Design of Secure and Stable Routing Protocols for the Adhoc Networks

Lamia F. Tulaib[1], Akbal O. Salman[2], Mazin A. Mohammed[3]

[1] College of Dentistry, University of Anbar, 31001, Anbar, Iraq

[2] Department of Control & Automation Techniques Engineering, Electrical Engineering Technical College, Middle Technical University, 06800, Baghdad, Iraq

[3]Information Systems Department, College of Computer Science and Information Technology, University of Anbar, 31001, Anbar, Iraq

Email: den.lamia.faris@uoanbar.edu.iq; akbal.o.salman@mtu.edu.iq; mazinalshujeary@uoanbar.edu.iq

Abstract

The desire to remain connected no matter where you are, when you want to be connected, or how you want to be connected has been a driving force behind the development of wireless networks, in particular in the field of persistent and ubiquitous computing. This need can be satisfied in a number of different ways. The Mobile Ad-hoc networks made up of a collection of nodes, each of which is equipped with wireless networking and communication capabilities. There may be any number of these nodes. It is not necessary to involve a central administrator in order for these nodes to communicate with one another since they may do so independently. Ad hoc networks also often referred to as infrastructure-less networks since they do not have a present topology or infrastructure. This is because ad hoc networks do not have a predetermined topology or infrastructure. Because each node in the wireless ad-hoc network functions as either a host or a router or both, In order to prevent unauthorized parties from accessing the data, it is essential to have developed secure and reliable routing protocols. The work that is presented in this proposed work is an attempt to develop an ad-hoc routing protocol that is safe and robust. The protocol in question called Energy Efficient Wireless Path Optimization (EEWPO). The dynamic route selection mechanism, which is based upon genetic programming, and the connection integrity assurance algorithm have been combined within the framework of the proposed model routing scheme for wireless ad-hoc networks to produce a routing-based mechanism that is secure, flexible, and robust. This is accomplished by combining the two mechanisms within the framework of the proposed model routing scheme. These two aspects are going to work together to form the foundation of this plan. The new combination has the ability to give a higher degree of security to the current network, hence reducing the likelihood that vulnerabilities in connection and fake route injections would be exploited. When it comes to speech-based ad-hoc networks, which need dedicated connections for the exchange of voice data over an ad-hoc channel, intelligent route selection throughout the multipath network becomes very important. This is because the transmission of speech data is essential to the functioning of these networks. In order to materialize the robust ad-hoc routing algorithm, the generation of the adaptive ad-hoc network routing solution requires the ideally layered combination of the genetic programming-based routing solution along with the connection integrity assurance model. Only then can the adaptive ad-hoc network routing solution be created. The effectiveness of the recommended routing protocol has been shown via testing in a number of different simulated situations.

Doi : https://doi.org/10.54216/IJWAC.010202

Keywords: wireless sensor networks; K-Means Clustering; IPv6; the IEEE 802.15.4; routing technique; multipath routing

1. Introduction

Mobile computing has emerged as an integral part of our everyday lives as a direct result of the rapid pace of technological advancement in mobile platforms and devices in the present day. We use wireless networks for daily tasks like making phone calls, watching online news, listening to audio files, or watching and listening to our favourite music from a variety of sources that are currently available and with the help of a variety of devices that are currently on the market, like a mobile phone or a laptop. The desire to be connected whenever, wherever, and however has resulted in the growth of wireless networks and the opening of new areas of research in determined and everywhere computing. This newly emerging field of technological advancement calls for a highly secure and stable routing protocol effectively manage communication among peers. An ad hoc wireless network [1] is a collection of nodes that may communicate with one another wirelessly either directly or indirectly via the use of other nodes. Because ad-hoc wireless networks lack any kind of consistent infrastructure, it is not unusual for their nodes to wander from place to place and at any time. Therefore, it is impossible for such networks [2] to provide for the prediction of the behaviour, activity, or performance of nodes or the arrangements of nodes. There is no centralized controller of any kind; hence, there is no way for nodes to communicate with one another.

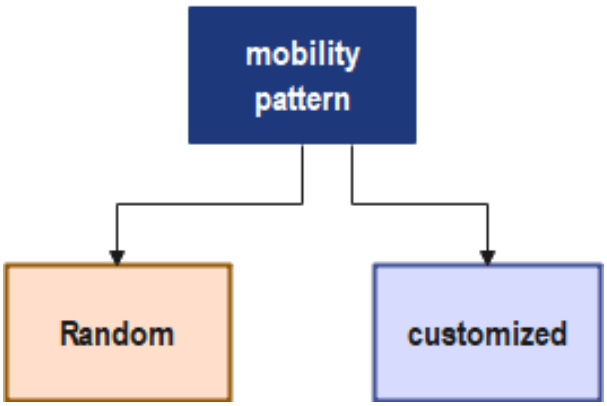

Figure 1: Adhoc Characteristic

There is no other node that can be reached from any of the other nodes. Ad-hoc networks, for the most part, are able to function without being dependent on any kind of permanent infrastructure, including military operations, rescue operations, academic organizations, institutions, and so on. Ad-hoc networks are often used in settings in which the installation of infrastructure or cabling [3] is either not feasible or would need excessive financial investment to do. We can better comprehend these types of networks by comparing them to wireless networks that are built on existing infrastructure. Consider the modern cellular networks, which are heavily reliant on the infrastructure that supports them. Coverage for cellular networks is provided by base stations, radio resources, and all of the devices themselves, all of which are maintained from centralized places. When we move away from central places in these types of networks, which are responsible for the whole of the communication and distance that is present in these networks, we discover that we are moving in the direction of ad-hoc networks [4]. Communication may take place via either a single hop or several hops using ad hoc networks. When information is sent in a multi-hop method, it is the responsibility of each node to ensure that it reaches its destination on behalf of the originating node. Nodes that are wireless and part of an ad hoc network are able to communicate directly with other nodes that are within their transmission range.

Additional pathways are available to send the packets toward their destination, which allows for the possibility of connecting with other nodes that are not within the range. Because of the unpredictability of the behavior and location of the nodes, the routing of packets is the primary challenge presented by ad hoc wireless networks. Imagine a scenario in which an individual, while driving in a vehicle in a large city with a small handheld wireless device, is able to see the entire environment ahead (including buildings, streets, highways, and shopping malls), and at the same time, he is able to track other vehicles that may come in his method to avoid any accidents. This would be a situation that would be ideal for preventing any mishaps. However, in the current day

Doi : https://doi.org/10.54216/IJWAC.010202

and age, wireless technologies have developed into a need for individuals. Many companies and research organizations all over the world, such as NTT DoCoMo, Qualcomm, Nokia, Ericsson, Motorola, Alcatel, WWRF, IEEE, IEEE, [5] Mobile VCE, and Ad-hoc network W-PCC, are getting ready to develop ad-hoc wireless systems, which are expected to make their debut on the commercial market in 2010 [6]. Therefore, consolidated solutions that are able to operate seamlessly on multiple or different networks are migrating to the ad-hoc networks' surroundings. In order to fulfill all of the needs of the next generation's dream visualizations, an Open Wireless Architecture (OWA) [7] should be designed as soon as possible.

