International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 8 Issue 07 Series. I || July 2019 || PP 89-97

Design challenges and Issues in Wireless Sensor Networks for next generation

Mr. Bharath Kumara[1]Dr. S AnanthaPadmanabhan[2]
Research Scholar VTU, Belgaum.Professor & Head, Dept. of ECE.
Asst. Professor RUAS, Bangalore.Gopalan college of Engg. Bangalore.
Corresponding Author: Mr. Bharath Kumara
e-mail:bharathkumara87@gmail.com

Abstract:*Wireless sensor networksareformed byinterconnection of multiple sensor nodes. Sensor nodes are very tiny partials and has the capability of data access, computation, processing, managing the resource. It has got numerous applications in the field of communication technology. The main focus of this paper is to study the design requirement, issues, challenges, research contributions and ongoing activities of the wireless sensor networks.*
Keyword: *wireless Sensor Network, sensor node, security, Quality of service, Localization.*

Date of Submission: 30-06-2019 Date of acceptance: 19-07-2019

I. Introduction:

A group of sensor nodes in the sensing field initiate the communication with each other to forward the data from source to destination [1]. Wireless sensor network (WSN) is formed by densely deployed sensor nodes in the sensing field. Sensor node is an embedded device consists of sensing element, processor, radio trans-receiver, battery. Sensor nodes are tiny devices which are limited in power (battery life),data computation capability, processing capability, range (coverage) for data communication [3]. Sensor networks formation lead to many applications in the field of agriculture, military, health care, electronic devices used in day to day life[2]. The major issues of WSN's are node deployment, network resource management, information routing, topology control, data security, network quality of services (QOS), and data processing and computation [1].
The essential components of the wireless sensor networks as shown in fig 1.

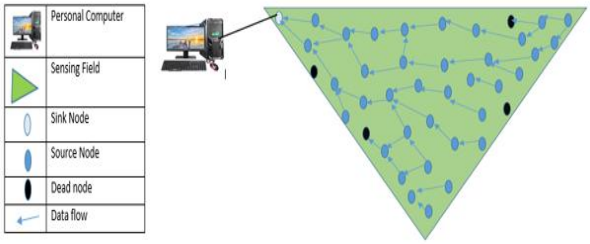

Fig 1: Wireless Sensor Network [3].
The components of the wireless sensor networks are described in table 1.

Table 1: Components of WSNs.

Components	Description
Sensing field:	Area of sensor node deployed.
Source nodes:	Nodes that sense the information and process the information to the next node.
Sink node:	Node that sense and collect the information from all surrounding nodes.
Neighboring nodes/ intermediate nodes:	Nodes appeared in between source node and the sink node during information transmission.
Gateway:	The interfacing unit between sensor node and the user. It may be computer, internet etc.

The important prediction of wireless sensor networks are:

- Low cost, low power utilizedmulti-functional device.

- Bulky and portable in nature.
- Flexible to future application developments.
- Software controlled and self-configuration capability.
- More immune to network disturbances, threat, and attacks.
- Simple to use and provides platform to cross layer design [2].

Advantages of wireless sensor networks[1, 9]:

- Static and dynamic networking infrastructure is possible.
- It can be placed to anywhere the appropriate places like mountains, under water, remote places etc.
- Flexible to adopt any new work stations and devices with in the network configuration.
- It avoids wiring, and can be operated in centralized monitoring.

The limitations of the sensor networks are:power consumption, security, data routing, localization, hardware and software design, storage, Quality of service, node deployment etc. The sensor networks had new technological growth with Ad-hoc networking, Internet of Things, data interpretations and mining etc. [1, 9].
Sensor node: The key role of sensor network is handled by sensor node (Mote) [2]. The sensor node consists of sensing unit (sensor and actuator), battery, memory, processor, and radio transmitter and receiver.

