www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 8 August 2016 Page No. 17702-17709

A Survey on Energy Efficient, Secure Routing Protocols for Wireless Sensor Networks

Yogeesh A C, Dr. Shantakumar B Patil, Dr. Premajyothi Patil
Research Scholar,
Dept. of CS&E, Nagarjuna College of Engineering & Technology Devanhalli, Bangalore-562 164
Prof & Head,
Dept. of CS&E, Nagarjuna College of Engineering & Technology Devanhalli, Bangalore-562 164
Professor,
Dept. of CS&E, Nagarjuna College of Engineering & Technology Devanhalli, Bangalore-562 164

Abstract— **The Wireless Sensor Network (WSN) in present generation has gained its popularity due its applicability nature in various areas Such as monitoring system of Oceans, wide life, manufacturing plants, earthquake prediction unit, military units, etc. The cost and structural complexity of a WSN are very low. In general, a WSN consists a sensor node (SN) that gathers the data from the atmosphere/environment. An SN exhibit very low power battery (LPB) and if the battery power gets drained SN will stop its functionality. Once the battery power is drained, it is impossible to recharge it back due to the wide spread network structure. The un-functionality of an SN may lead to failure of the routing protocol. Commonly a routing protocol facilitates an efficient routing path among the SNs. The security of data over the WSN is an always biggest issue which needs to be resolved. Many of the researchers have explained their views for energy efficient, secure routing protocol for a WSN. This survey paper discusses the various energy efficient techniques, secure routing techniques, classifications of routing protocol, attacks on WSN. The surveys towards the recent work on energy efficient & secure routing protocols are discussed with the research gap. Finally, future work is demonstrated followed by a conclusion.**

Keywords—Attacks on WSN, Energy Efficiency, Routing Protocol, Sensor Nodes, Security techniques.

I. Introduction

Wireless sensor network (WSN) is used to monitor the environment. In WSN sensor node sense data, collect data from other nodes then process that data and then transmit this collected data to the base station. Today the application of WSN is wide spread in many areas like wildlife, ocean, manufacturing, earthquake, national border security monitoring systems [1,2]. In future applicability of the WSN includes the monitoring of vehicle traffic system, record pollution monitoring, fire monitoring for the forest, measurement and monitoring the human and animals heart rates, etc. The major advantages of these WSN are on network application. WSNs pose unique challenges; traditional security techniques used in traditional networks cannot be applied directly. The advantage of WSN is low cost, SN are low powered, computation, and have communication capabilities. Also, SNs are placed in proper areas, presenting the added risk of physical attack. Also WSN interact with physical environments and with people, having security problems [3]. The existing security methods are not efficient, and advancement is necessary. Also the issues are giving research opportunity to address WSN security from the start [4].

In WSN, routing is a process of establishing a route and then forwarding packets from source to destination through some inter mediate nodes if the destination node is not directly within the range of sender node. The route establishment itself is a two steps process. First one is the Route Discovery where it finds the different routes from the same source to destination. Second, the Route Selection, where it selects a particular route among all routes found for the same source to destination. Traditional protocols and data structure are available to maintain the routes and to execute it by selecting the path that is having a minimum distance from the source to a destination where the minimum distance is in term of minimum hop count [5].

Routing protocols used in Sensor network are different from other networks routing protocols. Since the entire sensor nodes are battery powered devices, energy consumption of nodes during transmission or reception of packets affects the life time of the entire network. To increase the life time of sensor network number of protocols like LEACH and PEGASIS were developed and they show good progress then the previous routing protocols but still these are used for only static sensor nodes. Energy efficiency is important in wireless sensor network because it directly affects the life of the whole network, it is proved that in wireless network transmission of data consume more energy than data processing [6].

This survey paper discussed the various energy efficient WSN protocols, classification of WSN protocols and recent research work literature. The sectional organization of the paper is as below. Section II discusses the architecture of WSN, Significances and requirements of WSN, Applications of WSN in various areas and WSN Network Design Challenges; Section III gives the Classification of routing protocols, attacks on WSN. Section IV states the security techniques for WSN like Low-level and High-level techniques. Section V talks about Energy Efficient protocol for WSN; Section VI describes the Existing research survey; Section VII conveys the research gap and future research scope, Section VII concludes the paper.

II. Wireless sensor network

Wireless sensor network (WSN) is used to monitor the environment. In WSN sensor node sense data, collect data from other nodes then process that data and then transmit this collected data to the base station. WSN is wide spread in many areas like wildlife, ocean, manufacturing, earthquake, national border security monitoring systems. This section discusses the architectural structure of WSN and Significances and requirements of WSN, Applications of WSN in various areas and WSN Network Design Challenges [1].