The technology of ad-hoc networks offers a number of advancements to the wireless market. These include downlink data rates well ranging from a few kilobytes to several megabits per second (Mbps), low latency, very effective spectrum use, and low-cost implementations. Ad-hoc network technology also offers a number of other benefits. The development of ad-hoc networks holds the potential to take the wireless experience to an entirely new level by providing impressive user applications. For instance, it offers images of higher quality, videos of good quality, and an interface that is friendly to users. When compared to earlier forms of wireless technology, such as vehicular networks and urban area inter-nodal networks [8], ad-hoc networks that operate using wireless technology have a significant number of distinct advantages. Because the TCP/IP architecture [9] (open communication protocol) has more security issues compared to other networking models, the primary distinction between an ad-hoc network and other networking models is that the ad-hoc network operates on the TCP/IP architecture and suite of protocols. The technology of ad hoc wireless networks enables users to have access to specialized services that provide information on demand at a fast rate and at a cheap cost.
The Wireless Standards Group The Institute of Electrical and Electronics Engineers, better known as IEEE, was the organization that initially defined the standards for ad-hoc networks, which are now used as the international standard for 3G wireless communication. IMT-advanced is the name given to the plan that the IEEE is going to plan to implement in the near future to define wireless systems.

Wi-Max

Wi-Max may be broken down into two primary components, which are the access service network and the connection services network. The base station and the service network gateway are the two most important parts of the service networks, and they are connected to one another through an IP infrastructure. In addition to providing security anchoring, traffic accounting, and mobility support for mobile stations, the service network gateway also enables mobile IP home agents to participate in international mobility inside connectivity service networks (HA). Several essential components of the Wi-MAX network [10] architecture are responsible for the functioning of the Wi-MAX system. First, the AAA (Authentication, Authorization, and Accounting) server that is placed in service networks' networks processes control signals from service networks in order to authenticate the mobile station by comparing the mobile station's profile to the mobile station's profile that is stored in the database of the AAA server. This is done in order to prevent unauthorized access to the mobile station [11].

Following the completion of the authentication process, the AAA server will transmit the quality of service (QoS) characteristics together with the mobile station profile to the service networks. The function of the Home Agent is to exercise control over signals coming from service networks, assign a mobile IP address to the mobile station, and prop up the IP payload. The operation of HA consists of providing access to the internet so that data flow may take place. In the event that a mobile station initiates a Voice over Internet Protocol (VOIP) [12] call, control of the call is transferred to the server of the service networks' mobile station IP multimedia system. When a call comes in from a number that is not part of the Wi-Max network, the mobile station server selects the appropriate media gateway controller/media gateway so that it may interface with the public switched telephone network. If, on the other hand, the call is intended for an end unit that is part of a different 3GPP or 3GPP2 network, then the call will be routed via the interworking gateway unit that is part of the service networks [13]. The 802.16e air interface is used for communication between the mobile station and the base station. The mobile station and the base station conduct all of their communication via the use of IP carriers and controls. The carrier mode of time-division multiplexing does not function in Wi-Max. User traffic from WiMax mobile [14] stations is routed as payload between the base station and the access service network gateway. The end-to-end network architecture for mobile Wi-MAX is shown below in Figure 1, which may be found here.

Doi : https://doi.org/10.54216/IJWAC.010202

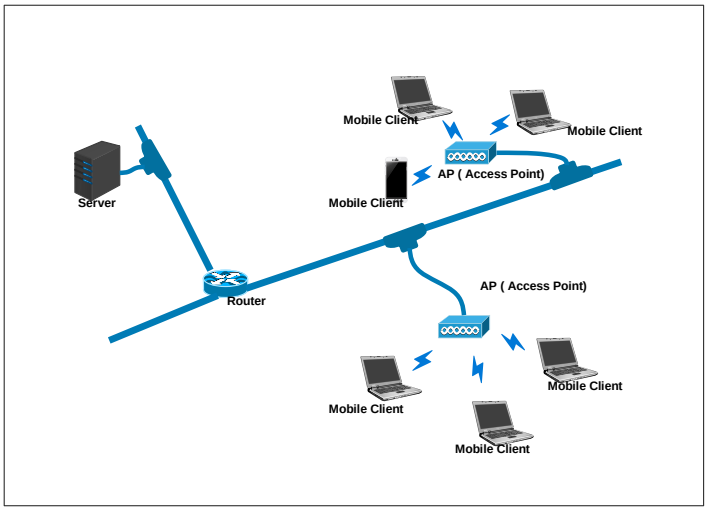

Figure 2: Mobile Wi-Max Architecture

In many different configurations of services, the components of the service network (connectivity service network) are designed to be redundant and geographically distinct from one another. The network components of service networks inside the service networks themselves are likewise structured in a redundant fashion, and they are often located within the same premises. Multiple service networks may be operated by a single network access provider. There is no need for mobility to be safeguarded at the service networks themselves inside these service networks. When a mobile station leaves its Home Network Service Provider and connects to a Visited Network Service Provider, this is an example of roaming, which may be supported. In situations like this, the AAA server in the Visited Network Service Provider will make use of control signalling in order to get the credentials and profiles from the Home network service provider. Bearer traffic is not sent back to the user's home network service provider from the network service provider that was visited. There are several mobility scenarios that are kept up to dates, such as intra-service network mobility, inter-service network mobility, and protected service network mobility. Signalling allows for the seamless transfer of calls when a mobile station moves from one base station to another base station that is operated by the same service networks.

2. Related Survey

The location estimate approach was introduced by [15] without using any methodologies based on wireless sensor networks. The many approaches to location estimate may be broken down into two categories: target and source localization, and self-location node. At the site of the goal, the implementation of approaches based on energy has taken place. Next, the author looks at the several nodes that make up the self-localization approaches. There are several difficulties to face depending on the circumstances. In this article, the author presents a comprehensive analysis of the following challenges: localization in non-line-of-sight, the node selection criteria to locate in planning energy constraint network sensor node for optimizing the compromise between the performance and the location of the energy consumption, the location of cooperation node, and the location algorithm in the heterogeneous network.

