A Survey on Dynamic wireless Sensor Network.

[1]Hemant patel,[2]Aakanksha S. Choubey
[1, 2] Department of Computer Science & Engineering
[1,2]Shri Shankaracharya College of Engineering & Technology, Bhilai, (C.G.)

[1]hemantrcet@gmail.com
[2]aakanksha022000@yahoo.com

***Abstract*— Dynamic Wireless sensor network (DWSN) is a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each with the help of the sink which can be moved in a certain sensor network area . In the DWSN sensor network does not move to its position but for the data gathering mobile sink move in a certain wireless sensor network . Due to the mobility in the network area we called it a Dynamic wireless sensor network . Now a days Dynamic wireless sensor network is one of the tremendous technology in the area of the wireless sensor network . Earlier days in the wireless sensor network sensor node do they all work like sensing , data collecting and data forwarding by doing that node lost their Energy quickly and get disconnected from the network to overcome this problem Dynamic wireless sensor network help to increase the lifetime of the wireless sensor network .**

Keywords — Wireless Sensor Networks (WSN), Mobile sink , Network Lifetime, Security.

I. INTRODUCTION

With the exponential growth of the network accessing devices and network technology DWSN make a more important role in the data communication. In the DWSN Each Sensor node has a radio transceiver for communicating into the marble sink, has a micro controller for processing the data and sensor for sensing the data from the environment or monitoring the data and a battery for the Energy . If a node wants to transmit the data to the other node in the Dynamic wireless sensor network it wait for the mobile sink. When mobile sink comes to the node or near the node send the data to the mobile sink. Due to the movable characteristics of the mobile sink mobile sink leave the containing data to its proper destination

1. Types of Dynamic wireless Sensor Network

We can classify the Dynamic wireless sensor network according the amount of sink use in the wireless Sensor network we can classify it by two categories Dynamic wireless sensor network work by the single sink [3] and Second one is by the use of multiple sink in the sensor network [2]. When we will talk about the single sink in the Dynamic Wireless sensor Network it has more error free .But its coverage area is less compared to the Dynamic wireless sensor network .When we will talk about the multiple sink in the Dynamic wireless sensor network it has more coverage area compare to the single sink in the dynamic wireless sensor network .According to the mobility we can divide the DWSN into the three categories dynamic wireless sensor network with movable node to gather the data from sensor node and transfer it to the sink. Second one is the node which moves between the sensor node and sink to collect and disseminate the data [4]. And the third one is using the sink to move in the network and to Collect the data and disseminate data into the network [4,5]. According to the data collection From the network DWSN can be divided by two type first one is event driven and the second one is query driven . In the event driven data from the node can be transmitted to the sink in time but the size of the memory engaged is large [6] . In the DWSN with query driven size of the sensor network memory engaged is small [5]. When we will talk about the data travel toward the sink we can divide the sensor network in two types one is one intermediate node between the sensor node and sink [2], and another is more than one intermediate node between the sensor node and sink [6,8].

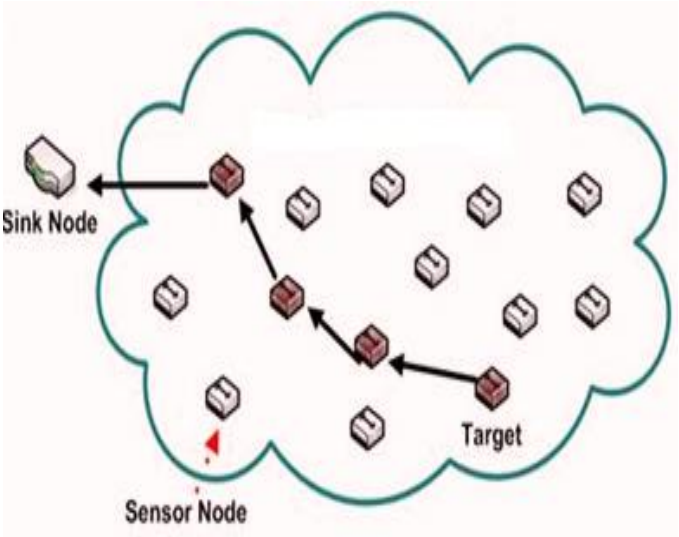

Figure 1: Dynamic Wireless Sensor Network.