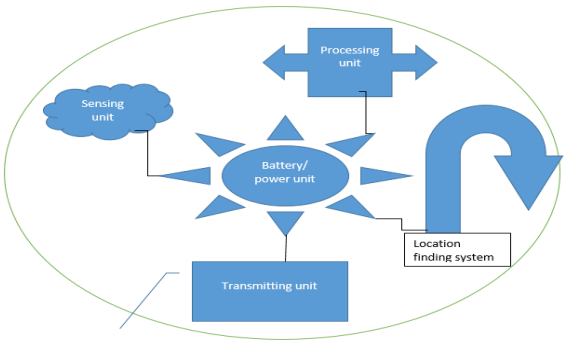

Fig 2: Internal architecture of sensor node [1].

Fig 2 shows the sensor node and its components. The sensing unit consists of sensing element and actuators. Sensing element sense the required data. Actuators process the sensing data with signal conditioning. Battery is a main power source to the sensor node. Battery status indicates the life time of the sensor node. Battery supports all operations performed in the sensor nodes. Processor performs the operations of data computing, processing, storing. Microprocessors and microcontrollers are used as a processing unit in [9]. Transmitting unit performs the operation of transmitting and receive the information using RF module.

Network designing issues:
The major design constraints in WSN's are node deployment, hardware and software development, routing, security, and QOS. In this paper some of the issues are discussed to set new challenges [1].
Sensor node deployment: sensor nodes randomly and densely deployed in sensing field that leads to poor control on the network and its topology [3]. The main aim of the sensor node deployment is to improve the coverage area, connectivity and reliability [5]. Principle behind the node deployment is angle connectivity between the nodes [4]. Some of the popular related works considered insensor node deployment are:
Dr.saadtalibhasson et.al, (2018) suggested angle based sensor deployment algorithm to improve the requirement by utilizing the angle between the sensor node and surrounding nodes [3].Wen-hwalia et.al, (2017) developed an algorithm to improve the coverage area of sensor nodes using Swarm optimization method [4].Gupta munish et.al, (2017) designed the scalable energy efficient deployment strategy to minimize the blanket coverage when least number of sensors in the area in the hexagonal geography [5].
Band ward et.al, (2016) suggested the model based on insurance coverage for the sensor node when the density of the node is critical. The surrounding sensor node provides coverage support by examine the actual sensor node using discrete approximation algorithm to probability calculation [6].Abdalnasir et.al, (2016) provides the node deployment algorithm using markov process [8]. In this algorithm the distance between the sensor nodes calculated first and then converted into probability to create the transition matrix depending on the movement of sensor node. The algorithm approach is suited for both dynamic and static sensor node deployment [7-8].The node deployment is either random or structured. The deployment scenario is shown in fig 3.

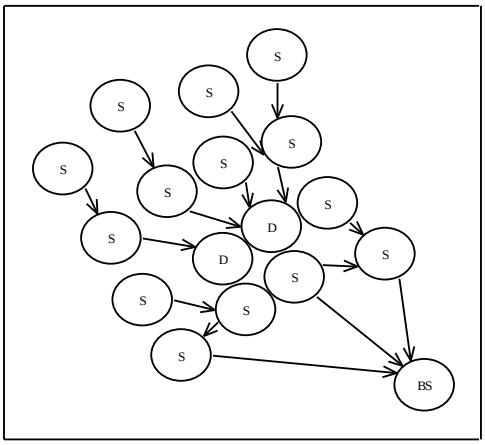

Fig 3:random and structured sensor deployment [4-8].

Communication model and its usefulness: Communication model was developed by International Standard Organization (ISO) [25]. It is an Open System Interconnection (OSI) model consisting of five layers each layer supported for data communication with its functionality. Fig 4 shows the OSI communication model and its layer functionalities.

