Challenges and Design Goals of Wireless Sensor Networks: A Sate-of-the-art Review

Chandrakant Mallick
Biju Pattnaik University of Technology
Rourkela, India

Suneeta Satpathy
Biju Pattnaik University of Technology
Rourkela, India

ABSTRACT
Wireless sensor networks (WSNs) have power of distributed communication, computing, sensing features. They are characterized as infrastructure less, fault tolerant and self-organizing networks which provide opportunities for low-cost, easy-to-apply, rapid and flexible installations in unattended and harsh environments in various prospective applications. In future, their wide range of applications will make them an integral part in Internet of Things (IoT) and hence in real life. However, implementation of sensor networks pose many challenges for researchers to satisfy the stringent constraints introduced by peculiar characteristics primarily, the scarcest energy sources, unattended and harsh deployment environment, insecure radio links, changing network topologies, heterogeneity of nodes and multi-hop communications etc. In this paper we surveyed the structure, characteristics of wireless sensor network and its prospective applications along with its implementation challenges as well as design goals in brief.

Keywords
Wireless, Sensors Network, Internet of Things, multi-hop, distributed communication

1. INTRODUCTION
Advances in wireless communications and electronics lead to development of low cost, low-power, multifunctional small size sensor nodes capable of short-ranged wireless communication. The main power elements of wireless sensor network are the tiny sensor nodes capable of sensing, data processing, and communicating between the components [1]. The sensor nodes work collectively to send the summarized data to the sink called as base station to monitor and obtain a conclusion about an environment. The base station does the result analysis on collected data [8].

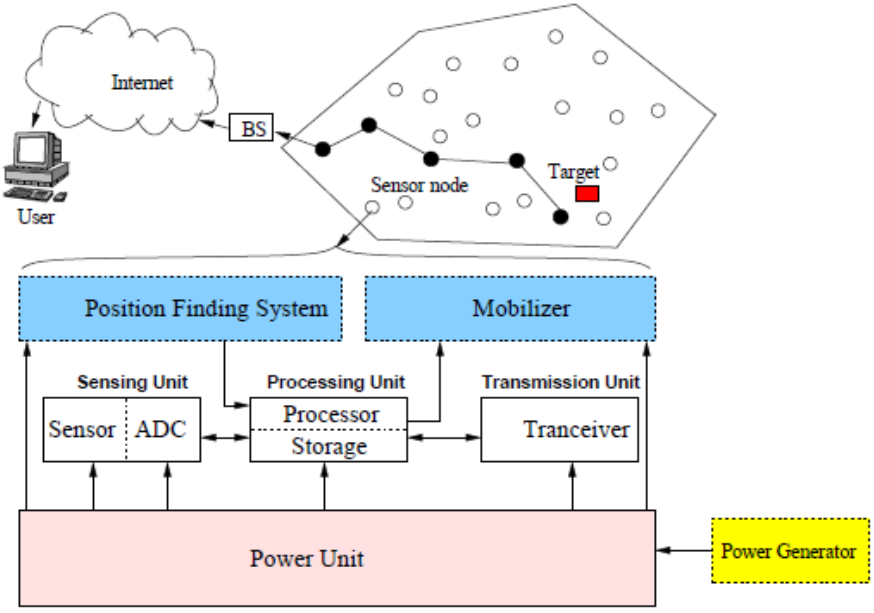

Fig.1: Wireless Sensor Network and Sensor node Architecture [9]

Base station is attached to the user interface through which user can establish the communication. Wireless Sensor Network consists of various autonomous devices which are scattered geographically, capable of monitoring physical and environmental conditions like temp, pressure, sound, vibration, motion etc [17]. Fig.1 depicts the architectural configuration of wireless sensor network. The characteristics, requirements, strengths, constraints, applications and types of wireless sensor network are thoroughly reviewed to get a full impending discussion. The wireless sensor networks major challenges with respective design goals are described in the next section. The conclusion ends with the concluding remarks for various research problems.

1.1 Characteristics of WSNs
There are many peculiar characteristics of WSNs that provides opportunities of large scale applications and some characteristics also pose constraints and challenges in designing the application specific wireless sensor networks. The main characteristics of WSNs are described in Table-1.

