A-SURVEY ON CONNECTIVITY MAINTENANCE AND PRESERVING COVERAGE FOR WIRELESS SENSOR NETWORKS

Joy Winston J.[1], **Paramasivan B.**[2]

[1]Lecturer, Department of Computer Science and Engineering, Einstein College of Engineering
[2]Head of the Department of CSE, National Engineering College, Kovilpati.
Email:[1] joywinston47@gmail.com,[2]bparamasivan@yahoo.co.in

ABSTRACT

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. Its a platform for a broad range of applications related to Security, surveillance, military, health care, environmental monitoring etc.WSN consists of large number of small size sensors which they can sense the environment and communicate with Each other and processing the sensing datas.Because of the deployment nature of the wireless Sensor network once it deployed we can't recharge the battery. so energy conservation is one of the important factor in QOS of WSN.Under this constraint maintaining good coverage and connectivity is so important factor of designing WSN.In this paper we survey about applications and basics about WSN, coverage and Connectivity issues, Existing algorithms proposed for coverage and connectivity, and their strength and weakness.

Index terms: Coverage, connectivity, Wireless sensor network, survey

I. INTRODUCTION

Sensor networks are envisioned as tiny power constrained devices, which can be scattered over a region of interest, to enable monitoring of that region for an extended period of time. The sensor devices are envisioned to be capable of forming an autonomous wireless network, over which sensed data can be delivered to a specified set of destinations.. The nodes sense environmental changes and report them to other nodes over flexible network architecture. Sensor nodes are great for deployment in hostile environments or over large geographical areas.Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. For example, a large quantity of sensor nodes could be deployed over a battlefield to detect enemy intrusion instead of using landmines. When the sensors detect the event being monitored (heat, pressure, sound, light, electro-magnetic field, vibration, etc), the event needs to be reported to one of the base stations, which can take appropriate action (e.g., send a message on the internet or to a satellite). Depending on the exact application, different objective functions will require different data-propagation strategies, depending on things such as need for real-time response, redundancy of the data (which can be tackled via data aggregation and information fusion techniques), need for security, etc.[1].Applications have been envisioned where sensor nodes are scattered from a helicopter over a region of interest, and the nodes self-organize themselves suitably. Once the network is established, the sensed data needs to be routed to a common base station, usually at the periphery of the network. A few potential applications are in order here. Military applications require sensors to be scattered in the enemy territory. The sensors sense the environment for acoustic signatures of vehicles (tanks, jeeps, etc.), and deliver the sensed data to the appropriate base stations. These and numerous other applications of sensor networks require that every point on the region of interest be sensed by at least one sensor

Sensor Nodes

A wireless sensor network consists of hundreds or thousands of low cost nodes, which could either, have a fixed location or randomly deployed to monitor the environment. Because of their small size, they have a number of limitations. The power of wireless sensor networks lies in the ability to deploy large numbers of tiny nodes that assemble and configure themselves.

The most straightforward application of wireless sensor network technology is to monitor remote environments for low frequency data trends. For example, a chemical plant could be easily monitored for leaks by hundreds of sensors that automatically form a wireless interconnection network and immediately report the detection of any chemical leaks. Unlike traditional wired systems, deployment costs would be minimal. Instead of having to deploy thousands of feet of wire routed through protective conduit, installers simply have to place quarter-sized device. The network could be incrementally extended by simply adding more devices B no rework or complex configuration. With the devices presented in this thesis, the system would be capable of monitoring for anomalies for several years on a single set of batteries.

In addition to drastically reducing the installation costs, wireless sensor networks have the ability to dynamically adapt to changing environments. Adaptation mechanisms can respond to changes in network topologies or can cause the network to shift between drastically different modes of operation. For example, the same embedded network performing leak monitoring in a chemical factory might be reconfigured into a network designed to localize the source of a leak and track the diffusion of poisonous gases. The network could then direct workers to the safest path for emergency evacuation.