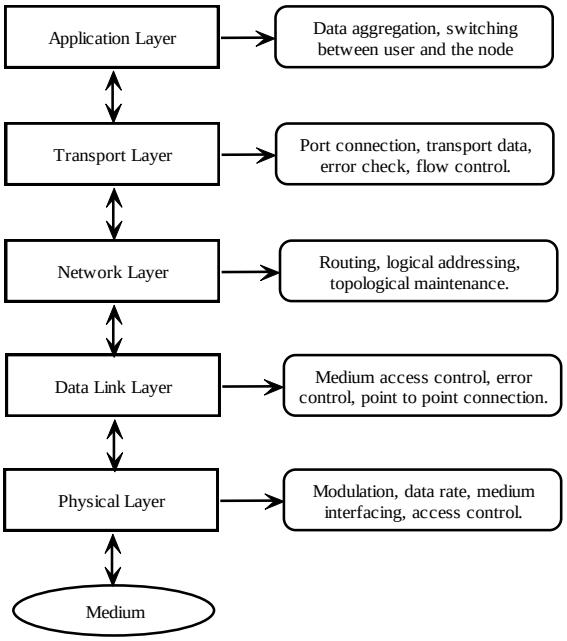

Fig 4: OSI Communication model and its functionality [9, 25].

Operating system architecture in WSNs provides resource and power management in any constrained environment.

The designing issues related to operating systems are [1, 9, and 15]:

- The function of sensor node is data extracting, computation, manipulation, processing etc. To perform all these function a real time response is necessary.
- Operating system is not only hardware dependent, it must be application specific and support for routing.
- Programming should be user friendly and it supports even the lower level hardware designs.
- Sensor node is battery powered hence it has built in feature to minimize the power consumption.
- Priority must be given to higher priority tasks.

Tiny OS with Nesc is supporting all the designed issues and supported for synchronized model [10].

Network Resource management:

The important resource managementis battery management or powermanagement to improve the life span of the sensor node. It uses feasible information routing technique, sensor scheduling technique, computation processing technique, memory management, traffic management etc. [1].

Routing:

Routing in wireless sensor network plays an important role in data transmission. The source is not able to transmit the data into the base station. An intermediate node should be active mode turns as a relay node to care about data transmission [10]. In sensor network data computation consumes less energy than data transmission based on the distance. Routing is the function of network layer which routes the information or data from source to destination through multiple intermediate networks/ nodes [12]. On other way routing is a set of protocols helps to route the information. In WSN multipath energy saving routing protocols are more popular [14]. The main aim of the routing protocols is to provide the security, QOS and less energy consumption to improve the life span of wireless sensor networks [2].Routing protocols development and its applications are scorching sensor network research area in the last few decades. The classes of sensor networks namely pro-active and re-active networks [15]. In pro-active network sensor node setup the routing table with it during the operation and in case of reactive network sensor node activate when the need of data transmission occurs. The classification of the routing protocols based on the network structures are as shown in Fig 5.

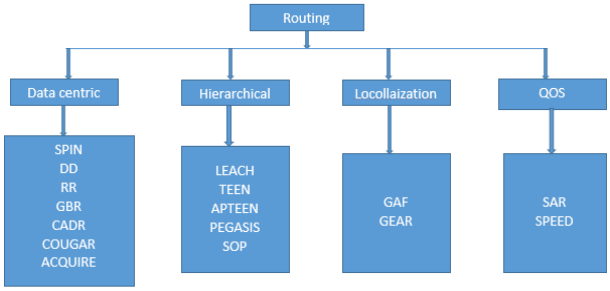

Fig 5: Classification of routing protocol [11]

Data centric routing protocols working on the basis of query. The sender initiates the query with the receiver with the naming before initiate the communication. The popular protocols supported for data centric are:

Sensor Protocol for Information via Navigation (SPIN), Directed Diffusion (DD), Rumor Routing (RR), Gradient Based Routing (GBR) and Constrained Anti strophicDiffusion Routing (CADR) etc. [11].

In hierarchical method the network structure divided into number of groups or cluster. In each group one node acts as a head (Cluster head) these clustered heads are responsible for data communication with its sub groups and other clusters head. These protocols are energy efficient and perform data aggregation. Most popular hierarchical protocols are: Low Energy Adaptive Clustering Hierarchy (LEACH), Threshold sensitive Energy Efficient sensor Network (TEEN), Adaptive TEEN, self-organizing protocol (SOP), Power Efficient Gathering in sensor Network Information (PEGSIS) etc. [12].