A. Architecture:

A WSN is a network of consists of low power devices known as sensor nodes (SN), which are distributed over the area to measure the atmospheric variations. The communication among the each SNs will form a network. One or more number of SNs among network will act as the sink that will bring the direct communication with users. The main component of WSN is sensor that collects the physical environmental conditions like sound, humidity, intensity, pressure etc., in different areas. The functionalities of SN include data processing, communication, leveraging the network with more SNs. The following figure.1 represents the architecture of WSN consisting of processing unit, sensing unit, power unit and communication unit.

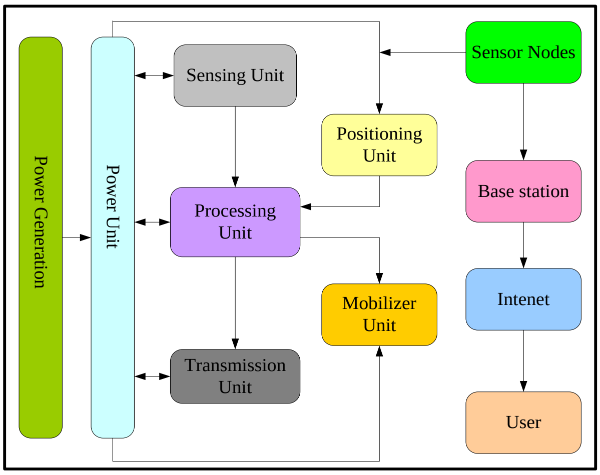

Fig.1. Architectural diagram of WSN

The sensing unit consists of various numbers of sensors and analog to digital converter (ADC). With the combination of ADC, sensors collect the information and returns back with the sensed data. The function of ADC is to inform the data collected by SN and suggest for further action with the data by sensing data. The function of communication unit is to receive the query or command from the transmitted data from central processing unit. The function of CPU is to interpret the query or command to ADC and monitoring & controlling the power over the received data and computes it to sink. The function of power unit is to supply power to all the units of WSN. Every unit of SN consists of location finding (used to find the location) and mobilize units (used for moving the sensors).
The SNs performs the computation and transmit the necessary data over the network. SN in this plays a function of router to communicate with battery constrained Wireless network. WSN is low power, scalable, fault tolerant network and the cost is very less as well as maintenance free. The WSN is restricted to certain bandwidth and it is software programmed. [1, 2, 3].

B. Significances and requirements of WSN:

The functional aim of a WSN is given below:

- This helps in determining the value of physical variables for a location.
- This detects the happening events, estimates the parameters of that particular event.
- This classifies the detected objects of the event.
- This tracks the object.

Hence to accomplish the above aims very accurately following points are needed to consider:

- The number of sensors is needed to be implanted.
- Need to have stationary sensors attachments.
- Should consume low energy.
- Should have self-organization ability.
- Should perform the collaborative signal processing.
- Should have Queering ability.

C. Applications of WSN in various areas:

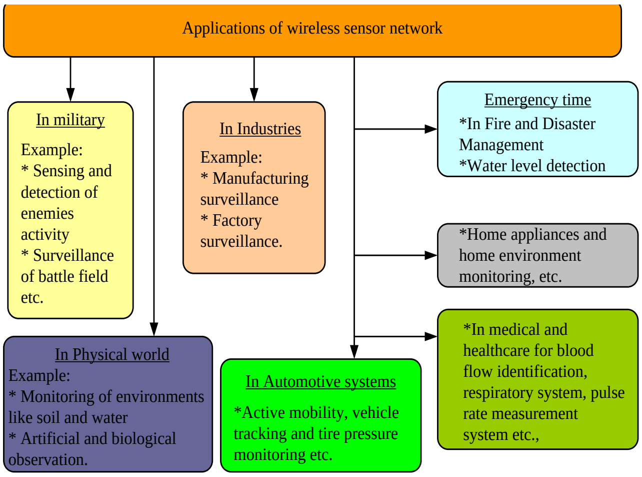
Applications of wireless sensor network
In military
Example:
* Sensing and detection of enemies activity
* Surveillance of battle field etc.
In Industries
Example:
* Manufacturing surveillance
* Factory surveillance.
Emergency time
*In Fire and Disaster Management
*Water level detection
*Home appliances and home environment monitoring, etc.
In Physical world
Example:
* Monitoring of environments like soil and water
* Artificial and biological observation.
In Automotive systems
*Active mobility, vehicle tracking and tire pressure monitoring etc.
*In medical and healthcare for blood flow identification, respiratory system, pulse rate measurement system etc.,

Figure.2. Application diagram of WSN

D. WSN Network Design Challenges

The applicability of WSN in every area has become more essential. As the routing protocol performance is related to the architectural model of a WSN, which poses more design challenges in WSN [1, 2, 7, 8]. Some of the issues that affect the design of a WSN are briefly described below.