Current wireless systems only scratch the surface of possibilities emerging from the integration of low-power communication, sensing, energy storage, and computation. Generally, when people consider wireless devices they think of items such as cell phones, personal digital assistants, or laptops with 802.11. These items costs hundreds of dollars, target specialized applications, and rely on the pre-deployment of extensive infrastructure support.

In contrast, wireless sensor networks use small, low-cost embedded devices for a wide range of applications and do not rely on any pre-existing infrastructure. The vision is that these devise will cost less that $1 by 2005.

Unlike traditional wireless devices, wireless sensor nodes do not need to communicate directly with the nearest high-power control tower or base station, but only with their local peers. Instead, of relying on a pre-deployed infrastructure, each individual sensor or actuator becomes part of the overall infrastructure. Peer-to-peer networking protocols provide a mesh-like interconnect to shuttle data between the thousands of tiny embedded devices in a multi-hop fashion. The flexible mesh architectures envisioned dynamically adapt to support introduction of new nodes or expand to cover a larger geographic region. Additionally, the system can automatically adapt to compensate for node failures.

Each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few pennies, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

Due to sensors' limited capabilities, there are a lot of design issues that must be addressed to achieve an effective and efficient operation of wireless sensor networks.

- **Energy saving algorithms**: Since sensor nodes use batteries for power that are difficult to replace when consumed (often sensor nodes are deployed in remote and hostile environments), it is critical to design algorithms and protocols in such a way to utilize minimal energy. So communication between sensor nodes should be reduced and computations are simplified and lightweight security solutions should be applied.
- **Location discovery**: Many applications can track an object require knowing the exact or approximate physical location of a sensor node in order to link sensed data with the object under investigation. Location discovery protocols must be designed in such a way that minimum information is to be exchanged among nodes to discover their location. Since sensor nodes are energy constrained, solutions like GPS are not recommended. Cost is another factor that influences design; manufacturers try to keep the cost at minimum levels since most sensor nodes are usually needed for many applications. If the cost is high, the adoption and spread of sensor technology will be prohibited.

- **Security**: Security solutions are constrained when applying them to sensor networks. For example, cryptography requires complex processing to provide encryption to the transmitted data. Secure Routing, secure discovery and verification of location, key establishment and trust setup, and attacks against sensor nodes, secure group management and secure data aggregation are some of the many issues that need to be addressed in a security context.

Types of Sensors

There are many types of sensors. They are used to measure and/or detect a huge variety of conditions including: temperature, pressure, level, humidity, speed, motion, distance, light or the presence/absence of an object and many other types. There are many versions of each type that may use a different sensing principle or may be designed to operate within different ranges.

Sensors in some cases react to the environment in which they are placed and this reaction is used to measure the property being sensed. For example, a common temperature detector is known as an RTD (Resistance Temperature Detector) and this contains a platinum wire. The electrical resistance of the wire changes with temperature so how the resistance changes can be used to measure the temperature. Many sensors use this type of principle where the variation of an electrical property of a sensing element is a measure of a property being sensed.

Other types of sensors emit a signal and either measure how the area reacts to the emission or measure the reflection of the signal bouncing off an object in front. Inductive proximity sensors are one of the commonest sensors in use. They emit a small electromagnetic field and use this to sense the properties of the area in front of the sensor. So they can detect a metal object. Some sensors send out a light signal and measure if it is reflected back. These are called photoelectric sensors. Some directly detect a reflected signal (Direct detection mode), some check if a beam being reflected from a reflector is interrupted (retroflective mode) and others send a beam to another sensor receiver and detect an interruption of the beam (Opposed mode sensor). Other sensor such as radar and ultrasonic sensors operate also by detecting the reflected signal from the object being detected.

Sensor Network Application Classes

The three application classes we have selected are: environmental data collection, security monitoring, and sensor node tracking. We believe that the majority of wireless sensor network deployments will fall into one of these class templates.