According to [16] the use of group communications in wireless networks has made it possible for many new applications to emerge. These applications need the transmission of packets from one or more sender(s) to many recipients. Group conversations that take place via unsecured wireless channels are vulnerable to a wide variety of different types of assaults. The supply of security in group communications in wireless networks continues to be a significant and complex topic, despite the fact that a number of approaches have been presented to protect group communications. This article presents a survey of recent advances in security requirements and services in group communications in three different types of wireless networks and discusses the challenges in designing secure group communications in these networks: wireless infrastructure networks, mobile ad-hoc networks, and wireless sensor networks. In addition, the article provides an overview of recent advancements in security

Doi : https://doi.org/10.54216/IJWAC.010202

requirements and services in group communications in wired networks. The number of applications that include group communications carried out over wireless networks is rapidly growing. Some examples of these applications include group-oriented military systems (in-field commander conferences carried out via wireless devices), as well as education systems (teacher lectures in a distance learning classroom).
However, communication carried out through wireless channels is inherently insecure and open to a wide variety of threats due to the nature of the medium itself. A significant amount of work that has already been done has sought to integrate security into such interactions. The authors have described known attacks that may significantly impair or even completely shut down group communications on wireless networks so that readers will have a better understanding of SGC over wireless networks. The authors have highlighted essential security needs, as well as provided examples of basic security services, in order to achieve these criteria and protect communications from these assaults. They have proved that the suggested security services are capable of preventing and mitigating a number of different types of threats. In addition to this, they have documented various studies that have already been done on SGC across the following three categories of wireless networks: wireless infrastructure networks, mobile ad-hoc networks, and wireless sensor networks. These works, in essence, make an effort to lessen the burden of communication and processing overheads, as well as to protect against certain kinds of assaults, taking into account the restricted computing capacity and the scarcity of wireless channels. They have highlighted certain open problems that still need to be addressed in order to finish the survey on SGC via wireless networks. This will allow them to complete the study.
[17] Signal Processing Magazine" has been brought up in conversation by the writers. In order to examine the cross-layer issue of joint power and rate management in multiple-access networks with quality of service (QoS) restrictions, a game-theoretic model has been presented as a method of investigation. Within the context of the game that has been suggested, each player's goal is to choose their own transmit power and rate in a decentralized fashion so that they may maximize their own utility while simultaneously meeting their QoS criteria. The user's quality of service requirements is given in terms of the average source rate as well as an upper limit on the average delay. The delay takes into account both transmission and queuing delays. The utility function that we are going to look at here assesses how efficiently energy is used, and it is especially well-suited for wireless networks that have energy restrictions. We derive the Nash equilibrium solution for the suggested noncooperative game, and we get a closed-form equation for the utility that may be attained after the game has reached equilibrium. It has been shown that the quality of service needs of a user are translated into a "size" for the user, which is an indicator of the number of network resources that are used by the user. The tradeoffs that exist between throughput, latency, network capacity, and energy efficiency are investigated with the help of this competitive multiuser framework. In addition, analytical equations are provided for users' delay profiles, and the delay performance of users at the Nash equilibrium is measured. Both of these features are presented in the paper.

The routing method that was suggested by [18] allows for a large reduction in the amount of energy that is spent by the network on the setup of the communication and control, which is a key problem in communication that has a low data rate. To do this, rather than sending a current from each individual sensor to the data destination, a single stream of data is sent from a family of sensors to the sink. This replaces the traditional method of sending a current from each sensor individually to the data destination. Since of this, the likelihood of packet collisions occurring in a wireless network is reduced, which is beneficial because the same amount of information may be transferred even if some nodes send bigger packets. Additional improvements are attainable with the use of effective data compression. This is accomplished via the use of lossless data compression, which entails encoding information in the sequence in which sensor packages are stored.
[19] According to the authors of this research, the fundamental objective of WSNs is to save energy, whereas throughput and latency are of lesser concern. This distinction was made clear by comparing the three metrics. Therefore, the amount of consumed energy is exchanged for throughput and delay. In WSNs, a unique notion of incompletely cooperative game theory is employed to accomplish all of the objectives at the same time. During the game, each node will alter its equilibrium strategy based on the best guess as to the current state of the game. Following a brief discussion of the game's utility function, the equilibrium method for playing the game in WSNs will next be described. In addition, a simpler game-theoretic MAC protocol known as G-MAC is presented for wireless sensor networks (WSNs). This protocol makes use of an auto-digressive back-off mechanism, which is simple to put into action. The results of the simulation show that the incompletely cooperative game has the potential to increase system throughput, while simultaneously reducing delay and the rate of packet loss, all while keeping energy consumption within reasonable bounds, and that G-MAC provides effective support for the game.

Doi : https://doi.org/10.54216/IJWAC.010202

3. Proposed Methodology

Within the framework of the proposed model routing scheme for wireless ad-hoc networks, a dynamic route selection based upon genetic programming mechanism and a connection integrity assurance algorithm have been combined to produce a routing-based mechanism that is secure, flexible, and robust. This scheme is based on the combination of these two components. The new combination has the potential to provide a greater degree of security into the existing network, hence minimizing the risk of false route injections and connection vulnerabilities being exploited. In speech-based ad-hoc networks, which need dedicated connections for the exchange of voice data through an ad-hoc channel, the smart route selection across the multipath network becomes highly crucial. This is because these networks are dependent on the transmission of voice data. In order to create the adaptive ad hoc network routing solution, a flawlessly layered mix of a genetic programming-based routing [20] solution and a connection integrity assurance model is required. Only then can the resilient ad hoc routing algorithm be created.

3.1 Connection Integrity Assurance (CIA) Model

The creation of a safe and adaptable routing model across a given network is made possible thanks to the CIA model's reliance on the availability assurance model and the connection integrity model.

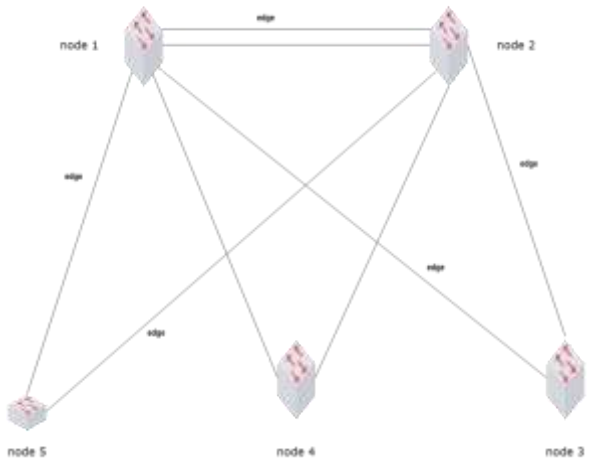

Figure 3: The Directed Path Mechanism of the CIA Model

Non-structured wireless ad-hoc networks, also known as sensor networks, are typically designed with an adaptive architecture that can adjust to the conditions of the network at any given time. The term "adaptive architecture" refers to a system that can modify its structure, behavior, or resources in response to changing circumstances. In most cases, the adaptation that is made is not too functional characteristics but rather to nonfunctional characteristics. The control of the unstructured ad-hoc networks is spread across an area with dimensions M by N. Here, the neighboring nodes of each wireless node are located and localized by using distance-based methods to determine the transmission range of the network. The CIA-based secure and efficient ad-hoc wireless networks make use of directed graphs over the given set of nodes. These directed graphs may, in certain circumstances, form non-directed vertices in contrast to the directed graphs. The subsequent illustration elucidates the ad-hoc, which was comprised of the 10 ad-hoc nodes, and it demonstrates the application of directed graph-based connection formation.

