*International Journal of Latest Trends in Engineering and Technology*
*Vol.(9)Issue(2), pp.182-185*
*DOI: http://dx.doi.org/10.21172/1.92.30*
*e-ISSN:2278-621X*

# CONCEPTUAL ARCHITECTURE, ISSUES AND APPLICATIONS OF WIRELESS SENSOR NETWORKS

Prabha Rani[1]

**Abstract: - In Wireless Sensor Networks (WSNs), sensor nodes are used for sensing network by detecting events in the surrounding environment. This gathered information from proximate sensors, assimilate this information and then send for further processing of user applications. Numerous jobs of WSNs include broadcasting, multicasting, routing, and advancing and path conservation. A WSN is vulnerable to countless sorts of attacks primarily owing to insecure as well as undefended nature of message link, unreliable broadcast medium, positioning in unfriendly surroundings, mechanized nature and narrow availability of resources. There are many vulnerabilities and attacks on WSNs.**
**Keywords: - WSN, Sensor Nodes, Characteristics, Protocols, Architecture, Issues, Applications, Attacks, Vulnerabilities.**

## 1. INTRODUCTION

In WSN architecture as shown in figure 1, nodes having measurement capability are deployed to measure physical quantities such as temperature, voltage, pressure and sound etc.

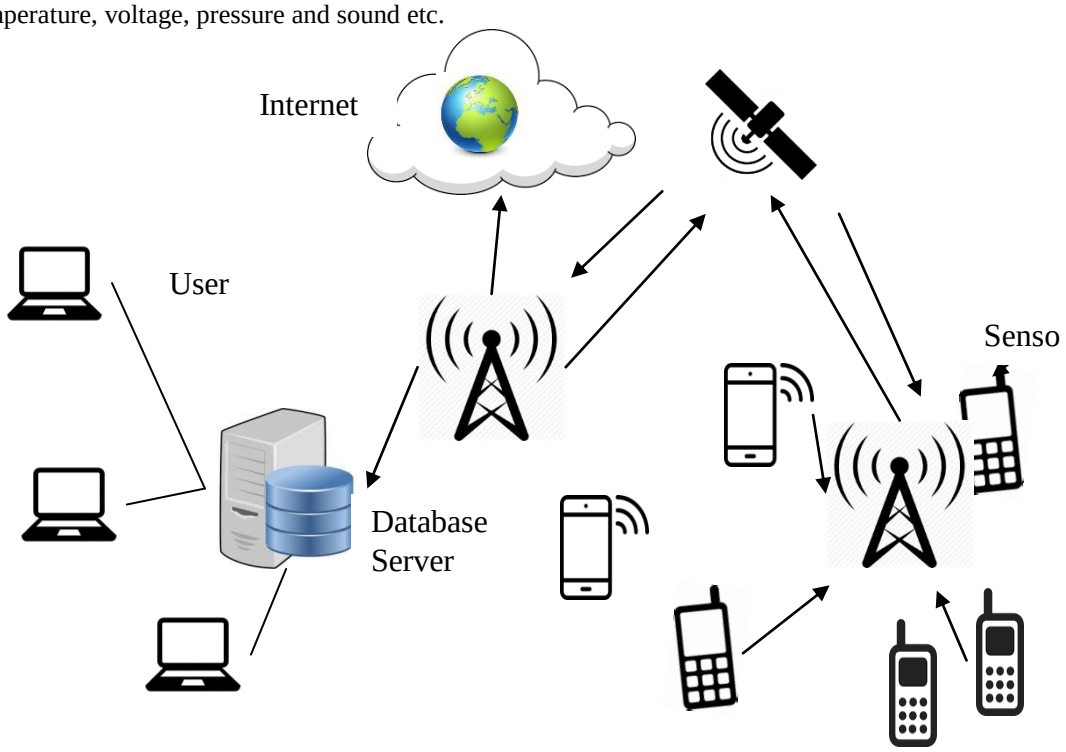


Figure 1: WSN's Architecture

The main aim of WSN is to deliver effectual connection amid physical as well as digital world. Nodes of a WSN are controlled through gateway, which administers network functions such as data security, client verification etc. In WSNs, sensory nodes collect information from real world surroundings which can be about a physical object or can be about occurrence of a certain event in the environment, then utilizes its processing capabilities to perform simple calculations locally for transforming it into digital signals which can be further processed, stored and advanced to a computing system known as base station. A BS offers an interface amid user as well as internet gateway which gathers measured data from every node and transmits it over a wireline link, usually an "Ethernet", towards a "Host Controller" where software can do advanced processing as well as scrutiny and presents data in a mode which meets user requirements [1] [2] [4][5][8][20].