Table 1. Main characteristics of WSNs

Characteristics	Description
Resource constraints	Nodes of WSN are smaller in size and gets power from the batteries. It justifies that service provided by the nodes like communication and computation amount of memory is very limited.
Communication paradigm	The data centric feature of WSN explains its data centric nature and justifies that the communication is restricted to nodes in a given location [2, 24].
Application specific design	WSN is application specific i.e. the architecture of WSN is based on application or on a particular task [2, 27].
Node failure and unreliable communication	Various factors like harsh operating conditions leading to instability, unpredictability, nodal mobility, environmental interferences makes typical WSN nodes to be error-prone [1, 8, 2].
Scalability and density	The number of nodes in WSNs may be large and densely deployed in a higher degree in various applications [2].
Dynamic Topologies	Nodes are free to travel randomly at different speeds in few applications and sometimes may fail to operate, to add or to replace. So there can be different network topology [27].
Communication models	WSNs use different communication models: Flat/ hierarchical /distributed WSNs; or homogenous/ heterogeneous WSNs [13].
Operating Environment	The WSNs are mostly deployed in remote and hazardous locations for unattended operations because of their ability to withstand harsh environmental conditions [1, 8].
Global ID	A typical WSN node does not have a unique global network ID [1, 8].

1.2 Requirements for WSNs

The features [1, 2, 8] required for WSNs that make the sensor networks popular and attractive for many new and exciting applications are:

Flexibility: The architecture of WSN is not fixed rather it varies from application to application which justifies that the protocols and algorithms have the characteristics of self organization.

Fault tolerance: The nodes in WSNs has the capability to sustain the functions carried out in the network even in the situations like limited battery power, interference from external sources, failure rate of nodes, harsh environmental conditions.

Lifetime: The two major factors that should be taken into consideration are load balancing and energy saving. These two factors can enhance the lifetime of the WSN architecture as long as possible.

Scalability: The number of nodes in a WSN network can be large. Accordingly WSN architecture and protocols should be designed.

Real-time: Various capabilities like sensing, processing and communication of WSN are used in various real world problems so should follow stringent time.

Security: The data offered by WSN network are private for example health care data and military data which are sensitive in nature. So security is evident in such architectures.

Production cost: The cost of nodes in WSN network has to be low as once the nodes run out of the energy it has to be replaced by newer nodes.

Deployment: In large-scale WSNs, there is random deployment of nodes whose maintenance and replacements

are not practically possible. So there is a huge requirement of re-configuration and re-programming.

Dependability: One can rely on WSN as the architectural design is robust that leads to secure collection of data and reliable delivery with no loss.

1.3 Constraints on WSNs:

WSNs also suffer from many constraints because of its peculiar characteristics. Some of the major constraints include [1, 8, 5, 12, 29]

1) **Resource Constraints**: Limited bandwidth, energy, memory and processing capabilities, multi-hop, insecure radio communication, and short communication range.
2) **Design Constraints**: Various design constraint include node failure, nodes are mobile, application specific network topology, heterogeneous network, physical size and total number of nodes etc.
   As WSN possess stringent resource and design constraints, there is a need to design new wireless networking techniques and protocols to enhance the capabilities of existing architectures.

1.4 Applications of WSNs

The applications of sensor networks are innumerable, since the three key services sensing, processing and communication are bunched in a single device called node capable of monitoring temperature, humidity, pressure and noise levels[1,4,7,14]. The application of sensor networks can be broadly classified into two categories: monitoring and tracking [8, 9].The classification of are several types of monitoring and tracking applications are depicted in Fig. 2.

