Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

A Review On Load Balancing In Data Routing Of Wireless Sensor Networks

Dinesh Kumar Gupta and Dr. Deepika Pathak

Department of Application, Dr. A. P. J. Abdul Kalam University, Indore (M.P.) India - 452010

Abstract

Load balancing is a standard functionality of the router software and it is available across all router platforms. It is inherent to the forwarding process in the router and is automatically activated if the routing table has multiple paths to a destination. It is based on standard routing protocols, such as Routing Information Protocol (RIP), RIPv2, Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Interior Gateway Routing Protocol (IGRP), or derived from statically configured routes and packet forwarding mechanisms. It allows a router to use multiple paths to a destination when forwarding packets in Wireless Sensor Network (WSN).

1. INTRODUCTION

WSN is a subset of Ad-hoc networks. WSN consists of specially distributed autonomous sensors to cooperatively monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion etc. Load balancing is a computer networking method to distribute work load across multiple computers or a computer cluster, network links, central processing units, disk drives, or other resources, to achieve optimal resource utilization, maximize throughput, minimize response time, and avoid overload. Using multiple components with load balancing, instead of a single component, may increase reliability through redundancy. The load balancing service is usually provided by dedicated software or hardware, such as a multilayer switch or a Domain Name System (DNS) Server.

When a router learns multiple routes to a specific network via multiple routing processes or routing protocols, such as RIP, RIPv2, IGRP, EIGRP and OSPF, It installs the route with the lowest administrative distance in the routing table. Sometimes the router must select a route from among many learned via the same routing process with the same administrative distance. In this case, the router chooses the path with the lowest cost (or metric) to the destination. Each routing process calculates its cost differently and the costs may need to be manipulated in order to achieve load-balancing.

2. LITERATURE REVIEW

Al-Karaki, J.N. et al [1], proposed the energy efficient routing protocol for wireless sensor networks. The design of energy-efficient protocols for wireless sensor networks (WSNs) is a crucial problem as energy is a strict resource in these networks. They proposed an energy-aware routing protocol using a new approach. This protocol is called high power short distance protocol (HPSD). HPSD is a node-based protocol that selects the route to the base station (BS) based on the closest node that has the highest battery power relative to its surrounding neighbors. Thus, the energy load can be distributed among all sensor nodes instead of using certain path each time. So, HPSD can increase the lifetime of the network.

Xiaoxia Huang, et al [2], proposed the Robust Cooperative Routing Protocol. In wireless sensor network, path breakage occurs frequently due to node mobility, node failure and channel impairments. It is challenging to combat path breakage with minimal control overhead, while adapting to rapid topological changes. Due to the Wireless Broadcast Advantage (WBA), all nodes inside the transmission range of a single transmitting node may receive the packet; hence naturally they can serve as cooperative caching and backup nodes if the intended receiver fails to receive the packet. They present a distributed robust routing protocol in which nodes work cooperatively to enhance the robustness of routing against path breakage. They compare the energy efficiency of cooperative routing with no cooperative routing and show that the robust routing protocol can significantly improve robustness while achieving considerable energy efficiency.

Peter Kok Keong Loh, et al [3], proposed the Reliable Routing Protocols for Fixed-Power Sensor Networks. In this protocol the Fixed-power wireless sensor networks are prevalent and cost-effective. However, they face mote failures, Radio Frequency interference from environmental noise and energy constraints. Routing protocols for such networks must overcome these problems to achieve reliability, energy efficiency and scalability in message delivery. Achievement of these requirements, however, poses conflicting demands. They propose an efficient and reliable routing protocol (EAR) that achieves reliable and scalable performance with minimal compromise of energy efficiency. The routing design of EAR is based on four parameters such as path length, a weighted combination of distance traversed, energy levels and link transmission success history, to dynamically determine and maintain the best routes. Simulation experiments of EAR with four existing protocols demonstrate that a design based on a combination of routing parameters exhibits collectively better performance than protocols based on just hop-count and energy or those using flooding.

