Extending the Lifespan of Wireless Sensor Networks: A Survey of LEACH and Non-LEACH Routing Protocols

Yakubu Abdul-Wahab Nawusu
Computer Science Department
Tamale Technical University
Tamale, Ghana, West Africa

Abdul-Barik Alhassan
Computer Science Department
University for Development Studies
Navrongo, Ghana, West Africa

Abdul-Mumin Salifu
Computer Science Department
University for Development Studies
Navrongo, Ghana, West Africa

ABSTRACT
Originated envisaged for military functions, Wireless Sensor Networks (WSN) have gain wide-ranging applicability including in home, business, agriculture, environment monitoring, health care and structural engineering. Despite the immeasurable benefits, Wireless Sensor Networks have inherent constraints arising mainly from its low battery powered sensor nodes. Many design efforts have focused on designing energy efficient means of monitory and transmitting required application specific events as long as required. Different energy-efficient schemes have been developed in past studies to varying successes. This paper reviews some relevant literature on existing routing protocols for wireless sensor network with much emphasis given to the Low Adaptive Clustering Hierarchy (LEACH) protocol, its variant protocols as well as its security-enabled versions.

General Terms
Wireless Sensor Networks, Routing protocols, LEACH, Security.

Keywords
Wireless Sensor Networks, Routing protocols, LEACH, Non-LEACH protocols, Network lifespan, Security.

1. INTRODUCTION
The future of information gathering and processing is promising. Advances in micro-sensor technologies and cooperative micro-sensing are the reasons to this hopeful future of intelligent data gathering, processing and prompt and reliable communication. The size and cost of micro-sensors have diminished over the years as a result of advances in MEMS electronics making micro sensors favoured option for data capture, computation and transmission to required destinations. Individually, these sensors may not be as powerful and beneficial as needed. As a result, researchers have focused on how to derive data collection, processing and communication from their collective cooperation. Wireless Sensor Network (WSN) is one such cooperative arrangements consisting of a network of sensors used to collect environmental parameters of interest.

The birth of Wireless Sensor Network started nearly forty years ago as a US Defense Advanced Research Project Agency (DARPA) project. It was as with many applications earmarked as a military application for dealing with warfare events. Its initial benefits culminated in several research interests in areas such as protocol designs, developing self-location algorithms and design of acoustic sensor [1]. Sophistication in MEMS, wireless and microprocessor technologies have lately however shifted the focus of wireless sensor network research towards routing and information processing techniques.

Wireless sensor network is a collaborative network of multitudes of densely deployed cheap tiny sensor nodes within an environment of interest to perceive and initiate the necessary actions of data processing, aggregation and transmission. The physical architecture of sensor node as micro-electronic device includes four basic parts; a sensing sub-system, which comes with a sensor and an ADC; a processing sub unit, that comes with a small memory area; an RF transceiver sub-system for data reception and transmission and a power unit all working as a unified system to meet the application specific intentions of the sensor network. Additionally, a sensor node may be fitted with, a location finding system such as GPS, an energy harvester to convert harvested energy into electrical energy for use by the sensor node and an actuator to facilitate node mobility [2], [3], [1]. figure 1 below depicts the components of a typical sensor node.

The operation of a sensor network begins with data sensing. This is taken charge by the sending unit. The sensing unit of sensor nodes are built with consideration of the environmental conditions to be monitored such as water level, pollution level, pesticide level, level of pollutants, plant height, heat level, heart rate, blood pressure, lightening conditions, temperature, humidity, vehicle movement, noise level, pressure, soil makeup, and more. The type of sensor varies for each of these conditions; including seismic, thermal, heat, acoustic, radar, visual and infrared, presence, light, proximity and fluid velocity [1]. Deployment can be close to the percept of interest or far away depending on the application area [1]. Deployment can also be planned or unplanned. Planned deployment requires placing the nodes one by one into the sense field by a human or a robot. Considering the sheer number of sensor node and their unattended deployment, planned deployment is often an uneconomical approach. These coupled with the fact that many environments are inaccessible or require relief of disaster, most deployments are random.

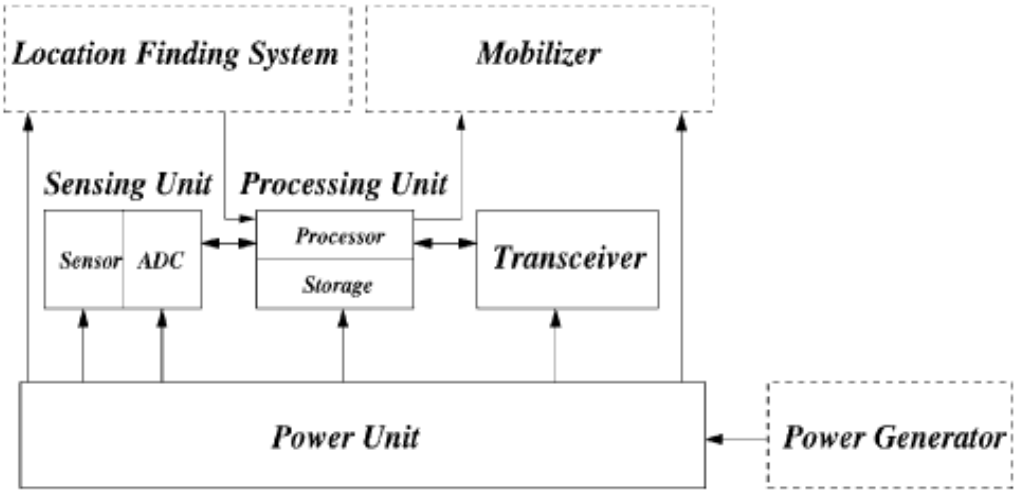

Fig 1: The components of a sensor node [1]

In a randomized deployment, sensor nodes can be thrown from a plane, an artillery shell, rocket or missile, or thrown by a catapult. Thus, these sensor nodes required the ability to self-organize themselves into an appropriate network infrastructure right from the point of deployment and during periods of topological changes.

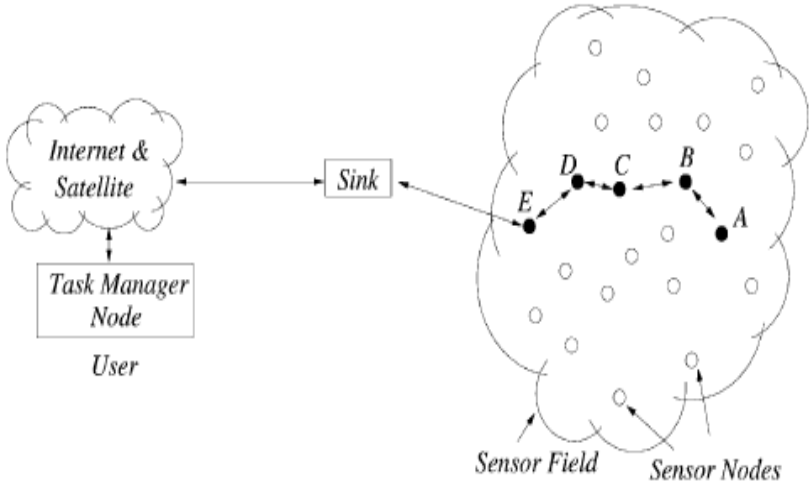

Fig 2: Sensor node deployment in sense field [1]

In the figure above, the sensor nodes are randomly scattered in the sensor field either close to or inside the events of interest. Each of these dispersed nodes are built with capabilities to measure the required event attribute, perform quick local data processing and push the data to a sink. An end user with some data analysis and reporting dues may interact with sink node via network services such as the internet or a satellite communication by issuing an appropriate query.

1.1.Sensor Node Platforms

A few commercial and research sensor node architecture have been manufactured over the past few years. Sensor node platforms vary in terms of size, target application and functional needs of the wireless sensor network. Beyond theses, each platform inherently has strength and weaknesses that require consideration when evaluating choices. Table 1 below mentions few examples of sensor node prototypes.

Table 1. Examples of Sensor Platforms: Adapted from [4]

MICA Motes	MICA mote is proprietary sensor platform that operates on the popularly used TinyOS an provides two-way communication at a speed of 50kbps. Its physical parts include an Atmel Atmega 128L processing chip and an energy source powered by an AA battery.
PC - 104	PC -104 is a DARPA funded platform with a much larger size than the MICA node. PC-104 based nodes run on an AMD ElanSC400 CPU,16MB RAM and Flash Disk.
Rockwell WINS	Rockwell WINS rather operates on a StrongARM 1100 CPU at a speed of 133 MHz an stores data on a 1MB flash memory and random-access memory. It uses two 9V batteries.
Smart Dust	Smart Dust is an air-based sensor node that presents a simply architecture for monitoring duties. It however has a stricter energy consumption constraint.

2. APPLICATION AREAS OF WIRELESS SENSOR NETWORKS

Researchers have for the last twenty years and perhaps beyond, shown a lot of interest in wireless sensor network. This interest steps from the fact that wireless sensor network applications are growing and offer solutions to a wide range of problems. Also, advancements in micro technologies, wireless technologies and microelectromechanical systems have made the production of tiny, yet productive and low cost, battery powered sensor nodes, allowing WSN technology to be used in a wide and varied application areas both in research and real world and industrial applications. It is believed that WSN would have a far-reaching impact on our lives than that which microcomputer have ever had [1]. Currently, WSNs have had applicability in various applications in the real world. They have been set up in monitoring and prompting appropriate disaster management units about impending havoc such as wildfires, floods, tsunamis, earthquakes, and hurricanes [5];[1];[6] and for monitoring the strengths and weaknesses of constructed edifices such as roads, buildings and bridges [7][8]. The life of humans and animals depends largely on availability and purity of water sources particularly for domestic consumption. WSNs have been applied to not only monitor the quality of water sources but also air quality which is just as equally life sustaining as water. Other applications include; tracing plants growth and movement of animals, predicting the advent of disaster and assessing disaster control measures, monitoring healthcare plans for patients and their responses, reconnaissance missions for secured homes and offices, inventory and stock control in stores and in military setups for target tracking [9].