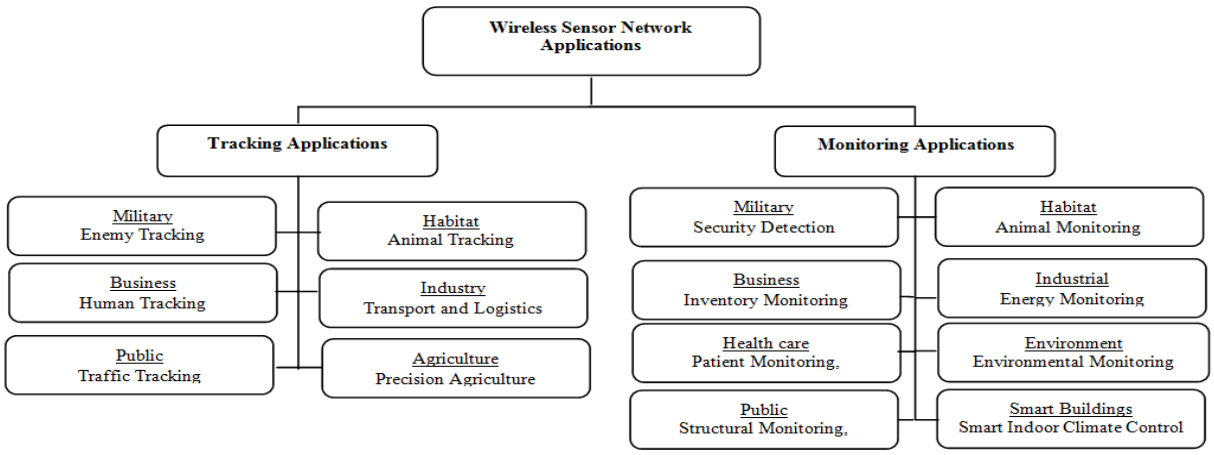

Fig 2: Classification of WSN applications

1.5 Types of Wireless Sensor Networks

WSN architecture is not fixed. It varies from application to application. So challenges and constraints are application environment specific. Accordingly, types of WSNs are: terrestrial WSN, underground WSN, underwater WSN, multi-media WSN, and mobile WSN [8, 12, 14, 16, 23, 25].

a) Terrestrial WSNs: Terrestrial WSN's sensor nodes are arranged in either ad-hoc or preplanned manner on land.

b) Underground WSN: Such WSN architecture is expensive and can sense underground situation.

c) Under water WSNs: In such architectures the communication is done by transmission of acoustic waves under the water.

d) Multimedia WSNs: such architectural configuration can be designed with low cost sensor nodes with cameras and microphones and can establish the communication through wireless connection for data retrieval, process, correlation, and compression.

d) Mobile WSN: Such architecture includes nodes mobility, repositioning and self organizing ability. The information gathered through a mobile WSN is communicated within the range of each other. The key goals in such architecture are deployment, localization, self-organization, navigation control, coverage and energy etc.

2. KEY CHALLENGES AND DESIGN GOALS

WSNs offer a wide variety of applications but they pose potential challenges to implement them. So more efficient components, protocols and algorithms are needed to address these challenges [5, 6, 7, 12, 20, 22, 27, 29].The challenges and their corresponding design goals are listed in Table-2.

Table 2: Key Challenges and design goals

Key Challenges	Design Goals
Resource constraints	Resource-efficient design
Infrastructure-less wireless communication	Secured application specific protocols
Changeable topologies and unpleasantly rough environmental conditions	Adaptive network operations with self-configuration and self-organizing capability.
Quality-of-service(QoS) requirements	Précised design with time synchronized application.
Security & Vulnerability	Secured design.
Extensive deployment	Provisional architecture and design of tiny, low-cost sensor node.
Integration with Internet	Extensible architectures and protocols.
Data redundancy	fusion and localization of processed Data
Packet errors and variable-link capacity	Fault tolerating and trustworthiness.
Storage	Flat cost tiny sensor nodes with high storage capacity

2.1 Resource constraints

A sensor node has limited processing, storage, communication capabilities and limited energy supply.

Battery is the only scarcest source of energy for the nodes and battery life time determines the lifetime of WSNs.

So sensor nodes should be equipped with effective power scavenging techniques, such as solar cells, because it is not easy to access or replace them after deployment. Hence, power conservancy and management take on additional importance. Battery characteristics such as recovery effects, thermal effects, discharge characteristics etc. are the most important aspects to be considered for increasing the lifetime of the battery [18]. Current research is more inclined towards full or partial sensing coverage in the context of energy conservation [3, 12].

2.1.1 Resource-efficient design

Resource constraints pose a great challenge to the researchers to focus on the resource efficient design of power-aware protocols and algorithms for wireless sensor networks to provide high energy efficiency [1]. Hybrid architecture of three existing sources of batteries, ambient environment, and wireless transfer can be implemented in order to increase the network lifetime [18].

2.2 Infrastructure-less Communication

WSN can be typically designed with little or no infrastructure. They can operate in structured and unstructured manner [8]. There exist few restrictions on the communication channel between the sensor nodes which may cause problems like unreliable communication. However, it provides the broadcast advantage. This feature supports a wide range of applications of WSNs with different requirements.

2.2.1 Secured application specific protocols

The advantages in various applications can be exploited by developing flexible, scalable and application specific protocols. The protocols can accommodate all requirements of heterogeneous applications and simultaneously ensure security in communication and data collection [27].