Environment Data Collection

A canonical environmental data collection application is one where a research scientist wants to collect several sensor readings from a set of points in an environment over a period of time in order to detect trends and interdependencies. This scientist would want to collect data from hundreds of points spread throughout the area and then analyze the data.

At the network level, the environmental data collection application[9] is characterized by having a large number of nodes continually sensing and transmitting data back to a set of base stations that store the data using traditional methods. These networks generally require very low data rates and extremely long lifetimes. In typical usage scenario, the nodes will be evenly distributed over an outdoor environment. This distance between adjacent nodes will be minimal yet the distance across the entire network will be significant.

After deployment, the nodes must first discover the topology of the network and estimate optimal routing strategies. The routing strategy can then be used to route data to a central collection points. Once the network is configured, each node periodically samples its sensors and transmits its data up the routing tree and back to the base station.

Security Monitoring

Our second class of sensor network application is security monitoring. Security monitoring networks are composed of nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors to detect an anomaly. A key difference between security monitoring and environmental monitoring is that security networks are not actually collecting any data. This has a significant impact on the optimal network architecture. Each node has to frequently check the status of its sensors but it only has to transmit a data report when there is a security violation. The immediate and reliable communication of alarm messages is the primary system requirement. These are “report by exception” networks.

Additionally, it is essential that it is confirmed that each node is still present and functioning. If a node were to be disabled or fail, it would represent a security violation that should be reported. For security monitoring applications, the network must be configured so that nodes are responsible for confirming the status of each other. One approach is to have each node be assigned to peer that will report if a node is not functioning. The optimal topology of a security monitoring network will look quite different from that of a data collection network.

In a collection tree, each node must transmit the data of all of its decedents. Because of this, it is optimal to have a short, wide tree. In contrast, with a security network the optimal configuration would be to have a linear topology that forms a Hamiltonian cycle of the network. The power consumption of each node is only proportional to the number of children it has. In a linear network, each node would have only one child. This would evenly distribute the energy consumption of the network. The accepted norm for security systems today is that each sensor should be checked approximately once per hour. Combined with the ability to evenly distribute the load of checking nodes, the energy cost of performing this check becomes minimal. A majority of the energy consumption in a security network is spent on meeting the strict latency requirements associated with the signaling the alarm when a security violation occurs. Once detected, a security violation must be communicated to the base station immediately. The latency of the data communication across the network to the base station has a critical impact on application performance. Users demand that alarm situations be reported within seconds of detection. This means that network nodes must be able to respond quickly to requests from their neighbors to forward data.

In security networks reducing the latency of an alarm transmission is significantly more important than reducing the energy cost of the transmissions. This is because alarm events are expected to be rare. In a fire security system alarms would almost never be signaled. In the event that one does occur a significant amount of energy could be dedicated to the transmission. Reducing the transmission latency leads to higher energy consumption because routing nodes must monitor the radio channel more frequently.

In security networks, a vast majority of the energy will be spend on confirming the functionality of neighboring nodes and in being prepared to instantly forward alarm announcements. Actual data transmission will consume a small fraction of the network energy.

Node Tracking Scenarios

A third usage scenario commonly discussed for sensor networks is the tracking of a tagged object through a region of space monitored by a sensor network. There are many situations where one would like to track the location of valuable assets or personnel. Current inventory control systems attempt to track objects by recording the last checkpoint that an object passed through. However, with these systems it is not possible to determine the current location of an object. For example, UPS tracks every shipment by scanning it with a barcode whenever it passes through a routing center. The system breaks down when objects do not flow from checkpoint to checkpoint. In typical work environments it is impractical to expect objects to be continually passed through checkpoints.

With wireless sensor networks, objects can be tracked by simply tagging them with a small sensor node. The sensor node will be tracked as it moves through a field of sensor nodes that are deployed in the environment at known locations. Instead of sensing environmental data, these nodes will be deployed to sense the RF messages of the nodes attached to various objects. The nodes can be used as active tags that announce the presence of a device. A database can be used to record the location of tracked objects relative to the set of nodes at known locations. With this system, it becomes possible to ask where an object is currently, not simply where it was last scanned.

