deployed in lots of cities (Stockholm, London and Brisbane) to monitor the power of dangerous gases for citizens. These can leverage the random wireless links instead of wired installations that also make them more mobile for testing readings in several areas.

5. Forest fire detection: A network of Sensor Nodes is usually positioned in a forest to detect every time a fire has begun. The nodes is usually with sensors to measure temperature, humidity and gases which are produced by fire within the trees or vegetation. The first detection is necessary to get a successful action of the fire fighters; As a result of Wireless as Sensor Networks, the fire brigade are able to know when a fire begins you bet it can be spreading.

6. Landslide detection: A landslide detection system uses a wireless sensor network to detect the slight movements of soil and modifications to various parameters that will occur before or throughout a landslide. With the data gathered it may be possible to know the appearance of landslides before it genuinely happens.

7. Water quality monitoring: Water quality monitoring involves analyzing water properties in dams, rivers, lakes & oceans, and also underground water reserves. The application of many wireless distributed sensors enables the creation of a accurate map on the water status, and allows the permanent deployment of monitoring stations in locations of difficult access, while not manual data retrieval.

8. Natural disaster prevention: Wireless sensor networks can effectively act to avoid the results of disasters, like floods .Wireless nodes have successfully been deployed in rivers where changes in the water levels have to be monitored in real time [8].

9. Industrial monitoring:

    a. Machine health monitoring: Wireless sensor networks happen to be developed for machinery condition based maintenance (CBM) as they offer significant personal savings and enable new functionality .In wired systems, installing enough sensors can often be tied to the price of wiring. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors.
    b. Data logging: Wireless sensor networks are also employed for the gathering of web data for monitoring of environmental information; this is often as easy as the monitoring from the temperature in a very fridge to the level of water in overflow tanks in nuclear power plants. The statistical information will then be employed to show how systems have been working. The main benefit of WSNs over conventional loggers is the "live" data feed which is possible.
    c. Water/Waste water monitoring: Monitoring the high quality and level of water includes many activities including checking the quality of underground or surface water and ensuring a country's water infrastructure for your benefit of both human and animal .It may be helpful to protect the wastage of water.
    d. Structural Health Monitoring: Wireless sensor networks enables you to monitor the fitness of civil infrastructure and related geophysical processes all around real time, and more than very long stretches through data logging, using appropriately interfaced sensors [8].

Research Challenges in Wireless Sensor Networks

A brief history on the research in SN, but more interesting may be the overview within the technical challenges and issues is presented, from where we could cite several relevant items: WSN working in a harsh environment; the ability with the network (leastways the neighbors); the network control and routing; querying and tasking (should be as simple and intuitive as it can be); plus security issues (low latency, survivable, low probability of detecting communications, high reliability) [10].

1. Security: Security is often a broadly used term encompassing the characteristics of authentication, integrity, privacy, non repudiation, and anti-playback. The greater the dependency on the info supplied by the networks may be increased, the more potential risk of secure transmission of information in the networks has increased. To the secure transmission of numerous kinds of information over

networks, several cryptographic, steganography and other techniques are utilized that happen to be renowned. In this section, we discuss the network security fundamentals you bet the techniques are meant for wireless sensor networks [11].

2. Cryptography: The encryption-decryption techniques devised for your traditional wired networks usually are not feasible to be employed directly for the wireless networks in particular for wireless sensor networks. WSNs include things like tiny sensors which really suffer from the possible lack of processing, memory and battery Applying the security mechanisms for instance encryption could also increase delay, jitter and packet loss in wireless sensor networks when applying encryption schemes to WSNs like, what sort of keys are generated or disseminated. How a keys are managed, revoked, assigned to your new sensor put into the network or renewed for ensuring robust to protect the network Adoption of pre-loaded keys or embedded keys could hardly be an efficient solution [11].

3. Steganography: While cryptography aims at hiding necessary of a message, steganography aims at hiding a good the message. Steganography is the art of covert communication by embedding a note in to the multimedia data (image, sound, video, etc.) . The leading objective of steganography is to modify the carrier in a fashion that is just not perceptible and hence, it looks the same as ordinary [11].