- *Battery power:* The battery is the major part of every network. But the SN have the low-powered battery, if the power of the SN drained or comes down below the threshold level it would not function properly and which can damage the network performance. Hence the limited power of a sensor network is a major issue.
- *Sensor location:* Designing a routing protocol with the management of location. The GPS-based location will be more advantageous in designing the routing protocol.
- *Hardware resources:* Most of the sensor networks perform the limited functionalities due its low storage and processing ability along with low power. These low hardware resources also pose an issue in developing the routing protocol.
- *Node deployment:* The improper deployment of sensor nodes also affects the network performance.
- *Network Characteristics:* The network characteristics may be prone issues to the node failure, sensor, and deletion/addition, failure of link, etc. Thus proper network coverage is needed to be focused.
- *Data aggregation:* The generated sensor nodes data redundancy is also a major issue. By using the data

aggregation mechanism the redundancy issue can be solved.

- *Diverse applications:* The applications of sensor networks are widespread in all areas with different applicability. Hence a proper protocol is needed to be designed for every application so that it will meet the complete requirement.
- *Scalability:* The scalability of a WSN is necessary during the communication. The routing protocols for the communication are needed to be designed for the Symmetric and Asymmetric sensors.

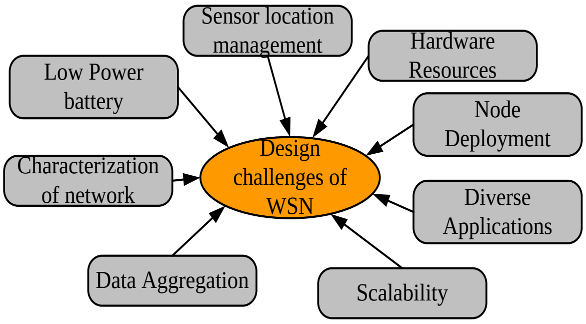

Figure.3. Design challenges of WSN

III. Routing Protocols in WSN

Both the convolution and WSN routing are entirely different. Presently no architecture exists that can resolve the unreliability in wireless links, power issues of the SN. There exist numerous kinds of routing protocols for WSN. Among these the table-is driven routing protocol will be used than reactive power if the SN are static. The routing protocols use more energy to the route.

A. Classification of routing protocols:

The design of routing protocol for a WSN will pose many issues that will affect the performance of entire WSN. Based on these issues many different routing protocols is classified and are shown in figure 3 [9, 10, 11].

Classification-1: Based on the routing objectives for successful message delivery. This classification exhibits real, non-real time applications and network lifetime.

Classification-2: Based on the architectural requirements the routing protocols are classified as data centric, Location based, hierarchical routing protocol.

Classification-3: Based on the energy optimality or power transmission the routing protocols are classified as adjustable and fixed routing. This protocol helps in minimizing the energy consumption.

Classification-4: The routing based on the functionaries is classified as a delivery model, quality of service and path selection routing protocol. The classification will help in saving the network resources.

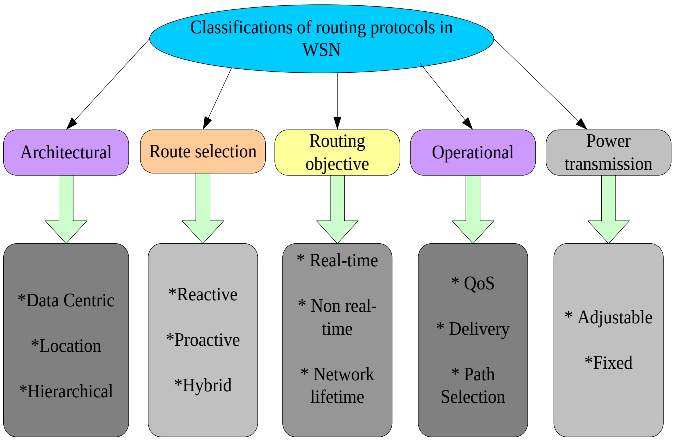

Figure.4. Classification of routing protocols in WSN

Classification-5: The classification based on the route selection is done as proactive, reactive and combination of both (Hybrid).

B. Types of attacks on WSN

During the transmission, the security attacks may take place in WSN. These security attacks are classified as, active and passive [1, 2].

1. Passive attack: In this the attacker can monitor and listen the communication channel and the privacy attack will be passive in nature. The collected data by the sensor can be transferred over the remote access.

2. Active attack: The attacker monitors listen and also modifies the data stream in the communication channel. In this routing, attacks will take place while routing the messages.

IV. Security Techniques for WSN

The security techniques are usually implemented to identify, restrict and recover from the attacks. There exists different security techniques for WSN and are divided as low-level and high-level technique [10 11, 12].

A. Low level techniques (LLT):

These techniques offer the protection against the low-level attacks on WSN. The LLT includes;

a. Key generation and trust building technique.
b. Privacy.
c. Secrecy and authenticity.
d. Securing routing.
e. Robustness against service denial.
f. Flexibility for node capture.