Unlike sensing or security networks, node tracking applications will continually have topology changes as nodes move through the network. While the connectivity between the nodes at fixed locations will remain relatively stable, the connectivity to mobile nodes will be continually changing. Additionally the set of nodes being tracked will continually change as objects enter and leave the system. It is essential that the network be able to efficiently detect the presence of new nodes that enter the network.

Hybrid Networks

In general, complete application scenarios contain aspects of all three categories. For example, in a network designed to track vehicles that pass through it, the network may switch between being an alarm monitoring network and a data collection network. During the long periods of inactivity when no vehicles are present, the network will simply perform an alarm monitoring function. Each node will monitor its sensors waiting to detect a vehicle. Once an alarm event is detected, all or part of the network, will switch into a data collection network and periodically report sensor readings up to a base station that track the vehicles progress. Because of this multi-modal network behavior, it is important to develop a single architecture that and handle all three of these application scenarios.

Lifetime

Critical to any wireless sensor network deployment is the expected lifetime. The goal of both the environmental monitoring and security application scenarios is to have nodes placed out in the field, unattended, for months or years.

The primary limiting factor for the lifetime of a sensor network is the energy supply. Each node must be designed to manage its local supply of energy in order to maximize total network lifetime. In many deployments it is not the average node lifetime that is important, but rather the minimum node lifetime. In the case of wireless security systems, every node must last for multiple years. A single node failure would create vulnerability in the security systems.

In some situations it may be possible to exploit external power, perhaps by tapping into building power with some or all nodes. However, one of the major benefits to wireless systems is the ease of installation. Requiring power to be supplied externally to all nodes largely negates this advantage. A compromise is to have a handful of special nodes that are wired into the building=s power infrastructure.

In most application scenarios, a majority of the nodes will have to be self powered. They will either have to contain enough stored energy to last for years, or they will have to be able to scavenge energy from the environment through devices, such as solar cells or piezoelectric generators. Both of these options demand that that the average energy consumption of the nodes be as low as possible.

The most significant factor in determining lifetime of a given energy supply is radio power consumption. In a wireless sensor node the radio consumes a vast majority of the system energy. This power consumption can be reduced through decreasing the transmission output power or through decreasing the radio duty cycle. Both of these alternatives involve sacrificing other system metrics.

Cost and Ease of Deployment

A key advantage of wireless sensor networks is their ease of deployment. Biologists and construction workers installing networks cannot be expected to understand the underlying networking and communication mechanisms at work inside the wireless network. For system deployments to be successful, the wireless sensor network must configure itself. It must be possible for nodes to be placed throughout the environment by an untrained person and have the system simply work.

Ideally, the system would automatically configure itself for any possible physical node placement. However, real systems must place constraints on actual node placements B it is not possible to have nodes with infinite range. The wireless sensor network must be capable of providing feedback as to when these constraints are violated. The network should be able to assess quality of the network deployment and indicate any potential problems. This translates to requiring that each device be capable of performing link discovery and determining link quality.

In addition to an initial configuration phase, the system must also adapt to changing environmental conditions. Throughout the lifetime of a deployment, nodes may be relocated or large physical objects may be placed so that they interfere with the communication between two nodes. The network should be able to automatically reconfigure on demand in order to tolerate these occurrences. The initial deployment and configuration is only the first step in the network lifecycle. In the long term, the total cost of ownership for a system may have more to do with the maintenance cost than the initial deployment cost. The security application scenario in particular requires that the system be extremely robust. In addition to extensive hardware and software testing prior to deployment, the sensor system must be constructed so that it is capable of performing continual self-maintenance. When necessary, it should also be able to generate requests when external maintenance is required.