4. Physical Layer Secure Access: Physical layer secure access in wireless sensor networks may very well be offered by using frequency hopping. A dynamic mixture of the parameters like hopping set (available frequencies for hopping), dwell time (interval per hop) and hopping pattern (the sequence in which the frequencies in the available hopping set is used) could be combined with a little expense of memory, processing and resources. Important points in physical layer secure access will be the efficient design in order that the hopping sequence is modified in less time than is required to discover it and for employing this both sender and receiver should maintain a synchronized clock. A scheme as proposed in may be utilized which introduces secure physical layer access employing the singular vectors while using channel synthesized modulation. Attacks against wireless sensor networks may very well be broadly considered from two different levels of views. One is the attack from the security mechanisms and this band are brilliant from the basic mechanisms (like routing mechanisms). Ideas signalize the most important attacks in wireless sensor networks [11].

5. Localization: It is amongst the key techniques in wireless sensor network. The place estimation method is usually classified into Target / source localization and node self-localization. In target localization, we mainly introduce the energy-based method. Then we investigate the node self-localization methods. Considering that the widespread adoption on the wireless sensor network, the localization methods are wide and varied in several applications. There are some challenges using some special scenarios. With this paper, we present a wide survey these challenges: localization in non-line-of-sight, node selection criteria for localization in energy-constrained network, scheduling the sensor node to optimize the tradeoff between localization performance and energy consumption, cooperative node localization, and localization algorithm in heterogeneous network. Finally, we

introduce the evaluation criteria for localization in wireless sensor network. The entire process of estimating the unknown node position inside the network is known as node self-localization. And WSN comprises a large number of inexpensive nodes which are densely deployed in a very region of interests to measure certain phenomenon. The leading objective would be to determine the location of the target [12]. Localization is significant travelers have an uncertainty with the exact location of some fixed or mobile devices. One example has been in the supervision of humidity and temperature in forests and/or fields, where thousands of sensors are deployed by way of plane, giving the operator minimal possible ways to influence may location of node. An efficient localization algorithm might utilize all the free information from the wireless sensor nodes to infer the positioning of the individual devices. Another application will be the positioning of an mobile robot determined by received signal strength from your number of radio beacons placed at known locations around the factory floor. The primary function of an location estimation method to calculate the geographic coordinates of network nodes with unknown position in the deployment area. Localization in wireless sensor networks is the process of determining the geographical positions of sensors. Only a number of the sensors (anchors) inside the networks have prior knowledge about their geographical positions. Localization algorithms utilize location information of anchors and estimates of distances between neighboring nodes to discover the positions in the rest of the sensors [13].

6. Power-Consumption: A wireless sensor node can be a popular solution when it is difficult or impossible to perform a mains supply towards sensor node. However, because the wireless sensor node is normally positioned in a hard to reach location, changing the battery regularly will not be free and inconvenient. An essential take into account the introduction of a wireless sensor node is making sure that there's always adequate energy accessible to power the system [14]. The facility consumption rate for sensors in the wireless sensor network varies greatly good protocols the sensors use for communications. The Gossip-Based Sleep Protocol (GSP) implements routing and many MAC functions in a energy conserving manner. The effectiveness of GSP has already been demonstrated via simulation. However, no prototype system has become previously developed. GSP was implemented for the Mica2 platform and measurements were conducted to discover the improvement in network lifetime. Results for energy consumption, transmitted and received power, minimum voltage supply necessary for operation, effect of transmission power on energy consumption, and different methods for measuring time of a sensor node are presented. The behavior of sensor nodes when they're all around their end of lifetime is described and analyzed [14].

7. Deployment: Sensor networks provide capability to monitor real-world phenomena in more detail and also at large scale by embedding wireless network of sensor nodes in the environment. Here, deployment is anxious with establishing an operational sensor network inside a real-world environment. On many occasions, deployment is often a labor-intensive and cumbersome task as environmental influences trigger bugs or degrade performance in a way that is not observed during pre-deployment testing within a lab. The real reason for this really is that the real life features a strong influence for the function of your sensor network by governing the output of sensors, by influencing the existence and excellence of wireless communication links, and also by putting physical strain on sensor nodes. These influences is only able to be modeled to your very restricted extent in simulators and lab testbeds. Home the typical problems encountered during

deployment is rare.You can only speculate for the grounds for this. On one side, a paper which only describes what actually transpired during a deployment seldom constitutes novel research and could possibly be hard to get published. However, people might often hide or ignore problems that are not directly related to their field of research. It is additionally often tough to discriminate desired and non-desired functional effects for the different layers or levels of detail [15].

References

[1] Wireless Networking Complete The Morgan Kaufmann Series in Networking Series Editor , David Clark, M.I.T., Pei Zheng, Feng Zhao, David Tipper, Jinmei Tatuya, Keiichi Shima, Yi Qian, Larry Peterson, Lionel Ni, D. Manjunath, Qing Li, Joy Kuri, Anurag Kumar, Prashant Krishnamurthy.

