VOL. 18, NO. 3, FEBRUARY 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

PATH PLANNING AND SECURE ROUTING IN WIRELESS SENSOR NETWORKS FOR MULTI-CONSTRAINED QUALITY OF SERVICE

Hyder Ali Hingoliwala and Gandharba Swain
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
E-Mail: hyderali.hingoliwala@gmail.com

ABSTRACT

In recent decades wireless sensor networks (WSN) are becoming important and playing important role in IoT applications. But because of limited battery power and the small size of sensor nodes, energy efficiency is the key parameter that is to be efficiently utilized. In this paper, Path Planning and Secured Routing for Multi-Constrained Quality of Service (QoS) in the WSN algorithm are proposed. The projected system can distribute the workload over alternate paths so as to keep away from congestion and minimize travel costs. It will guarantee reliable routing with less bandwidth and request a high packet delivery ratio since it keeps away from packet loss. WSN could likewise be impacted by attacks on routing resulting in altering messages and routes which can have an adverse effect on QoS parameters. The projected calculation can distribute the workload over alternate methods. Accordingly, we tend to get routing and path planning subject to multiple Quality of Service constraints for secure WSN communication.

Keywords: wireless sensor network, load balancing, path planning algorithm, multi-constrained, reliable routing, quality of service parameters.

1. INTRODUCTION

WSN has become a very important topic of discussion in the current decade, as all IoT applications are using WSN to drive the smart world. But due to very limited battery, small size, and unfavourable environmental application, energy efficiency has become an area of concern, and therefore a lot of work has been done in this area, but there is still room for improvement in this area.

Earlier some work has been done on WSN which was thought of designing multi data path which had some disadvantages like it failed to affect the average travel cost. The Ant Colony Optimisation rule tries to find the best way to target any location where different ants follow the way the leading ants run. Avoidance of overcrowding was not thought of for this situation. Thus predictive computation for multi-restricted quality of service in WSNs can work with path planning and secure routing information clusters to reduce congestion and uniform traffic evenly throughout the organization. Computation Rule has set its primary goal to provide an alternative path to information clusters to avoid congestion or accidents and to guarantee safe and reliable routing that can address multiple QoS constraints. Similarly taking into account relocation strategies for moving on purpose, the transfer speed requirement will be reduced, because traffic will be balanced. The system guarantees path planning and secure routing that can fully utilize network resources, so the average total cost of data packets is significantly reduced and traffic congestion is avoided.

2. RELATED WORK

Routing is considered to be an important factor while designing WSNs. The literature survey of the following related papers and summarized table have been shown below

The author [1] suggests the PDORP as the orientation of the information transfer path. Both a data-intensive data-collecting system and router DSR system processes are supported by the proposed PDORP protocol. In addition, the proposed route protocols use a combination of genetic algorithms and bacterial feeds to uncover effective energy-saving ways.

To enable sensitive delays, hungry, crucial bandwidth, and QoS-aware applications, the author [2] offers a multi-channel WSN power protocol. The proposed QoS-aware and heterogeneously clustered routing (QHCR) protocol not only saves network power but also gives key applications dedicated real-time routes and delays. Different WSN power levels are installed to offer network stability while decreasing latency for applications that are sensitive to delays.

The author [3] proposed an energy-saving centroid-based routing protocol that was approved. Another distributed bunch design that allows adjacent format node creation and another sequence of calculations for jumbling and turning the group head are covered by the EECRP. in light of the centroid region of fair force load distribution across all sensors, as well as a superior strategy to reducing the power usage of substantial distance communication In the EECRP, the residual power nodes are taken into account while computing the area of centroids.

The author [5] presented a new protocol for WSN system reliability that incorporates several characteristics of sensory nodes in terms of communication, data, power, and recommendation. The suggested dependability model is based on an enhanced slide time window that evaluates the frequency of attacks in order to detect attacker aggression. Active route acquisition and repair protocol are included.

Paper [6] proposes a numerical model for the next generation of QoS router determinants that includes the

assignment of an appropriate QoS border to aid a wide range of IoT applications that demand correspondence. The model is used to investigate the effects of multi-hop correspondence on a traffic framework model constructed using the Markov discrete-time M = M = 1 line model.