In location based protocols the data will be send to desired region without aware of the networking. The location is identified through the Global Positioning System (GPS). Optimal path can be calculated using the distance between two nodes. The popular routing protocols are: Geographic Adaptive Fidelity (GAF), Geographic and Energy Aware Routing (GEAR) [15].

Quality of service is the most important requirement in WSNs; the routing protocols must support better QOS to improve the network performance. Normally used QOS routing protocols are: Sequential AssignmentRouting (SAR), Stateless Real Time Routing

Protocol (SRTRP) [12].

The major designing and development issues considered in routing are [11, 12, and 13]:

- Designing the routing algorithm to minimize the power consumption, network failure and to improve the network life span.
- Designing the suitable load balanced centralized routing algorithms for multiple controllers.
- Develop an efficient route blocking avoidance protocols for data transmission.
- Develop the routing protocols to improve the performance of the network in terms of QOS, Security.

Some of the popular works contributed towards the improvements in routing issues.

Yu wei et.al, proposed the mechanism of load balanced control routing to upload the data. Each sensor must report their topological information to the controller, then controller will initiate the routing rules using load balanced algorithm and it distributed the rules to all sensor nodes. The load balanced mechanism avoids the choice of unstable links to route the information with lower packet loss and it contribute higher bandwidth for data transfer. Due to the fact of centralized control the controller takes the control on topological structure and link quality to compute the routs based on load balance [10].

M.Devika et.al, proposed a route block avoiding algorithm for cluster based routing mechanism. Mobile sinks starts the data collections from the cluster head in single hop range, and after collecting all data it

will return to the initial position. To create the dynamic topological structure the spanning graph is essential, spanning graph identify the energy efficient shortest path without obstacles. The proposed method provides the efficient solution to energy hole issues. The proposed work is the combination of cluster based architecture with mobile sink[11].

Chikhsidy et.al, proposed a gate way selection technique for multi-hop energy aware clustering mechanism. The backbone network will be created in the routing path to support the reliable constant connection sensor nodes[12].

Jiehuang proposed a double clustered head based routing protocol algorithm. The cluster head acts as a master till the energy of the node comes down. Once energy drop occurs the subordinated sensor node in the cluster will take the action of data computing and processing with the nearby nodes depending on the energy within it [13].

Qiaoling wand proposed an energy efficient routing algorithm using swarm optimization to optimize the phase cluster and improve the efficiency. Also the author proposed the method of dynamic priority based data scheduling in cluster formation [14].

Security

A Secure transmission of information from point to point is one of the challenging issues in WSNs. Sensor networks easily affected by threats or attacks and misconduct. The major security services as shown in fig 5. Security constraints in wireless sensor networks are [15]:

- Energy consumption is the main constrain in the sensor network. Data computation and processing is the key point where more energy utilization. To improve the life span of sensor network optimized secure routing protocols are essentially needed [1].
- Sensor networks are more sensitive to threats and risks. The common threats are data integrity; snoop on message, wrong message communication, destroying the network resources by un-authorized entry [15].
- The main limitation considered in security is message storage, message computation, message processing and communication [16].
- High bit error rate due to atmospheric noise, multipath propagation and interference [19].
- Topological problems in both dynamic and static hidden threats [14].

The security issues can be managed by different techniques: Cryptography, key management schemes, securerouting protocols, secure data aggregation and intrusion detection etc. [16].The major security issues as shown in Fig 6.

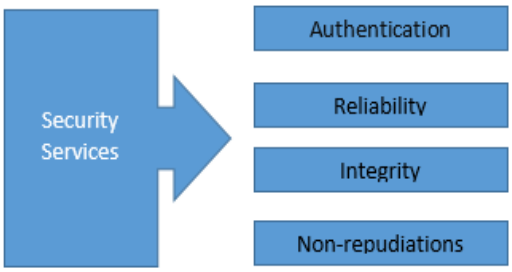

Fig 6: Network services [16].