2.1 Military applications

WSNs like many other technologies, are borne out of research for military applications [10] Designers of military systems recognized long ago the benefits of sensor networks and became a crucial component of network-centric warfare. WSNs are deployed in military environments to support detection of information about enemies and enemy strategies, and other phenomena of interest [11]. "Sensor networks can improve detection and tracking performance through multiple observations, geometric and phenomenological diversity, extended detection range, and faster response time" [12]. WSNs can serve information dissemination needs in various military scenarios including blast localization, perimeter surveillance and protection, nuclear, chemical, and biological attacks detection, and missile monitoring. WSN generate real time and accurate data which can decrease fatality rate [12].

2.2 Health Applications

WSN application in quality health delivery is becoming popular. Growing population of patients have a need for instant, inexpensive and flexible systems to monitor their body parameters. Sensor nodes can offer these needs. Sensor nodes can also be integrated into a wireless body area network (WBAN) to enable a proactive personal health management system that has the potential to transform the future of healthcare [13][14]. Sensors for patient's health monitoring takes the forms of wearables or implantable are used in monitoring patient's physiological data such as pressure rate and heart rate, surveillance of patients and doctors in health units; there are sensor support for the aged; there are also sensor usefulness in drug administration and prescription in hospitals, monitoring the movements and internal processes of insects or other small animals and many more of the like.

2.3 Environmental Applications

Quality air and quality water for humans, animals, and plants are the essentials of all living things. A polluted air or a contaminated drinking water source can cause diseases and at worst death to humans and animal [15][16]. WHO (2014) reports that 14 % of deaths in recent times are due to air pollution which cause chronic obstructive pulmonary disease or acute lower respiratory infection in victims. Hence information about air quality is important to saving lives. Additionally, acute water contamination is considered one of the major problems affecting the environment [17]. Therefore, water quality monitoring is a necessity. Water quality management involves monitoring water sources such as rivers, lakes ponds, wells and wetlands to ensure safe drinking and for other human and animal uses [18][19][20]. Limitations and several error sources in traditional manual water quality monitoring techniques have initiated the integration of wireless sensor networks in such endeavors. The use of WSNs for WQM is particularly appealing due to the cheap deployment cost of sensor nodes the ability to acquire and process data at several distributed water sites, and the ability to communicate the data timely manner [12]. Another environmental application of wireless sensor network is flood and bushfire relief and management. Flooding, domestic and bush fires are a seasonal headache of environmental and fire management agencies particularly in Ghana many a times causing loss of several lives and properties. Wireless sensors can be handy in forest fire detection, air pollution detection and food detection. In agricultural applications, wireless sensor networks can be deployed to facilitate irrigation, monitor crop and livestock conditions. Additionally, sensors can be used for tracking the movement of insects and other small animals.

2.4 Home, Industrial and Commercial Applications

Human homes are becoming intelligent with embedded sensor appliances. Appliances like furniture, vacuum cleaners, micro-wave ovens, video cassette recorder and refrigerators come with intelligent capabilities that allow owners to manage home functions more easily. Environment control is another area of application of WSN. Air flow and temperature can be controlled from different parts of an office room with the added benefit of reduce energy consumption [21]. In detecting and monitoring theft, sensors can be fixed into cars, home and office gates and any movable or fixed valuables to detect and alert a remote user of potential theft threat [22]. In business centres, sensor nodes are applied in; monitoring product quality, managing inventory and locating items in a warehouse or in a retail store. In structural health monitoring, sensors are used to globally monitor the strength and damage caused to the support of a structure or building. Acoustic sensors are used to measure the content of pipeline; piezoelectric sensors are used to measure movement; magnetic sensors are used to measure movement of vehicles and many other more applications in home and industrial application.

3. CHARACTERISTICS AND DESIGN ISSUES OF WSN

WSNs are characterized by the following; nature of deployment, fault tolerance, frequent topology change, data redundancy, limited computation, storage and battery capacity, battery lifespan and data redundancy. WSNs are application specific and come with unique design constraints and objectives. The application specificity of WSNs makes it

almost impossible to provide an all-in-one list of design objectives. A combination of the following would often characterize or be the object for setting up a WSN.

Reduction in node size: reduction in nodes size is aimed at speeding up and easing node deployment with the added benefit of reduced cost and reduced energy consumption.

Low node cost: the cost of the entire sensor network is related to the cost of the individual nodes and the extent and density of deployment.

Low power consumption*:* sensor nodes are powered by low energy batteries. These batteries are in most instance, difficult to replace if at all not impossible. Meanwhile the lifespan of a WSN is depended on the length of life of its constituent sensor nodes. As such a design objective for setting up a WSM may require that least amount of battery power is consumed during the activity of data sensing and transmission. When battery life is prolonged the consummate benefit is that lifespan of the network increases. Another objective in a WSN design could be on how the network would respond to additional nodes. It should be possible to deploy and maintain network of all sizes whiles maintaining similar output of interest.

Reliable network: the need also arises to ensure reliable data transmission even in the events of errors, interference and noisy channels. Bandwidth utilization, self-configurability, Security, fault tolerance, energy-awareness, quality of service interests are some other design objectives have challenged researchers in the field of WSNs.

Deployment cost*:* It is important that the cost feasibility of a WSN be determined prior to deployment. The cost of single sensor node provides a meter to the overall cost of a wireless sensor network. Accordingly, [1] asserts that "[t]he cost of a sensor node should be much less than 1$ in order for the sensor network to be feasible". Meeting this cost value per sensor node is obviously a challenging proposition given the multi-part architecture of a sensor node. It is expected that the cost of any WSN would be cheaper than that of a traditional network for it to be worthwhile.

Fault tolerance: Sensor nodes like any mechanical device are subject to failures due to power outages, physical damage, or environmental interference such as noise. A sensor network's overall tasks should not be affected by node failures and other adverse environmental conditions. This is to say, it should be reliable or fail tolerant. Thus, in designing a sensor network, fault tolerant capabilities should be built in them so it is able to provide required services without adverse effects when sensor nodes fail. Fault tolerant mechanisms may include automatics formation of new links and routes to bases station; adjusting transmission power on existing links to reduce energy consumption or directing packet transmission through regions with more energy.

Node Deployment: Sensor nodes can be deployed on a randomized or deterministic manner. Manual deployment requires the sensors to be manually placed in the sensing environment and data is transmitted through pre-specified paths. In random node deployment, the nodes are placed randomly, creating an ad hoc routing infrastructure. While deterministic node deployment may be restricted to few application areas, random deployment can lead to non-uniform distribution of nodes resulting in poor node connectivity and energy inefficiency.

Energy consumption: Sensor nodes are battery powered and so many of the challenges in WSN such as the constraint in energy, processing, and storage capacities are related to power consumption. In particular, network lifespan suffers when battery lifetime deteriorates. Thus, a careful resource management is needed sustain sensor batteries and prolong network lifetime. Many of the research efforts are in the area of building power-aware protocols and algorithms because of the added importance of node power conservation nana management to the entire sustenance of a wireless sensor network. Energy consumption in WSN occurs in the data sending, processing and communication. Energy expended in sending and data processing are each far less than that which is spent in communication. Communication energy is dispensed for data reception and data transmission.

Coverage: network coverage is another of the important design parameters in WSN. Since sensors can only cover limited physical areas of the application environment, a given sensor's reach of the environment is limited in both range and accuracy.

Connectivity: Network connectivity depends on the deployment type enforced (partly); network node density and node failure rate. From the outset if the nodes are randomly deployed and node distribution sparse, connectivity suffers. Also, if the node density in sensor network is high nodes are closer to each other and will therefore be highly connected. Additionally, network size reduces as sensor nodes failure rate increases keeping nodes less connected.

Node/link heterogeneity*:* depending on the application is decision is needed to be made on whether nodes are homogenous or heterogeneous. While some applications require nodes to have equal computation, energy and communication capacities, some others allow a blend of different sensor functionalities built independently or included in the same sensor nodes.

Scalability*:* Sensor networks size vary from a few hundred to several hundred thousand of nodes. As such any developed WSN implementation scheme must be able to work with any network size and be able to maintain adequate performance from deployment to end of the network's mission. Added scalability benefits includes sensor nodes ability to adequately respond to environmental stimulus.

Node Mobility*:* The assumption in most network arrangements is that nodes are immobile. However, mobility is required sometimes for all or some of the sensor nodes especially when it is pertinent to dynamically vary the placement of cluster heads and bases stations. The level of mobility may vary from intermittent node movement within longer periods of node movement to protracted periods of mobility. In setups where mobility is required, clustering becomes difficult to manage as cluster size, cluster membership and number of clusters progressively evolve [23].

4. ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORK

Routing in WSN are unlike those found in established wireless communications network. The challenges of routing in wireless sensor network arises from their inherent characteristics which distinguish them from conventional communication networks and wireless adhoc networks (MANets) [24]. One routing challenge in wireless sensor network is the difficulty in building an addressing scheme for the huge numbers of deployed sensors. Secondly, many wireless sensor network setups unlike modern communication

networks, provide a single data sink into which sensed data from multiple sources are flown into. Again, because sensor nodes deployment is often randomly dispersed in an area of interest, nodes that are nearby may generate data that are the same. In such instances the level of redundancy would be significant [24]. These and many other challenges have urged researchers to devise different mechanism and protocols to route data in a wireless sensor network at different energy efficient levels. The need for routing protocols is to deal with design issues such as scalability, energy efficiency, robustness, latency, low computation and memory usage. Different classification options exist to classify the routing protocols for wireless sensor networks. One of such is based on network structure. According to network structure, routing protocols can be put into Flat, Hierarchical and Location-based protocols. The table and figure below represent the classes and sub-classes of routing protocols for wireless sensor network.

Table 2. Classes of Routing protocols for WSN [25], [24], [26].