Paper [7] classified industrial sensory data into three types and assigned a value to each. We also provide reliability standards and time constraints, as well as a rival move region set to assess power usage. Following that, with the development of a power-saving calculation and a QoS global positioning framework, many types of data may be exchanged with various systems. In addition, the main industrial sensor data is designed to be conveyed to the sink via a reliable and timely means, and normal data can be effectively delivered.

By examining the power consumption of cluster networks and a wide range of power levels across multiple WSNs, Paper [8] offered an enhanced route protocol that saves energy for an integrated super-heterogeneous network (E-BEENISH). E-BEENISH is based on a thorough selection process.

E-BEENISH is based on the strict election possibilities for each node to become the group's leader, based on the remaining power and distance between the sink and the location. Furthermore, we investigate the impact of node heterogeneity on power.

For packet dump assaults, the author [9] created an acquisition mechanism. The degree of compression assessment method is then provided using sleep delays and linear lengths in asynchronous duty-cycled low-power listening (LPL) modes. Finally, we present QoS metrics for the development of a QoS awareness protocol, which can improve QoS performance in terms of exit, latency, and packet loss.

In a real-world environment, the stability of the WSN node line in ZigBee PRO was tested in a paper [10]. Changes in following hops on the route between the source and the destination can result in an unwanted increase in WSN power utilisation. As a result, route stability indications include the employment of the suitable route technique, the usage of the next hop, and the computation of the alternating frequency.

This paper [11] describes a dynamic and secure multi-jump routing (ESMR) protocol, which recognises the mystery of the giving scheme while assuring the security of multi-hop information against malicious activity. Three important points of view are addressed in the proposed convention. The organisation field is first separated into interior and exterior portions in light of the hub area. Furthermore, based on the location closest to the hub, unique bunches are formed in each area. Second, the proposed dynamic security sharing structure ensures that information is securely communicated from the headers to each area and finally to the submersion location. Finally, in order to reduce course impedance, the recommended layout considers the quantitative analysis of information links.

In order to expand the WSN network's existence, paper [12] proposed an innovative protocol for the effective energy source region (alluded to as ER-SR). Using a circulated power circuit computation, the power channel node in ER-SR is selected as the dynamic residual node at the network's highest point. The source network hubs then compute the correct source path for each normal hub, allowing the hubs to participate in the course cycle and assess the power consumption of the sensor nodes. We also provide an effective way for remotely developing an ant colony in order to determine the optimal ground transfer mechanism for each site in order to minimise data transfer power.

A paper [13] described the Adaptive Trust-based Routing Protocol (ATRP), which used twofold tests to integrate direct trust, circuitous trust, and multi-layered dependable trust (assets and security) into its dependability. The suggested method allows for a more thorough evaluation of a large number of potential hubs in just a few bounces, resulting in better power usage and network life.

Paper [14] employed a transmitting display on a nearby route to convey a few non-essential data messages from the sensor node. Without the requirement for a pioneer, the node can spontaneously converge and relate upward along these lines. A pair of sensor hubs can be utilised in this scenario to integrate data from a single incident. We show that information integration rate and energy usage are reduced in any way when compared to non-combination utilising simulations.

Paper [15] designed and implemented the RH-MAC standard using CSMA and TDMA MAC Protocols. For Improving Service Quality, RH-MAC (QoS, for example, PDR, PLR, Throughput, start-to-finish delays, congestion control, and reliability). Congestion control utilising the TDMA convention from a single sink hub. CSMA is used by all hubs. In the second model, we must apply cluster-based information distribution.

In a study [16], a multi-hub charger was proposed, which can receive and charge many sensors at the same time. The suggested plot is both static and dynamic, and it employs a weighted heuristic approach to find a near-optimal charge scheme. The residual energy of sensors is mentioned as network boundaries in the weight function. The weight function takes into account residual energies, contribution count values, and distances to the charging component when determining the sensors' charging scheduling priority.