2. Application of DWSN

In the every field we can use the dynamic wireless sensor Network there are following field in which we can use the dynamic wireless sensor network .

Spot monitoring : Spot monitors one of the most important application of the DWSN in which we know the knowledge about what is happing in the certain spot . Like we have to understand the phenomenon of the enemy in the certain or know about the activity of civilian in the certain range then we can use the DWSN .

Ecological monitoring: When we will talk about the ecological monitoring then during the term of the ecological monitoring we see the wireless sensor network in the many fields like the Wireless Sensor network use about earth science . This includes activity about the volcano [2] .Activity about oceans, activity about glaciers, activity about forests, and many more . Some of the major areas are listed below.

Air quality monitoring : By the help of the DWSN we can measure that the how much our air has been polluted either it is suitable for our health or not .By the help of the DWSN we can save our environment. In unsafe environment, real time monitoring of injurious gases is a concerning process because the climate can alter with brutal consequences in an instant way. Luck, wireless sensor networks has been launched to produce specific solutions for people.

Monitoring quality of water: According to the properties of the water with the help of wireless sensor network we can know how much water has been polluted of rivers , lakes and ocean , as well as the underground water reservoir .By the use of the wireless sensor network we recognize the water pollution and take the strong action for the prevention of water pollution [11].

Earthquake detection: By the help of the DWSN we can detect the sliding of the land or movement of the soil in the earth .With the help of the DWSN it may be possible to detect the unusual activity of the earth long time before when actually it happen with the help of the various parameters of the data gathering scheme in the dynamic wireless sensor network and we can save the life in the earth [10].

Usual disaster avoidance: By the help of the Dynamic wireless sensor network we can avoid the usual disaster like flooding in the ocean and river .With the help of the wireless sensor network we can monitor the water level in the ocean and take the beneficial action against disaster .

Machine health monitoring: By the help of the Dynamic wireless sensor network we can help in the maintenance of industries .Instrument . We can care the machine , according to the certain parameter lodging in the wireless sensor network and take the fruitful action against the production of the goods .We can apply this concept where the wired network cannot work .

Agriculture: In the field of agriculture, we can use the dynamic wireless sensor network .By the concept of the gravity feed water system we can monitor the water tank level and we can control the pump using the wireless I/O devices and save the water by sending the data to the control center for billing [15].

Tracking and identify the location: By help of dynamic wireless sensor network we can track our target i.e. the location of the something it application It is generally used to identify the location of the thief, and enemy and also find the location of something that has been theft by the thief [12] .

3. Characteristics of DWSN

Lifetime: Lifetime is the most promising factor in the Dynamic wireless sensor network. In the Dynamic wireless sensor network node use the battery for their life , when node involve any of the activity like data processing , sensing , or transmitting or receiving the data it uses the energy .Even though when the node is in standard mode it consumes a regular amount of energy [19,20]. Compare to the simple wireless sensor network dynamic wireless sensor network tries to reduce the energy consumption by the node.

Flexibility: Sensor network should be flexible; it can adapt easily any changes in node density and topology. It will be self configure and when the mobile sink comes near to the node then it can automatically identify the range of the sink and connect to the sink [20].

Maintenance: When we will talk about the maintenance in the dynamic wireless sensor network then we need to maintain only the programming code of the sensor node over the wireless sensor channel . When the new node introduce in the sensor network then the programming of the sensor network should be like that it can maintain the availability of the new node automatically .One more thing it programming should be like that when the same programming code of wired network introduced then sensor node programming should not accept these programming [21]. It should be self configuration means that the node allows them self to configure without the human intervention [23]. It should be the self time synchronizing properties [24].