Doi : https://doi.org/10.54216/IJWAC.010202

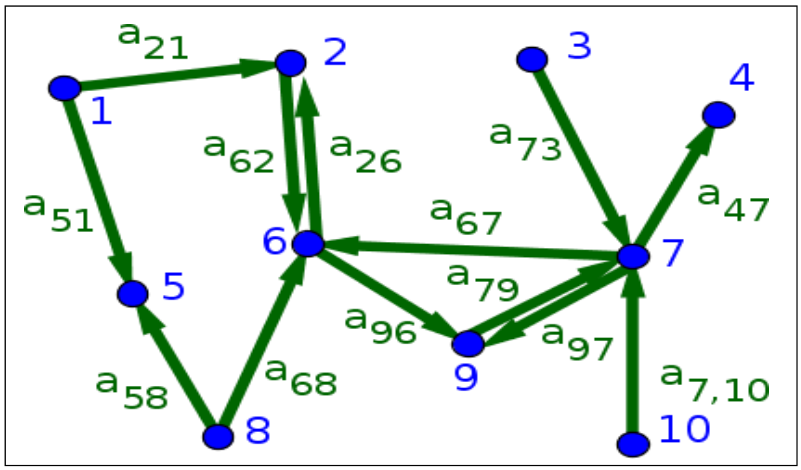

Figure 4: Wireless Ad-Hoc Network using CIA Model

The completely organized and layered model, which is supplied by the set of rules and symbols for the CIA model, is used to define the network availability relationships. This is done in accordance with the model. Both A and F yield the probability for nodes, with A indicating that the node is available and F indicating that the node is not available. N stands for the total number of nodes, s refers to the sparse matrix that exists throughout the network, and f details the many paths that may be taken via the sparse matrix. As a result, it is possible to define in a straightforward manner that the availability of the node is determined by deducting the probability of failures from 1 and doing the opposite calculation for failures.

$$\boldsymbol{Ku} = \frac{u^{u}}{R \cdot (\mathrm{SINRu}) \cdot Nt} \quad (1)$$

In (1), the value of the parameter Ku is determined by computing it using the total network load experienced by the wireless ad-hoc cell as a representation of the user density. This load is denoted by the symbol Nt. The following formula may be used to get the total network load that is present throughout the specified ad-hoc network cell (denoted c):

$$c = \sum_{u|X(u)=c} \boldsymbol{Ku} \geq \mathbf{0} \quad (2)$$

The symbol 'c', also known as the cell load, is assigned to the variable X, which gives the array of users' resources and contains information about all of the users or resources in the given network. This information is given in the equation that was just presented. The condition of Ku, which is used to denote overall load and must be greater than or equal to 0 in order to be satisfied. The value can be determined by using the equation that is provided here:

$$\text{utility}_{\ i} = \begin{cases} U_i + x_i \\ \left| \frac{U_i + x_i}{c + \sum_{j=1}^{i} k_u} \right|, \end{cases} \quad \text{otherwise } 0 \leq c_i \leq 1 \quad (3)$$

Algorithm 1: Balance Cluster Routing Algorithm for Expanding Wireless Networks (BaCRA-EWN)

1. Obtain information about the paths among the wireless network for each possible route in the cluster that is being used by the wireless technology.

Doi : https://doi.org/10.54216/IJWAC.010202

2. Determine the number of available resources for each individual node by calculating the load for each node and collecting the on-link factors for each node.

3. Determine the availability of resources for the specified network segment by making use of the information from step 2.

4. Determine the cluster utility index, which provides an overview of the current state of the wireless cluster if an inter-cluster connection is established.

To determine the priority among the nearby units, a utility index is appended to each micro-cluster that is part of the wireless network.

6. Utilize the method for making decisions to choose the most optimal route available inside the existing network; this will be the path that will be used for path forwarding.

Step-by-step information on the way nodes are selected depending on the availability of computer resources is provided in the preceding method, which is based on the balancing cluster routing algorithm for growing wireless networks.

3.2 Proposed Model Visualization

The proposed protocol is capable of single path routing, multipath routing, and routing data around connection problems all at the same time. The destination node is made fixed throughout the process of route construction, and the color Yellow is given to it. After that, the source node from which one wishes to transfer data must be specified. After that, the Energy Efficient WSN Path Optimization (EEWPO) algorithm collects all of the nodes that fall within the range of the source and the destination by utilizing the coordinates of the source and the destination. All of these are nodes that contribute to the development of paths from the source to the destination. The next step is called the Path creation phase, and during this phase, several potential pathways will be constructed. This route construction is going to be done on the basis of greedy forwarding, which implies that only those pathways are going to be picked that give progress toward the sink. These pathways may consist of a single path or numerous paths, depending on the options that are open to them. During this stage, all of the nodes that are located within a certain range of the source node are picked, and their respective distances from the source are then determined. The node that is the farthest away from the target is the one that gets chosen. This node has been given the label of "Idx node" for the time being. Once again, the process keeps on, and a route in the direction of the sink is produced. Following the completion of the path construction phase, the path forwarding phase sends data along the pathways that were created in the phase before it. If there is just one route, it will send data packets down that way if there is only one path. In the event that more than one route is constructed, the choice method will be implemented. First of all, the energy of both pathways, specifically the energy of the node in each path with the lowest energy, is compared. The route that has the most available power will be chosen as the optimal one for data transmission. In the event that there is a tie between the energies of both pathways, the subsequent metric will be examined. After that, the energy of the node that has the second least energy is compared to the energies of both pathways to determine which has the second lowest total. Checking the bandwidth of the source node and the next node in both paths is done similarly if a tie occurs for a second time. When it comes time to forward the path, the end node id will be checked, and the path that has a node with a higher id will be chosen. In this manner, the decision metric reveals the course of action that is most advantageous for data forwarding. The Push back Algorithm is responsible for the discovery of connection holes. In order to identify any gaps in connection, it examines three aspects of each node. It examines energy, avail, and queue factors. In this case, avail will tell you whether the node is still active or not, and the queue will tell you whether or not a node's queue is currently at capacity. In addition to this, should there be any such node, the data will be sent through the second way.

Doi : https://doi.org/10.54216/IJWAC.010202

4. Simulation of Energy Efficient Wireless Path Optimization (EEWPO)

Using network simulator version 2.35, the Energy Efficient Wireless Path Optimization (EEWPO) is simulated. The. Nam and. tr files are used to do the analysis of the findings. The abbreviation name refers to the network animator, which illustrates the data flow between the nodes and the node deployment scenario. The letters tr are short for "trace file." Trace files are files that record the values of parameters that are used to check the performance of a network. These files also give the values that correspond to those parameters, which can be used for further graphical analysis and can also be used to compare the values of one trace file to those of another trace file. The following table details the many simulations of EEWPO, along with the organization's various stages:

4.1 Node deployment

There are 28/56/100/500 nodes deployed in a random manner, and they are all given the color green at the beginning, with the destination fixed as node number 26, and the source node is assumed to be node number 1 at the same time. The straightforward configuration of the node deployment is shown in the next figure, which is 5 when there are just 28 nodes in operation and they are all colored green as was discussed previously.