3. THE EXISTING METHOD

The current technique employs the Ant Colony Optimization Method to generate computer-generated routes on WSNs within various QoS constraints. It is used during the time spent watching a route based on the amount of pheromone present. When the pheromone has worn off, the path is abandoned in favour of a much better one. It uses an adaptive graph focused on the hub to verify the validity of traffic signal messages transmitted between hubs. To achieve the goal of a secure route, the framework employs the Secure Ant-Based Multi-Constrained QoS Routing Algorithm (S-AMCQ). Every ant in this colony follows the ants leading them to their goal. Assuming that the problem is large, which implies that there is a lot of

gridlocks, the time it takes to travel the route will be extended. As a result, delivering the proper route for the unanticipated number of hubs will take longer. Because all ants travel in the same direction, the network may get congested. The calculation saves some energy. These elements should be considered in order to ensure a compelling and reliable route across WSNs.

3.1 Proposed Work

The proposed framework problem is to devise a competent, unobtrusive, and secure routing scheme for the WSN, a network that operates in an unregulated and, at times, hostile environment. Because traffic is growing at a faster rate, the course cycle should provide elective traffic light frameworks, and WSN regions have resources (especially limited limit and restricted interior capacity limit), route regulation should be less energy efficient and not challenging. At the top of the hubs is a capacity region. Additionally, by detecting and preventing hub attacks, the safe multi-hop transmission of data packets is enabled.

The goal of this study is to see how routing approaches can be used to work with QoS on WSNs with various restrictions, avoid security risks in the routing cycle, and work on all-inclusive use. The Path Planning and Multi-Constrained QoS (PPMCQ) Route Planning Algorithm is used for this.

Design Considerations

a) Providing substitute path

b) Avoid Congestion

c) Minimize start to finish delay

d) Increase packet delivery ratio

e) Increase Reliability

f) Secure directing or routing

g) Improve execution or performance

h) Perform Load adjustment

Plan Considerations

A. System Architecture

a) Roadside unit (RSU): Correspondence occurs between hubs or between hubs and RSUs. Each RSU has its own development schedule. RSU1, RSU2, RSU3, and RSU4 make up the four sets in Figure-2: C1, C2, C3, and C4. The tone of the hubs varies as they move from one RSU cover to the next.

b) Base station: The organization is screened by a focused framework.

c) Intermediate hops: The vertices of our network are the intermediate hops or hubs. These are the network's static hubs that serve as points of interaction for the route.

d) Nodes: These are dynamic substances that use energy to choose their path. They suggested that RSU relocate the course from its original location to the optimum location. They passed through many RSU-related assortments. In the event of a crisis, such as overcrowding, they also contact their neighbours' route.

B. Path Planning based Multi-Constrained QoS Routing Algorithm (PPMCQ)

a) The PPMCQ route is used in our proposed design to avoid network congestion. We have considered the state of the metropolitan street. To achieve our goal, we employ additional local tactics that reduce traffic flow and the predicted data transfer capacity. These aspects will also aid us in achieving a greater packet delivery rate, reducing delays, and providing a reliable and secure route. Following that, framework execution will improve, leading to a compelling and effective solution to the problem. It is a powerful street board device that improves the use of the street organisation and tries to reduce the cost of driving in order to avoid gridlock hubs. The driver has complete control over the path to his goal when driving. As a result, calculating a path becomes difficult. The route arranging calculation will generate multiple routes in the same location, allowing traffic to cycle across the organisation and the driver to select the optimal path to their destination. In WSNs, general street use is improved by avoiding congestion. When congestion is avoided, we can easily reach QoS boundaries, such as increasing packet delivery rates, which will help WSNs run more reliably. Due to the size of the shipments, heap adjustment procedures are used, which involve breaking the packet into pieces and sending it in the other direction.

C. Secure Information Exchange

b) In WSNs, network correspondence occurs between vehicles (V2V) or between side-of-the-road units (V2R). Expected correspondence for Route control message transmission (RCM). Despite the fact that we are cultivating a good route calculation, we must also protect this route data to ensure a strong and reliable route. Messages should be protected from potential WSN attacks in this way. Attacks may induce small changes in message details, causing route data to vary and network traffic to increase. To protect the firm from such threats, we must ensure that the routing system is secure. To use WSN security, consider the following boundaries: message verification, message access, message denial, message privacy, and message confidentiality. We use public key cryptography to accomplish this goal. The Elliptic Curve Cryptography (ECC) calculation is used in our circumstance of protecting RCMs and converting them into decipherable arrangements. The Certificate Authority will generate public and private keys for hubs and RSUs (CA). This will ensure the secure transmission of communications across WSNs.