In a real deployment, a fraction of the total energy budget must be dedicated to system maintenance and verification. The generation of diagnostic and reconfiguration traffic reduces the network lifetime. It can also decrease the effective sample rate

II. BASICS OF COVERAGE AND CONNECTIVITY

The sensor networks used for many potential applications of small, low-power devices that integrate sensors and actuators with limited processing and wireless communication capabilities. These sensor networks open new vistas for many potential applications, such as battlefield, environmental monitoring, etc. Since most of the low-power devices have limited battery life and replacing batteries on tens of thousands of these devices is infeasible, it is well accepted that a sensor network should be deployed with high density (up to 20 nodes/m3) in order to prolong the network lifetime. In such a high-density network with energy-constrained sensors, if all the sensor nodes operate in the active mode, an excessive amount of energy will be wasted, sensor data collected is likely to be highly correlated and redundant, and moreover, excessive packet collision may occur as a result of sensors intending to send packets simultaneously in the presence of certain triggering events. Hence it is neither necessary nor desirable to have all nodes simultaneously operate in the active mode. One important issue that arises in such high-density sensor networks is density control.ie)the function that control the working density of the sensors to a certain level. but it should full fill the following two requirements. Coverage and connectivity.

Coverage

A sensor network that has blind spots may fail to monitor events that happen at the location of such blind spots. The capability to monitor every coordinate on the sensor field has been termed the problem of coverage [8]. A generalized version of the coverage-preserving problem requires a point to be covered by at least K sensors called the K-coverage problem. Each sensor node can detect the the events with in some very limited distance from itself. That distance is called as sensing range. in this coverage. A convex region of A has a coverage degree of K or is K- covered if every location inside A is covered by at least k- nodes.[2]A network with higher degree of coverage has higher sensing accuracy and robustness to failures.

Classifying Coverage Schemes

Extensive research effort have been made to develop energy efficient schems integrating coverage and connectivity for Wireless sensor network(WSN).depending upon the coverage objectives and applications, they can be classified into three categories, they are area coverage,Point coverage, path coverge.

Area coverage

It cover or monitor the region.ie)the collection of all space points with in the sensor field. and each point of the region to be monitored.

Point coverage

It covers a set of point with known location that need to be monitored. The point coverage scheme focus on determining sensor nodes exact positions, where guarantee efficient Coverage application for a limited number of immobile points.

Path coverage

The goal of path coverage is minimize the probability of undetected penetration through the region.

Connectivity

The ability to report the Sink node. A network is said to be fully connected if every pair of node can be communicated with each other either directly or via intermediately relay nodes[10]. Due to larger number of sensors in networks, the total cost could be high for the whole network, though the cost of the individual sensor is low. therefore its important to find the minimum number of sensors for a WSN to achieve the connectivity. The connectivity of a graph is minimum number of nodes Must be removed in order to partion the graph in to more than one connected component. Connectivity affects the robustness and throughput of the wireless sensor network.in the connectivity we should know the following.

Connectivity Degree:

A sensor network is said to be 1-connected if at least one path between Any two sensors. if sensor network is said to be k- connected if there are at least k- disjoint Path between any two sensors.

Graph Models:

The connectivity of WSN is usually studied by considering a graph associated with the WSN[10]. The WSN is often represented by a graph in which vertices correspond to the communication nodes, and the directed edge from one vertex to another indicates that the node corresponding to the former can send data directly to the corresponding node later. it is common to assume that propagation conditions can be modeled simply be there being a transmission range with in which transmission is possible, and outside off which it is impossible. If all the nodes have equal transmission ranges, then the graph become undirected. A network is called connected if the corresponding graph is connected.

A Graph 'G' is connected if and only if there exists a path between any two pair of vertices. If a network is connected then any pair of nodes can communicate with each other, possibly taking multiple hops through relay nodes.

III. CLASSES OF COVERAGE AND CONNECTIVITY

Both the coverage and connectivity are related to each other for improving the performance of Wireless sensor networks. Based on the type of applications the coverage and connectivity mainly classified in two three classes.