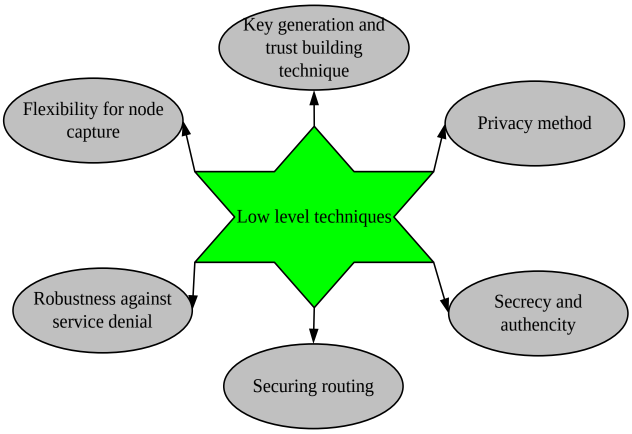
Key generation and trust building technique
Flexibility for node capture
Privacy method
Low level techniques
Robustness against service denial
Secrecy and authencity
Securing routing

Figure.5. Low level techniques

- *Key generation and trust building technique:* The first necessary thing to building the security is generating the encryption key. As the SN have low power and also, the encryption key primitives are also costlier to follow. This technique is required for scaling more sensors and build the Also, the communication patterns of WSNs. SNs are required to generate keys along with data aggregation (DA) nodes But in this attackers can also reconstruct the entire key to break the scheme.

- *Privacy*: The sensor networks have privacy concerns. Initially, the sensor networks are deployed for the legitimate purpose might subsequently be used in unanticipated ways. Providing awareness of the presence of sensor nodes and data acquisition is of particular importance.

- *Secrecy and authenticity:* For complete communication, the complete cryptography will bring security against attacks, but needs a key to set up among all end focuses and be communicating with neighborhood telecast and uninvolved cooperation. Join layer cryptography with a system-wide shared key disentangles key setup and backings latent investment and neighborhood telecast, yet moderate hubs may listen stealthily or change messages. The most punctual sensor systems are prone to utilize join layer cryptography since this methodology gives the best simplicity of sending among at present accessible system cryptographic methodologies.

- *Securing routing:* Data forwarding and routing are an urgent administration for empowering communication in sensor networks. The exiting routing mechanisms face security and security vulnerabilities. The least difficult attacks include infusing malicious information routing data into the system, bringing about directing irregularities.

- *Robustness against service denial:* The attacker attempts the system's operation by delivering the high-vitality signal. If the transmission is sufficiently effective, the whole framework's correspondence could be stuck. More modern attacks are likewise conceivable; the attacker may restrain correspondence by disregarding the 802.11 medium access control (MAC) convention by, say, transmitting while a neighbor is additionally transmitting or by persistently asking for channel access with a solicitation to send a signal.

- *Flexibility for node capture:* The issues in sensor systems are strength against node catch attacks. In many applications, SN is liable to be set in areas effortlessly open to attackers. Such introduction raises the likelihood that an aggressor may catch SNs, extract the cryptographic secrets, adjust their programming, or supplant them with malicious SNs under the control of the attacker. Algorithmic answers for the issue of nodes capture are ideal.

B. *High Level Techniques (HLT):*

High-level security mechanisms for securing sensor networks, includes secure group management, intrusion detection, and secure data aggregation.

This technique is used to protecting the sensor networks, including data aggregation, group management, and intrusion detection.

a. *Securing data aggregation:* The advantage of a WSN is the fine grain sensing which offers dense and large SNs. The sensed data need to be aggregated to avoid to the base station. The system average a geographic region temperature, combines sensor values for computation of moving object velocity and location or in real time application for event detection with data aggregation. Depending WSN architecture, aggregation may take place in many places in the network. Every aggregation locations are needed to be protected.

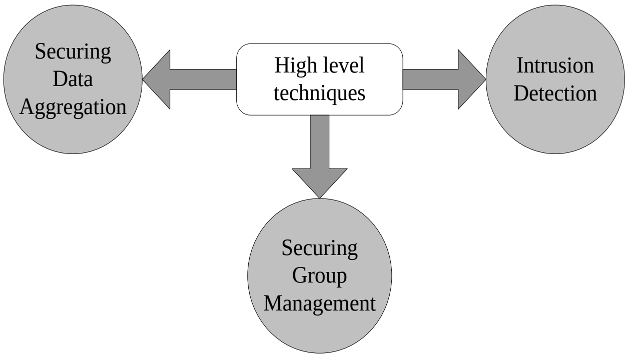

Figure.6. High level techniques

b. *Securing group management:* Each node in WSN has limited communication ability. A standout amongst the most difficult issues in sensor systems is strength against hub catch assaults. In many applications, sensor hubs are liable to be set in areas effortlessly open to assailants. Such introduction raises the likelihood that an aggressor may catch SNs, separate cryptographic privileged insights, adjust their programming, or supplant them with pernicious hubs under the control of the assailant. Alter safe bundling might be one safeguard. However it's costly since current innovation does not give an abnormal state of security. Algorithmic answers for the issue of hub catch are ideal.

c. Intrusion detection: WSNs are susceptible to very intrusion. WSNs require a solution which is less expensive and distributed regarding memory energy requirements and communication. The use of secure groups may be a promising approach for decentralized intrusion detection.