[1] Haryana Education Department, Rohtak

## 2. PROTOCOL ARCHITECTURES

The protocol stack comprises of five layers namely "Application layer, Transport layer, Network layer, Data link layer, Physical layer, as well as three planes namely Power management plane, Mobility management plane, and Task management plane" shown in figure 2. The functionalities of the layers are more or less similar to adhoc networks or other wireless networks[5] [2] [9] [11].

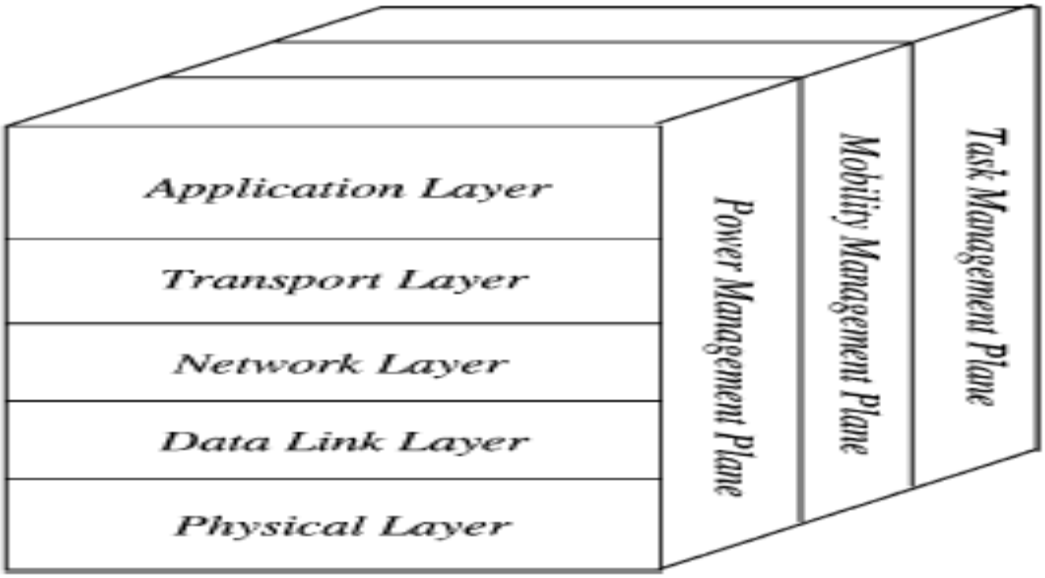


Figure 2: WSNs Protocol Stack

## 3. ISSUES

Maximum sensor networks are solicitation specific and have varied solicitation necessities. Consequently, following prime design goals are deliberated in designing of sensor networks like Smaller size of node, Lower cost of node, Lower power intake, Expendability, Consistency, Self-configurability, Adaptableness, Link usage, Fault forbearance, Capability to handle failures of nodes as well as link failures, Security, QoS support, Energy-efficiency and robustness to prolong system uptime, Self-configuration, ease of deployment of network, Heterogeneity and mobility of nodes, Dynamic network topology, Latency-awareness, to gather information of end user as quickly as possible, Relative to application specific nature of sensor network and Ability to withstand harsh environmental conditions [1] [15][16][18] [19][ 21][22] [23] [25] [28].

## 4. VULNERABILITIES

For a resourceful as well as unswerving communication in WSNs, the designing mission of a routing protocol necessitates additional careful deliberations comparison to other wireless ad-hoc networks which includes network topology, methods of data reporting, node as well as linkage heterogeneity, node adaptableness, power efficiency, coverage of area, data accumulation, and Quality of Service (QoS) [15] [21] [28] [30]. WSNs are susceptible to countless sorts of attacks such as Stealing (reengineering, conceding as well as duplicating), Restricted capabilities (DoS attacks, restriction in usage of encryption tactics), Arbitrary positioning (hard pre-configuration),Unmanned deployment on unfriendly locations (physical access, captured node and node obliteration),Insider attacks, Inappropriate/impracticable customary security methods, Ad-hoc centered positioning, Resources dearth, Devices with restricted capabilities, ubiquity (privacy uncertainties), wireless (medium) as well as mobility, Untrustworthy communication, Untrustworthy transfer, broadcast nature of links, Encounters, multi-hop routing and network congestion as well as node processing, Dormancy, Huge scale (highest density, mountable security method necessity), Re-designing security architectures (distributed & self-organized) [3][6][7][10][13][17][21] [22][23][25][31]. WSNs are susceptible to numerous attacks primarily owing to its elementary features of broadcasting nature of transmission link, unmanned operation after positioning. In a WSN, there are two categories of attacks namely "Active attacks as well as Passive attacks". "Passive attacks" are related to observation and eavesdropping of communication link by illegal users. "Active attacks" are related to observation by illegal users who eaves drops and alters data stream in a communication link [3][6][7][10][13][17][23].