Full Connectivity and Coverage (CC):

Full connectivity and coverage means that every location in the field is covered by at least one node and information at the place can be send to sink (server) or the sink node can be get information at any location of the whole surveillance field. Full connectivity and coverage (CC) mainly used in the application of field monitoring, intrusion detection etc.

To achieve this Full coverage and connectivity, k-coverage and k-connectivity may be desirable[2].To be more specific k-coverage (connectivity) at least provide k-1 failures while maintaining coverage and connectivity. Such applications include distributed monitoring, event tracking in highly protected area, mobile tracking etc.the relations ship between the coverage and connectivity studied in [3].

Partial Coverage and Connectivity (CC):

For some of the applications does not need full coverage and connectivity. For example For finding the temperature of every location in the field, finding the 80% of area might provide Sufficient information for the temperature of the field. Compare to the Full connectivity and coverage (CC) partial coverage and connectivity require less sensor nodes.

Constrained coverage with Connectivity (CC):

For some of the applications the sensor detect when particular event occurs. that time only it need to be active. this type of situations we are classify as Constrained coverage with connectivity (CC) for example consider sensor network deployed to find forestwildfire. Constrained CC implies that it is required that a wildfire must be detected, before it propagated to a particular field of a certain size. Another example of Constrained coverage and Connectivity is to collect the data that are spatially correlated, such as temperature, and humidity. Therefore Constrained coverage and connectivity provide great flexibility to balance the tradeoff between surveillance quality and deployment cost.

Table 1. Comparison of the types of connectivity and coverage

Classification	Performance
Full connectivity with coverage	Best
Partial connectivity with coverage	Average or Good
Constrained connectivity with coverage	Depends on Situation

So we know that without connectivity Coverage is useless. In this paper we are studied about the current status about the coverage and connectivity, what are the existing algorithms are proposed for Coverage and connectivity, their advantages and limitations, finally our conclusion also.

IV. DEPLOYMENT STRATEGY

In generally WSN there are two types of deployment of nodes are available[10]. they are 1.

Deterministic deployment, 2. Random deployment. In deterministic deployment sensors are placed exactly at pre-engineered position. Networks are carefully planned and the nodes are placed at desired position. If specifications of nodes are not known, it is not difficult to determine whether the network is connected and if not to add relay nodes where needed. Where in random deployment the nodes are deployed randomly. Although deterministic deployment have many advantages, in order to reduce installation costs, it has often been proposed that larger WSNs

V. EXISTING SOLUTIONS

We first introduce how we evaluate the performance of the region covered by the Wireless Sensor Network (WSN).given a set of sensors deployed in a monitored region, coverage evolution problem is all the region is covered by at least k- sensors. Where k is a given number of sensors.[2].lot of existing protocols are available we discuss about that one by one

Coverage configuration protocol: (CCP)

The main aim of the Coverage configuration protocol [4] is to achieve the guaranteed degree of coverage and connectivity while achieving long life time of the sensor by maximizing the number of sleeping nodes. The eligibility rule of CCP decides if a sensor node is active or not according with the actual coverage of its sensing area.

If its sensing area is already covered by the sensing nodes. the node in inactive and can be enter in SLEEP mode. A node can be in three states: SLEEP, LISTEN and ACTIVE. In the SLEEP mode a node sleeps to conserve energy. In ACTIVE mode the node monitor the environment and communicate with the another nodes. Periodically the node enters into the LISTEN state to collect the HELLO messages from its neighbors and revaluate its eligibility rule to determine its next state. In high density area the coverage degree exceeds the requirements; the redundant nodes go to the SLEEP mode. When the ACTIVE mode sensor run out of energy, sensors that are in the sleep state will find themselves eligible to enter the ACTIVE state. Timers are associated with each sate to avoiding the collisions among the nodes which are decided to join or withdraw the ACTVE .To self configure for a wide range of applications when the communication range is more than twice as a sensing range. To ensure k-coverage they need to check whether the intersection points inside its sensing area are K-covered. But the main limitation is it cannot guarantee the connectivity when the communication range is less than twice of the sensing range.To avoid this limitation by combining Coverage configuration protocol with SPAN(a distributing connectivity preserving mechanism for multi hop adhoc wireless networks that reduces energy consumption without significantly affecting the connectivity of the network.).By combining the Coverage configuration protocol and SPAN achieving the dynamic coverage and connectivity which is mainly useful for many applications. Then the connectivity and coverage also achieved in any case. But in CCP should need accurate locate information and neighborhood table. this is the limitation of Coverage configuration protocol.