Routing Protocol	Protocols description and example types
Flat-based (Data Centric)	All nodes are assigned same roles or functionalities. Sensing duties are done collaboratively. Flat-based protocols include Sensor Protocols for Information via Negotiation (SPIN), Directed Diffusion (DD), Sequential assignment Routing (SAR), Cougar, Constrained Anisotropic Diffusion Routing CADR), ACtive Query forwarding in sensoR nEtworks (ACQUIRE). Collision overheads are far more present in flat based protocols than in hierarchical protocols.
Location-based	In this protocol, all nodes know their neighbouring node position allowing data to be routed to these known locations rather than the entire network. Examples are: Geographic Adaptive Fidelity (GAF), Geographic and Energy Aware Routing (GEAR), SPAN, Greedy Other Adaptive Face Routing (GOAFR). The efficiency of the scheme relies on the even distribution on nodes and the presence of traffic.
Hierarchical-based	Unlike in flat-based protocols, nodes in hierarchical protocols play different roles. High energy nodes perform data aggregation in addition to transmission. Dedicated nodes called cluster heads (CHs) performs the additional tasks of data aggregation of data from sensor nodes that are in range. Hierarchical based routing protocols include; LEACH, TEEN, APTEEN, Power Efficient Gathering in Sensor Information Systems (PEGASIS), Stable Election Protocol (SEP). Data aggregation and diffusion reduce the number and size of data transmitted to base station. As a result, reduces transmission distance and thus the transmission energy far more than in both location-based and flat-based routing protocols. Additionally, clustering improves upon the scalability of the system. There is also efficient point-to-point communication. The major drawback is that there is additional overhead on the entire network.

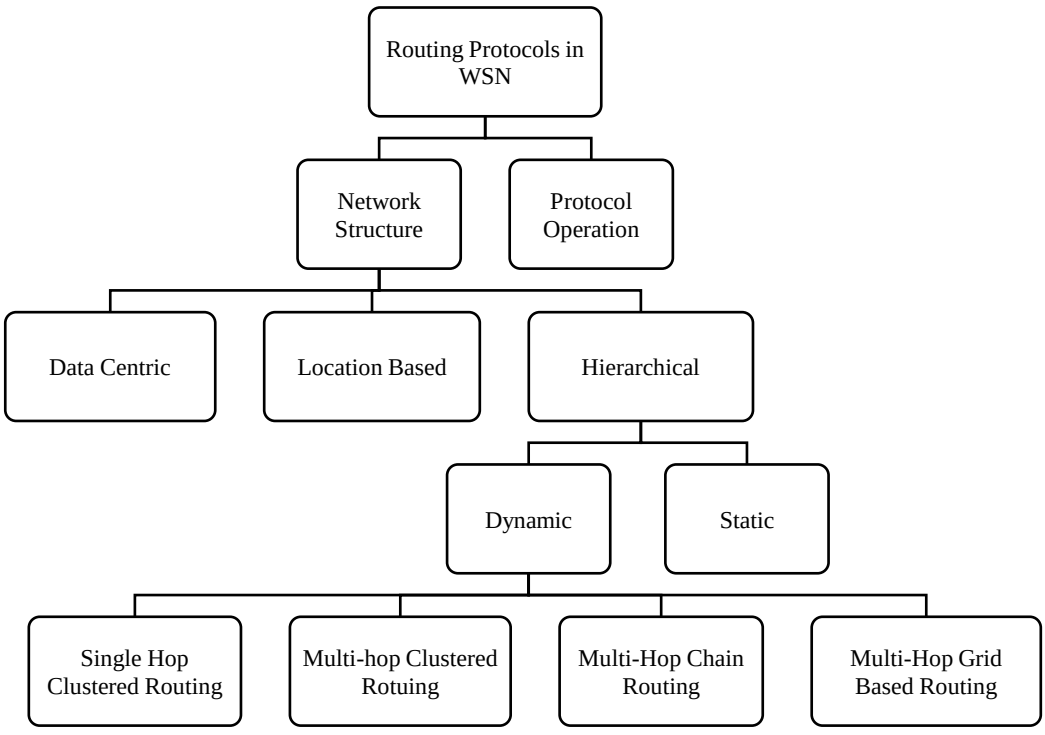

Fig 3: Classification of Routing Protocols for WSN. Adapted from [27]

Of the classification above, this research is particularly interested in the hierarchical group of routing protocols of which LEACH is the first. We would however be following from here with a briefly discuss the different routing protocols and their types.

4.1 Data Centric Routing Techniques

Routing in WSN can be organized in a data-centric fashion with the benefit of avoiding cluster formation overheads. Protocols in this class of routing protocols include; gossiping, flooding, sensor protocol for information negotiation, Energy aware routing, rumor routing, gradient-based routing and Constrained Anisotropic Diffusion Routing (CADR) are example of data centric routing techniques [1], [28], [29], [30], [31]. SPIN and its suit of protocols together with Directed Diffusion have encouraged the design of these and many other data centric protocols.

4.1.1 Gossiping and Flooding

Flooding and Gossiping pioneered data routing in WSN in the data-centric class of protocols. These protocols are implemented without a planned routing procedure [1] out of the simplicity of the two approaches. In Flooding a node is required to propagate a received data and control packet to all of its neighbor nodes until the data packets reaches its destination or a threshold hop number is satisfied. Flooding bares no cognizance of the energy constraints of the sensor nodes and leads to issues such as implosion and overlap [32], [30]. Since flooding blindly broadcast data packet from one node to all other nodes in the network, duplicate or similar data get sent out to neighboring nodes by two or more nodes. This phenomenon is termed implosion. Another concern that arises from the flooding protocol is its lack of consideration to the eternity reserve of sensor nodes. In [33] the gossiping technique is proposed to remove the drawback of implosion by sending data packets to a randomly selected few other nodes until the data reaches the intended destination, rather than to all neighbor nodes as is the case in Flooding. Data communication amongst sensor nodes is however slow in Gossiping especially when the density of the network increases.

4.1.2 Sensor Protocol for Information Negotiation

Sensor Protocol for Information Negotiation (SPIN) applies a negotiation scheme that averts the failing of the flooding protocol. SPIN operates with the assumption that nodes in close proximity to each other have sensed data that are alike. In this regard, SPIN employs high order name descriptors to initiate a negotiation process between a community of nodes in a bid to reduce energy waste arising from sending similar data of neighboring sensor nodes. The negotiation process allows neighboring nodes to distribute only data that are not similar. Data delivery may delay or not take place at all in this arrangement however, if for instance intermediate nodes between two communicating nodes are not interested in the data packet. Another noticeable drawback of SPIN is that idle nodes have their transmitters and receivers on even during periods of inactivity resulting in needless energy consumption [1]. Two variants of SPIN exist, SPIN-1 and SPIN-2. Energy efficiency is built into SPIN-2 unlike in SPIN-1 which is not energy aware.

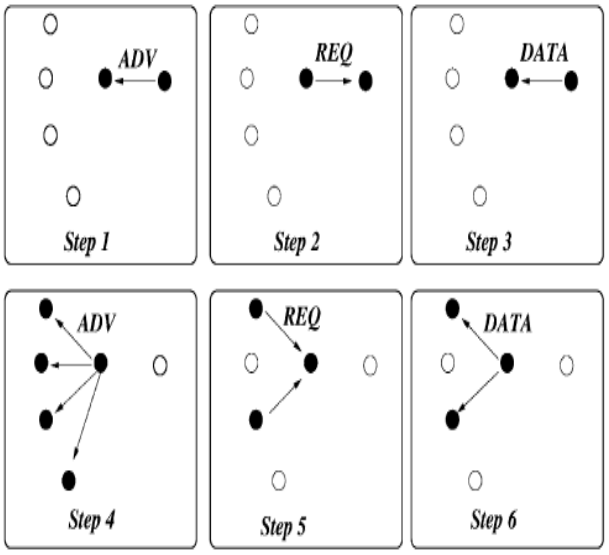

Fig 4: The SPIN Protocol [30].

In the arrangement above, a member sensor node has to show interest in an advertised data description before the actual data packet is sent to the interested node. In the setup above, the SPIN process initiated with an advertisement message (ADV from above) containing named descriptors of a sensed data sent to a neighboring node(s). Neighboring node(s) that are interested in such data send a request for the data (REQ from figure above). The request is acknowledged and the actual data is the forwarded to the interested node (s). This process is repeated by the recipient nodes until all interested nodes receive a copy of the data packet. The whole concept of SPIN thus is based on interest showing and negotiation and data is only sent to the nodes that need it utilizing three message types ADV, REQ and DATA [1].

4.1.3 Directed Diffusion

[34] proposes a paradigm for data dissemination called Directed Diffusion. Directed diffusion marked an important milestone in data centric routing by setting up an application-dependent, query-based data delivery model for sensor networks in which the sink sends out an interest meta data of tasks marked by attribute-value pair to all sensors in a network. All sensors in the network maintains a buffer of the interest entries containing a gradient field. Interested nodes propagate the interest throughout the network. Afterwards, the changes in the attribute value is monitored whiles it is transmitted from source to sink. A path from sink to source can be shored up by repeatedly resending the interest message. Path failures and its effects can be minimized in directed diffusion by building multiple paths. Less traffic build-up is experienced in directed diffusion protocol as a results. The protocol is better than flooding in energy consumption. Its efficiency is bound out of the use of paths with best local gradient. Retransmission of attribute values when required makes directed diffusion an effective protocol. Directed diffusion however is hindered by its inherent application dependent nature. Directed diffusion would consequently not be an effective protocol choice for application that require steady data transmission to a base station [1]. Additionally, retransmission and alternative path maintenance is needed and generates additional overhead [4]. The figure below depicts an illustration of directed diffusion. In figure 5 (a), the sink node propagates a required interest. In figure 5 (b), a gradient form source to sink is set up. And in figure 5 (c) the actual data is sent through the gradient path.