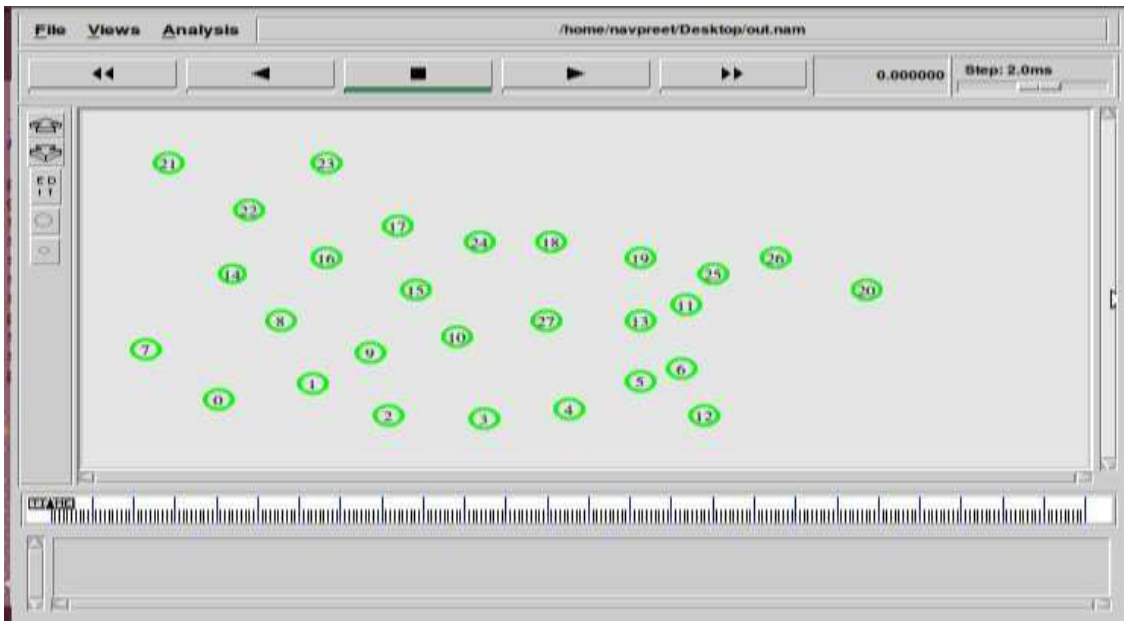

Figure 5: Node Deployment

a) Single Path Routing: The single route routing phase is successful if there is just a single path accessible between a source and a destination. This instance's source node and destination node are shown to be node 1 and node 26, respectively. The color purple has been designated for the source, and the color yellow has been designated for the destination. Only the nodes that are physically present between the source node and the destination node will be considered for selection by the Map route function. In order to do this, the coordinates of both the source and the destination are examined. Because of this, the overhead associated with employing any additional nodes for route construction will be reduced. A snapshot of the map route function is given in figure 6; in this illustration, all nodes that are colored red will be used for path construction.

Doi : https://doi.org/10.54216/IJWAC.010202

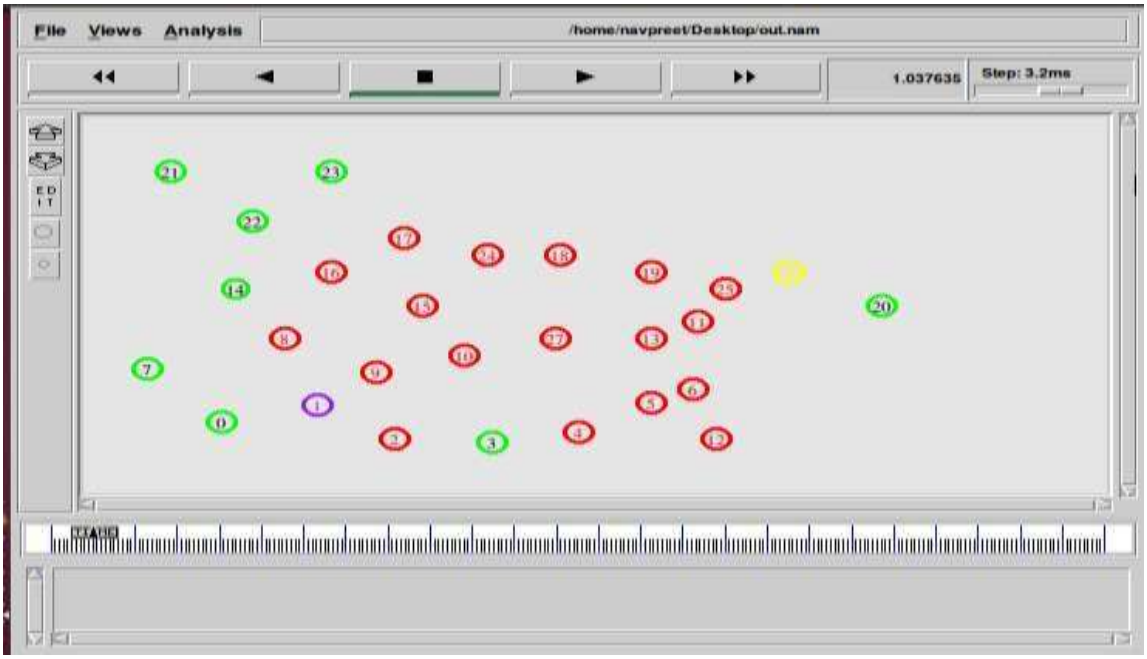

Figure 6: Selection of Nodes by Map Route Function

The source and destination nodes are taken as node 1 and node 26 respectively for the given scenario. Then only the required nodes that come within the range position between node 1 and node 26 are selected by map route and they are marked with the color red. The selection process is done by marking the network area that covers the source node 1 and sinks node 26 and all the nodes that comes between them. This is achieved by applying the left, right, top, and bottom areas of these two nodes by using simple directional coordinate formula. The path formation phase will form the best possible path. The path formed by BERP consists of nodes 1-9-10-27-13-25-26. As the path formed on the basis of greedy forwarding is single path routing, data is forwarded to this path as shown in figure 7. And, the traffic will be generated through this path.