D. Mathematical Model

Set Theory (A)

Let S be a framework, with S=N, CA, RSUs, and PTH.

1) Vehicle (hubs): N= N1, N2,..., Nn N is the total number of hubs.

2) Graph: G is a collection of all diagram vertices, such as G = g1, g2,....gn.

3) Sc (source hub)

4) D is the destination hub.

5) Base Station/Certified Authority: The base station is the CA that all hubs trust and relies on to verify hubs in the network.

6) Roadside Units: RSUs are roadside units that serve as a route.

7) Paths available: PTH= P1, P2,..., PN

PTH is a collection of all feasible routes from point A to point B.

E. Equations

1) PDR (Packet Delivery Ratio):

1) PDR (Packet Delivery Ratio): This is the ratio of the number of parcels successfully delivered to a destination, such as PR, to the number of parcels shipped, for example. PS.

$$PDR = PR/PS \quad (1)$$

2) RDT (Route Discovery Time): Time spent tracking down a route to an objective by evaluating start and end times, such as ST and E.

$$RDT = ET - ST \quad (2)$$

3) Energy ETx (Energy for Transmission): The energy required to transfer a message is determined by calculating the energy required to power transmitter gear, for example.

$$ETx (k; d) = Eelec * K+ amp * k * dn \quad (3)$$

ERx (Energy for Receiving): The energy required to receive a message is calculated in the same way as the energy required to send a message by obtaining the energy required to drive the recipient circuit and k pieces per message.

$$ERx(k) = Eelec * k \quad (4)$$

UE (Updated Energy) is the excess energy from available energy, such as AE, after sending and receiving messages.

$$UE = (ETx + ERx) - (AE) \quad (5)$$

IV. ALGORIHM

Input: Request for route from source to destination.

Stage 1: Begin

Stage 2: Begin the important channel functions as a Certificate Authority (CA)

Stage 3. CA issues hubs and RSU with certificates to verify them.

Stage 4: RSU makes an impact on the hubs within their reach, allowing them to view their surroundings and detect collisions.

Stage 5: Apply for an immediate course at RSU by specifying the source and destination.

Stage 5: Apply for an immediate course at RSU by specifying the source and destination.

Stage 6. RSU will create the optimum route from source to area by listing all possible routes.

Dijkstra's directed computation for shortest path is used to determine the most limited path.

```
 Dijikstras(G,S
{
for every hub g in G
dist[g] <-boundlessness
prev[g] <-unclear
 add g to G
distance[S] <-0
while G isn't vacant
m <-g in G with least
 dist[m]
eliminate m from G
for each neighbor g of m
alt <-dist[m] + length(m,g)
in the event that alt < dist[g]
            dist[g] <-alt
 prev[g] <-m
 return dist[], prev[]
 }
```

Stage 7. In case of an impact on the course, observing RSU will make an impression on the base station

Stage 8: Another RSU is illuminated by the base station.

Stage 9: RSU sends out an urgent message to all hubs and offers an elective course.

Stage 10: Present a vehicle in the best possible light when it is required.

Stage 11: Make the key.

W = rc, where W denotes the public key.

r: irregular number between 1 and n-1

r: irregular number between 1 and n-1

Stage12: Send the message after encoding it.

C2 = k * P

C1 = M + kW, where C1, C2 are the figure text

M is the unique message.

Stage 13: If a message comes from an authorised hub, the recipients should acknowledge it and decode it.

C2 - d * C1

stage 14: else , dispose the bundle.