Data Collection: In the dynamic wireless sensor network when we talked about the data collection then at the time of data collection we concentrate that the data collection mechanism should consume less energy so that the network lifetime will be more to make the network lifetime longer we use the mobile sink to gather the data and transmit the data to the particular destination .Mobile sink act as a gateway in the dynamic wireless sensor network and one property of the mobile sink is that sink can move from one place to another place [28,29]. When data collection is performed by the mobile sink than in the dynamic wireless sensor network also try to reduce the data redundancy [28], data confidentiality [30], data integrity algorithm these make the dynamic wireless sensor network more perfect than the simple wireless sensor network and network with wired technology.

4. Security issues in DWSN

Security in the Dynamic wireless sensor network is one of the most challenges issue .To understand all types of the possible attack are always a good solution to the security solution:

Privacy: Is one of the most important for any type of the dynamic wireless sensor network . It ensures that the message of the sender is received by the actual receiver .For the

privacy in the dynamic wireless sensor network it uses the many techniques for the privacy toward the sink some network use efficient one way hash chains [7] in sensor must confirm the source of the beacon message before they are able to send the data to the sink node .

Data reliability: Privacy in the data in the dynamic wireless sensor ensure that the data has not been stolen by the intruder but it doesn't mean that till now data is secure .There may be chances that data can be hacked by the intruder .To provide the more reliability i.e error free transmission of the data, The data reliability mechanism provides a security that the data has been reached to its current destination without modification of data [13].

Data newness: In the data it should be ensured that we are not using the old data we are using the current data .Data newness suggests that we are using the current data .This is required when we use the shared key. This assuring can be done by adding a time dependent counter with the packet [13].

Network simulators: Many dynamic wireless sensor network simulative studies based on the simulation tools .Which gives the benefits to the developer because tools provide predefined models for most communication protocols .

Authentication: Besides modifying packets, a challenger can also Potentially modify the stream of the packets through The addition of fake packets to the network. Therefore, The challenger can make receiving node consider that the data comes from a genuine source. Moreover, verification is needed for several administrative tasks (i.e., dynamic network Reprogramming, controlling node duty cycle). Thus, We can establish that message confirmation is Important for many sensor network applications.

II. EVOLUTION

In 2001, I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci studied about wireless sensor networks in which they describe the concept of sensor networks which has been made viable by the convergence of microelectro- mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor network applications are explored, and a review of factors influencing the design of sensor networks is provided. Then, the communication architecture for sensor networks is outlined, and the algorithms and protocols developed for each layer in the literature are explored. Open research issues for the realization of sensor networks are also discussed [1].

In 2002, Jason Lester Hill design System Architecture for Wireless Sensor Networks they present an operating system and three generations of a hardware platform designed to address the needs of wireless sensor networks. Their operating system, called TinyOS uses an event based execution model to provide support for fine grained concurrency and incorporates a highly efficient component model. TinyOS enables us to use a hardware architecture that has a single processor time shared between both application and protocol processing. They show how a virtual partitioning of computational resources not only leads to efficient resource utilization but allows for a rich interface between application and protocol processing. This rich interface, in turn, allows developers to exploit application specific communication protocols that significantly improve system performance [36].

In 2004, Raquel A.F. Mini, Antonio A.F. Loureiro, Badri Nath develops The distinctive design characteristic of a wireless sensor network: the energy map in which The key challenge in the design of a wireless sensor network is maximizing its lifetime. This is a fundamental problem and new protocol engineering principles needing to be established in order to achieve this goal. The information about the amount of available energy in each part of the network is called the energy map and can be useful to increase the lifetime of the network. They propose using the energy map as a protocol engineering principle for this kind of network. They argue that an energy map can be the basis for the entire design trajectory including all functionalities to be included in a wireless sensor network. Furthermore, They show how to construct an energy map using both probabilistic and statistical predictions-based approaches. Simulation results compare the performance of these approaches with a naive one in which no prediction is used. The experiments performed as an energy dissipation model that They have proposed to simulate the behavior of a sensor node in terms of energy consumption. The results show that prediction-based approaches outperform the nave in a variety of parameters [37].