2.3 Changeable Topologies and Rough environmental conditions

WSNs are often deployed in unattended and harsh environment. In such cases, nodes may stop functioning and surviving nodes may go in or out of the transmission radii of other nodes [13]. So WSNs may involve dynamic changes in topologies due to mobility and failure of nodes.

2.3.1 Adaptive network operations with self-configuration and self-organizing capability

In self-configurable WSNs, new sensor nodes can be added to replace failed sensor nodes and existing nodes can also be removed without affecting the objectives of the application [12, 19, 26, 27]. The changeable topologies also necessitate the use of self-organizing architectures and protocols. Protection against attacks like node failure and changeable topologies can be ensured with robust and adaptive WSNs protocols [8].

2.4 Quality-of-service (QoS) requirements

The QoS provided by WSNs may refer to the accuracy between the data reported to the base station and data actually collected in the deployed environment. As sensor data are typically time-sensitive, e.g., military surveillance, response time is important at the base station in right time. Late response time due to processing or communication may be outdated and useless [23, 27, 28].

2.4.1 Application-specific design

There exists no universal WSN design that fits all applications; Application specific WSNs, have variety of QoS requirements [28]. So the traditional QoS metric cannot be applied to WSNs. Hence, application specific designs and techniques based on QoS requirements should be developed to provide right service at right time.

2.4.2 Time synchronization

In WSNs, large numbers of sensor nodes need to collaborate to perform the sensing task, and the collected data are usually delay-sensitive [17, 18]. Thus, the communication protocols must be designed based on time synchronization requirements to meet the deadlines of the application. However, due to resources and size limitations and lack of fixed infrastructure, as well as the dynamic topologies in WSNs, existing time synchronization strategies designed for traditional wireless networks may not be appropriate. So, adaptive and scalable time-synchronization protocols are required for WSNs.

2.5 Security and vulnerability

Many WSNs are used for sensitive applications like military or surveillance purposes in which nodes communicate important private data in the network. So security in communication is a crucial issue to be considered for making the communication safe from external denial-of-service (DoS) attacks and intrusion. WSNs may suffer from passive attacks by eavesdropping on transmissions that include traffic analysis or disclosure of message contents etc. and active attacks may include node capturing, routing attacks, or flooding [27].

2.5.1 Secure design

The traditional cryptographic system for data security is not suitable from efficiency and resource usages point of view. So security mechanisms for WSNs, must consider both low-level designs: key establishment and trust control, confidentiality and authentication, preventing Denial of Service attacks, secure routing, resilience to node capture etc. and high-level designs: secure group management, intrusion detection, secure data aggregation etc[28].

2.6 Large-scale deployment and ad-hoc architecture

Te sensor nodes in the WSN network are spread on uniformly to establish connections and maintain network connectivity in the deployment field [27, 30].

2.6.1 Tiny and low-cost sensor nodes

The large scale WSNs design demand small, compact and cost minimized sensor nodes or in other words we can say the nodes in WSN should be affordable in terms of cost, replacement, training, servicing and logistics [18].

2.7 Integration with Internet

WSNs are capable of retrieving useful information from anywhere anytime. So, the architecture of WSN should have integration compatibility with internet protocol architecture to provide a gateway for integration [17]. Current research is focused on building IPv6-enabled WSN applications and protocols which can be a pillar stone for Internet-of-Things (IoT) for next generation applications including IPv6 will be able to with sensor nodes [3, 21].

2.7.1 Scalable architectures and protocols

WSNs have a support for heterogeneous applications with diversified requirements. So the need of the hour is to design flexible and extensible architectures to accommodate the diversified requirements. Modular clustering systems is capable of enhancing the system flexibility, robustness, and reliability [13]. In addition, WSNs network architecture must be interoperable with existing conventional networks such as Ethernet-based systems and other wireless networks [3, 21].

2.8 Data redundancy

The data collected and gathered from heterogeneous sources are always irrelevant and redundant which are never efficient for storage and energy. Flexible protocols and procedures are required for maintain the balance among the accuracy, time, resources and latency adaptive [27].

2.8.1 Data fusion and localized processing

Data Fusion can play a promising role in data processing by not sending the organic data to the sink node rather filtration can be done locally at sensor nodes. The application specific filtered are transmitted to the user. Such fusing and filtering ability based on data fusion feature can reduce redundancy and communication overhead. [27]. Clustering technique can also be used to prepare different clusters and transmit the information to cluster heads which are capable of doing data fusion and then transmit it to the sink. Clustering and reclustering technique with data fusion feature can minimize data redundancy and encourage data aggregation [7].