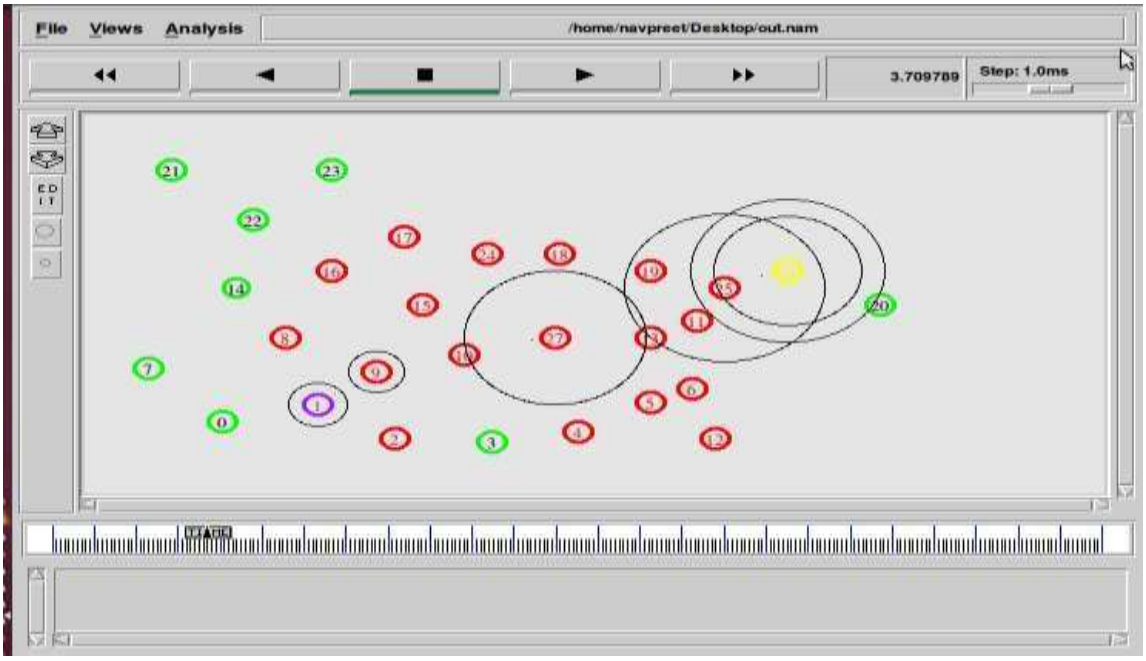

Figure 7: Data Forwarding in Single Path Routing

Doi : https://doi.org/10.54216/IJWAC.010202

b) Multipath Routing: Multipath routing is a technique in which there is more than one path available for data forwarding. In EEWPO, multipath routing is done in three phases, path formation, decision algorithm, and path forwarding. In the path formation phase, more than one path is formed or we can say an alternate path is also formed as a backup. After path formation, the decision-making algorithm is followed to take a decision as to which path to follow among the path formed in phase one. In the last phase, path forwarding takes place and traffic is generated through that path. Then the routing technique can select the best possible path to forward data. For load balancing, data can be forwarded to more than one path also. In this, if the path formed by EEWPO is more than one, then the best path is selected using a decision algorithm, and routing is performed on that path. Figure 8 shows the map route area for source 1 and sink 26. But here instead of one path, the algorithm is applied to provide more than one path to achieve the aim of multipath routing. This technique of multipath routing is more beneficial as it provides an alternate path in case of emergency or whenever required.

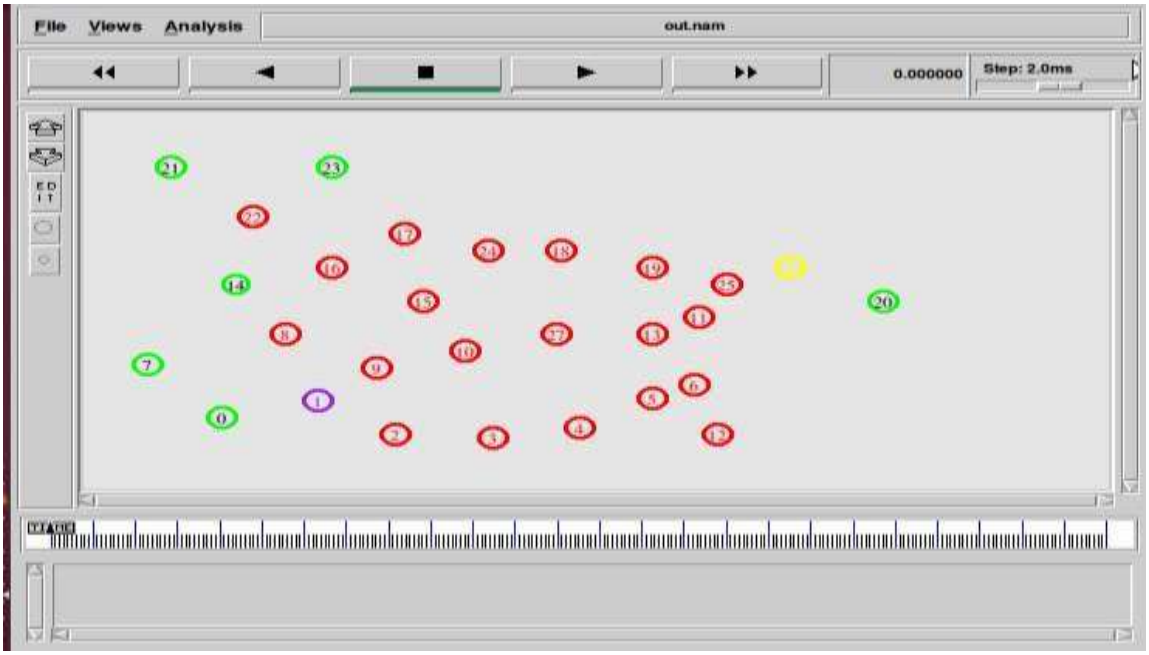

Figure 8: Selection of Nodes by Map route Function

The path formation module gives two paths for the source-destination pair (1-26). These two paths are 1-2-3-4-5-6-11-26 and 1-9-10-27-13-25-26. The after this, the Decision algorithm selects the best path from these two. The path 1-9-10-27-13-25-26 is selected on the basis of Node id. Figure 9 shows the simulation of the best path selected from the two and data is forwarded through that path to destination 26.