Kiran K. Rachuri et al [4], proposed the Energy Efficient and Scalable Search protocol. The proposed protocol is considering the problem of information discovery in a densely deployed Wireless Sensor Network (WSN), where the initiator of search is unaware of the location of target information. They propose two protocols: Increasing Ray Search (IRS), an energy efficient and scalable search protocol, and k-IRS, an enhanced variant of IRS. The priority of IRS is energy efficiency and sacrifices latency where as k-IRS is configurable in terms of energy-latency trade-off and this flexibility makes it applicable to varied application scenarios. The basic principle of these protocols is to route the search packet along a set of trajectories called rays that maximizes the likelihood of discovering the target information by consuming least amount of energy. The rays are organized such that if the search packet travels along all these rays, then the entire land area will be covered by its transmissions while minimizing the overlap of these transmissions. In this way, only a subset of total sensor nodes transmits the search packet to cover the entire land area while others listen. They believe that query resolution based on the principles of area coverage provides a new dimension for conquering the scale of WSN. They compare IRS and k-IRS with existing query resolution techniques for unknown target location such as Expanding Ring Search (ERS), Random walk search and variants of search. They show by analysis, simulation and implementation in test that IRS and k-IRS are highly scalable, the cost of search (total number of transmitted bytes) is independent of node density and it is much lower than that of existing proposals under high node density.

Carlos F. García-Hernández at el. [5], specifies that the refinement of energy harvesting techniques that can be gather useful energy from vibrations, blasts of radio energy, and self power circuitry is a very real possibility with networks of millions of nodes, deployed through paint brushes, injections and aircraft. Also the introduction of an additional type of sensor nodes allows the network to self-organize and learn by embedding smart and adaptive algorithm. On the other hand, the use of adoptive power control in IP networks that utilizes reactive routing protocols and sleep-mode operation, more powerful mobile agents, QoS (Quality of Service) to guarantee delivery, security mechanisms, robustness and fault-tolerance.

Mohammad Hossein Anisi at el. [6], Propose the EDR (Energy Data Routing) Algorithm. In this algorithm, instead of broadcasting the packets, the algorithm considers the residual energy of the nodes and the time of packet delivery. Hence, data packets are sent directly toward the Base Station (BS). Additionally the algorithm takes into account the type of request data and it is able to meet the satisfy QoS requirements of incoming data such as fast data deliver for real-time applications. Also, by comparing data in each node, we limit the number of redundant and unnecessary responses from the sensor nodes. Hence the total number of messages sent is reduced which results in high packet delivery ratio. This allows the solution to ensure optimal energy consumption and extend the network lifetime.

It is a data-centric routing algorithm. The aim is to achieve an energy-efficient solution for data routing in wireless sensor networks. In this mechanism, each sensor node sends its data only to one neighbor and this neighbor is selected according to some criteria such as remaining energy of the node and the time of data delivery. The nodes with redundant data do not send any response. The main contribution of this algorithm are: ability to use in both event-driven and query-driven applications, ensuring taking the shortest routing path, transmitting very less number of packets, simplifying the implementation, maintaining the routs, high probability of completeness of responses while realizing significant power savings and increasing the network lifetime.

Aamir Shaikh and Siraj Pathan [7] specified that Zigbee is a new wireless communication technology with short distance, low complexity, low energy consumption, slow data rate and low cost. It is based on IEEE 802.15.4 Standard with the capacity of coordinating mutual communication among thousands of tiny sensors. Through the radio waves, these sensors can transmit the data from one sensor to another with small energy cost and high efficiency. Compared with various existing wireless communication technology, Zigbee technology has the lowest energy consumption and cost. Because of the slow data rate and the small range of communication, Zigbee technology is extremely suitable for agriculture field which has small amount of data flows. Zigbee has self-organizing features that one node can sense other ones without any human interventions and connect with each other automatically to create a completed network. It also obtains self-recovery function that the network can repair itself when a node is added or deleted, the position of a node is changed, or a breakdown occurred. It has also the topology structure to ensure that the whole system can work normally without any human interventions.