4.1.4 Rumour Routing

In [28] Romour routing is proposed for application areas where geographical routing is infeasible. The technique uses random network movements to find a single path to an event of interest from the source. When the sensor environment is engulfed with events, each node builds a table of events, consisting of source node and last accessible node and generate an agent packet. The agent packet travels through sensor network and informs visited nodes of the occurrence of a local event of interest. On its way to deliver the event information, the agent updates it lists of events with sensor nodes on its path to ensure harmony of events. All other nodes that hear the agent's updates, accordingly update theirs too. The agent has a lifespan of few hops and dies after making such number of hops moves on the network. This process ensures that the shortest path to the event is maintained.

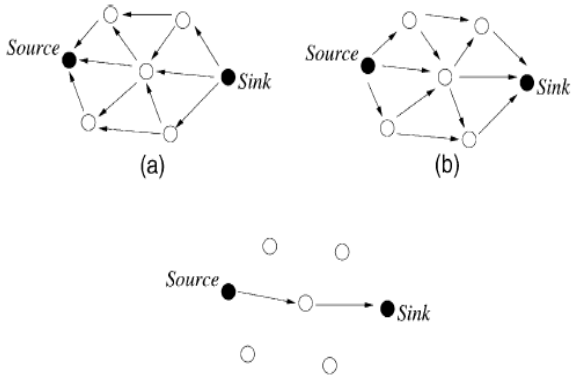

Fig 5: Example depiction of Directed Diffusion [35].

4.2 Location Based Protocols

In this class of protocols, all nodes are engineered with the capability to know their neighbouring node position allowing data to be routed to these known locations rather than the entire network. Location-based schemes are effective primarily because the offer an even distribution of nodes within the sensing field and increases the data traffic. Geographic Adaptive Fidelity (GAF), Geographic and Energy Aware Routing (GEAR), Minimum Energy Communication Network (MECN), SPAN, Greedy Other Adaptive Face Routing (GOAFR) are examples of location-based routing protocols.

4.2.1 Geographic Adaptive Fidelity (GAF)

GAF adopts a geographic information system for generating location information of sensor nodes. This location information is used to set up a grid of sensor nodes scheduling some nodes to be put off to conserve energy and consummately extend the network lifespan. The grid arrangement used in GAF is intrinsically ordered at levels of clusters using nodes location information. A cluster representative is tasked to transmit perceived intra cluster data to other external nodes [4].

4.2.2 Geographic and Energy Aware Routing (GEAR)

In directed diffusion, interest messages are sent to all regions of a network. In GEAR, the object is to direct such interest message to a select section of the network instead of to all as is the case in Directed Diffusion. Similar to GAF, GEAR uses location information from a GPS to transmit interest to selected regions of the entire network.

4.2.3 Minimum Energy Communication Network (MECN)

Minimizing network energy consumption using low power GPS devices is the aim of MECN. With a high-end node as a focal node, MECN develops a minimal power topology for each node. Each of these nodes transmits to a relay region of surrounding nodes through routes that are energy efficient. Node to node transmission is based on a sub set of nodes that consumes less power. Optimal routes to achieve power efficiency in MECN is based on nodes position. Coordinates tracked using GPS. MECN is scalable and self-configuring as to allow elimination and addition of new sensor nodes. The assumption in MECN is that node is able to transmit to each other. This may not be the case in regions where obstacles separate two or more nodes. This deficiency in MECN is minimized with Small MECN that is built to deal with network-based obstacles.

4.3 Quality of Service (QoS) Based Protocols

Many wireless sensor networks are formed to meet user specified QoS requirements. Quality metrics such as delay, throughout and reliability of data emanating from different sensor nodes are the design objectives of some application areas. Few network flow and QoS-based protocols consider these and other quality of service metrics in building paths in the sensor network. QoS-based protocols include the very first of this class of protocols - Sequential Assignment Routing (SAR) proposed in [36]; Maximum Life Energy Routing (MLER) proposed in [37]; QoS-aware MAC is proposed in [38] and Reinforcement Learning based MAC (RL-MAC) proposed in [39].

4.4 Hierarchical Routing Protocols

A major shortfall of the protocol classes discussed already is the absence of clustering and leadership in sensing duties. Sensor node clustering is an option that allows additional similar and dissimilar nodes in the network as well as provides for extended coverage and communication distances by forming communities of nodes. Clustering offers invaluable mechanism to enhance the efficiency of a WSN and stabilize the quick energy dissipation of the energy reserve of sensor nodes. Clustering benefits the network by improving upon network performance [12].

Cluster-based approaches are particularly useful for environment monitoring [40]. Clustering is thus by far the better option to conserve the energy consumption of sensor nodes by utilizing relatively high-powered nodes for the task of data transmission. The benefits of clustering include scalability, long network lifetime, and energy efficiency. Clustering options include static clustering and dynamic clustering. In static clustering-based Routing Protocols, clusters once formed remain same throughout the network lifetime. That is clusters are formed once at the start of the network operation and remain same throughout the operational life the network. The advantage of static clustering is that clustering is not needed. Nonetheless, the drawback is that when the cluster head is overworked and its energy is exhausted, its cluster members will lose connectivity with the sink. Even though static clustering removes the overhead of dynamic clustering, static clustering and conventional protocols such as direct transmission, minimum-transmission energy and multi-hop routing may not be optimal for sensor networks [32]. For instance, when traditional static clustering algorithm is used, as soon as the cluster-head node dies, all nodes from that cluster effectively die since there is

no way to get their data to the base station. In dynamic clustering-based protocols, clusters are formed and change (diminish or increase) dynamically across the network lifetime. The concern with adaptive clustering is the added overhead resulting from rotation of the cluster headship, advertisement of cluster head status and the like. Yet still advantages of dynamic clustering far outweigh those of static clustering [32]. Hierarchical routing applies clustering technique o route data from a wireless sensor network to a target use base [32]. Hierarchical routing puts nodes into at least two hierarchies making it energy efficient. One tier of nodes are high energy nodes which take part in processing and sending of information. The other order of nodes are low energy nodes which are basically used sensing function only. In such protocols, the two levels of sensor nodes combine to form a cluster. Cluster heads with considerably higher energy are used to process and send aggregated attribute valuess to the sink. In addition to routing data to sink node, cluster heads have the responsibility of data processing and fusion. Cluster heads are often selected based on network parameters that enhances the extension of the lifespan of the entire network. Randomized selection was originally proposed in [32] but have been proven to be ineffective as it does not consider the energy reserves of the nodes selected for the headship. Improvements have appeared in several works that rather than base cluster headship on a random process, considers network and node parameters such as distance, energy reserve, link strength, node position and more with their fine combination in selecting cluster head. Hierarchical routing protocols can be sub classified into the following [26]:

1. Single-Hop Clustered Routing
2. Multi-Hop Clustered Routing
3. Multi-Hop Chain Routing
4. Multi-Hop Grid Based Routing

4.4.1 Single Hop Clustered Routing

In single-hop clustered routing, upon reception of data from cluster members, the cluster head performs the required data processing and aggregation and communicates the data to the sink directly in a single hop. Single-hop clustered routing protocols include LEACH, LEACH-C and LEACH-Enhanced.

4.4.2 Multi-Hop Clustered Routing

In contrast to single-hop routing, in multi-hop clustered routing, data received from cluster members by the cluster head are communicated with the other cluster heads that are on route that reduces the transmission energy to reach the data to the sink. It is similar to that of single-hop, but it communicates with multiple nodes to transmit the data to base station. Multi-hop clustered routing protocol include; Threshold Sensitive Energy Efficiency Sensor Network (TEEN), Threshold Sensitive Energy Efficiency Sensor Network (APTEEN), BCDCP, Hybrid Energy Efficient Distributed Clustering (HEED), Energy Efficient Uneven Clustering (EEUC), Extended Lifetime of Cluster-Head (ELCH), Scaling Hierarchical Power Efficient Routing (SHPER), Energy Efficient Cluster Head Selection and Data Coverage (EECHDC) and Least Power Adaptive Hierarchy Cluster (LPAHC).

4.4.3 Multi-Hop Chain Routing

In order to reduce transmission energy, nodes in a multi-hop chain routing form a chain series of nodes. Data is forwarded from one node to the other on the chain. At each stop node the data aggregated and push further to the next node until it is at the designated base station. Chain based multi-hop routing protocols include Power-Efficient Gathering in Sensor Information Systems (PEGASIS), Power Efficient Data Gathering and Aggregation Protocol (PEDAP), General Self-Organized Tree-Based Energy-Balanced Routing Protocol (GSTEB) and Sleep/Wake Schedule.

4.4.4 Multi-Hop Grid Routing

Nodes in multi-hop grid routing form a grid pattern to transmit the data to the sink and data reception and transmission takes place in such a grid pattern throughout the network. Grid based multi-hop routing protocols include Virtual Grid Architecture Routing (VGA), Two-Tier Data Dissemination (TTDD) and Grid-Based Data Dissemination (GBDD).

5. LOW ENERGY ADAPTIVE CLUSTERING HIERARCHY (LEACH)

LEACH is a pioneer energy efficient hierarchical clustering protocol that has inspired the design of many variants yet often improved routing protocols. LEACH is an adaptive clustering protocol than uniformly distributes the data transmission task among sensor nodes in network.

LEACH uses the clustering technique to organize nodes into a community of nodes with a randomly selected number of heads for each community of sensors known as cluster head. Cluster heads are chosen randomly and the number of cluster heads for a given sensor network according to the LEACH arrangement matches the number of clusters which is determined before the start of the network operation.

LEACH appeared as an improvement to the traditional static clustering that had the clusters and cluster head fixed though out the life history of the sensor network. Static clustering had the disadvantage of burdening selected cluster heads and they often die pretty quickly disallowing it members to contribute useful sensed data to the sink.