Doi : https://doi.org/10.54216/IJWAC.010202

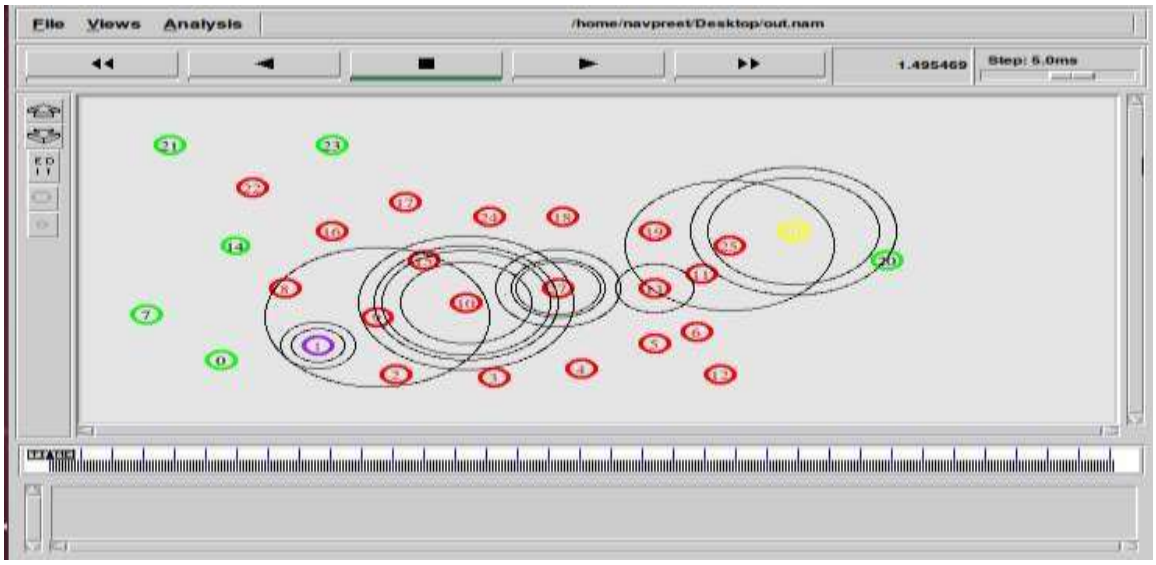

Figure 9: Data Forwarding on Best Path Based on Decision Algorithm

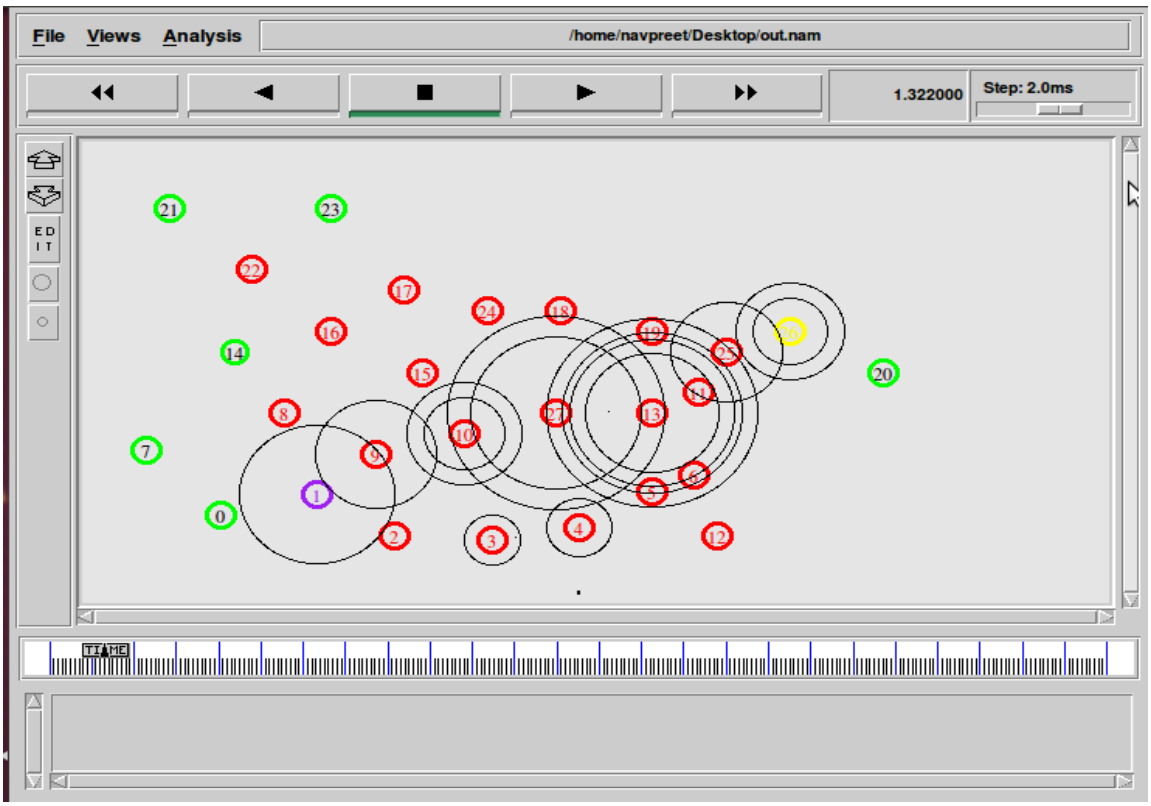

Figure 10: Data Forwarding on Two Paths for Load Balancing.

c) Load Balancing: Load balancing means balancing the load of the network by routing data to multiple paths. In this module, Data is forwarded through multiple paths to sink. It will send data packets on multiple paths so as to reduce the load of one path. Figure 10 shows the simulation of load balancing. It shows that data packets are sent from both paths formed by the path formation phase. The two paths formed for the source-destination pair (1-26) consist of nodes 1-2-3-4-5-6-11-26 and 1-9-10-27-13- 25-26. And, data is forwarded to both paths.

Doi : https://doi.org/10.54216/IJWAC.010202

4.2 Push Back Algorithm

Push back algorithm detects if there occurs any connectivity holes in the network. It will check the energy, availability, and queue status of the node. If it finds that the node is not alive then push back outputs that node as a dead end and the path forwarding module will not send data on that path. The color of the node which is a connectivity hole is changed to orange. In the simulation snapshot, the source is specified as node1 and the destination is a node. The path formation selects two paths 1-2-3-4-5-6-11-26 and 1-9-10-27-13-25-26. But

node 11 is a connectivity hole, so, the decision algorithm will send data on the second path to avoid the connectivity hole.