Stage15. Rehash stages 6 to 14 until all solicitations are handled

Stage16. Stop

4. RESULTS AND COMPARISION

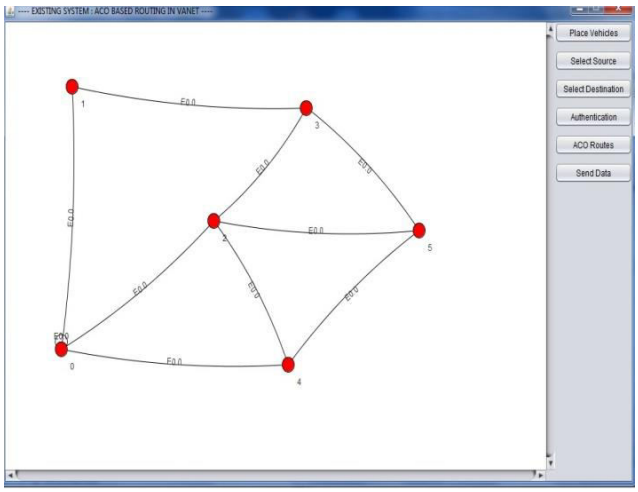

Figure-1. A graph with 5 nodes, with red dots indicating hops and paths linking the hops.

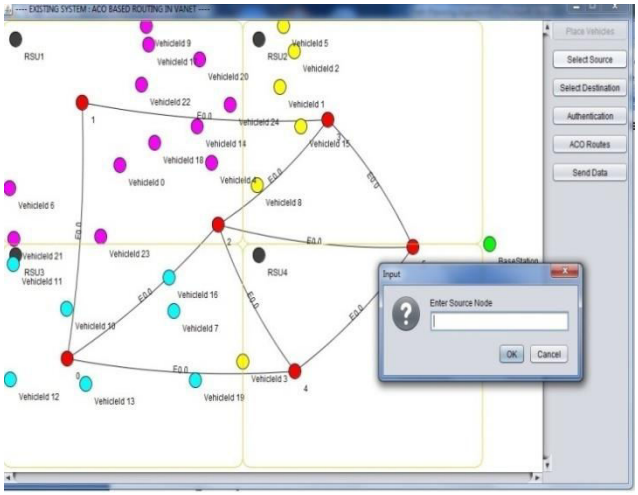

Figure-2. Demonstrates source node selection the select source button allows the user to select a source to move from.

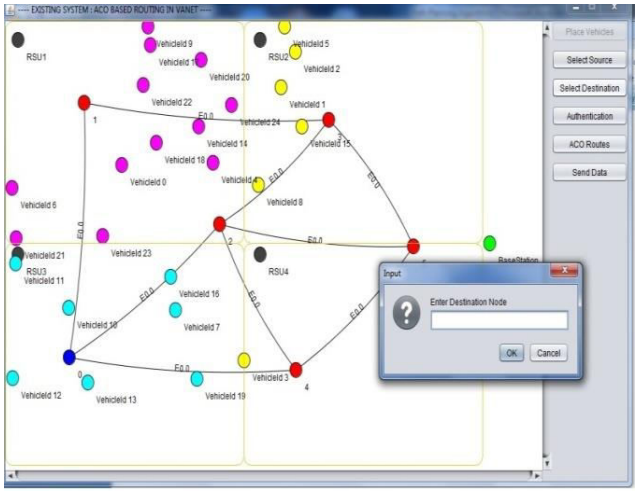

Figure-3. Explains how to choose a destination node. The user can select a destination by hitting the select destination button.

ClusterList [VehicleId 6, VehicleId 22, VehicleId 0, VehicleId 21, VehicleId 20, VehicleId 9, VehicleId 14, VehicleId 18, VehicleId 17, VehicleId 24, VehicleId 23, VehicleId 4] [VehicleId 1, VehicleId 2, VehicleId 5, VehicleId 8, VehicleId 15] [VehicleId 13, VehicleId 10, VehicleId 16, VehicleId 12, VehicleId 19, VehicleId 11, VehicleId 7] []
rsu 1: x 21.0
rsu 1: y 25.0
rsu 1: x 427.0
rsu 1: y 25.0
rsu 1: x 21.0
rsu 1: y 315.0
rsu 1: x 427.0
rsu 1: y 315.0
rsu 1: x 812.0
Authenticating RSUs and Vehicles from Base Station
For RSU: RSU1, RSU2, RSU3, RSU4
For Vehicle: VehicleId 6, VehicleId 13,VehicleId 22, VehicleId 0,VehicleId 21
Authenticating RSUs and Vehicles from Base Station
For RSU: RSU1
CA assigns unique certificate
RSU: RSU1 registered successfully
Requesting The Path From RSU1
Source node 0
Destination node 5
Path0: [0, 1, 3, 5]
The Distance Between The Node 0 And Node 1 Is 344.90723390500233
The Distance Between The Node 1 And Node 3 Is 410.6446152088202
The Distance Between The Node 3 And Node 5 Is 222.27235545609355
The Total Distance For the Path [0, 1, 3, 5] Is 977.8242045699161