PEAS

PEAS stands for probing environment and adaptive sleeping [6] protocol. It is a simple protocol. Its mainly targeted for hostile environment. The basic principle of this algorithm is turnoff the nodes and tries to achieving good coverage and connectivity. PEAS consist of two simple algorithms. They are 1. Probing environment 2. adaptive sleeping.

Probing environment

It determines which node should work and Adaptive sleeping, which determines how to adjust dynamically the sensors sleep times in order to keep a constant wake-up rate. At the starting all the nodes are sleeping for a exponentially distributed random time. When a nodes wakes-up it broadcast a PROBE message with a certain range Rp. any working node within the range Rp sending the REPLY message. if the node receiving at least one REPLEY message then it continue the SLEEPING state otherwise it goes to the ACTIVE state.

Adaptive sleeping

It adjusts the wake-up sleeping neighbors for each working node to ensure the level of redundancy required by the application. Limits of the PEAS are there are not mentioning any relationship between the sensing range and communication range. The node should have the capability of dynamically changing the transmitting power based on Rp required by the environment. there is no strong guarantee for coverage or connectivity. Their evaluation shows that the robustness of PEAS and the network life time extension which varies linearly with the with the number of deployed nodes.

OGDC

Optimal geographical density control (OGDC) protocol [5] is mainly focusing on maintaining coverage and connectivity using small number of nodes. there the relationship between the coverage and connectivity is established. It's a localized density control algorithm.

In OGDC the nodes in the one of the following states UNDECIDED,ON or OFF. the algorithm runs in rounds. at the beginning of each round all the nodes should set their state to UNDECIDED and participate the selection of active nodes. any one of the node is a starting node with probability P. after a back-off time the node broadcast a power-on message to its neighbor and change the state to ON. this message consists of the location of the node and the direction along with the second working node to be located. The node will change their state either ON or OFF based on power-on message recived.each node maintain a table about their neighbor. after receiving the power-on message it checks if its sensing area is already covered by its neighbors. If its covered then its change the state to OFF. Otherwise its change the state to ON. The back off timer . Timer is used to avoid the packet collision. At end all the node set their states in ON or OFF until the end of the each round. Once one node enter the ON state it can't go Back to the OFF state in that round. But different nodes can be ON state in different rounds. so energy can be balanced in all those nodes. The OGDC maintain 1-coverage and 1-connectivity.

The nodes should know their location its one of the assumption of this OGDC protocol. Then the OGDC protocol is compared with PEAS it shows that reduce number of nodes are enough to produce good coverage than PEAS. the life time of the nodes also increased compared to PEAS. They compare the OGDC with CCP also. it shows that when number of nodes are increased the Collision also increased but the OGDC the collision of packets are low.

Randomized Scheduling Algorithm (RSA)

Randomized scheduling algorithm [7] also try to achieving both connectivity and coverage by turnoff the redundant nodes. in this protocol first it give number to all the nodes. then assume the subset S for a given number k each sensor node randomly joins k disjoint subset of S. once the k sub sets are determined they work alternatively at anytime anyone of the subset is working and all the nodes belonging to the subset is on. the intention is it should cover all the portion of the region now the coverage problem is solved. but still there is no guarantee for connectivity. To achieve the connectivity in inside the subset no node in that subset should not participate in any other schedule of no duty cycle still there is not guarantee in connectivity between the subsets. to achieve this they are introducing the extra-on rule: it shows that assume that sensor node A is said to be upstream node of node B. if node A and B are neighboring nodes