The LEACH approach allow dynamism in cluster formation and headship selection. Such dynamic clustering process allow the high demanding cluster head duties to be rotated amongst cluster member curing the quick drainage of battery power of a particular sensor node as in common in conventional clustering algorithms. In another respect, LEACH's energy efficiency is borne out of the performance of local data fusion by cluster heads data coming from cluster members before sending the compressed data to the sink node. Nodes become cluster heads once in the life time of the network and election chances is based on probability at each given time round. Nodes that become cluster heads need to inform cluster members about their new status. They do this through an advertisement packet containing their new status to other sensors in the network. Non-cluster members that receive this advertisement packet determines which cluster they wish to be members of often based on the strength of advertisement packet. Once cluster membership is finalized, each cluster head creates a TDMA transmission schedule for their respective cluster members. Cluster members transmit data to the cluster head only at their allotted time slide. In this vain, the transmission radio of non-transmitting nodes is put off at all periods when the node is not transmitting. This is one way in which energy is conserved in LEACH. When all the data from cluster members reach the cluster head, data aggregation takes place to eliminate any redundancies and to

reduce the size of final data that is transmitted to the sink node.

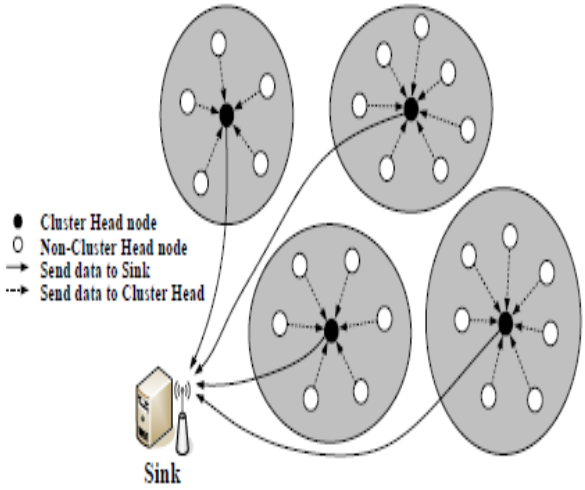

Fig 6: Depiction of the LEACH Protocol

The Operation of the LEACH Protocol

The LEACH operation is summarized in figure 7.

The operation of LEACH is divided into two phases (rounds). Phase one involves setting up of the clusters and the selection of a cluster head and phase two involves data sensing and transfer from non-cluster nodes to the cluster-head and data aggregation and transfer from cluster heads to remote base station [40].

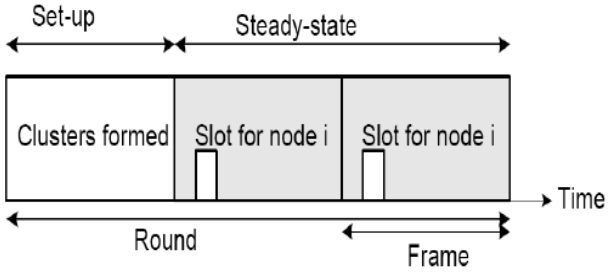

Fig 7: The LEACH setup phase [32]

LEACH disallows long-distance communication with the base station whiles no knowledge of the exact location of any of the nodes in the network is provided. In addition, no global communication is needed to set up the clusters. For homogeneous WSN, cluster formation should be done in such a way as to give each network node equal headship turns. In LEACH a cluster head is determined based on the selection of a random number r, valued between 0 and 1. If the random number r is less that the threshold value ρ (formulae given below) then the sensor node becomes the cluster head for the current round.

$$\rho(n) = \begin{cases} \frac{p}{(1-p)*\left[rmod\left(\frac{1}{p}\right)\right]} & n \in G \\ 0 & Otherwise \end{cases} \quad (1)$$

The equation [32], above incorporates the desired percentage to become a cluster-head, the current round, r, and the set of nodes that have not been selected as a cluster-head in the last $(1/p)$ rounds, p is cluster head probability. In each round the selected cluster head broadcasts an advertisement message containing information about its new status as the head of the cluster to all of its neighbouring nodes. Based on the received signal strength of each advertisement message, non-cluster head nodes decide which of round's cluster head it would become a member of by appropriately sending a joint request message. Once cluster member is decided, each cluster head sets up a Time Division Multiple Access (TDMA) schedule and transmits this schedule to the nodes in each cluster. A TMDA schedule benefits the network in two ways; (1) it ensures that there are no collisions data transmission and (2) It allows the normal nodes to go into a state of dormancy, thus minimizing the energy dissipated. The LEACH protocol makes the following assumptions about the sensor nodes and the underlying network [32].

1. Sink is located in the center of the node deployment area, and has unlimited amount of energy.
2. Sink and sensor nodes are stationary once they are deployed.
3. Sensor nodes are homogeneous and are assigned unique identifier.
4. Sensor nodes have limited amount of energy.
5. Sensor nodes are capable of transmitting with different power levels to the target recipient.
6. Sensor nodes are capable of communicating with each other and sink.
7. Sensor nodes always have some data to be sent.
8. Communication links are symmetric.
9. Cluster Heads always receive highly correlated data from the member nodes. Thus, data aggregation is possible.

Many drawbacks exist in the original LEACH protocol chiefly because each cluster head communicates with the sink node that may be far apart from the cluster heads and again because cluster heads are always on, energy consumption is often high and cluster heads do die pretty faster than the normal nodes. Consequently, when majority of the cluster heads die, the connectivity between the non-cluster nodes and the cluster heads diminishes and disintegrates the affected clusters. Beside this, LEACH does not provide a definite answer to the number of cluster heads in the network. Also, the randomized division of clusters can cause uneven distribution of clusters. Uneven distribution can come about as a result of differences in cluster membership. It could also arise because of the position of a cluster head compared to other member nodes. This disproportionate distribution of clusters increases the energy consumption in transmitting data to cluster heads and the attendant impact on the quality of the network performance. These and more of the drawbacks of the LEACH protocol has led to new extended versions. LEACH-Centralized (LEACH-C), Fixed Cluster LEACH, Enhanced-LEACH (E-LEACH), Mobile-LEACH (M-LEACH), LEACH-Advanced (LEACH-A) and Balanced-LEACH (LEACH-B) [41].

5.1 LEACH-Centralized (LEACH-C)

LEACH-C is a proposal in [42]. The setup of LEACH-C is similar to LEACH except in the criteria for selecting cluster heads. In LEACH-C, the sink node takes responsibility of cluster head selection. A centralized simulated annealing algorithm [26] is used in which the base station uses nodes position information and energy levels to nominate cluster heads for each round of the network operation. The first benefit of LEACH-C is the formation of good clusters.

Secondly, it balances the energy load among all the sensor node. Clusters are formed based on minimal power required to transmit data to the appointed cluster heads.

[43] improves LEACH-C with the Low-Energy Adaptive Clustering Hierarchy-central constrained (LEACH-CC), by means of changing range of nodes that have ever been cluster head achieving a network of balanced energy distribution.

5.2 Fixed-Cluster LEACH (LEACH-F)

In [42] LEACH-F is proposed as a fixed cluster version of LEACH-C. LEACH-F uses the same algorithm implemented in LEACH-C to form clusters but the cluster once formed remain unchanged through the lifespan of the network. However, the cluster head position is shared periodically by nodes in a cluster as is the case in LEACH-C.

5.3 Enhanced-LEACH (E-LEACH)

E-LEACH is more LEACH than LEACH-C as it uses near the same setup. In the first round, as in LEACH [32], cluster heads are selected randomly using the same random probability distribution as in equation (1) above. In subsequent rounds afterwards, cluster head selection is based on remnant energy of the node. Nodes with highest remaining battery energy are elected as cluster heads each round. The steady state phase in E-LEACH is same as in LEACH [26].

5.4 Mobile-LEACH (M-LEACH)

The assumption in LEACH is that nodes are immobile. However, mobility is required sometimes for all or some of the sensor nodes especially when it is crucial to dynamically vary the placement of cluster heads and bases stations for energy efficiency. Mobile-LEACH is proposed to provide such mobility support. In Mobile-LEACH, sensor nodes can move but sink node like in LEACH is assumed to be fixed. In the setup phase of Mobile-LEACH, cluster heads are selected based on minimum mobility and minimum energy reduction. Selected cluster heads transmit their new status and position via GPS to the other reachable non-cluster nodes. Non-cluster nodes then decide which cluster head to join. Mobile-LEACH offers an efficient mechanism for nodes to switch on to new cluster-head to deal with the problem of ineffective cluster formation in LEACH.

5.5 LEACH-ADVANCED (LEACH –A)

LEACH-A is a LEACH type protocol developed to enhance reliable data transfer and improve energy conservation by using mobile agents – CAG nodes. These CAG nodes are built with extra energy than other sensor nodes and as a result are assigned with the duty of acting as gateway or cluster heads. All other nodes are used for data sending and transmission functions only.

5.6 LEACH-B (Balanced LEACH)

LEACH-B applies a decentralized algorithm to form clusters. In LEACH-B instead of the sink tracking the location information of sensor nodes, the sensor nodes themselves are equipped with location information about themselves and other nodes. Each sensor node uses this location information to decide on its cluster head by measuring the energy lost in the path between it and the advertised cluster heads. LEACH-B offer better network benefits and performance compared to the parent LEACH protocol.

6. NON-LEACH TYPES PROTOCOLS

Many routing protocols exist that are structured in a dissimilar manner from the LEACH protocol. These include; Threshold Sensitive Energy-Efficient Sensor Network (TEEN), Adaptive Threshold Sensitive Energy-Efficient Sensor Network (APTEEN), Power-efficient Gathering in Sensor Information System (PEGASIS), Hybrid Energy Efficient Distributed Clustering (HEED), Stable Election Protocol (SEP), Energy-Efficient Chain-Cluster Routing (ECR) and EERP.