Path1: [0, 1, 3, 2, 5]
The Distance Between The Node 0 And Node 1 Is 344.90723390500233
The Distance Between The Node 1 And Node 3 Is 410.6446152088202
The Distance Between The Node 3 And Node 2 Is 231.01947969814148
The Distance Between The Node 2 And Node 5 Is 326.3816784073518
The Total Distance For the Path [0, 1, 3, 2, 5] Is 1312.9530072193159

Path2: [0, 2, 5]
The Distance Between The Node 0 And Node 2 Is 309.6837096135346
The Distance Between The Node 2 And Node 5 Is 326.3816784073518
The Total Distance For the Path [0, 2, 5] Is 636.0653880208863

Path3: [0, 4, 5]
The Distance Between The Node 0 And Node 4 Is 380.3800730848029

The Distance between The Node 4 And Node 5 Is 258.25955935840983
The Total Distance For the Path [0, 4, 5] Is 638.6396324432128

Path4: [0, 4, 2, 5]
The Distance Between The Node 0 And Node 4 Is 380.3800730848029
The Distance Between The Node 4 And Node 2 Is 234.93190502781866
The Distance Between The Node 2 And Node 5 Is 326.3816784073518
The Total Distance For the Path [0, 4, 2, 5] Is 941.6936565199733

Path5: [0, 2, 3, 5]
The Distance Between The Node 0 And Node 2 Is 309.6837096135346
The Distance Between The Node 2 And Node 3 Is 231.01947969814148
The Distance Between The Node 3 And Node 5 Is 222.27235545609355
The Total Distance For the Path [0, 2, 3, 5] Is 762.9755447677696

Path6: [0, 2, 4, 5]
The Distance Between The Node 0 And Node 2 Is 309.6837096135346
The Distance Between The Node 2 And Node 4 Is 234.93190502781866
The Distance Between The Node 4 And Node 5 Is 258.25955935840983
The Total Distance For the Path [0, 2, 4, 5] Is 802.8751739997631

Path7: [0, 4, 2, 3, 5]
The Distance Between The Node 0 And Node 4 Is 380.3800730848029
The Distance Between The Node 4 And Node 2 Is 234.93190502781866
The Distance Between The Node 2 And Node 3 Is 231.01947969814148
The Distance Between The Node 3 And Node 5 Is 222.27235545609355
The Total Distance For the Path [0, 4, 2, 3, 5] Is 1068.6038132668566

Path8: [0, 1, 3, 2, 4, 5]
The Distance Between The Node 0 And Node 1 Is 344.90723390500233
The Distance Between The Node 1 And Node 3 Is 410.6446152088202
The Distance Between The Node 3 And Node 2 Is 231.01947969814148
The Distance Between The Node 2 And Node 4 Is 234.93190502781866
The Distance Between The Node 4 And Node 5 Is 258.25955935840983
The Total Distance For the Path [0, 1, 3, 2, 4, 5] Is 1479.7627931981926

The Minimum Distance Is 636.0653880208863
The Minimum Distance Path Is [0, 2, 5]

Routing Initiated With Path Generation By Ant Colony Optimization
The data at the source 1 is Data78179197
The generated MAC of data at source is b3616e61783fbeb1c893ec76b5e504c4
The Data Received At The 0 Is Data78179197
The data received at final destination is Data78179197
Authenticating Data
The generated hash at the destination is b3616e61783fbeb1c893ec76b5e504c4
The Valid MAC Generated Of The Data At The Final Destinaion