In 2005, Daniele Puccinelli and Martin Haenggi studied about Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing in which Sensor networks offer a powerful combination of distributed sensing, computing and communication. They lend themselves to countless applications and, at the same time, offer numerous challenges due to their peculiarities, primary the stringent energy constraints to which sensing nodes are typically subjected. The distinguishing traits of sensor networks have a direct impact on the hardware design of the nodes at at least four levels: power source, processor, communication hardware, and sensors. Various hardware platforms have already been designed to test the many ideas spawned by the research community and to implement applications to virtually all fields of science and technology. They are convinced that CAS will be able to provide a substantial contribution to the development of this exciting field [38].

In 2006, Adam Dunkels, Niclas Finne, Joakim Eriksson, Thiemo Voigt suggest that while in general the overhead of a virtual machine is high, a combination of native code and virtual machine code provide good energy efficiency. Dynamic run-time linking can be used to update the native code, even in heterogeneous networks [39].

In 2006 Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA describes security solutions for collecting and processing data in Wireless Sensor Networks (WSNs). Adequate security capabilities for medium and large scale WSNs are a hard but necessary goal to achieve to prepare these networks for the market. They include an overview of security and reliability challenges for WSNs and introduces a toolbox concept to support such a framework [40].

In 2006 John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary decribes As wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network/ computer security. There is currently an enormous research potential in the field of wireless sensor network security. Thus, familiarity with the current research in this field will benefit researchers greatly. With this in mind, They survey the major topics in wireless sensor network security, and present the obstacles and the requirements in the sensor security, classify many of the current attacks, and finally list their corresponding defensive measures [41].

In 2006 Liang Song and Dimitrios Hatzinakos, propose to develop wireless Sensor Networks with Mobile Sinks (MSSN). The proposed MSSN is highly energy efficient because the multi-hop transmissions of high volume data over the network are converted into single-hop transmissions. They focus their investigation on sparsely deployed networks, where a single node to sink transmission is considered. The Transmission Scheduling Algorithm (TSA-MSSN) is proposed, where a parameter ¸ is employed to control the tradeoff between the maximization of the probability of successful information retrieval and the minimization of the energy consumption cost. It is shown that the proposed implementation of the TSA-MSSN has a complexity of *O* (1). Their study serves as the foundation for understanding fundamental laws behind the above mentioned tradeoff with useful implications for the design of more complex sensor networks with mobile sinks [42].

In 2006 Yong WangGarhan AtteburyByrav Ramamurthy present a survey on security issues in WSNs First they outline the constraints, security requirements, and attacks with their corresponding countermeasures in WSNs. Then they present a holistic view of security issues. These issues are classified into five categories: cryptography, key management, secure routing, secure data aggregation, and intrusion detection. Along the way they highlight the advantages and disadvantages of various WSN security protocols and further compare and evaluate these protocols based on each of these five categories. They also point out the open research issues in each Subarea and conclude with possible future research directions on security in WSNs [43].

In 2006 Al-Sakib Khan Pathan Hyung-Woo Lee Choong Seon Hong investigate , Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in the future. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. They identify the security threats, review proposed security mechanisms for wireless sensor networks. They also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks [44].

In 2007 Prabhudutta Mohanty, Sangram Panigrahi Nityananda Sarma, Siddhartha Sankar Satapathy they explored explored general security threats in wireless sensor network and made an extensive study to categorize available data gathering protocols and analyze possible security threats on them. [45].

In 2008 Luis E. Palafox , J. Antonio Garcia-Macias they present the growing challenges related to security in wireless sensor networks. They show possible attack scenarios and evidence the easiness of perpetrating several types of attacks due to the extreme resource limitations that wireless sensor networks are subjected to. Nevertheless, they show that security is a feasible goal in this resource-limited environment; to prove that security is possible they Survey several proposed sensor network security protocols targeted to different layers in the protocol stack. The work surveyed in their chapter enable several protection mechanisms vs well documented network attacks. Finally, they summarize the work that has been done in the area and present a series of ongoing challenges for future work [46].