Aamir Shaikh and Siraj Pathan [7] specified that RFID (Radio Frequency Identification) is a non-contact automatic identification technology that uses radio frequency signals which automatic recognizes target and access to relevant data. The identification work does not require human interference and can work in variety of harsh environments. But if there is no network to transmit data, it will be difficult to play its advantage.

Reshma I. Tandel [8] specified that LEACH is a Low Energy Adaptive Clustering Hierarchy protocol. The main goal of cluster based sensor networks is to decrease system delay and reduce energy consumption. Leach is a cluster based protocol for micro sensor networks which achieves energy efficient, scalable routing and fair media access for sensor nodes.

LEACH protocol is the first protocol of hierarchical routing which proposed data fusion. It is milestone significance in clustering routing protocol. Hierarchical protocols are defined to reduce energy consumption by aggregating data and to reduce the transmissions to the base station. LEACH is a TDMA based MAC protocol. The main aim of this protocol is to improve the life time of wireless sensor networks by lowering the energy. Leach protocol is a typically representation of hierarchical routing protocol. It is self-adaptive and self-organized. Operations of Leach protocol consists of several rounds with two phases in each round. Leach protocol uses round as unit, each round is made up of cluster set-up phase and steady phase for the purpose of reducing unnecessary energy costs.

Suzan Shukry [9] proposed the Efficient Node Stable Routing (ENSR) protocol. It is introduced to guarantee the stability of transmission data between the source and destination nodes in a dynamic WSN conditions. The stability of the node is defined in both the global and local aspects of stability. The stable node is explored by introducing the stable between centrality and switching packets based on the locality dependency energy degree to guarantee the global and local stability of the node, respectively. The packet retransmission times is taken into account, where the accurate calculated packet retransmission times decrease the extra overhead of the network. This routing algorithm guarantees the energy conversing factor and mitigates “hot-spots” by changing the stable over time.

2.1 Algorithm Paradigms for Wireless Sensor Networks

Luis Javier Garcia Villalba [10] specifies that Sensor applications demand the communication of nodes to execute certain procedures or algorithms. In fact, three kinds of algorithms can be executed on wireless sensor networks:

- Centralized Algorithms: They are executed in a Base node that posses the knowledge of the whole network. These algorithms are quite rare because of the cost of transmitting the data to make the node know the status of the complete network.
- Distributed Algorithms: The nodes are communicated with each other. The communication is supported by message-passing.
- Localized Algorithms: The nodes use restricted data acquired from a close area. With this local information, the algorithm is executed in one node.

The algorithm paradigm is an important factor to take into account when deciding about the routing protocol to employ in the network. If localized algorithms are used, the routing protocol should reinforce and optimize the communication between neighbors. On the other hand, for centralized algorithms, combining the messages that simultaneously go to the central node (even when they are generated by different sources) could be an advantage. The distributed algorithms should efficiently support the communication between any two pairs of nodes. Finally, Local based algorithms depend on some solution that provides geographic coordinates, like GPS, making the solution more expensive.

3. IP ROUTING

If the router receives and installs multiple paths with the same administrative distance and cost to a destination, load-balancing can occur. The number of paths used is limited by the number of entries the routing protocol puts in the routing table. Four entries is the default in IOS for most IP routing protocols with the exception of Border Gateway Protocol (BGP), where one entry is the default. Six different paths configured is the maximum number.
The IGRP and EIGRP routing processes also support unequal cost load-balancing. You can use the variance command with IGRP and EIGRP to accomplish unequal cost load-balancing. Issue the maximum-paths command in order to determine the number of routes that can be installed based on the value configured for the protocol. If you set the routing table to one entry, it disables load balancing.