Source node 0
The resetnode list is[4, 3, 1, 0, 2, 5]
allvertice0->1->3->5
The nodeList is [0, 1, 3, 5]
allvertice0->1->3->2->5
The nodeList is [0, 1, 3, 2, 5]
allvertice0->2->5
The nodeList is [0, 2, 5]
allvertice0->4->5
The nodeList is [0, 4, 5]
allvertice0->4->2->5
The nodeList is [0, 4, 2, 5]
allvertice0->2->3->5
The nodeList is [0, 2, 3, 5]
allvertice0->2->4->5
The nodeList is [0, 2, 4, 5]
allvertice0->4->2->3->5
The nodeList is [0, 4, 2, 3, 5]
allvertice0->1->3->2->4->5
The nodeList is [0, 1, 3, 2, 4, 5]
Pheromone Paths [[0, 1, 3, 5], [0, 1, 3, 2, 5], [0, 2, 5], [0, 4, 5], [0, 4, 2, 5], [0, 2, 3, 5], [0, 2, 4, 5], [0, 4, 2, 3, 5], [0, 1, 3, 2, 4, 5]]
Routing Initiated With Path Generation By Ant Colony Optimization
hash.....f6e9ec7837b5f576c157412b809abc2b
Cypher f6e9ec7837b5f576c157412b809abc2b

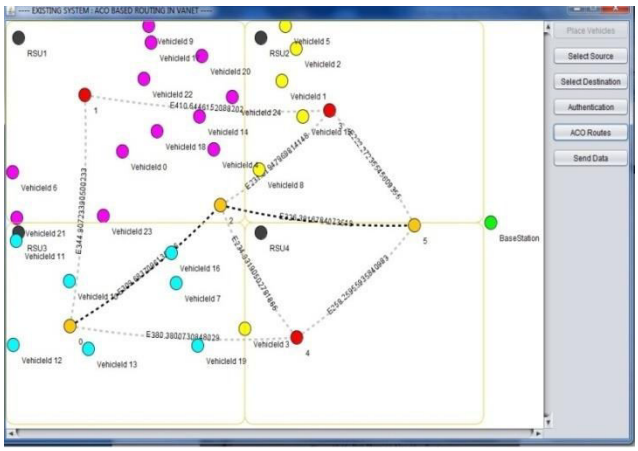

Figure-4. Depicts the ant colony optimization algorithm in action.

Each edge has a certain amount of weight given to it. The shortest route chosen by the leading ant to travel from source to destination is depicted by the black dotted line. The pheromone pathways to the goal are the grey dotted lines.

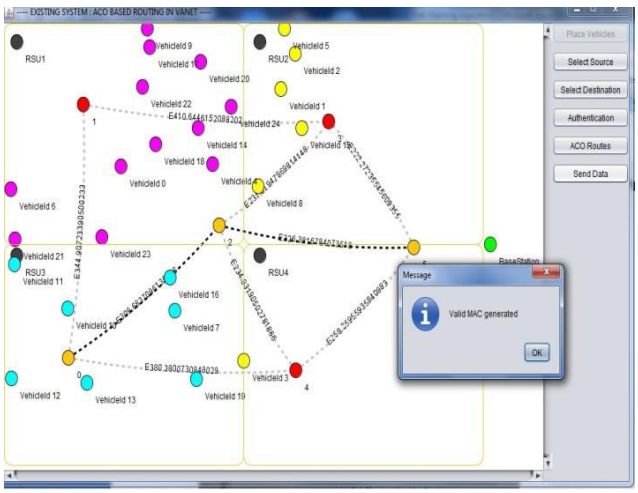

Figure-5. Depicts the data flow from the source to the destination node. The MAC is created at the source, and data is sent to the destination hop by hop. Then, at the destination, a hash is formed; if the MAC matches, the data is accepted; otherwise, it is rejected.

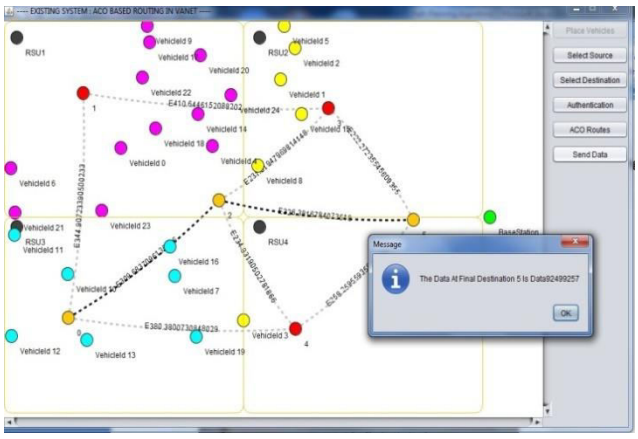

Figure-6. Depicts the best route from source to destination.