In 2008 Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz deals with some security issues over wireless sensor networks (WSNs). A survey of recent trends in general security requirements, typical security threats, intrusion detection system, key distribution schemes and target localization is presented. In order to facilitate applications that require packet delivery from one or more senders to multiple receivers, provisioning security in group communications is pointed out as a critical and challenging goal. Presented issues are crucial for future implementation of WSN [47].

In 2008 Jennifer Yick, Biswanath Mukherjee, Dipak Ghosa The goal of their survey is to present a comprehensive review of the recent literature since the publication of [I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Communications Magazine, 2002]. Following a top-down approach, they give an overview of several new applications and then review the literature on various aspects of WSNs. They classify the problems into three different categories: (1) internal platform and underlying operating system, (2) communication protocol stack, and (3) network services, provisioning, and deployment. We review the major development in these three categories and outline new challenges [48].

In 2009 Chiara Buratti Andrea Conti Davide Dardari and Roberto Verdone their survey paper aims at reporting an overview of WSNs technologies, main applications and standards, features in WSNs design, and evaluations. In particular, some peculiar applications, such as those based on environmental monitoring, are discussed and design strategies highlighted; a case study based on a real implementation is also reported. Trends and possible evolutions are traced. Emphasis is given to the IEEE 802.15.4 technology, which enables many applications of WSNs. Some example of performance characteristics of 802.15.4-based networks are shown and discussed as a function of the size of the WSN and the data type to be exchanged between nodes [49].

In 2010 Amar Adnan Rasheed M.S., Northeastern Dr. Rabi N. Mahapatra In their dissertation, they consider a number of security schemes for WSN (wireless sensor network) with MS. The schemes offer high network's resiliency and low communication overhead against nodes capture, MS replication and wormhole attacks. They propose two schemes based on the polynomial pool scheme for tolerating nodes capture: the probabilistic generation key pre-distribution scheme combined with a polynomial pool scheme, and the Q-composite generation key scheme combined with a polynomial pool scheme. The schemes ensure low communication overhead and high resiliency. For anti MS replication attack scheme, they propose the multiple polynomial pools scheme that provides much higher resiliency to MS replication attack as compared to the single polynomial pool approach. Furthermore, to improve the network resiliency against wormhole attack, two defensive mechanisms were developed according to the MS mobility type. In the first technique, MS uses controlled mobility. They investigate the problem by using a single authentication code from sensor networks to verify the source of MS beacons, and then they develop a defensive approach that divides the sensor network into different authentication code's grids. In their second technique, random mobility is used by MS. They explore the use of different communication channels available in the sensor hardware combined with polynomial pool scheme [50].

In 2011 Dr. Manoj Kumar Jain in their paper they attempt to present a survey on the major topics in wireless sensor network security, and also present the obstacles and the requirements in the sensor security, classify many of the current attacks, and finally list their corresponding defensive measures [51].

In 2011 A. LAKSHMI S.V. MANISEKARAN DR.R.VENKATESAN in their paper they propose novel energy efficient algorithm FDPCA for Wireless Sensor Networks (WSN). However, energy consumption is one of the major drawbacks in most of the Wireless Sensor Networks. Parameters like End to End Delay and Received Signal Strength Indicator (RSSI) are considered in exercising the influence on transmit power. These parameters are fuzzified and optimal transmission power levels are selected. The throughput for both DPCA and FDPCA are compared. High throughput is obtained by using FDPCA. In their first phase, the parameters are calculated. Their proposed algorithm can effectively save energy without degrading the throughput of the network and reduce the energy consumption of the network. Their experimental results demonstrate that the proposed algorithm significantly overtake previous method, in terms of throughput [52].