Confidentiality/ privacy are an important factor to protect the information transfer between the sender and the base station or sink node. If message transmission is not provided confidentiality it leads to eavesdropping in the communication network. Sensitive information must be protected and not given a chance to access for un-authorized parties or nodes. Better confidentiality can be maintained by using some traditional techniques like symmetric key cryptography, asymmetric key cryptography [16].

Integrity provides the support to transfer the data from source node to destination node without changing the original pattern of the information generated. Integrity level is less in the network could leads to horrific information about the network management. [16]. Authentication serviced behind with integrity. Authentication measures the identification of sensor nodes in the communication. Authentication is very essential component in each sensor node and sink node to verify the received data is the true data from the authorized and trusted node [19].

Non-repudiations is a kind of attack, sink node must not able to send the message when the message is accepted by the sender. Consultative may confine the messages but replay to the node is delayed to cause the confusion in the network [22].

The security issues must be built strongly from the base station or sink level, because the communication is ended up in base station. Key distribution is the most important measure in between nodes. In order to establish the encryption, and routing the information made to secure. In cluster based network formation each cluster head follows the authentication mechanisms for secure communication. The security mechanisms should be much simpler to minimize the overhead and to improve the performance of the network [19].

Availability is one of the important measures in security. The capacity of WSNs is to provide services for the required users at any instants of time. The attackers are actively participated in attacking the nodes to reduce the performance of the network or to destroy the system. The Denial Service attack is one of the unsafe attack caused by transmitting radio interference, destruct the network protocols, defeating the power needed by the nodes through various methods to make the network service improper [16].

To provide more flexibility, increase the size of the network size an efficient key distribution technique is required. Attacks can be majorly classified as passive attacks and active attacks. Attacks can be of the form cryptographic primitive class and node or mote class. The threats can be characterized as internal threats and external threats. Detection of internal treats is slightly complex compared to external threats because of availability of cryptography. The network keying, group keying, pair-wise keying are the three main keying procedures normally used in security exchanges with in the network. The attacking types and its behavior is tabulated in Table 2 [16, 17].

Table 2: Security attacks description [15-22].

Types of attacks	Description
Jamming	It is an attack appeared in physical layer. Due to radio frequencies used by the sensor nodes in the network. The Unique radio frequency transfer between the nodes leads to network damage. Because of intrusive malicious packets from malicious nodes. In such case to avoid the jamming the real node can stop the communication or it will be switched to sleep mode. Once the jamming period is completed the authorized node can able to forward the data.
Tempering	It is an attack appeared in physical layer. Attacker physically tempersthe senor node and manipulates the data. The attacker extracts the security keys. This leads to loss of important high level information to get protection form tempering. Temper proof physical packages is the only possible strategy.
Continuous channel access	It as an attack appeared in data link layer. The attacker continuously senses the channel to ask queries and transmit data. Due to these process legal nodes does not have a chance to access the channel. They lost the energy only to check the ideality of the channel. To overcome this problem each sensor node must allocate some time slots for data transmission.
Collision	It is an attack appeared in data link layer. The information routed by different sources simultaneously the collision occurs. Due to collision data packets get damage. To prevent the collision error correcting codes can be used.
Routing attack	It is an attack appeared in network layer. Due to routing attack the routing protocol changes the path of information flow. To prevent from the attack message along with MAC codes is used.
Black hole attack	It is an attack appeared in network layer. During the communication malicious nodes selectively transmit the packets and drop the rest. This leads to loss of data. To overcome this problem multipath data transmission is helpful.
Sink hole attack	It is an attack appeared at network layer. The surrounding nodes of the sink are attacked by hackers. They attract the node with attractive bandwidth. It leads to packet drop. To overcome this problem multipath routing is the better solution.
Sybil attack	It is an attack appeared at network layer. The hackers have multiple identities to take control