[2] Localization inWireless Sensor Networks, King-Yip Cheng ,The University of Hong Kong December 2006.

[3] AD HOC NETWORKS Technologies and Protocols, Edited by PRASANT MOHAPATRA University of California, Davis,SRIKANTH V. KRISHNAMURTHY University of California, Riverside ©2005 Springer Science + Business Media, Inc.

[4] A Microscopic Analysis of TCP Performance over Wireless Ad-hoc Networks, Vaidyanathan Anantharaman, Raghupathy Sivakumar

[5] Wireless Sensor Networks1, F. L. LEWIS Associate Director for Research Head, Advanced Controls, Sensors, and MEMS Group Automation and Robotics Research Institute The University of Texas at Arlington 7300 Jack Newell Blvd. SFt. Worth, Texas 76118-7115.

[6] Vehicular ad hoc networks (VANETS): status, results, and challenges, Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen ,Angela Irwin · Aamir Hassan, © Springer Science+Business Media, LLC 2010.

[7] http://en.wikipedia.org/wiki/Fixed_wireless.

[8] Wireless Sensor Networks, The Morgan Kaufmann Series in Networking Series Editor, David Clark, M.I.T., Feng Zhao, Leonidas J. Guibas Morgan Kaufmann Publishers is an imprint of Elsevier

[9] A Comparative Study of Wireless Sensor Networks and Their Routing Protocols, Debnath Bhattacharyya , Tai-hoon Kim , and Subhajit Pal, Sensors 2010, 10, 10506-10523; doi:10.3390/s101210506 www.mdpi.com/journal/sensors.

[10] Challenges in Wireless Sensor Networks, Er. Barjinder Singh Kaler,Er. Manpreet Kaur Kaler,RIMT-MAEC,Mandigobindgarh.

[11] Security in Wireless Sensor Networks: Issues and Challenges, Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, ISBN 89-5519-129-4 Feb. 20-22, 2006 ICACT2006.

[12] A Survey of Localization inWireless Sensor Network, Long Cheng,ChengdongWu, Yunzhou Zhang,HaoWu, Mengxin Li, and CarstenMaple, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2012, Article ID 962523, 12 pages doi:10.1155/2012/962523.

[13] New Technique of Wireless Sensor Networks Localization based on Energy Consumption, Anouar Abdelhakim Boudhir Bouhorma Mohamed Ben Ahmed Mohamed, International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.

[14] Energy Consumption in Wireless Sensor Networks using GSP, María Gabriela Calle Torres, Electronics Engineer, Universidad Pontificia Bolivariana, Medellín, Colombia, 1995, Copyright © by María Gabriela Calle Torres 2006

[15] Deployment Techniques for Sensor Networks, Jan Beutel, Kay Romer, Matthias Ringwald, Matthias Woehrle.

[16] Preetam Suman; Amrit Suman, An Enhanced TCP Corruption Control Mechanism For Wireless Network, HCTL Open International Journal of Technology Innovations and Research, Volume 1, January 2013, Pages 27-40, ISSN: 2321-1814, ISBN: 978-1-62776-012-6.

[17] Arpit Gupta; Gaurav Shrivastava, APDA with Data Collective: A Survey to Prevent Attacks in VANET, Edition on Wired and Wireless Networks: Advances and Applications, Volume 3 - November 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62951-015-6.

[18] Raj Gaurav Mishra, Distributed Fibre Optic Virtual Fencing System, Edition on Wired and Wireless Networks: Advances and Applications, Volume 3 - November 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62951-015-6.

[19] Anil Kumar Khurana; Vishal Srivastava, QoS and Energy Efficient Routing Protocols in WSN, Edition on Wired and Wireless Networks: Advances and Applications, Volume 3 - November 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62951-015-6.

[20] Yufang Cheng; Jian Zhou, S-CRAHN: A Secure Cognitive-Radio Ad-Hoc Network, Volume 6, HCTL Open Science and Technology Letters (STL), August 2014, ISSN: 2321-6980, ISBN: 978-1-62951-779-7.

[21] Prashant Tiwari; Varun Prakash Saxena; Raj Gaurav Mishra; Devendra Bhavsar, A Survey of Localization Methods and Techniques in Wireless Sensor Networks, HCTL Open International Journal of Technology Innovations and Research (IJTIR), Volume 14, April 2015, eISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3.