2.9 Packet errors and variable-link Capacity

The level of the receiver being tampered decides the attainable capacity of each wireless link. The obstructions and noise in the environment are responsible for widely varying characteristics in terms of time and space. The variation in location dependency justifies capacity and delay attainable and is a major key challenge [27].

2.9.1 Fault tolerance and reliability

The reliable transmission of sensed data to its sink in WSN is based on environmental situations, message considerations, and reliability considerations [11]. The reliability of transmission has danger of physical damage, blockage and interference. Repetitive and reestablishment of sensor nodes and network, and overlapped sensing regions can increase the fault tolerant capability. Simultaneously it can guarantee the fault tolerant capacity of sensor node in the entire network [19].

2.10 Storage

The minimized cost of sensor nodes and ubiquitous applications in a large scale use demands the sensor nodes to be tiny with high storage and computing capacity.

2.10.1 Low cost and tiny sensor nodes with high storage capacity

The sensor nodes in WSN should be capable of performing high computational tasks, can enable communication with huge storage capacity. Miniaturization with minimized cost can be availed from the recent and future development in the field of micro-electro-mechanical systems (MEMs). Several aspects of WSN nodes can be miniaturized with MEMs technology [3].The wireless channels and reliable sensor nodes can show the way for data storage and data retrieval in terms of data compression and data aggregation.

3. Conclusion and Future Research

We have identified various challenges and the corresponding design factors of sensor networks in the literature and encourage new researchers to give more insight into the problems and to work in the related areas in search of appropriate solutions. Still WSNs leave us with many new challenges and open research opportunities. WSN will bring revolutionary changes in information technology and will play an integral part of our lives because of its peculiar features that motivates the academic and industrial research. Current research is going on to develop IPv6-enabled WSN applications and protocols to make WSN as an integral component of Internet-of-Things (IoT). The future generation Internet application using by IPV6 will compatible to establish the communication with sensor nodes. The highly stringent constraints for WSN demand the design of new wireless ad hoc networking techniques with new hardware, efficient algorithms and power-aware communication protocols. These days' potential advances and applications of Digital Informational Network have increased the volume of data creation and storage exponentially. The technology is being misused to commit various computer frauds and cyber crimes around the world. The mysterious ideas and concepts in wireless sensor networking have always encouraged cyber criminals to deceive the systems response which creates difficulties for digital investigators and the court of law authorities to prove the digital crime and prove the identity of the criminal. In future research we will explore, security issues of wireless network and more specifically our work will focus on intrusion detection mechanisms in WSNs applied on security and surveillance systems to enhance digital forensic investigation and analysis.

4. REFERENCES

[1] Akyildiz, I.F., Su, W., Sankarsubramaniam, Y., Cayirci, E., "A Survey on Sensor Networks", IEEE Communication Magazine, pp.102–114, 2002.

[2] Ajay J.,Swati R., Priyanka, "Wireless Sensor Network (WSN): Architectural Design issues and Challenges", (IJCSE) International Journal on Computer Science and Engineering, ISSN : 0975-3397 3089, Vol. 02, No. 09, pp-3089-3094, 2010.

[3] A. Perrig, J. Stankovich, and D. Wagner, "Security in wireless sensor networks," Commun. ACM, vol. 47, no. 6, pp. 53–57, 2004.

[4] Aqeel R., Abu Z. A., Noman I., Zubair A. Shaikh. "A review of wireless sensors and networks' applications in Agriculture", Computer Standards & Interfaces 36, pp-263–270, 2014.

[5] C.Komalavalli, "Convergence of Wireless Sensor Networks, Internet of Things, Big Data: Challenges," International Journal of Scientific Research Engineering & Technology, Volume 6, Issue 6, 2017.

[6] Chih-Chieh Hung, Chu-Cheng Hsieh, " Big Data Management on Wireless Sensor Networks Big Data Analytics for Sensor-Network Collected Intelligence," 2017.

[7] Daniele Puccinelli and Martin Haenggi, "Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing", IEEE Circuits and Systems Magazine, third quarter, 2005.

[8] K. H. Wandra, Sharnil Pandya,: "A Survey on Various Issues in Wireless Sensor Networks", International Journal of Scientific & Engineering Research, pp. 2229-5518 Volume 3, Issue 12, 2012.