And the minimal hop count of the node A is less than the hop count of B. then node B is called as node A's downstream node. if a sensor node A has a downstream node B which is in active at time slot i. and none of B's upstream is active in that time slot then A also should active in time it requires the minimum hop count of sink and the list of its upstream nodes. But it create lot of overhead because of large dependencies. To avoid the overhead they using join scheduling. It consists of three steps. Randomly select the subset, propagate minimum hop count, exchange information with the local neighbors and finally they enforcing the extra-on rule. now the overhead is reduced. The advantage of this protocol is no need for knowing the location of nodes, dynamic Coverage adjustments based on the application. But the limitation is when comparing with CCP+SPAN it does not provide full coverage.

VI. CONCLUSION

In this survey paper we discuss about the basic concepts and types of classes about the coverage and connectivity issues in wireless sensor networks. And it=s presented the existing solutions and their strength and weakness.

The existing research focus on the following consideration of improving coverage performance by maintaining connectivity and improving network lifetime. but still there is no effective algorithm is proposed to solve the problem of coverage and connectivity.

REFERENCES

[1] Y. Jennifer, M. Biswanath, and G. Dipak, AWireless sensor network survey@, Computer Networks, 2008, vol. 52, pp.=2292B2330.

[2] W. Wang, K.C. Chua and V. Srinivasan, ACoverage in Hybrid Mobile Sensor Networks,@ IEEE Transactions On Mobile Computing, 2008, vol. 7, no. 11, pp. 1374-1387.

[3] R. Meester and R. Roy, *Continuum Percolation*, Cambridge University Press, 1996.

[4] G. Xing, X. Wang, Y. Zhang, C. Lu, R. Pless, and C. Gill, AIntegrated coverage and connectivity configuration for energy conservation in sensor networks,@ ACM Transactions on Sensor Network, 2005, vol. 1, no. 1, pp. 36B72.

[5] H. Zhang and J.C. Hou, AMaintaining Sensing Coverage and Connectivity in Large Sensor Networks,@ Ad Hoc & Sensor Wireless Networks, 2005, vol. 1, no. 1, 89-124.

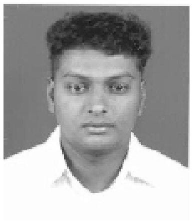
[6] Fan YE,Gary Zhong,Song wu lu,Lixia Zhang,@Robust energy conserving protocol for long-lived sensor networks Aproceedings of the 10th IEEE conference on network protocols,2002,pp.1-2.

[7] Chong liu,yang Xiao, Arandom coverage with guarented connectivity;joint scheduling for wireless Sensor networks.@IEEE transactions on parallel and distributed systems.2006,vol.17.no.6,pp.562-575.

[8] C.F. Huang and Y.C. Tseng, AThe coverage problem in a wireless sensor network,@ In ACM International Workshop on Wireless Sensor Networks and Applications (WSNA), 2003, pp. 115B121.

[9] M. Castillo-Effen, D.H. Quintela, R. Jordan, W. Westhoff, W. Moreno, Wireless sensor networks for flash-flood alerting, in: Proceedings of the Fifth IEEE International Caracas Conference on Devices, Circuits,and Systems, Dominican Republic, 2004.

[10] Ji Li, Lachlan L.H. Andrew, Chuan Heng Foh , Moshe Zukerman and Hsiao-Hwa Chen,@Connectivity, Coverage and Placement inWireless Sensor Networks@ Journels on sensors 2009, pp-7665-7692.



J. Joy Winston, is the lecturer in the Department of Computer Science and Engineering at Einstein college of Engineering, Tirunelveli, TamilNadu, India. He obtained his Bachelor and Master degree in Computer science and Engineering from Anna University Chennai and Tirunelveli in the year 2006, 2009 respectively. He has two years teaching experience and presented 03 apers in National level conference. His current area of research is Wireless Sensor Networks. He is a life member of ISTE and MIE.