V. ENERGY EFFICIENT PROTOCOL FOR WSN

The energy constraints of SNs raise issues on routing protocols (RPs) design for WSNs. The RPs at load balancing, energy optimization in completes packet transmission and avoids low energy nodes. The classification of energy efficient RPs is given as data centric, opportunistic hierarchical and geographical protocol [11, 12].

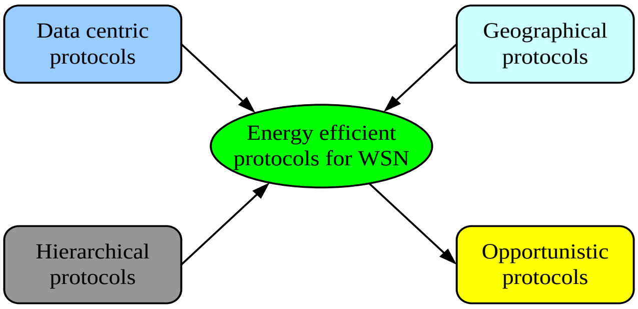

Figure .7. Energy efficient protocols for WSN

A. Data centric protocols

This protocol aims energy saving by questioning sensors in light of their information properties or interest. Protocols make the suspicions that information conveyance is portrayed by a question driven model. SNs routes any packet data at its substance. For the most part, two methodologies were presented for interest dissemination. Method 1 is SPIN in which any SN promotes the accessibility of information and looks for interested messages from the interested node. Method 2 is Directed Diffusion (DD) that sinks telecast an interesting message to sensors. Numerous different routings are made for example rumor routing, COUGAR, gradient based routing, CADR.

B. Hierarchical protocols

The clustering protocols are designed to enhance scalability and minimize the network traffic towards the sink. The cluster-based methods offer low energy utilization than level systems in spite of the overhead presented by Cluster development and development. One of the Clusters based RP is LEACH. In this convention, sensors compose themselves in nearby groups with one node going about as a cluster head. To adjust vitality utilization, a randomized turn of bunch head is utilized. PEGASIS is another case of various leveled convention. It improves LEACH by sorting out all nodes in a chain and letting hubs substitute the leader of the chain. It fabricates groups of various levels until achieving the sink. The information driven angle is illustrated by utilizing two limits for detected properties: Hard edge and delicate edge. The previous will trigger the sensor hub to transmit to its group head. Another transmission is just allowed when the quality worth gets to be higher than the delicate edge. This system can decrease the quantity of transmission and along these lines vitality utilization. Since TEEN is not versatile to intermittent sensor information reporting, an augmentation called APTEEN was presented.

C. Geographical protocol

No geological RP experiences the problem in scalability and effectiveness as they rely on upon flooding for route disclosure and updates. Geographical RP exploit sensing area to execute the routes. The energy protocol GEAR comprising of two stages. In the main stage, the message is sent to the objective locale. In the second stage, the message is sent to the destination inside the locale. The essential thought behind GEAR is to improve DD by sending the interests just to a specific district as opposed to the entire system. GAF guarantees vitality proficiency by building virtual networks taking into area account data of hubs. Just a solitary hub should be turned on in every cell; different hubs are kept in dozing state. SPEED guarantees load adjusting among different courses with its nondeterministic sending module.

D. Opportunistic Protocol

The essential thought of OP is to exploit i. Broadcast and space assorted qualities gave by the remote medium or ii. Scalability.

The classification is done as:

- *Medium protocols:* These methods keep up different sending competitors and wisely choose which sets of hubs are great and organized to shape the sending applicant set.
- *Mobility protocols:* By presenting scalability in WSN, system lifetime can be expanded. Undoubtedly, portable nodes can move to disconnected parts of the system and consequently availability is again come to. A few works combining steering and portability have shown that this class of directing convention displays littler vitality utilization when contrasted with established strategies.
- *Mobile sink protocols:* In this scalability of the sink and directing are nodes. Sensors in the region of the sink take in its development design after some time and factually portray it as a likelihood conveyance capacity.
- *Mobile relay protocols:* Their model coordinates an irregular stroll for portability design and joins framework variables, for example, the number of MULEs, sensors, and access focuses.

VI. Existing Research Survey

The section describes the survey of existing and recent research in WSN, routing protocol, security and energy efficiency.

Rahman et al. [13] have presented the energy efficient zigzag routing protocol for WSN. In this study author has gone through the issues of sensor nodes i.e. limited power and developed a routing protocol to optimize the energy consumption.

A research study was carried out by Li et al. [14] on security mechanisms for WSN. The author has broadly explained the various routing protocols and mainly focused on the SPIN routing protocol. Author has compared the each routing protocol by performing the simulation over NS2 Simulator and through analysis concluded that the SPIN algorithm is secure and maintains more confidentiality.