	over surrounding nodes. To overcome this problem encryption and authentication mechanism is used.
Worm hole attack	It is an attack appeared at network layer. The attackers continuously listen to the communication between the nodes. They physically attack the nodes and replay to the message to create the confusion. To overcome this problem encryption and authentication is the better solution.
Hello flood attack	It is an attack appeared at network layer. The hello message is casting to the neighboring node. The malicious nodes used high frequency radio waves to say the message. Hence the surrounding nodes can understand the surrounding nodes as malicious.
Flooding	It is an attack appeared at transport layer. Un-legalized connection requests send by malicious nodes continuously to damage the resource. To overcome this problem the continuous request must be ignore.
Denial service attack	It is an attack appeared in both physical layer and network layer. The malicious node sends abundant packets to destroy the network. To avoid the attack temper proof packing is employed.

The protocols supported for secure communications are [22, 23, 24]:
SPIN: It provides confidentiality, data freshness and authentication.
SSPIN: It provides message integrity using authentication codes.
TINYEC: It provides media access control, integrity and authentication.
LLSP: It provides integrity and node authentication.
ZIGBEE: It provides trust management between two devices. The two network entities used in the system are FFD, RFD.
MINSEC: Energy aware secure routing protocol. It reduces the calculation time and improves the authentication and confidentiality at one stretch.
LISP: It provides key renewable and key generated protocol. It avoids the key reuse.
SM: It provides key agreement protocol to prevent un-authorized entry.
SECROUT: It provides message storage and routing support.
The research contribution towards security is more in different assumptions. Few contributions discussed below:

Majid R et.al, proposed an energy efficient key distribution protocol. The designed protocol not only calculates the energy consumption. It also supports for energy computation. To verify the efficiency of the designed protocol they compare the automatic cryptographic period. The result showed that the proposed method is one of the best in key distribution technique [17].
Toyokazuakiyama et.al, proposed a data center monitoring system to provide better encryption and authentication. MQTT/MQTT-SN is used to develop the infrastructure. The method is effectively works for improve the throughput and minimize the operation cost [26].

Quality of service (QOS):

Quality of service is a service provided by WSNs. WSNs are used in various applications; the responsibility of the sensor network is to provide better quality service to the user mandatorily [1]. Due to dynamic topological structure of WSNs better QOS maintenance is difficult. The bandwidth required from each sensor nodes to improve the QOS [24]. Normally the QOS is designed for unbalanced traffic structure to minimize the energy constraints during routing. Addition, termination, re-joins the sensor nodes in dynamic topology leads to non-scalability. Due to constant changes of topology node management, path management, path re-establishment is difficult [21]. In un-balanced multipath routing the data aggregation is one of the major issue. Buffer management in sensor node could lead to better QOS. The QOS attributes in WSNs are shown in Table 3 [20]:

Table 3: QOS parameters [19, 20, 25].

QOS Parameters	Description
Reliability	Flow of packets to the base station. Lack of reliability leads to re-transmission of information.
End to End delay	It is one of the flow characteristics. The information reached to destination without and time implication.
Jitter	Variation in the delay of the packets belongs

	to the same flow.
Bandwidth utilization	The message carrier, the bandwidth is an essential factor to convey the message from source to destination.
Throughput	It measures the actual data speed.
Packet delivery ratio	The ratio of packet delivered to the destination over packet sent.
Packet error ratio	The packet corrupted in channel during transmission.
Energy consumption	The energy consumed by the nodes for data processing. The focusing area of WSNs is power or energy consumption.
Signal to Noise ratio	Measure of signals affected by noise during data transmission.
Bit error rate	It measures the corrupted bits over transmitted bits.
Data rate	Indicates the number of bits transmitted per second.

Some of the literature contribution towards the improvement in QOS:

Da-Ren Chen et,al. proposed an collaborative link aware protocols to improve energy efficiency and QOS. Due to cross-layer mechanism MAC layer and physical layer functionalities are integrated. The MAC layer protocol uses twin token bucket model and real time scheduling to activate Interleaving and beacon shifting technique. The method improves the QOS in terms of end to end delay and reduction in packet collision. The strategies considered for the energy efficiency are: low power physical layer design and efficient transmission control protocol [21].