5. CONCLUSIONS

By offering an appropriate route management technique, our system gives a source-to-destination path-planning solution to the problem. In traffic situations, path planning and secured routing based on multiple QoS to WSNs are utilised to give alternate routes to minimise congestion on WSNs. The suggested method ensures a reliable path by meeting several QoS requirements, including lowering delays, boosting delivery rate, conserving energy, and avoiding traffic congestion. Cryptographic features in routing control messages protect the route process. As a result, our proposed algorithm ensures a secure and dependable path on WSNs.

REFERENCES

[1] G. S. Brar, S. Rani, V. Chopra, R. Malhotra, H. Song and S. H. Ahmed. 2016. Energy Efficient Direction-Based PDORP Routing Protocol for WSN. Vol. 4.

[2] M. Amjad, M. K. Afzal, T. Umer and B. S. Kim. 2017. QoS-Aware and Heterogeneously Clustered Routing Protocol for Wireless Sensor Networks. IEEE Access. 5: 10250-10262.

[3] J. Shen, A. Wang, C. Wang, P. C. K. Hung and C. F. Lai. 2017. An Efficient Centroid-Based Routing Protocol for Energy Management in WSN-Assisted IoT. IEEE Access. 5: 18469-18479.

[4] W. Qu and X. Wang. 2017. uXaving routing strategy based on ant colony optimization in wireless sensor networks. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10385 LNCS, pp. 277-284.

[5] B. Sun and D. Li. 2017. A Comprehensive Trust-Aware Routing Protocol with Multi-Attributes for WSNs. IEEE Access. 6: 4725-4741.

[6] M. Z. Hasan, F. Al-Turjman and H. Al-Rizzo. 2018. Analysis of Cross-Layer Design of Quality-of-Service Forward Geographic Wireless Sensor Network Routing Strategies in Green Internet of Things. IEEE Access. 6: 20371-203898.

[7] W. Zhang, Y. Liu, G. Han, Y. Feng and Y. Zhao. 2018. An Energy Efficient and QoS Aware Routing Algorithm Based on Data Classification for Industrial Wireless Sensor Networks. IEEE Access. 6: 46495-46504.

[8] Y. Zhang, X. Zhang, S. Ning, J. Gao and Y. Liu. 2019. Energy-efficient multilevel heterogeneous routing protocol for wireless sensor networks. IEEE Access. 7: 55873-55884.

[9] P. Shi, C. Gu, C. Ge and Z. Jing. 2019. QoS Aware Routing Protocol Through Cross-layer Approach in Asynchronous Duty-Cycled WSNs. IEEE Access. 7: 57574-57591.

[10] C. L. Lim, C. Goh and Y. Li. 2019. Long-Term Routing Stability of Wireless Sensor Networks in a Real-World Environment. IEEE Access. 7: 74351-74360.

[11] K. Haseeb, N. Islam, A. Almogren, I. Ud Din, H. N. Almajed and N. Guizani. 2019. Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs. IEEE Access. 7: 79980-79988.

[12] C. Xu, Z. Xiong, G. Zhao and S. Yu. 2019. An energy-efficient region source routing protocol for lifetime maximization in WSN. IEEE Access. 7: 135277-135289.

[13] N. A. Khalid, Q. Bai and A. Al-Anbuky. 2019. Adaptive Trust-Based Routing Protocol for Large Scale WSNs. IEEE Access. 7: 143539-143549.

[14] K. Hadi. 2019. Analysis of exploiting geographic routing for data aggregation in wireless sensor networks. Procedia Comput. Sci. 151(2018): 439-446.

[15] H. A. Hingoliwala and G. Swain. 2018. Improving Qos parameters in wireless sensor network. ARPN J. Eng. Appl. Sci. 13(8): 2873-2881.

[16] N. Kumar, G. Swain and S. Routray. 2022. On-demand charging planning for WRSNs based on weighted heuristic method. Int. J. Inf. Technol.