The combined study of Tarabovs and Zagursky [15] provided the efficient communication purpose medium access protocol for clustered WSN. In WSN, the resource allocation and energy efficiency is the challenging issues as the SN of it have low power battery. Hence author has presented the cluster based MAC protocol for WSN to bring efficiency.

The low power adaptive RP for WSN is presented in Ji et al. [16]. To bring the energy efficiency and resolve, the data aggregation issue author has presented the adaptive routing algorithm for clustering. In this clustering, head was selected based on node density in the measuring area. The results of adaptive routing algorithm are compared with LEECH algorithm and concluded that the algorithm brings energy optimization & improved communication quality in distribution situation.

The work of Hu and Li [17] presented the geography region based clustering algorithm in WSN. In this, the every region chooses its respective cluster head. To reduce the energy usage and proper resource allocation, multi-hop and single hop combination is used. The simulation result of the geographic region algorithm satisfies the above requirement. A mechanism of load balance in WSN using compressive sensing is described in Cao and Yu [18]. In this work the energy consumption of SNs is considered. The load is balanced by using compressive sensing, and the performance is evaluated by Tiny OS and simulation results represent the significant results.

The multipath routing for cluster tree WSN (ZigBee) in Bidai et al. [19]. The study is also concerned with efficiency, throughput and data transmission at low and high data rates.

Thaskani et al. [20] have introduced a cross-layer design protocol for WSN to bring the energy efficiency using token passing mechanism. To overcome the issues of traditional energy efficient WSN method, the design, and optimization layer of WSN is presented. The mechanism gives efficient results than some other routing mechanisms.

Author Othman et al. [21] have implemented the self-stabilizing algorithm to minimize the energy usage in WSN. In this, the approximation algorithm is presented to build the backbone for a sensor that brings the efficient routing. The author has achieved the efficiency in their method by simulation results.

In order to balance the load in WSN, a multipath routing protocol is presented in Ming-hao et al. [22]. A load balance algorithm is designed to balance the network over the established paths. The data packets are distributed over more number of SNs and help in energy optimization. The simulation is performed and compared the results with a various routing protocol. The mechanism brings the energy optimization in WSN.

For the uneven node deployment of WSN, a clustering routing algorithm is presented in Gu et al. [23]. In this, the sensing area was divided as various nodes and concentric annuli which are distributed over uneven area. The method outcomes with better load balancing mechanism and energy optimization.

The work of Chabalala et al. [24] also described the cross layer adaptive RP for WSN. The method is intended to minimize the usage of routing packets on WSN by which energy optimization will take place.

The work carried by Zhang and Li [25] have introduced the routing protocol for WSN. In this multi-level protocol between cluster heads and more sink nodes is presented. By simulation of this protocol, the author concluded that scalability increased and WSNs lifetime enhanced.

Authors Liu and Zhang [26] given the hybrid (Adaptive dynamic) routing algorithm for WSN. Authors have considered issues like redundant low rate data, low reliability, and energy balance in the communication channel. From the simulation results of the algorithm obtains better network transmission rate, communication channel reliability, energy balance.

A routing protocol with trust and link state is presented in Raha et al. [27], which eliminates the un-trusted nodes. Later it finds the most trustworthy link by calculating the trustworthiness of each route. The study gives the comparison of both direct and indirect trust.

A public transportation system monitoring mechanism is presented by using the WSN in Tianmin and Yao-yao [28]. The presented monitoring mechanism is completely implemented, and its structure of hardware and software is finally explained. The presented mechanism offers the better data transmission function.

To overcome the intermittent and crash failure issues authors Kamei and Fujita [29] presented the Reliable and fast routing protocol. In this author first analyzed the different existing techniques for reliability and latency.

- *Summary of existing research survey:*

The summary of the above literature survey is given in following table.1.

Table.1: Summary of existing work

Work/Author	***Mechanism***	***Method***	***Purpose***
Rahman et al. [12]	Energy efficient zigzag routing protocol	zigzag routing protocol	To get energy efficiency in WSN
Li et al. [13]	Security mechanisms	SPIN routing protocol	Comparison of SPIN algorithm with other algorithm
Tarabovs and Zagursky [14]	Efficient communication purpose medium access protocol for clustered WSN	MAC protocol	To bring efficiency
Ji et al. [15]	Low power adaptive RP for WSN	Low power adaptive RP	To brings energy optimization & improved communication quality in distribution situation

Table.1: Summary of existing work (Cont…)