[9] Fernando M., Loren S., "Introduction to Wireless Sensor Networking", Handbook of Sensor Networks: Algorithms and Architectures, Edited by Ivan Stojmenovic, John Wiley & Sons, Inc. , 2005.

[10] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, "Issues in Wireless Sensor Networks", Proceedings of the World Congress on Engineering, Vol - 1, WCE, 2008.

[11] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15.4 networks," Internet Engineering Task Force RFC-4944, 2007.

[12] Gurbhej S., Harneet A.,"Design and Architectural Issues in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, pp: 2277- 2138, Volume 3, Issue 1, 2013.

[13] Hossein Jadidoleslamy, **"**An introduction to various basic concepts of clustering techniques on wireless sensor networks", International journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.1, 2013.

[14] Indu, Sunita Dixit,"Wireless Sensor Networks: Issues & Challenges", International Journal of Computer Science and Mobile Computing, ISSN: 2320–088X, IJCSMC, Vol. 3, Issue. 6, pg.681 – 685. 2014.

[15] I. F. Akyildiz, T. Melodia, and K. Chowdhury, "A survey on wireless multimedia sensor networks," Computer Network. vol. 51, no. 4, pp. 921–960, 2007.

[16] Jennifer Y., Biswanath M., Dipak G., "Wireless sensor network survey", Computer Networks, Science Direct, 2008.

[17] Janakiraman S., Rajasoundaran S, Narayanasamy P., "A Dynamic Intrusion Detection on Data Flow at Low Data Rate in Wireless Sensor Networks", European Journal of Scientific Research, Euro Journals Publishing, Inc. 2012.

[18] Junaid A. K., Hassaan K. Q., Adnan I., "Energy management in Wireless Sensor Networks: A survey", Computers and Electrical Engineering 41, pp-159-171, 2015.

[19] Kamaldeep Kaur, Parneet Kaur, Er. Sharanjit Singh, "Wireless Sensor Network: Architecture, Design Issues and Applications", International Journal of Scientific Engineering and Research (IJSER), ISSN (Online): 2347-3878, Volume- 2 Issue 11, 2014.

[20] Matthew N. O. Sadiku and Sarhan M. Musa , Omonowo D. Momoh, "Wireless Sensor Networks: Opportunities and Challenges", Int. Journal of Engineering Research and Applications, Vol. 4, Issue 1(Version 1), pp.101-103, 2014,

[21] Mohd F., Othmana K. S., "Wireless Sensor Network Applications: A Study in Environment Monitoring System", International Symposium on Robotics and Intelligent Sensors Procedia Engineering 41,pp-1204 – 1210, 2012.

[22] Sarita V. Halde, Sucheta T. Khot, "Big Data in Wireless Sensor Network: Issues & Challenges", International Journal of Advanced Engineering, Management and Science (IJAEMS), Vol-2, Issue-9, 2016 .

[23] Nirvika Chouhan, P. D.Vyavahare, Rekha Jain, "Wireless Sensor Network –A Survey", International Journal on Computer Science and Engineering (IJCSE), Vol. 5 No. 07, 2013.

[24] Reshmi V1, Sajitha M, "A Reactive Hierarchical Trust Management Scheme for Wireless Sensor Networks," International Journal Of Engineering And Computer Science,Vol 03 Issue 07, Pp. 6982-6984, 2014

[25] Rajkumar, Vani B A , Kiran Jadhav, Vidya S, **"**Wireless Sensor Networks Issues and Applications", International Journal of Computer Technology & Applications, Vol 3 (5), pp.1667-1673, 2012.

[26] S. Muthukarpagam, V. Niveditta, S. Neduncheliyan," Design issues, Topology issues, Quality of Service Support for Wireless Sensor Networks: Survey and Research Challenges", International Journal of Computer Applications (0975 – 8887), Vol. 1 , No. 6, 2010.

[27] S. V. Halde and S. T. Khot, "Efficient collection of big data in WSN," International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, pp. 1-5, 2016

[28] Giri P.K. "A Survey on Soft Computing Techniques for Multi-Constrained QoS Routing in MANET," International Journal of Computer and Information Technology (IJCIT), ISSN 2218-5224, VOL. 03(2), MANUSCRIPT CODE: 130103, 2012.

[29] T. Akshatha, Praveena. T, Data Aggregation in Wireless Sensor Network for Big Data International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 8, 2016.

[30] Vehbi C. Gungor, and Gerhard P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches", IEEE Transactions on Industrial Electronics, Vol. 56, No. 10, 2009.