6.1 Threshold Sensitive Energy-Efficient Sensor Network (TEEN) And Adaptive Periodic TEEN (APTEEN)

The protocols TEEN and its improvement APTEEN are proposed by [44] and [45] respectively for time critical application. Time critical applications are special application area of wireless sensor networks that require timely alert on changes to sensed attributes like temperature. TEEN was the first to be designed for such time-critical applications. Cluster formation starts the network operations in TEEN. After the clusters are formed, the cluster head broadcasts two threshold values to cluster members. These threshold values represent hard and soft thresholds for the sensed data. Considering the fact that the transmission functions of a sensor node constituent the bulk of its energy needs, the threshold values are specified to minimize the number of transmissions in the network. The specification of the hard threshold is to allow nodes to only transmit if and only if the sensed data within the threshold limit. The soft threshold is specified to allow transmission if there is small change in the value of the required data.

APTEEN is similar to TEEN in many ways including its application area but treats the sensed attribute differently. When the sense attribute exceeds the specified hard threshold, its value is measured against the value of the soft threshold. Data transmission only take place when the value of that attribute is modified by an amount not less than the soft threshold. Cluster formation in both TEEN and APTEEN are more complex in addition to the energy overhead.

6.2 Power-efficient Gathering in Sensor Information System (PEGASIS)

One of the many challenges often mentioned about the LEACH protocol is the added overhead resulting from the dynamic cluster formation. In [46] , the LEACH protocol is extended with the introduction of a chain-based protocol called PEGASIS that rather than gernerate clutters of nodes, forms a chain of neighboring nodes with one of the nodes in the chain talked with the headship responsibility. Node on a chain transmit and receives data from each other. When the chain head receives data, it transmits it directly to the sink. PEGASIS increases the lifespan of a sensor network through its coordinated reception and transmission of data among neighbor nodes as bandwidth consumed is minimal. Additionally, the number of transmission and receptions in PEGASIS is reduced as an outcome of data aggregation. This benefit however is offset by the length of time it takes distant node to transmit.

6.3 Hybrid Energy Efficient Distributed Clustering (HEED)

HEED is proposed in [47] to extend the basic scheme of LEACH. HEED remedies the sole reliance on random processes for the determination of cluster head and cluster sizes. HEED uses two network parameters for cluster selection - primary parameter and a secondary parameter. The primary parameter is the remaining energy of nodes which is used to evaluate the chance of a node to become a cluster head. The secondary parameter counts the number of nearby

nodes associated with each sense node. The primary parameter is used as an initial bases to select a set of cluster heads. Where ties exist, the secondary parameter is used for tiebreaking. Cluster heads selected out of the HEED scheme are well distributed across the network. However, basing cluster head selection of just two of parameters of many of the networks makes it suitability and benefits for the entire wireless sensor network needs limited.

6.4 Stable Election Protocol (SEP)

Many LEACH-type schemes are setup with the assumption that nodes of the sensor network are of the same energy levels. Such schemes are homogeneous sensor networks. SEP, proposed in [48] introduces heterogeneity as an extension to the LEACH protocol. In [48] heterogeneity is suggested to be achieved by boosting the sensor network with advance nodes that have more energy than normal nodes. Thus, SEP considers two types of nodes and two-level hierarchies [49].

Cluster headship in SEP is based on respective weighted probabilities of each node which take into consideration the initial energies of nodes. The stability period which is marked by the time passed before the death of the first node is prolonged. SEP is useful for applications where the reliability of data is of utmost priority.

6.5 Energy-Efficient Chain-Cluster Routing (ECR)

The drawbacks of LEACH essentially arise from the fact that cluster head selection is randomized. ECR proposed in [50] removes the randomness in cluster head selection by using a greedy algorithm instead to select sensor nodes with maximum rest energy in order to balance energy consumption. ECR outperforms both LEACH and PEGASIS in terms of energy efficiency. ECR protocol is good, it has some drawbacks. The algorithm used in ERC causes unnecessary delay in data transmission. It also suffers for the early death of cluster heads causing sections of the network to be not surveyed.

6.6 Energy Efficient Routing Protocol (EERP)

Nodes typically come with an assigned maximum transmit power. In many schemes, nodes transmit at this power irrespective of the distance between the communication nodes resulting in unwanted power dissipation. EERP avoid this by adjusting the threshold transmission radius in order to reach the furthermost neighbor. It then sends the first packet to such node. The readjustment is particularly necessary, when the node remaining energy reaches a threshold level. Additionally, EERP establishes an on-demand route finding process to transmit to nodes that are not present in its routing table. The on-demand route finding process in EERP conserves energy. When node typology changes as a result of loss of a node or change in node radius, a route maintenance process is triggered. The EERP protocol is hence a four-part process made up of initial transmission radius selection, route discovery, transmission radius readjustment and route maintenance. The EERP protocol consumes less energy compared to LEACH, PEGASIS, TEEN and ERC. It has a longer network lifetime too. Table 3 gives a comparison of the LEACH protocol as against its variants and other non-LEACH type protocols.

Table 3. Comparison of LEACH and non-LEACH type protocols. Adapted from [51].

Routing Protocol	Power Management	Latency	Stability Period	Scalability	Load Distribution	Protocol Complexity
LEACH	Very low	Very small	Moderate	Very limited	Moderate	Low
HEAD	Moderate	Moderate	High	Moderate	Moderate	Moderate
UCS	Very low	Small	High	Limited	Bad	Moderate
EECS	Medium	Small	High	Limited	Moderate	Very high
CCM	Very low	Small	High	Very limited	Moderate	Moderate
LEACH-VF	Moderate	Small	High	Very limited	Moderate	Moderate
MWBCA	Moderate	Very small	Moderate	Very limited	Very good	Moderate
HCTE	Very low	Very small	Moderate	Very limited	Very good	Moderate
GAF	Moderate	Very small	Moderate	Large scale	Moderate	Moderate
PANEL	Moderate	Moderate	Low	Limited	Good	High
TTDD	Very low	Very large	Very high	Limited	Good	Low
HGMR	Low	Moderate	High	Very limited	Bad	Low
SLGC	Moderate	Very small	Moderate	Very limited	Moderate	Moderate
PEGASIS	Low	Very large	Low	Very limited	Moderate	High
CCS	Low	Large	Low	Limited	Very bad	Moderate
TSC	Moderate	Moderate	Moderate	Moderate	Bad	Moderate
TEEN	Very high	Small	High	Limited	Good	High
APTEEN	Moderate	Small	Very low	Limited	Moderate	Very high

7. SECURITY ISSUES IN THE LEACH PROTOCOL

The clustering approach used in the LEACH protocol makes it difficult to attacks compared to multi-hop protocols. In multi-hop protocols, nodes that are near the sink acts as relay nodes for other remote nodes and transmit data to the sink. Not only are they prone to early death but also are attractive to enemy attack. The strength of LEACH against such security compromises is because cluster heads which are the only nodes that directly communicate with the sink have no fixed location. They are also periodically changed in round turns and so attacks on these cluster heads is difficult (not impossible). However, when a cluster head is attacked, it impacts on network performance is devastating. Why because in LEACH, the cluster heads play central role in the data gathering duties of the sensor network by receiving, aggregating and forwarding required data to the sink. When an adversary succeeds in an attack involving one, some or all of the cluster heads then it can cause the most damaging of impacts on the network's activities. For instance, if an attacker infiltrates the sensor network with a cluster head node, then the attacker can advertise this node using the strongest signal causing every node to join it as their cluster head. If such situations, the intruder can selectively forward information to the sink or modify or dump information about the sense phenomena. LEACH protocol is susceptible to attacks such as Sybil, selective forwarding and Hello flooding which degrade the performance of a sensor network [52].

7.1 Sybil Attack

Sybil attacks are based on identity theft. An adversary infiltrates the network with a node that has the same identity as of many other legitimate nodes in order to reveal and use communication data between trusted nodes. Such attacks affect the network in many ways including packet drops, flooding the network with packets and consequently reducing network lifetime. These forms of network attacks are the most difficult to identify. Many encryption and authentication methods can guard a network against Sybil attack [53] [54].

7.2 Selective Forwarding

Another of the attacks on the LEACH protocol is selective forwarding. This attack allows an attacker gain access to a communication path of two legitimate nodes. It intercepts the data communicated by the legitimate nodes in the path. In the mildest of selective forwarding attack, the malicious node instead of forwarding the intercepted data drops it against reaching the destination node. In the worst form of selective forwarding attack, the malicious nodes instead of dropping the data selectively forwards the non-essential bits of the data. This case of selective forwarding is the most malignant and difficult to detect [54].

7.3 HELLO Flooding Attack

Many a times when nodes need to send data, they send an advertisement packet that gives a measure of how far they are from their neighbors. In hello flooding attack, an adversary node would overflow the network with a succession of Hello advertisement packets in an attempt to increase the network traffic and cause collisions. HELLO flooding attack drains the energy of sensor nodes with the incessant HELLO packets thereof shortens the lifespan of the larger network [54].

7.4 Wormholes

A wormhole attack involves an enemy rechanneling a message to poor latency paths and to other parts. Wormhole attacks causes a misjudgment of the distance between nodes by routing packets along an external route that is accessible only to the adversary. The big damage of wormhole occurs when an attacker succeeds in situating itself close to the sink and disrupts packet transmission to the sink. Worm hole can be devastating when combined other attack types like eavesdropping, selective forwarding and Sybil attack [53] [54].

7.5 Sinkhole Attack

Single point base station is the dominant provision in many wireless sensor networks. All sensed data are forwarded directly or via other nodes to the base station as the ultimate destination. This makes wireless sensor networks prone to sinkhole attacks.

In sinkhole attack, a mythical sinkhole is created by an attacker and diverts network data routing through to it. Sinkhole attack starts off with an attacker taking control of a compromised node and making it attractive in its route quality to neighboring nodes thereby diverting data transmission to it. Since all data are routed through the compromised node, data could be selectively forwarded, replayed, spoofed and altered in ways the attacker deems damaging [54].