You can usually use the **show IP route** command to find equal cost routes. For example, below is the **show IP route** command output to a particular subnet that has multiple routes. Notice there are two routing descriptor blocks. Each block is one route. There is also an asterisk (*) next to one of the block entries. This corresponds to the active route that is used for new traffic. The term 'new traffic' corresponds to a single packet or an entire flow to a destination, depending on the type of switching configured.

- For process-switching—load balancing is on a per-packet basis and the asterisk (*) points to the interface over which the next packet is sent.
- For fast-switching—load balancing is on a per-destination basis and the asterisk (*) points to the interface over which the next destination-based flow is sent.

The position of the asterisk (*) keeps rotating among the equal cost paths each time a packet/flow is served.

M2515-B# **show ip route 1.0.0.0**
Routing entry for 1.0.0.0/8
Known via "rip", distance 120, metric 1
Redistributing via rip
Advertised by rip (self originated)
Last update from 192.168.75.7 on Serial1, 00:00:00 ago
Routing Descriptor Blocks:
192.168.57.7, from 192.168.57.7, 00:00:18 ago, via Serial0
Route metric is 1, traffic share count is 1
192.168.75.7, from 192.168.75.7, 00:00:00 ago, via Serial1
Route metric is 1, traffic share count is 1

4. PER-DESTINATION AND PER-PACKET LOAD BALANCING

You can set load-balancing to work per-destination or per-packet. Per-destination load balancing means the router distributes the packets based on the destination address. Given two paths to the same network, all packets for destination1 on that network go over the first path; all packets for destination2 on that network go over the second path, and so on. This preserves packet order, with potential unequal usage of the links. If one host receives the majority of the traffic all packets use one link, which leaves bandwidth on other links unused. A larger number of destination addresses leads to more equally used links. To achieve more equally used links use IOS software to build a route-cache entry for every destination address, instead of every destination network, as is the case when only a single path exists. Therefore traffic for different hosts on the same destination network can use different paths. The downside of this approach is that for core backbone routers carrying traffic for thousands of destination hosts, memory and processing requirements for maintaining the cache become very demanding.

Per-packet load-balancing means that the router sends one packet for destination1 over the first path, the second packet for the same destination1 over the second path, and so on. Per-packet load balancing guarantees equal load across all links. However, there is potential that the packets may arrive out of order at the destination because differential delay may exist within the network. For per-packet load balancing, the forwarding process determines the outgoing interface for each packet by looking up the route table and picking the least used interface. This ensures equal utilization of the links, but it is a processor intensive task and impacts the overall forwarding performance. This form of per-packet load balancing is not well suited for higher speed interfaces.

Per-destination or per-packet load-balancing depends on the type of switching scheme used for IP packets. By default, on most routers, fast switching is enabled under interfaces. This is a demand caching scheme that does per-destination load-balancing. To set per-packet load-balancing, enable process switching (or disable fast switching), use these commands:

Router# **config t**
Router(config)# **interface Ethernet 0**
Router(config-if)# **no ip route-cache**

Router(config-if)# **^Z**

Now the router CPU looks at every single packet and load balances on the number of routes in the routing table for the destination. This can crash a low-end router because the CPU must do all the processing. To re-enable fast switching, use these commands:

Router# **config t**

Router(config)# **interface Ethernet 0**

Router(config-if)# **ip route-cache**

Router(config-if)# **^Z**

Newer switching schemes such as Cisco Express Forwarding (CEF) allow you to do per-packet and per-destination load-balancing more quickly. However, it does imply that you have the extra resources to deal with maintaining CEF entries and adjacencies.

When you work with CEF, you could ask: Who does the load balancing, CEF or the routing protocol used? The way in which CEF works is that CEF does the switching of the packet based on the routing table which is being populated by the routing protocols such as EIGRP. In short, CEF performs the load-balancing once the routing protocol table is calculated.

5. ENERGY EFFICIENCY

As sensor nodes are generally battery-powered devices, the critical aspects to face concern how to reduce energy consumption of nodes, so that the network life time can be extended to reasonable times.