## 5. APPLICATIONS

WSNs have recently emerged as a know-how which has stemmed in a range of solicitations including Military as well as Civil environment. WSN are used in various manners such as Imaging of target field, Detecting intrusions, Security and Tactical Surveillance, Military surveillance and tracking, Traffic control, Health care monitoring, Medical diagnostics, Monitoring weather, Environmental/Earth monitoring, Environmental magnitudes (Temperature, Humidity, Light), Air

quality monitoring, Area monitoring, Industrial automation, Civil structural monitoring, Gas & particle concentration, Atmospheric monitoring (Atmospheric pressure, Rainfall, Wind direction, UV levels, Wind speed etc.), Air pollution monitoring, Rapid Emergency Response, Disaster management, Water catchment & ecosystem monitoring, Interior monitoring, Exterior monitoring, Smart Home/ Smart Office, Air traffic control, Process control, Inventory management, Industrial and manufacturing automation, Land slide detection and monitoring, Distributed robotics, Remote Sensing in Disaster Management, sensing of fire in Forest area, Natural disaster deterrence, Landslide sensing, Monitoring of quality of water, Agriculture, Greenhouse observation, Structural monitoring, Structural Fitness Magnitudes, Environs Conditions, Breeze and climate conditions, Traffic and Toxic waste effects, Distributed computing, and Smart home monitoring etc. [1] [12] [16] [19] [21] [23].

## 6. CONCLUSION

This paper covers the conceptual view of Wireless Sensor Networks, that the mechanism how sensor nodes are used for sensing network by detecting events in the surrounding environment. The head or gateway sensor nodes after gathering information from proximate sensors assimilate this information and then send for further processing of user applications. This various tasks of WSNs are broadcasting, multicasting, routing, and advancing and path conservation. WSNs are also vulnerable to countless sorts of attacks primarily owing to insecure as well as undefended nature of message link, unreliable broadcast medium, positioning in unfriendly surroundings, mechanized nature and narrow availability of resources. There are many vulnerabilities and attacks on WSNs which are very harmful to the actual use. Still with these characteristics, technical issues, attacks and vulnerabilities WSNs have lot of application in real life and growing over time.

## 7. REFERENCES


[1] Akyildiz I. F., W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless sensor networks: a survey", Computer Networks, Vol.38, pp. 393-422 (2002).

[2] Zheng Jun, Abbas Jamalipour, “Wireless Sensor Networks: A Networking Perspective”, John Wiley & Sons (2009).

[3] Neeraj Sharma, B.L. Raina, Prabha Rani, Yogesh Chaba, Yudhvir Singh, “Attack Prevention Methods for DDoS Attacks in MANETs”, Asian Journal Of Computer Science And Information Technology, ISSN – 2249-5126,Vol 1, Issue 1, pp. 18 – 21 (2011).

[4] Parveen Kumari, Yudhvir Singh, “Delaunay Triangulation Coverage Strategy for Wireless Sensor Networks”, Proc. of IEEE sponsored Second International Conference on Computer Communication and Informatics (2012).

[5] Yoneki E., J. Bacon, “A survey of Wireless Sensor Network technologies: research trends and middleware’s role”, Technical Report, No. UCAM-CL-TR-646, University of Cambridge, pp 1-46 (2005).

[6] Pooja, Manisha, Yudhvir Singh, “Security Issues and Sybil Attack in Wireless Sensor Networks”, International Journal of P2P Network Trends and Technology, ISSN: 2249-2615, Volume3, Issue1, pp7-13, 2013.

[7] Preeti, Yogesh Chaba, Yudhvir Singh, “Review of Detection and Prevention of DDOS attack in MANET”, Proc. National Conference on Challenges & Opportunities in Information Technology (COIT –2008), India, pp. 56-59 (March 29,2008).

[8] Krishnamachari B., D. Estrin, S. Wicker, "Impact of Data Aggregation in Wireless Sensor Networks", Proc. 22nd IEEE International Conference Distributed Computing Systems, Jul. 2002, pp. 575-578 (2002).

[9] Hill J., R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, “System Architecture Directions for Networked Sensors”, ACM SIGOPS operating systems review, vol , issue 5, pp 93-104 (2000).

[10] Prabha Rani, Yogesh Chaba, Yudhvir Singh, “Hybrid Approach for Detection and Prevention of Blackhole Attack in Mobile Adhoc Network”, International Journal of Wireless Communication, ISSN 0974-9640, pp 885-890, August, 2011.

[11] Despaux Francoisx, “Modelling and evaluation of the end to end delay in WSN”, Networking and Internet Architecture, Universit´e de Lorraine (2015).

[12] Miodrag Živković, "A Survey and Classification of Wireless Sensor Networks Simulators Based on the Domain of Use," Adhoc & Sensor Wireless Networks, Vol 20, issue 4-3, pp 245-287 (2014).