8. SOME SECURITY BASED LEACH PROTOCOLS

Many protocols have appeared to provide varied levels of protection to the conventional LEACH protocol with wide-ranging successes and applicability. SLEACH is the first of such protocol to provide some semblance of security to the LEACH protocol against outsider attack. SLEACH proposed in [55] studied the challenge of securing node to node communication in situation of constrained energy capability of sensor nodes. The security provision in SLEACH is based on the combined strength of Security Protocol for Sensor Network (SPINS), symmetric-key methods and Message Authentication Code (MAC). SLEACH is successful in curtailing bogus data to and from cluster heads as well as curbing attacks such as Hello flooding, selective forwarding and sinkhole attack.

However, sensor networks based on the SLEACH are still opened to DoS attacks and bridges of data confidentiality. The FLEACH protocol is proposed in [55] to offer security to a LEACH based network during node to node communication. FLEACH security strength including authenticity, integrity and confidentiality lies in the use of both a random key pre-distribution technique and a symmetric FLEACH combines a random key pre-distribution scheme and symmetric cryptographic schemes. In [56] the efficient security model of routing is proposed for securing the LEACH protocol against external attacks. ESMR uses only public key cryptography technique and it proven to be much efficient in environments where attack cases are more and common. However, ESMR suffers from similar computational challenge as in [57] due to the use of public key cryptography. In [57] a cluster based secure routing protocol for wireless sensor network is proposed to deal with insider attacks and security holes. It is a security protocol based on the LEACH protocol that uses both public key and private key cryptography. Considering the already limited energy resource and computational limitations of sensor nodes, the practicability of the security protocol presented in [57] is not worthwhile because of the use of public key cryptography, which is computationally intensive. Sec-LEACH is proposed in [58] to provide an efficient communication security in LEACH. Sec-LEACH ensures confidentiality by using a randomly generated symmetric keys and a uni-directional hash chain. In [59] a secure hierarchical

protocol, SS-LEACH is proposed. SS-LEACH uses key pre-distribution and self-localization techniques to provide security to the LEACH protocol. SS-LEACH bars compromised nodes from partaking in network activities and as well preserves the confidentiality of shared packets. Beyond providing strong security measure against selective forwarding, HELLO flooding and Sybil attack, the SS-LEACH protocol extends the lifespan of a sensor network through an improved cluster head election method. A secure solution for LEACH, RLEACH is presented in [60] where a one-way hash chain, symmetric and asymmetric cryptography is used to provide security in the LEACH protocol. The strengths of RLEACH is in its resistance to attacks such as Sybil attack, HELLO flooding, selective forwarding, sinkhole and wormhole attacks. A Novel Hierarchical Routing Protocol Algorithm for wireless sensor network (NHRPA) is proposed in [61] that deals with the node compromise attack. The routing technique used in NHRPA is based on the better combination of node distance to the sink node, node density and residual energy. Unlike the protocols discussed supra, NHRPA does not use any cryptographic scheme as such its computational overhead is minimal. Additional to the security benefits, NHRPA offers more efficiency in terms of energy consumption and packet delivery rate better than the likes of LEACH, PEGASIS and Directed Diffusion.

9. SIMUATION TOOLS FOR WIRELESS SENSOR NETWORKS

In WSN research, simulation tools are the common means often used to imitate the behavior of sensor nodes and measurement of required performance metric due to the intricacies and the lack of access to the networks in some terrains. The need for simulation is for the evaluation of the performance of a wireless network in different dimensions as per the application area. Additionally, these tools help WSN researcher's inexpensive means to evaluate the feasibility and practicability of schemes before deciding to channel research funds into actual implementation. There are simulation tools for general purposes and there are those that are design for specific WSN applications. Different generic network simulator exists including Network Simulator (NS-2), Object Modular Network Testbed (OMNET++), J-Sim, NCTUns2.0, JiST/SWANS, GloMoSim, SSFNet, Ptolemy II. WSN simulation tools for specific purpose include; TOSSIM, EmStar /EmSim /EmTOS, ATEMU, SENSE, Prowler/JProwler, SNAP [62], [63].

Table 4. Wireless sensor network simulators compared [64]

Tools Features	Interface	Accessibility & User Support	Availability of WSNs Modules	Scalability
NS-2	Built with C++/OTcl and with limited visual support	Provides better user support and offers open source capabilities.	Provide excellent WSNs code units	Low
OMNeT++	Built using C++/NED and provides friendly GUI and debugging capabilities	Commercially available to users. User support provisions good.	Provides excellent WSNs code units	High
GloMoSim	Built on C-based Parsec. Visual support is inadequate	Available to user on open source terms, but the user support provision is poor.	Provides good WSNs code units	High
OPNET	Built using C++ or C or java and provides friendly GUI and debugging capabilities	Commercially available to users. User support provisions good. It is accessible to the academic community free	Provide excellent WSNs code units	Moderate
SENSE	Built using C++ and present a friendly user interface	Available to users free and on open source terms. User support provisions poor rather.	Provides excellent WSNs code units	High
TOSSIM	The interface is good and based on C++/Python	Available to users on a free as well as excellent user support provisions.	Provides good WSNs code units	High
GTSNetS	Developed using C++ with enhanced user interface and visual support	Available to users on open source terms, User support provisions poor	Provide excellent WSNs code units	Very High

10. CONCLUSION

Intelligent monitoring and reporting of environmental data and beyond are infinitely beneficial to humans and human society. Wireless sensor networks coupled with advances in MEMs technologies have enhanced the widespread use of micro sensor for data gathering and transmission. The dominant areas of challenge in wireless sensor networks includes issues of scalability, fault tolerance, typology control node cost, node mobility, heterogeneity, QoS, coverage and connectivity and network lifetime extension. All of these arise chiefly because of the limited energy resource caused by a non-reachable and irreplaceable low power battery. Constraints in node battery life directly affects the network lifetime of WSNs. Efficient use of sensor battery is therefore imperative. Many protocols for routing data in a wireless sensor networks and enabling energy efficiency have been proposed which fall into one of the three categorizations by network structure. According to network structure WSN's operation can be data centric, location based or hierarchical.

Hierarchical routing which applies a clustering approach to data transmission in wireless sensor network are dominantly used to prolong the lifespan of a wireless sensor network for real world application because of the often-large number of nodes deployed to a sensing field. This routing technique is energy efficient in that nodes are put into at least two hierarchies of nodes. One order of nodes are high energy nodes which take part in processing and sending of information. The other order of nodes are low energy nodes which are basically used sensing function only. In such protocols, the two levels of sensor nodes combine to form a cluster. In hierarchical routing, non-head nodes with comparatively low-energy are used to perform the sensing function in the sensed field transmit to the cluster head. The survey then perused through routing protocols for energy efficiency in wireless sensor networks, looking at both LEACH and non-LEACH protocols. Even though LEACH has gained household popularity, many of the non-LEACH protocols have proven adequately useful in some deployment areas. Many research gaps still existing that can be explored to further enhance the lifetime challenge in wireless sensor networks.

11. ACKNOWLEDGMENTS

Our heartfelt appreciation to the anonymous reviewers for their useful insight regarding the structure and contents of this article.

12. REFERENCES

[1] Akyildiz, I.F., Su, W., Sankarasubramaninam, Y., and Cayirci, E. 2002. Wireless sensor networks: a survey. Computer Networks, 30.

[2] Kochlan, M. Zak, S. Micek, J. and Milanova. J. 2015. Control unit for power subsystem of a wireless sensor node. In Proceedings of the 2015 Federated Conference on Computer Science and Information Systems (FedCSIS'15). IEEE, 1239–1246. DOI: http://dx.doi.org/10.15439/2015F355.

[3] Basagni, S. Conti, M. Giordano, S. and Stojmenovic. I. 2013. Mobile Ad Hoc Networking: The Cutting-Edge Directions. Vol. 35. John Wiley & Sons, New Jersey.

[4] Yang, Z., and Mohammed, A. 2010. A Survey of Routing Protocols for Wireless Sensor Networks, Sustainable Wireless Sensor Networks (Y. K. Tan, Ed.). Retrievedfromhttp://www.intechopen.com/books/sustainable-wireless-sensor-networks/a-survey-on-routing-protocolsfor- wireless-sensor-networks

[5] Estrin, D. Sayeed, A. and Srivastava, M. 2002. Wireless sensor networks. In Proceedings of the Tutorial at the 8th ACM International Conference on Mobile Computing and Networking (MobiCom'02), Vol. 255. ACM, New York, NY.

[6] Devasena, A. and Sowmya, B. 2015. Wireless sensor network in disaster management. Indian J. Sci. Technol. 8, 15, 6.

[7] Kim, S., Pakzad, S., Culler, D.E., Demmel, D., Fenves, G., Glaser, S. and Turon, M. 2007. Health monitoring of civil infrastructures using wireless sensor networks, Proceedings of the 6th International Conference on Information Processing in Sensor Networks.

[8] Hu, X., Wang, B. and Ji, H. 2013. A Wireless Sensor Network-Based Structural Health Monitoring System for Highway Bridges Article in Computer-Aided Civil and Infrastructure Engineering 28(3). DOI: 10.1111/j.1467-8667.2012.00781.

[9] ELkhediri, S. Nasri, N. Kachouri, A. 2011. Synchronization Issues in Wireless Sensors Networks, IEEE the 23 International Conference of Microelectronics. TUNISIA: ICM, 2

[10] Chong, C. Y., & Kumar, S. P. 2003. Sensor networks: evolution, opportunities, and challenges. Proceedings of the IEEE, 91(8), 1247-1256.

[11] Yoneki, E. and Bacon, J. 2005. A survey of Wireless Sensor Network Technologies: Research Trends and Middleware's Role. A technical Report, No. 646.

[12] Adu-manu, K.S., Adam, N., Tapparello, C., Ayatollahi, H. and Heinzelman W. 2018. Energy-Harvesting Wireless Sensor Networks (EH-WSNs): A Review. ACM Trans. Sen. Netw. 14, 2, Article 10

[13] Pantelopoulos and N. G. Bourbakis, 2010. A survey on wearable sensor-based systems for health monitoring and prognosis, IEEE Trans. Syst. Man Cybern. Part C Appl. Rev., vol. 40, no. 1.