5.1. General approach to energy conservation

Depending on the specific application, sensor nodes may also include additional components such as a location finding system to determine their position, a mobilizer to change their location or configuration as antenna’s orientation.

The communication subsystem has much higher energy consumption than the computation subsystem. It has been shown that transmitting one bit may consume as much as executing a few thousands instructions. Therefore, communication should be operating for computation.

The radio energy consumption is of the same order in the reception, transmission and idle states, while the power consumption drops of at least one order of magnitude in the sleep state. Therefore, the radio should be put to sleep or turned off whenever possible.

Depending on the specific application, the sensing subsystem might be another significant source of energy consumption, so its power consumption has to be reduced as well.

6. ROUTING CATEGORIES

There are following routing categories.

6.1. Centralized vs. Distributed

In centralized routing, the route that a message is supposed to take, is calculated by the source and is embedded into the message. Intermediate nodes just check this route and forward the message to the next node on the route. Conversely, In distributed routing, each node calculates the next node on the route based on the routing protocol. The message consists of only the actual data as the payload with minimal routing overhead.

6.2. Static vs. Dynamic

Static routing provides the means for explicitly defining the next node from any intermediate node for a particular destination. This means that every node has as entry for each destination node in a table stating the next node to be chosen in case a message arrives for that destination. Dynamic routing chooses the next node on the route from multiple nodes based on various criteria like network load and density.

6.3. Flat vs. Hierarchical

The entire network is treated as a flat topology in flat routing. In hierarchical routing, the network topology is assumed to be hierarchical in nature. Groups of nodes form a cluster. Clusters are aggregated to from a higher-level cluster and so on till the entire network topology is defined. Routing is carried out based on communications between these clusters.

6.4. State vs. Stateless

In case of distributed routing, each node calculates the next node on the route. For doing this, it may require to store some information regarding its neighbors and/or the message itself. The node maintains expensive routing tables to keep track of what route to follow for a particular destination. Over a period of time, the nodes identify the entire topology of network. Routing protocols that store such information are known to follow the state routing whereas those protocols, which do not store any information, provide stateless routing. While state protocols are expensive in terms of memory, stateless protocols appear to be expensive in terms of time. A good compromise would be to keep track of just enough network information that would enable a node to calculate the next hop correctly without doing any resource consuming calculations. By correctly, it means that the next hop chosen should confirm to some routing protocol and not be chosen randomly.

7. ROUTING PROTOCOLS IN WSN

Routing protocols are classified in the following categories:

i. In general, routing in WSN can be divided into flat based routing; hierarchical based routing and location based routing depending on the network structure.
    a. In flat based routing, all nodes are typically assigned equal roles or functionality.
    b. In hierarchical based routing, nodes will play different roles in the network.
    c. In location based routing, sensor nodes positions are exploited to route data in the network.

ii. A routing protocol is considered adoptive if certain system parameters can be controlled in order to adapt to the current network conditions and available energy levels. Furthermore, these protocols can be classified into multi path-based, query based, negotiation-based, QoS based, or coherent based routing techniques depending on the protocol operations.

iii. Routing protocols can be classified into three categories namely proactive, reactive and hybrid protocols depending on how the source finds a route to the destination.
In proactive protocols, all routes are computed before they are really needed, while in reactive protocols, routes are computed on demand. Hybrid protocols use a combination of these two ideas. When sensor nodes are static, it is preferable to have table driven routing protocols rather than using reactive protocols. A significant amount of energy is used in route discovery and setup of reactive protocols.

iv. Another class of routing protocols is called the cooperative routing protocols. In cooperative routing, nodes send data to a central node where data can be aggregated and may be subject to further processing. Hence reducing route cost in terms of energy use. Many other protocols rely on timing and position information.