[13] Rahul Rishi, Dheer Dhwaj Barak,Yudhvir Singh, Prabha Rani, “Mobility Analysis of Blackhole Node Attacks in Mobile Adhoc Networks”, International Conference on Recent Trends in Computing, Mechatronics and Communication, India,pp 93-97, February 25-26, 2012.

[14] Renu Dalal, Manju Khari, Yudhvir Singh, “Survey of Trust Schemes on Ad-hoc Network”, Springer - Lecture Notes of the Institute for Computer Sciences, Social Informatics & Telecommunications Engineering (LNICST), Series 84, Springer, NETCOM-3, CCSIT-2012, pp 170-180,(2012).

[15] Vikash Siwach, Yudhvir Singh, Seema, Dheer Dhwaj Barak, “An approach to optimize QoS routing protocol using genetic algorithm in MANET”, IJCSMS, ISSN: 2231-5268, Vol 12, Issue 3, pp 149-53, (Sept 2012).

[16] Lewis F. L., “Wireless Sensor Networks”, Smart Environments: Technologies, Protocols, and Application, John Wiley, pp 11-46 (2004).

[17] Yogesh Chaba, Yudhvir Singh, Prabha Rani, “Comparison of Various Passive Distributed Denial of Service Attack in Mobile Adhoc Networks” Proc. WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communication (EHAC10), Cambridge, UK (ISBN: 978-960-474-155- 7), pp 49-53 (2010)

[18] Yogesh Chaba, Yudhvir Singh, KP Singh, Prabha Rani, “Performance Modeling of MANET Routing Protocols with Multiple Mode Wormhole Attacks”, Communications in Computer and Information Sciences, Springer [Online : Springer Digital Library] (2010) Volume 101, Part 3, pp 518-527, (2010).

[19] Peha Jon M., "Wireless Communications and Coexistence for Smart Environments,” Proc of IEEE Conference on Personal Communications, Vol 7, pp. 66-68 (2000).

[20] Yogesh Chaba, Yudhvir Singh, Aarti, “Performance Analysis of Scalability and Mobility on Routing Protocols in MANETs” International Journal of IT & Knowledge Management (ISSN: 0973-4414), Vol. 1, No. 2, pp. 327-336 (July-Dec, 2008).

[21] Pathan Al-Sakib Khan, Hyung-Woo Lee, Choong Seon Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, IEEE 8th International Conference Advanced Communication Technology, Vol. 2, pp 6-12 (2006).

[22] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak, "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks", Third IEEE International Conference on Advanced Computing & Communication Technologies, 2012.

[23] Chong Chee-Yee, Srikanta P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges", Proc of the IEEE, vol 91, no. 8, pp 1247-1256 (2003).

[24] Yudhvir Singh, Yogesh Chaba, Prabha Rani, "Integrating – VPN and IDS – An approach to Networks Security", International Journal of Computer Science & Security (ISSN:1985-1533), Vol. 1, Issue 3, pp. 1-13(2007)

[25] Wu Di, Gang Hu, Gang Ni, "Research and Improve on Secure Routing Protocols in Wireless Sensor Networks", Proc. of 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC), pp: 853-856 (2008).

[26] Yudhvir Singh, Amit Kumar, Prabha Rani, and Sunil Kumar Kaushik, "Impact of CBR Traffic on Routing Protocols in MANETs", IEEE UKSim-AMSS 16th International Conference on Computer Modeling and Simulation, [Online: IEEE Xplore Digital Library], University of Cambridge, United Kingdom, 26-28, March 2014.

[27] Yudhvir Singh, Dheer Dhwaj Barak, Vikash Siwach, Prabha Rani, "Attacks on wireless sensor networks: a survey", IJCSMS, ISSN: 2231-5268, Vol 12, Issue 3, pp 143-148, (Sept 2012).

[28] Stankovic John A., "Research challenges for wireless sensor networks", Special issue on embedded sensor networks and wireless computing, ACM SIGBED, Volume 1, Issue 2, pp: 9-12 (2004).

[29] Almazaydeh Laiali, Eman Abdelfattah, Manal Al- Bzoor, Amer Al- Rahayfeh, "Performance Evaluation of Routing Protocols in Wireless Sensor Networks", International Journal of Computer Science and Information Technology, Volume 2, Num. 2, pp 64-73 (2010).

[30] Punyani Heena, Yudhvir Singh, "Efficient Coverage Connectivity Technique in Wireless Sensor Networks: For Coverage Optimization and increasing connectivity", LAP LAMBERT Academic Publishing, Germany, pp 1-52 (2012).

[31] Bojkovic Zoran S., Bojan M. Bakmaz, Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International Journal of Communications, Volume 2, issue 1, pp 106-115 (2008).