[14] Omer, R. M.D. and Al-Salihi, N. K. 2017. HealthMate: Smartwearable system for health monitoring (SWSHM). In Proceedings of the 2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC'17). IEEE, 755–760.

[15] Owa, F. W. 2014. Water pollution: Sources, effects, control and management. Int. Lett. Natural Sci. 3, 6.

[16] P. J. Landrigan and R. Fuller. 2016. Pollution, health and development: The need for a new paradigm. Rev. Environ. Health 31, 1, 121–124.

[17] Derbew, Y. and Libsie, M. 2014. A wireless sensor network framework for large-scale industrial water pollution monitoring. In Proc. of IST-Africa Conference.

[18] Jiang, P. Xia, H. He, Z. and Wang., Z. 2009. Design of a water environment monitoring system based on wireless sensor networks. Sensors 9, 8 2009, 6411–6434.

[19] Zhu, X. Li, D. He, D. Wang, J. Ma, D. and Li, F. 2010. A remote wireless system for water quality online monitoring in intensive fish culture. Computers and Electronics in Agriculture 71, S3–S9.

[20] Nasirudin, M. A., Za'bah, U.N. and Sidek, O. 2011 Fresh water real-time monitoring system based on Wireless Sensor Network and GSM. In Proc. of the IEEE Conference on Open Systems (ICOS). IEEE, Langkawi, Malaysia,354357.DOI:http://dx.doi.org/10.1109/ICOS.2011.6079290

[21] Rabaey, J. M., Ammer, M. J., da Silva, J. L., Patel, D. and Roundy S., 2000. PicoRadio Supports Ad Hoc Ultra-Low Power Wireless Networking. IEEE Computer, Vol. 33, No. 7.

[22] Pottie, G. and Kaiser, W. 2000 Wireless integrated network sensors. Communication of ACM, 43(5):51–58.

[23] Pradeepaa, K., Raggis Anne, W. and Duraisamy, S. 2012 Design and Implementation Issues of clustering in Wireless Sensor Networks. International Journal of Computer Applications. Volume 47 – 10.

[24] Meena, R. and Talwai, P. 2015 Comparison of Flat Routing Protocols of Wireless Sensor Network.

International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-3, Issue-10.

[25] Devika, R., Santhi, B. and Sivasubramanian, T. 2013. Survey on Routing Protocols in Wireless Sensor Network.

[26] Jothikumar, C., and Venkataraman, R. 2016. A Review of Hierarchical Routing Protocol for Wireless Sensor Network. Indian Journal of Science and Technology, 9(32). https://doi.org/10.17485/ijst/2016/v9i32/76215

[27] Kaur, N., & Singh, T. 2016. A Review of Wireless Sensor Network with Its Applications. 7, 4.

[28] Braginsky, D., & Estrin, D. 2002. Rumor routing algorithm in sensor networks. Proceedings ACM WSNA, in Conjunction with ACM MobiCom'02, 22-31.

[29] Dan, T. V. and Langendoen, K. 2003. An adaptive energy-efficient mac protocol for wirelesssensor networks, the first international conference on Embedded Networked Sensor Systems,ACM press.

[30] Heinzelman, W., Kulik, J., & Balakrishnan, H. 1999. Adaptive protocols for information dissemination in wireless sensor networks. The 5th Annual ACM/IEEE International of the First Workshop on Sensor Networks and Applications (WSNA), Altlanta, GA, USA.

[31] Niculescu, D. 2005. Communication paradigms for sensor networks, IEEE Communication Magazine.

[32] Heinzelman, W., Chandrakasan, A., and Balakrishnan, H. 2000. Energy-efficient communication protocol for wireless sensor networks. The Hawaii International Conference System Sciences, Hawaii.

[33] Hedetniemi, S. M., Hedetniemi, S. T. and Liestman, A. L. 1988. A Survey of Gossiping and Broadcasting in Communication Networks, Networks, Vol. 18, No. 4. doi:10.1002/net.3230180406.

[34] Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. 2000. Protocols for self-organizing of a wireless sensor network. IEEE Personal Communications Journal, Vol.7, No.5.

[35] Chang, J.-H. and Tassiulas L. 2000. Maximum Lifetime Routing in Wireless Sensor Network, in the Proceedings of the Advanced Telecommunications and Information Distribution Research Program (ATIRP'2000), College Park, MD.

[36] Liu, Y, Elhanany, I. and Qi, H. 2005. An energy-efficient QoS-aware media access control protocol for wireless sensor networks. IEEE International Conference on Mobile Adhoc and Sensor Systems Conference. 10.1109/MAHSS.2005.1542798

[37] Liu, Z., and I. Elhanany. 2006. RL-MAC: A QoS-aware reinforcement learning based MAC protocol for wireless sensor networks. In Networking, Sensing and Control.

[38] Bandyopadhyay, S. and Coyle E. J. 2003. An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks, IEEE INFOCOM.

[39] Heinzelman, W., Chandrakasan, A., and Balakrishnan, H. 2000. Energy-efficient communication protocol for wireless sensor networks. The Hawaii International Conference System Sciences, Hawaii.

[40] Barai, Y.L., Gaikwad, M.A. and Bokoe, A.K. 2014. A LEACH protocol for Wireless Sensor Network; A review. International Journal of Computer Applications.

[41] Kaur, A. and Grover, A. 2015. LEACH and extended LEACH protocols in Wireless Sensor Network – a survey. International Journal of Computer Applications. Vol-116, No. 10.

[42] Heinzelman, W., Chandrakasan, A. P., & Balakrishnan, H. 2002. An Application-Specific Protocol Architecture for Wireless Microsensor Networks. IEEE Transaction on Wireless Communications, 1(4).

[43] Ma, Z., Li, G. and Gong, Q. 2016. Improvement on LEACH-C Protocol of Wireless Sensor Network (LEACH-CC). International Journal of Future Generation Communication and Networking Vol. 9, No. 2. DOI:10.14257/ijfgcn.2016.9.2.19.

[44] Manjeshwar, A., and Agrawal, D. P. 2001. TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. Proceedings 15th International Parallel and Distributed Processing Symposium. IPDPS 2001, 2009–2015. https://doi.org/10.1109/IPDPS.2001.925197

[45] Manjeshwar, A., and Agrawal, D. P. 2002. APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks. 8.

[46] Lindsey S. and Raghavendra C. S. 2002. PEGASIS: Power-efficient gathering in sensor information systems, The IEEE Aerosapce Conf.Montana: IEEE Aerosapce and Electronic Systems Society, pp. 1125-1130.

[47] Younis, O. and Fahmy, S. 2004. HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks. IEEE Transactions on Mobile Computing 3(4). DOI: 10.1109/TMC.2004.41

[48] Smaragdakis, G. and Bestavros, I.M. A. 2004. SEP: A Stable Election Protocol for clustered heterogeneous wireless sensor networks, in International Workshop on SANPA.

[49] Kour, H. (2012). Hierarchical routing protocols in wireless sensor Networks. International Journal of Information Technology and Knowledge Management, Volume 6, No. 1.

[50] Tian, Y., Wang, Y., Zang, S.-F. (2007). A novel chain cluster-based Routing protocol for wireless sensor networks, International Conference on Wireless Communications, Networking and Mobile Computing.

[51] Singh, S. P. and Sharma, S.C. 2014. Cluster Based Routing Algorithms for Wireless Sensor Networks. International Journal of Engineering & Technology Innovations, Vol. 1 Issue 4

[52] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, 293–315.

[53] Li, Z. and Gong, G. n.d. A survey of security in wireless sensor networks.

[54] Brindha, P. and Senthilkumar, A. 2016. Security on Wireless Sensor Networks: A Survey, International Journal of Computer Science and Information Technologies, Vol. 7 (6).

[55] Oliveira, L.B., Wang, H.C. and Loureiro, A. 2005. LHA-SP: Secure protocols for hierarchical wireless sensor network. Conference: Integrated Network Management, 2005. IM 2005. 2005 9th IFIP/IEEE International Symposium on DOI: 10.1109/INM.2005.1440767

[56] Zhang H., Chen J. and Hu. J. 2008. An efficient security model of routing protocol in wireless sensor networks. In2008 Second Asia International Conference on Modelling and Simulation, pages 59–64, Washington, DC, USA, 2008.

[57] Reddy A. V., Srinath R. and Srinivasan, R. 2007. Ac: Cluster based secure routing protocol for wsn. In Third International Conference on Networking and Services, page 45, Washington, DC, USA.

[58] Vilaa, M. A., Wong H. C., Bern M., Dahab R., Oliveira, L. B., Ferreira A. and Loureiro. A. A. F. 2007. Sec-LEACH-on the security of clustered sensor networks. (87(12)):2882–2895, December 2007

[59] Hu G., Wu D. and Ni. G. 2008. Research and improve on secure routing protocols in wireless sensor networks. In 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008).

[60] Wang, C., Zhang, K. and Wang. C. 2008. A secure routing protocol for cluster-based wireless sensor networks using group key management. In4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM08).

[61] Geng Y., Hong-bing C. and Su-jun. H. 2008. Nhrpa: a novel hierarchical routing protocol algorithm for wireless sensor networks. China Universities of Posts and Telecommunications.

[62] Levis, P., … 2003. TOSSIM: Accurate and scalable simulation of entire TinyOS applications.In: Proceedings of the 1st International Conference on Embedded Networked SensorSystems. ACM.

[63] Egea-Lopez, E. Vales-Alonso, F, Martinez-Sala, A. S., Pavon-Marino, P, Garcia- Haro, J. 2005. Simulation Tools for Wireless Sensor Networks, Summer Simulation Multiconference, SPECTS.

[64] Khan, M. Z. 2011. Limitations of Simulation Tools for Large-Scale Wireless Sensor Networks, Workshops of International Conference on Advanced Information Networking and Applications.