8. ROUTING CHALLENGES AND DESIGN ISSUES IN WSN

WSNs have several restrictions such as limited energy supply, computing power and limited bandwidth of the wireless links connecting sensor nodes. One of the main design goals of WSNs are to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation by employing aggressive energy management techniques.
The designs of routing protocols in WSNs are influenced by many challenging factors. These factors must be overcome before efficient communication can be achieved in WSNs. In the following some of the routing challenges and design issues that affect routing process in WSNs.

8.1. Node Deployment

Node deployment in WSNs is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-deterministic paths. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad-hoc manner. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation. Inter-sensor communication is normally within short transmission ranges due to energy and bandwidth limitations. Therefore, it is most likely that a route will consist of multiple wireless hopes.

8.2. Energy consumption

Without losing accuracy, Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment, because energy conserving forms of communication and computation are essential. Sensor node lifetime shows a strong dependence on the battery lifetime. In a multi-hop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

8.3. Data Reporting

Data sensing and reporting in WSNs is depending on the application and the time criticality of the data reporting. Data reporting can be categorized as time-driven, event driven, query driven and hybrid. The time driven delivery is suitable for applications that require periodic data monitoring. Sensor nodes will periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest at constant periodic time intervals. In event driven and query driven models, sensor nodes react immediately to sudden and drastic changes in the value of a sensed attribute due to the occurrence of a certain event or the base station generates a query. These are well suited for time critical applications. The routing protocol is highly influenced by the data reporting with regard to energy consumption and route stability.

8.4. Node/Link Heterogeneity

Generally, all sensor nodes were assumed to be homogeneous such as having equal capacity in terms of computation, communication and power. However, depending on the application a sensor node can have different role or capability. The existence of heterogeneous set of sensors raises many technical issues related to data routing. For example, some application might require a diverse mixture of sensors for monitoring temperature, pressure and humidity of the surrounding environment, detecting motion via acoustic signatures and capturing the image or video tracking of moving objects. These special sensors can be either deployed independently or the different functionalities can be included in the same sensor nodes. Even data reading and reporting can be generated from these sensors at different rates, subject to diverse quality of service constraints and can follow multiple data reporting models. For example, hierarchical protocols designate a cluster-head node different from the normal sensors. These cluster heads can be chosen from the deployed sensors or can be more powerful than other sensor nodes in terms of energy, bandwidth and memory. Hence, the burden of transmission to the BS is handled by the set of cluster-heads.

8.5. Fault Tolerance

Some sensor nodes may fail or be blocked due to lack of power, physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base stations. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption or reducing packets through regions of the network where more energy is available. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

7.6. Scalability

The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands or more. Any routing scheme must be able to work with this large number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment. Most of the sensors can remain in the sleep state with data from the few remaining sensors providing a rough quality until an event occurs.

8.7. Network Dynamics

Most of the network architectures assume that sensor nodes are stationary. However, mobility of either base station or sensor nodes is sometimes necessary in many applications. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, in addition to energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application such as it is dynamic in a target detection/tracking application, while it is static in forest monitoring for early prevention. Monitoring static events allows the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting and consequently generate significant traffic to be routed to the Base station.

8.8. Transmission Media

In a multi-hop sensor network, communicating nodes are linked by a wireless medium. The traditional problems associated with a wireless channel may also affect the operation of the sensor network. In general, the required bandwidth of sensor data will be low; on the order of 1-100 kb/s. The transmission media is related to the design of media access control (MAC). One approach of MAC design for sensor networks is to use TDMA based protocols that conserve more energy compared to contention based protocol like CSMA. Bluetooth technology can also be used.

8.9. Connectivity

High node density in sensor networks prevents them from being completely isolated from each other. Therefore, sensor nodes are expected to be highly connected. However, this may not prevent the network topology from being variable and the network size from being shrinking due to sensor node failures. In addition, connectivity depends on the possibly random, distribution of nodes.