Subhakanta swain et, al. Proposed a congestion control mechanism to improve the congestion control strategy. The bandwidth is distributed fairly depending upon the priority, queue size and the lode in sensor network. It isconsideredasthe real time and non-real time cases for analyzing the fairness measurement. The algorithm is implemented in NS-2 simulator for the analysis. The algorithm is verified for throughput, loss and delay [22].

Ziyadkhalaf et.al, verified the QOS of WSN's for Ad-Hoc networks used for large E-health care applications. The performance verified are latency, throughput, number of hops transmission rate. The applications are simulated in OPNET by applying audio, video, image as the input sources [23].

Discussion on related issues in WSNs:

Self-Management: Sensors were placed in remote area where lack of human interaction. During non-interacted situation the node should able to manage the network, maintain the resources, ability to self-reconfiguration [15].

Architecture: It is a fundamental issue of sensor deployment, development of hardware and its functionalities. Sensor architecture must be durable to achieve the QOS, and flexible for target applications. Architecture also affects to the radio transmission rate, data path, speed of data transmission [2, 3].

Calibration: It is a process of adjusting the sensing reading into the standard reading. Manual calibration is time consuming and too expansiveduring network failure the calibration from the sensor node is not accurate [9].

Fault tolerance: An efficient routing protocol is needed to re-configure the network during sensor fails [15].

Data interpretation and recovery: development of new protocols is essential to address the noise, data and interference. Due to unpredictablewith system it creates data uncertainty [9].

Secure Localization: Ability of sensor network to locate the faults and provide the accurate information of the faults. The attackers easily targeted the fault location and easily manipulate the signals [16, 23].

II. Conclusion:

The wireless sensor networks having huge scope in an electronics communication networks.The paper addressed several issues related to wireless sensor networks.In this work many issues are discussed with help of available literatures.Also, elaborates the researchcontribution in many area of electronics communication network.Few applications of WSNs are discussed to show the interrelation with other communication applications. WSNs technology is an emerging tool to put-up communication protocol better and innocuous.

Acknowledgment:

Thanks to my family members and friends to their constant support. Hearty thanks to Dr. Sanjeev Nayak for his un-conditional support. Thanks to Ramaiah University for their resource contribution.

Reference:

[1]. Khushboo Gupta, VaishaliSikka, ''Design Issues and Challenges in Wireless Sensor Networks''International Journal of Computer Applications (0975 – 8887), Volume 112 – No 4,[2015].
[2]. Anjali1, Shikha2, Mohit Sharma3, ''Wireless Sensor Networks: Routing Protocols and Security Issues'', 5th ICCCNT – 2014.
[3]. Prof. Dr. SaadTalib Hasson, Abd Al-Nasir Riyadh Finjan ''A Suggested Angles-based Sensors Deployment Algorithm to Develop the Coverages in WSN'' Proceedings of the Second International Conference on Inventive Systems and Control (ICISC), 2018.
[4]. Liao, Wen-Hwa, Yucheng Kao, and Ying-Shan Li. "A sensor deployment approach using glowworm swarm optimization algorithm in wireless sensor networks." Expert Systems with Applications 38.10 (2011): 12180-12188.
[5]. Y. Yoon and Y. H. Kim, "An efficient genetic algorithm for maximum coverage deployment in wireless sensor networks," IEEE Transactions on Cybernetics, (2013).
[6]. Gupta Munish, Krishna C Rama, Prasad D. SEEDS: scalable energy efficient deployment scheme for homogeneous wireless sensor networks. In: International conference on issues and challenges in intelligent computing techniques (ICICT); 2014. p. 416–23.
[7]. Bang Wang, Jiajun Zhu, et al. "Sensor Density for Confident Information Coverage in Randomly Deployed Sensor Networks". Transactions on Wireless Communications IEEE, 2016.
[8]. AbdAlnasir R. Finjan, and Hasson, SaadTalib. "MARKOV-BASED DEPLOYMENT APPROACH TO IMPROVE WSN COVERAGE." 1st International Conference on Information Technology ICoIT'17, LFU, Erbil, 2017.
[9]. Ivana Tomi´c and Julie A. McCann, ''A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols''IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 6,2017.
[10]. Yu Wei, Wu Muqing, Liao Wenxing, Zhao Min, ''The Design of Load-balance Based Routing Algorithm in Software Defined Wireless Sensor Networks'', IEEE/CIC International Conference on Communications in China (ICCC), 2017.
[11]. M. Devika , Dr. S.MaflinShaby, '' Efficient Route Block Avoiding Algorithm in Cluster based Routing Method for Wireless Sensor Networks'', International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS). 2017.
[12]. CheikhSidy Mouhamed Cisse, Ismail Bennis, MarwaneAyaida, CheikhSarr, ''Gateway Selection Technique for Efficient Multi-Hop Routing in Wireless Sensor Networks'', IEEE. 2017.
[13]. Lie Huang, ''A Double Cluster Head Based Wireless Sensor Network Routing Algorithm,'' IEEE.2017.
[14]. Qiaoling Wang, Jun Liu, ''An Energy-efficient Routing Algorithm for Real- Time Wireless Sensor Networks'', IEEE, 2018.
[15]. Ahmad Salehi S., M.A. Razzaque, ParisaNaraei, Ali Farrokhtala, ''Security in Wireless Sensor Networks: Issues and Challenges, Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), 2013.
[16]. Tarek AZZABI, Hassene FARHAT, Prof Nabil SAHLI, ''A Survey on Wireless Sensor Networks Security Issues and Military Specificities'', International Conference on Advanced Systems and Electric Technologies (IC_ASET), 2017.
[17]. Majid R Alshammari and Khaled M Elleithy, ''Efficient Key Distribution Protocol for Wireless Sensor Networks'' IEEE, 2018.
[18]. Da-Ren Chen , Member, and Wei-Min Chiu, ''Collaborative Link-Aware Protocols for Energy-Efficient and QoS Wireless Body Area Networks Using Integrated Sensors'', IEEE INTERNET OF THINGS JOURNAL, VOL. 5, NO. 1, 2018.
[19]. SunilKumar K N, Shivashankar ''A Review on Security and Privacy Issues in Wireless Sensor Networks''2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology, 2017.
[20]. SubhaKanta Swain and Pradipta Kumar Nanda,'' Priority Based Fairness Rate Control in Wireless Sensor Networks'' WI SPenet Conference, IEEE, 2017.
[21]. Dr. ZiyadKhalafFarej, ''Investigation on the Performance Analysis of the IEEE 802.11a Standard Based WSN withQoSApplication''International Conference on Advances in Sustainable Engineering and Applications (ICASE), Wasit University, Kut, Iraq. 2018.
[22]. Parli B. Hari, Dr. Shailendra Narayan Singh, ''Security Issues in Wireless Sensor Networks: Current Research and Challenges'', IEEE, 2016.
[23]. Sukhwinder Sharma, Rakesh Kumar Bansal, Savina Bansal'' Issues and Challenges in Wireless Sensor Networks'', International Conference on Machine Intelligence Research and Advancement, 2013.
[24]. Ibrahim abdulaisawaneh, ibrahimsankoh, davidkanumekoroma, '' a survey on security issues and wearable sensors in wireless body area network for healthcare system'', IEEE, 2017.
[25]. B. Forozon "Computer Networks" text book, NMI edition.
[26]. Toyokazu Akiyama, Morito Matsuoka, Kazuhiro Matsuda, ''Secure and long-lived wireless sensor network for data center monitoring'', 42nd IEEE International Conference on Computer Software & Applications. 2018.

Mr. Bharath Kumara" Design challenges and Issues in Wireless Sensor Networks for next generation" International Journal of Engineering Science Invention (IJESI), Vol. 08, No. 07, 2019, PP 89-97