Work / Author	***Mechanism***	***Method***	***Purpose***
Hu and Li [16]	Geography region based clustering algorithm for WSN	clustering algorithm	To reduce the energy usage and proper resource allocation
Cao and Yu [17].	A mechanism of load balance for WSN	Compressive sensing	Energy consumption minimization
Bidai et al. [18]	Multipath routing for cluster tree WSN (ZigBee)	multipath routing protocol	efficiency, throughput and data transmission at low and high data rates
Thaskani et al. [19]	A cross layer design protocol for WSN to bring the energy efficiency using token passing mechanism	A cross layer design protocol	Energy consumption minimization.
Othman et al. [20]	Self stabilizing algorithm to minimize the energy usage in WSN	self stabilizing algorithm	minimize the energy usage
Ming-hao et al. [21]	A load balance algorithm is designed to balance the network over the established paths	Load balance algorithm	balance the network over the established paths
Gu et al. [22]	For the uneven node deployment of WSN, a clustering routing algorithm	clustering routing algorithm	load balancing mechanism and energy optimization
Chabalala et al. [23]	Cross layer adaptive RP for WSN	cross layer adaptive RP	minimize the usage of routing packets on WSN by which energy optimization will take place
Zhang and Li [24]	Multilevel routing protocol for WSN	Survey	scalability and lifetime enhancement
Liu and Zhang [25]	Hybrid (Adaptive dynamic) routing algorithm for	hybrid routing algorithm	To solve the redundant low rate data, low

	WSN		reliability, and energy balance in communication channel.
Raha et al. [26]	A routing protocol with trust and link state	Trust and link state based routing algorithm	To eliminate the un-trusted nodes
Tianmin and Yao-yao [27]	A public transportation system monitoring mechanism	Monitoring mechanism	To get better data transmission
Kamei and Fujita [28]	Reliable and fast routing protocol for intermittent and crash failure issues	Reliable and fast routing protocol	To overcome the intermittent and crash failure issues

VII. Research gap and Future scopre

Routing in a sensor network is a very attractive phase of wireless communication. This paper summarized recent research in data routing to save energy of sensor network and classified the approaches into three main categories, namely direct approach, attribute-based and location-based. Data aggregation is an open issue in sensor network routing protocols in terms of energy saving and traffic optimization. Protocols, which name the data and query the nodes based on some attributes of the data are categorized as data-centric or attribute based. Many of the researchers follow this paradigm in order to avoid the overhead of forming clusters, the use of specialized nodes, etc. However, the naming schemes such as attribute-value pairs might not be sufficient for complex queries, and they are usually dependent on the application. Efficient standard naming schemes are one of the most interesting future research direction related to this category. Many routing protocols follow the criteria in which sensor network is integrated with a wired network like in monitoring application need the data that is collected by SNs and to be transmitted to the server for further classification. On the other hand, the requests from the user should be made to the sink through Internet. Since the routing requirements of each environment are different, further research is necessary for handling these kinds of situations. And in the case of cluster-based routing protocols, the selection of cluster head is a challenge because sometimes those nodes are selected as a cluster head whose energy or battery level is less. The factors affecting cluster formation and head cluster communication are open issues for future research.

- ***Issues in Different Routing Protocols***

  The table.2. Gives the different comparative issues in the routing protocol.

Table. 2: Issues in routing protocol

Issues/ Protocol	***Directed Diffusion***	***LEACH***	***PEGASIS***	***Direct Approach***	***HEED***	***Rumour Routing***
Distributed Cluster Head And Its Stability	N/A	Limited	N/A	N/A	G	N/A
Data Security	N	H	H	N	H	L
Data Aggregation	L	Y	N	N	Y	L
Latency	H		H	L	A	A

In above table.2 N represents ‘No’, Y represents ‘Yes’, H represents ‘High’, G represents ‘Good’, L represents ‘Low’ and N/A represents ‘Not Applicable’.

VIII. Conclusion

This paper surveyed different categories of routing protocols to save energy and extend the life time of sensor network. We have summarized and compared different proposed designs, algorithms, protocols, and services. There are still many issues to be resolved around WSN applications such as communication architectures, security, and management. By solving these problems, we can close the gap between technology and application.

IX. References

[1] S.Raghavendra, Cauligi S, K. M. Sivalingam, and T. Znati, “eds Wireless sensor networks”, Springer, 2006.

[2] I.F. Akyildiz, and M. C.Vuran, “ Wireless sensor networks”, John Wiley & Sons, Vol. 4, 2010.

[3] K. Yang, “Wireless sensor networks”, Principles, Design and Applications, 2014

[4] A. Kemal, and M. Younis "A survey on routing protocols for wireless sensor networks." Ad hoc networks 3.3, 325-349, 2005.

[5] A. Swami, Ananthram, "Wireless Sensor Networks", Signal Processing and Communication Perspectives, pp.102-114, 2007.

[6] D. Goyal, and M. R. Tripathy, "Routing protocols in wireless sensor networks: a survey", Second International Conference on Advanced Computing & Communication Technologies, IEEE, 2012.

[7] T. Zahariadis, "Design and implementation of a trust-aware routing protocol for large WSNs", International Journal of Network Security & Its Applications (IJNSA), Vol. 2.3, pp.52-68, 2010.

[8] Roopashree, H.R., Kanavalli, A.: Study of secure and energy efficient hierarchical routing protocols in WSN. Int. J. Eng. Res. Technol. **3**(6), 1–10 June 2014

[9] K. Romer, and F. Mattern, "The design space of wireless sensor networks", IEEE wireless communications, Vol. 11.6, pp. 54-61, 2004.