In 2011 Luís M. L. Oliveira Joel J. P. C. Rodrigues in their paper they surveys a comprehensive review of the available solutions to support wireless sensor network environmental monitoring applications [53]

In 2012 Xiaojiang Ren Weifa Liang In their paper they consider data collection in an energy harvesting sensor network with a mobile sink, where a mobile sink travels along a trajectory for data collection subject to a specified tolerant delay constraint T. The problem is to find an optimal close trajectory for the mobile sink that consists of sojourn locations and the sojourn time at each location such that the network throughput is maximized, assuming that the mobile sink can only collect data from one-hop sensors, for which they first show that the problem is NP-hard. Then they devise novel heuristic algorithms. They finally conduct extensive experiments to evaluate the performance of the proposed algorithms. They also investigate the impact of different parameters on the performance. The experimental results demonstrate that the proposed algorithms are efficient. To the best of our knowledge, this is the first kind of work of data collection for energy harvesting sensor networks with mobile sinks [54].

III. CONCLUSION AND FURTHER DEVELOPMENT

Now a day's wireless technology is going to use in everywhere to maintain the communication needs of the end user. The importance of the Dynamic wireless sensor network in our day to day life has been discussed in these papers, we have discussed the different types of the dynamic wireless sensor network and we have discussed the advantages of these technologies over the wired technology.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci "A survey on sensor networks", IEEE Communications Magazine, 40(8), pp. 102–114, 2002.

[2] C. Long, C. Can-Feng, Ma Jian,"Selection scheme of mobile sinks in wireless sensor networks", Journal on Communications, Vol. 11, No. 11, pp.12-18,2008.

[3] SHI Gao-Tao, LIAO Ming-Hong,"Movement-assisted data gathering scheme with load-balance for sensor networks",Journal of Software, Vol. 18, No. 9, pp. 2235-2244, 2007.

[4] Wang W. Srinivasan V, Chua KC,"Using mobile relays to prolong the lifetime of wireless sensor networks", In Proceeding of the 11th Annual Int'l Conf. on Mobile Computing and Networking, pp. 270-283, 2005.

[5] Luo J, Hubaux JP,"Joint mobility and routing for lifetime elongation in wireless sensor networks", In Proceeding of the 24th IEEE INFOCOM., pp.1735-1746, 2005.

[6] Rahul C. Shah, Sumit Roy, Sushant Jain, Waylon Brunette,"Data MULEs: Modeling and analysis of a threetier architecture for sparse sensor networks", In Proceeding of the IEEE Workshop on Sensor Network Protocols and Applications, pp. 30-41, 2003.

[7] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770-772, November 1981.

[8] Debnath, Ashmita; Singaravelu, Pradheepkumar; Verma, Shekhar (19 December 2012). "Efficient spatial privacy preserving scheme for sensor network". Central European Journal of Engineering 3 (1): 1–10.

[9] Surie, D., Laguionie, O., Pederson, T.: "Wireless Sensor Networking of Everyday Objects in a Smart Home Environment". In Proceedings of the 4th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Sydney, Australia, pp. 189-194, (2008).

[10] J.D. Kenney, D.R. Poole, G.C. Willden, B.A. Abbott, A.P. Morris, R.N. McGinnis, and D.A. Ferrill, "Precise Positioning with Wireless Sensor Nodes: Monitoring Natural Hazards in All Terrains", 2009 IEEE International Conference on Systems, Man, and Cybernetics, San Antonio, TX, USA, Oct. 2009.

[11] T.L. Dinh, W. Hu, P. Sikka, P. Corke, L. Overs and S. Brosnan, "Design and Deployment of a Remote Robust Sensor Network: Experiences from an Outdoor Water Quality Monitoring Network", 2007 32nd IEEE Conference on Local Computer Networks.

[12] F. Viani, P. Rocca, M. Benedetti, G. Oliveri, A. Massa , "Electromagnetic passive localization and tracking of moving targets in a WSN-infrastructure environment " in Inverse Problems, vol. 26, (2010), p. 1-15.

[13] Palafox-secwsn Security in Wireless Sensor Networks Luis E. Palafox CICESE Research Center, Mexico J. Antonio Garcia-Macias CICESE Research Center, Mexico.

[14] L. Lazos and R. Poovendran. Sherlock: Robust localization for wireless sensor networks. ACM Trans. Sen. Netw., 1(1):73–100, 2005.