8.10. Coverage

In WSN, each sensor node obtains a certain view of the environment. A given sensor's view of the environment is limited both in range and in accuracy. It can only cover a limited physical area of the environment. Hence, area coverage is also an important design parameter in WSN.

8.11. Data Aggregation

Since sensor nodes may generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions is reduced. Data aggregation is the combination of data from different sources according to a certain aggregation function such as duplicates suppression, minima, maxima and average. This technique has been used to achieve energy efficiency and data transfer optimization in a number of routing protocols. Signal processing methods can also be used for data aggregation. In this case, it is referred to as data fusion where a node is capable of producing a more accurate output signal by using some techniques such as beam forming to combine the incoming signals and reducing the noise in these signals.

9. CONCLUSION

WSNs are used to collect data from the environment. They consist of large number of sensor nodes and one or more Base Stations. The nodes in the network are connected via Wireless communication channels. Each node has capability to sense data, process the data and send it to rest of the nodes or to Base Station. These networks are limited by the node battery lifetime.
Each message generally has a header identifying its source node, destination node, length of the data field, and other information. This is used by the nodes in proper routing of the message. In encoded messages, parity bits may be included. In packet routing networks, each message is broken into packets of fixed length. The packets are transmitted separately through the network and then reassembled at the destination.

REFERENCES

1. Al-Karaki, J.N., Al-Malkawi, I.T, “On Energy Efficient Routing for Wireless Sensor Networks”, International Conference on Innovations in Information Technology”, Al Ain UAE,16-18 Dec. 2008 , Page(s).465-469.
2. Xiaoxia Huang,, Hongqiang Zhai and Yuguang Fang, Peter Kok Keong Loh, Hsu Wen Jing, and Yi Pan, “Robust Cooperative Routing Protocol in Mobile Wireless Sensor Networks”, IEEE Transactions on Wireless Communications, Volume. 7, Issue. 12, Dec. 2008, Page(s).737-758.
3. Peter Kok Keong Loh, Hsu Wen Jing and Yi Pan, “Performance Evaluation of Efficient and Reliable Routing Protocols for Fixed-Power Sensor Networks”, IEEE Transactions on Wireless Communications, Volume. 8, Issue.5, May 2009, Page(s). 601-628.
4. Kiran K. Rachuri and C. Siva Ram Murthy, “Energy Efficient and Scalable Search in Dense Wireless Sensor Networks”, IEEE Transactions on Computer, Volume. 58, Issue. 6, June 2009, Page(s).561-579.
5. Carlos F. García-Hernández, Pablo H. Ibargüengoytia-González, Joaquín García-and Hernández, “Wireless Sensor Networks and Applications: a Survey”, IJCSNS International Journal of Computer Science and Network Security, Volume 7, Issue.3, March 2007, Page(s). 264-273.
6. Mohammad Hossein Anisi, Abdul Hanan Abdullah, Yahaya Coulibaly and Shukor Abd Razak, “EDR: Efficient Data Routing in Wireless sensor Networks”, International Journal of Ad-hoc and Ubiquitous Computing, Vol. 12, No. 1, 2013, Page(s). 46-55.

7. Aamir Shaikh and Siraj Pathan, "Research on Wireless Sensor Network Technology", International Journal of Information and Education Technology, Vol. 2, No. 5, 2012, Page(s). 476-479.
8. Reshma I. Tandel, "Leach Protocol in Wireless Sensor Network: A Survey", International Journal of Computer Science and Information Technologies", Vol.7(4), 2016, Page(s). 1894-1896.
9. Suzan Shukry, "Stable routing and energy-conserved data transmission over wireless sensor networks", EURASIP Journal of Wireless Communication and Networking, Vol. 36, 2021, Page(s). 01-29.
10. Luis Javier Garcia Villalba, Ana Lucila Sandoval Orozco, Alicia Trivino Cabrera and Claudia Jacy Barenco Abbas, "Routing Protocols in Wireless Sensor Netwroks", Sensors, Vol. 9, 2009, Page(s). 8399-8421.