[10] L. Shujiang, D. Kuan and K. Lixin, "Improvement and simulation of clustering routing algorithm in wireless sensor network," 6th IEEE Conference on Industrial Electronics and Applications, Beijing, pp. 1068-1073, 2011

[11] H. Bizagwira, J. Toussaint and M. Misson, "Multi-channel routing protocol for dynamic WSN”, Wireless Days (WD), Toulouse, pp. 1-3, 2016

[12] S. B. Amsalu, W. K. Zegeye, D. Hailemariam and Y. Astatke, "Design and performance evaluation of an energy efficient routing protocol for Wireless Sensor Networks," Annual Conference on Information Science and Systems (CISS), Princeton, NJ, pp. 48-53, 2016

[13] Z. Rahman, A. Rahim and M. Aslam, "ZRIC (Zigzag routing inside cluster) energy efficient routing protocol for wireless sensor networks," Open Systems (ICOS), IEEE Conference on, Langkawi, pp. 381-383, 2011

[14] Y. Li, F. Liu and L. Ding, "Research about security mechanism in wireless sensor network," International Conference on Image Analysis and Signal Processing, Hubei, pp. 447-451, 2011

[15] R. Taranovs and V. Zagursky, "Medium access protocol for efficient communication in clustered wireless sensor networks," Telecommunications Forum (TELFOR), 19th, Belgrade, pp. 582-585, 2011.

[16] P. Ji, C. Wu, Y. Zhang and F. Chen, "A Low-Energy Adaptive Clustering Routing Protocol of Wireless Sensor Networks," Wireless Communications, Networking and Mobile Computing (WiCOM), 7th International Conference on, Wuhan, pp. 1-4, 2011,

[17] C. Hu and X. Li, "A clustering algorithm based on geography region for WSN," Electrical and Control Engineering (ICECE), International Conference on Yichang, pp. 480-483, 2011.

[18] G. Cao and F. Yu, "The Analysis of Load Balance for Wireless Sensor Network Using Compressive Sensing," Computational Science and

Engineering (CSE), IEEE 14th International Conference on, Dalian, Liaoning, pp. 100-105, 2011

[19] Z. Bidai, H. Haffaf and M. Maimour, "Node disjoint multi-path routing for ZigBee cluster-tree wireless sensor networks," Multimedia Computing and Systems (ICMCS), International Conference on, Ouarzazate, pp. 1-6, 2011.

[20] S. Thaskani, K. V. Kumar and G. R. Murthy, "Energy efficient cross-layer design protocol by using token passing mechanism for WSN," Computers & Informatics (ISCI), IEEE Symposium on Kuala Lumpur, , pp. 572-575, 2011

[21] J. Ben-Othman, K. Bessaoud, A. Bui and L. Pilard, "Self-stabilizing algorithm for energy saving in Wireless Sensor Networks," Computers and Communications (ISCC), IEEE Symposium on Kerkyra, pp. 68-73, 2011

[22] T. Ming-hao, Y. Ren-lai, L. Shu-jiang and W. Xiang-dong, "Multipath routing protocol with load balancing in WSN considering interference," 2011 6th IEEE Conference on Industrial Electronics and Applications, Beijing, pp. 1062-1067, 2011

[23] Y. Gu, Y. Shao, H. Han and T. Yi, "A clustering routing algorithm of WSN based on uneven nodes deployment," Wireless Communications and Signal Processing (WCSP), International Conference on, Nanjing, pp. 1-6, 2011

[24] S. C. Chabalala, T. N. Muddenahalli and F. Takawira, "Cross-layer adaptive routing protocol for wireless sensor networks," AFRICON, Livingstone, pp. 1-6, 2011.

[25] Zhang and Y. z. Li, "Based on more sink nodes of routing protocolfor wireless sensor networks," Computer Sciences and Convergence Information Technology (ICCIT), 6th International Conference on, Seogwipo, pp. 25-30, 2011

[26] G. Liu and H. Zhang, "Adaptive dynamic hybrid routing algorithm in WSNs," IT in Medicine and Education (ITME), 2011 International Symposium, Cuangzhou, pp. 1-6, 2011

[27] A. Raha, S. S. Babu, M. K. Naskar, O. Alfandi and D. Hogrefe, "Trust integrated link state routing protocol for Wireless Sensor Networks (TILSRP)," 2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS), Bangalore, pp. 1-6, 2011

[28] D. Tianmin and S. Yao-yao, "Design of the intelligent public transportation monitoring system based on WSN," Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on, XianNing, pp. 4024-4027, 2011

[29] S. Kamei, T. Nagai and S. Fujita, "Fast and Reliable Route Maintenance Protocols for WSN with Crash and Intermittent Failures," Networking and Computing (ICNC), Second International Conference on Osaka, pp. 40-49, 2011