[15] S. ˘Capkun and J.-P. Hubaux. Secure positioning in wireless networks. IEEE Journal on Selected Areas in Communications, 24(2):221–232, 2006.

[16] A. Goldsmith and S. Wicker, "Design challenges for energy-constrained ad hoc wireless networks," IEEE Wireless Communications Magazine, vol. 9, pp. 8–27, Aug. 2002.

[17] L. Yuan and G. Qu, "Energy-efficient Design of Distributed Sensor Networks," in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, M. Ilyas and I. Mahgoub, eds., Boca Raton, FL, pp. 38.1–38.19, CRC Press, 2004.

[18] M. Haenggi, "Twelve Reasons not to Route over Many Short Hops," in IEEE Vehicular Technology Conference (VTC'04 Fall), Los Angeles, CA, Sept. 2004.

[19] M. Haenggi, "Energy-Balancing Strategies for Wireless Sensor Networks," in IEEE International Symposium on Circuits and Systems (ISCAS'03), Bangkok, Thailand, May 2003.

[20] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava,"Coverage problems in wireless ad-hoc sensor networks," in Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'01), vol. 3, Anchorage, AK, pp. 1380–1387, Apr. 2001.

[21] N. Reijers and K. Loangendoen, "Efficient code distribution in wireless sensor networks," in Second ACM International Workshop on Wireless Sensor Networks and Applications, San Diego, CA, Sept. 2003.

[22] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly resilient,energy efficient multipath routing in wireless sensor networks," in Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'01), Long Beach, CA, pp. 251–254, 2001.

[23] M. Mauve, H. Hartenstein, H. Fuessler, J.Widmer, and W. Effelsberg, "Positionsbasiertes Routing fuer die Kommunikation zwischen Fahrzeugen," it—Information Technology (formerly it + ti)—Methoden und innovative Anwendungen der Informatik und Informationstechnik, vol. 44, pp. 278–286, Oct. 2002.

[24] F. Sivrikaya and B. Yener, "Time synchronization in sensor networks: A survey," IEEE Network, vol. 18, pp. 45–50, July–Aug. 2004.

[25] R.C. Shah, S. Roy, S. Jain, and W. Brunette, "Data MULEs: Modeling and analysis of a three-tier architecture for sparse sensor networks," in Ad Hoc Networks Journal, vol. 1, pp. 215–233, Elsevier, Sept. 2003.

[26] A. Chakrabarti, A. Sabharwal, and B. Aazhang, "Using predictable observer mobility for power efficient design of sensor networks," in Information Processing in Sensor Networks (IPSN'03), Palo Alto, CA, Apr. 2003.

[27] O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks," in IEEE Transactions on Mobile Computing, vol. 3, pp. 366–379, 2004.

[28] R. Govindan, J. Hellerstein, W. Hong, S. Madden, M. Franklin, and S. Shenker, "The Sensor Network as a Database," Tech. Rep. 02–771, University of Southern California, 2002.

[29] M. Yarvis and W. Ye, "Tiered Architectures in Sensor Networks," in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, M. Ilyas and I. Mahgoub, eds., Boca Raton, FL, pp. 13.1–13.22, CRC Press, 2004.

[30] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in 7th International Workshop on Security Protocols, Cambridge, UK, Apr. 1999.

[31] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, "Denial-of-service Attacks on battery-powered mobile computers," in Proceedings of the 2nd IEEE Pervasive Computing Conference, Orlando, FL, pp. 309–318, Mar. 2004.

[32] Hart, J. K. And Martinez, K. (2006) Environmental Sensor Networks:A revolution in the earth system science? Earth-Science Reviews, 78 . pp. 177-191.

[33] I. Vasilescu, K. Kotay, D. Rus, M. Dunbabin, and P. Corke. 2005. Data collection, storage, and retrieval with an underwater sensor network. In Proceedings of the 3rd international conference on Embedded networked sensor systems (SenSys '05. ACM, New York, NY, USA, 154-165.

[34] Martinez, K, Hart, J. K. And Ong, R (2009) Deploying a Wireless Sensor Network in Iceland. Lecture Notes in Computer Science, Proc. Geosensor Networks, 5659, 131-137.