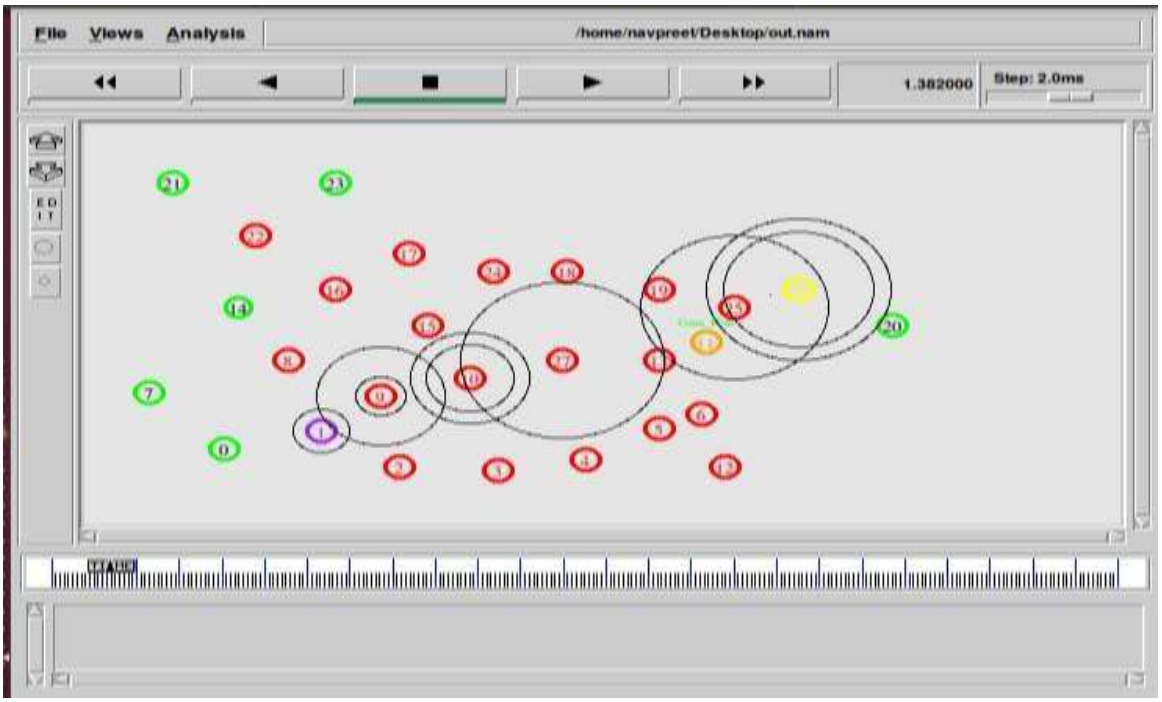

Figure 11: Connectivity Hole Detection

6. Conclusion

The fact that the sensor nodes only have a limited amount of energy available served as the impetus for the work that is outlined in the proposal. In the work that has been presented, the protocols for effective routing in WSN have been provided, and evaluations have been carried out by simulating the systems using NS-3 and Contiki/Cooja. Within the confines of this proposed work, an updated version of an energy-efficient cluster-based routing protocol that makes use of IPv6 has been provided. This protocol is based on both the static and mobile sink. In order to improve lifetime, latency, and reliability, the energy-efficient hierarchy-based clustering routing (EEHCR) protocol was designed. This protocol identifies multiple paths between the source and the sink in order to improve lifespan, latency, and reliability. Hierarchical structures were used in order to achieve this goal successfully. When used with wireless sensor networks (WSNs) that make use of IPv6 addressing systems, the protocol supports anycast, unicast, multicast, and multipath routing in its application. When it comes to the transmission of data, there is more than one alternative routing path that may be accessed. In the case that one way is unable to convey the data properly, another path will be used. It is possible for the sensor nodes to enter a condition known as "sleep" in order to save energy if it turns out that they are not required for the route that the data is being transmitted along. It has been brought to everyone's attention that the control packet overhead required for route discovery and maintenance is rather minimal. Because of this, the goal that was set for the improvement in energy efficiency was accomplished with flying colors. In order to reduce the quantity of duplicate data that is sent and the amount of traffic that is present in the network, the cluster-

Doi : https://doi.org/10.54216/IJWAC.010202

based multipath routing protocol is used. This is done in order to achieve both of these goals. In addition to this, the protocol reduces the strain that is exerted on the sensor nodes and confers more mobility on the sink. In this scenario, it is up to the sink to choose the node that will serve as the cluster head, choose the path that will provide the best possible routing, and keep track of the sensor nodes' current energy levels. It has been constructed as a tree-based routing with node and sinks mobility, and it is able to manage the mobile sink in the network in an efficient way. Additionally, it contains both of these mobility features. In order to gather the data, the sink is now making its way across the network. The formation of the tree is initiated by a sensor node, which subsequently develops into the root node of the tree. Between relay nodes, the connection may move in either direction; however, when traveling between a relay and a non-relay node, the connection can only proceed in one direction.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] C. K. Toh, "Ad Hoc Mobile Wireless Networks," Prentice Hall Publishers, 2002.
[2] Z. Bojković, M. Stojanović, and B. Milovanović, "Current Developments towards the 4G Wireless System," Proceedings of International Conference TELSIKS, Niš, Serbia, pp. 229- 232, September 2005.
[3] Chlamtac I.,Conti M.and Liu, J. J. N, "Mobile adhoc networking: imperatives and challenges" Ad Hoc Networks. Vol. No.1, pp. 13-64, 2003.
[4] Haoya Tan; Hoi-Lun Nagan; Yunhuai Liu; Nionel, L.M., "Measurement Study of MobilityInduced Losses in IEEE 802.15.4" IEEE International Conference on Communications (ICC 2010). pp.23-27, May 2010.
[5] H.Takagi and L. Kleinrock, "Optimal transmission ranges for randomly distributed packet radio terminals,"IEEE Trans on Communication,Vol. 32, No. 3, pp.246-257, March 1984.
[6] T.C Hou and V. O.K. Li, "Transmission range control in multihop radio networks," Trans On Communication, Vol. 34, No.1, pp.38-44, January 1986.
[7] Al-Akaidi M.: Alchaita, M., "Link Stability and mobility in adhoc wireless networks,", IET Communication, Vol.1, No.2, pp.173-178, April 2007.
[8] Ionis Nikolaidis, Michel Barbeau, Evangelos Krankis, "Ad-hoc and wireless Network," Third International Conference, ADHOC_NOW,Vol. 3158, Springer, pp. 651-660, 2004.
[9] Jing Deng, Yunghsiang S. Han, Po-Ning Chen and Pramod K. Varsheny,"Optimal Transmission Range for Wireless Ad Hoc Network Based on Energy Efficiency," .IEEE Transaction on Communications. Vol.55, No.9, 1439-1439, September 2007.
[10] Tien, T. C. and Upadhaya, S. J., "A Local/Global Strategy Based on Signal Strength for message Routing in Wireless Mobile Ad-Hoc Networks," IEEE Wireless Communication and Networking Conference, Vol.3 pp. 227-232, 2000.
[11] M.Abolhasan, B.Hagelstein, J.C.P Wang, "Real world performance of current Proactive multi-hop mesh protocols," IEEE APCC, October 2009.
[12] Neyre Tekbiyik,ElifUysal-Biyikoglu, Energy efficient wireless unicast routing alternatives for machine to machine networks, Journal of Network and Computer Application, Vol. 34, pp. 1587-1614,2011 101
[13] V.Kaudia and P.R. Kumar, "Power control and clustering in adhoc networks," IEEE INFOCOM, Vol.1, pp.459-469, 2003.
[14] S.Singh and C.S. Raghavendra, "PAMAS: power aware multi-access protocol with singling for adhoc networks," Computer communication review, Vol.28, No.3, pp. 5-26, 1998.
[15] A. EI Gamal, C.Nair, B. Prabhakar, E. Uysal-Biyikoglu, and S. Zahedi,"Energy –efficient Scheduling of Packet Transmissions over wireless networks," IEEE/ACM Trans. Networking, Vol.10 pp. 487-499, Aug2002.
[16] Swain, A.R., Hansdah, R.C., Chouhan, V.K,"Energy Aware Routing Protocol with Sleep Scheduling for Wireless Sensor Networks," 24th IEEE International conference on Advanced Information Networking and Applications (AINA), 20-23 pp. 933-940, April 2010.
[17] J. Gomez-Castellanos, A. Campbell, M. Naghshineh, and C. Bisdikian PARO: A Power – aware routing optimization scheme for mobile adhoc networks IETF Internet Draft, Section 10 of RFC2026, draft-gomez-paromanet-00.txt, March 2001
[18] Jones CE, Siva lingam KM, Agrawal P, and Chen JC, "A survey of energy efficient networks protocols for wireless network," Wireless Networks, Vol.7.No.4, pp. 343- 358, 2001.
[19] Henry Kumagi "Wireless Networking Security Consideration," published in Lasa Knowledgebase," Available at: http:/www.ictknowledgebase.org.uk/wirelesssecurity

Doi : https://doi.org/10.54216/IJWAC.010202

[20] Baker, D.J. & Ephremides, A. "The Architectural organization of a mobile radio network via distributed algorithm," IEEE transactions on communications COM- pp.1694-1701, 1981.

Doi : https://doi.org/10.54216/IJWAC.010202