[35]http://www.libelium.com/wireless_sensor_networks_to_detec_forest_fires/ Air Quality Monitoring

[36] Jason Lester Hill "System Architecture for Wireless Sensor Networks", University of California, Berkeley , Spring 2003.

[37] Raquel A.F. Mini, Antonio A.F. Loureiro, Badri Nath, "The distinctive design characteristic of a wireless sensor network: the energy map" , Computer Communications 27 (2004) 935–945.

[38] Daniele Puccinelli and Martin Haenggi, "Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing ",IEEE circuits and systems magazine third quarter 2005.

[39] Adam Dunkels, Niclas Finne, Joakim Eriksson, Thiemo Voigt "Run-Time Dynamic Linking for Reprogramming Wireless Sensor Networks" SenSys'06, November 1.3, 2006, Boulder, Colorado, USA.

[40] Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA, "Security Solutions for Wireless Sensor Networks",Neo Technical Journal Vol. 01, 03/2006.

[41] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey" , Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.),2006 Auerbach Publications, CRC Press.

[42] Liang Song and Dimitrios Hatzinakos, "Architecture for Wireless Sensor Networks with Mobile Sinks: Sparsely Deployed Sensors" , IEEE Trans. on Vehicular Technology, june 2006.

[43] Yong WangGarhan AtteburyByrav Ramamurthy, "A Survey of Security Issues In Wireless Sensor Networks" , CSE Journal Articles. Paper 84. http://digitalcommons.unl.edu/csearticles/84.

[44] Al-Sakib Khan Pathan Hyung-Woo Lee Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Feb. 20-22, 2006 ICACT2006.

[45] Prabhudutta Mohanty, Sangram Panigrahi Nityananda Sarma, Siddhartha Sankar Satapathy, "Security issues in wireless sensor network data gathering protocols: a survey", Journal of Theoretical and Applied Information Technology.

[46] Luis E. Palafox , J. Antonio Garcia-Macias , "Security in Wireless Sensor Networks", 2008, IGI Global.

[47] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International journal of communications Issue 1, Volume 2, 2008.

[48] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosa, "Wireless sensor network survey" , Computer Networks 52 (2008) 2292–2330.

[49] Chiara Buratti Andrea Conti Davide Dardari and Roberto Verdone, "An Overview on Wireless Sensor Networks Technology and Evolution " , Sensors 2009, 9, 6869-6896.

[50] Amar Adnan Rasheed M.S., Northeastern Dr. Rabi N. Mahapatra, "security schemes for wireless sensor networks with mobile sink", Texas A&M University.

[51] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", 2011 ijcit, issn 2078-5828 (print), issn 2218-5224 (online), volume 02, issue 01, manuscript code: 110746.

[52] A. LAKSHMI S.V. MANISEKARAN DR.R.VENKATESAN, "fuzzified dynamic power control algorithm for wireless sensor networks", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4 Apr 2011, Pp: 3023 – 3028.

[53] Luís M. L. Oliveira Joel J. P. C. Rodrigues, "Wireless Sensor Networks: a Survey on Environmental Monitoring" , journal of communications, vol. 6, no. 2, april 2011, Pp: 143-151.

[54] 2012 Xiaojiang Ren Weifa Liang, "Delay-Tolerant Data Gathering in Energy Harvesting Sensor Networks With a Mobile Sink" , globecom 2012, ad hoc and sensor networking symposium.

Hemant Patel , B.E., M.E. Scholar in Computer Technology & Application from Shri Shankaracharya College of Engineering & Technology, Bhilai, India. Research areas are Wireless Sensor Network, mobile ad hoc network & its enhancement.

Aakanksha S. Choubey, Asst. Professor in Dept. of Computer Science & Engineering at Shri Shankaracharya College of Engineering & Technology, Bhilai. India**.** Having Wide experience in the field of teaching. Research areas are Wireless Sensor Network, its Enhancements, and Her research work has been published in many national and international journals.