International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

# Node Deployment Based on Shortest Path Creation on Mountain Road for Wireless Sensor Networks

**Napoleon Khoisnam[1], Aruna Ramalingam[2]**

[1]*Digital Electronics and Communication, AMC Engineering College, Bengaluru, India*

[2]*Department of ECE, AMC Engineering College, Bengaluru, India*

## ABSTRACT

*In wireless sensor networks (WSN), node deployment and optimal path creation are the most important tasks and also critical issue. WSN is much constrained for computational power, energy and memory. Nodes in wireless sensor network works on battery power and energy consumption plays a very important role in WSN. Usually communication i.e. transmission and reception consumes more energy compare to data processing and sensing. Hence maximum energy can be saved by controlling the communication with the help of proper routing. Wireless sensor networks on mountain roads will form winding and long transmission paths. As per the reception and data transmission analysis maximum energy wasted due to longest path, unnecessary route request flow and due to some attacks. To increase lifetime of network by reducing energy consumption new shortest path technique on mountain road is introduced in this proposed paper. Dijkstra's technique is used in this system is to create shortest path and also explains functional steps involved in Blackhole node estimation and solution procedure to overcome that problem. In this paper, it has been analysed thevarious parameters such as maximum transmission rounds, network lifetime comparison and packet delivery ratio.*

***Keywords:*** *Wireless Sensor Networks, Dijikstra's Technique, Shortest Path, Blackhole Attack, Transmission.*

## I. INTRODUCTION

Wireless sensor networks (WSNs) are called as wireless sensor and actuator networks (WSAN). Wireless networks are circulated or distributed large collection of sensors to monitor environmental or physical conditions. The WSNs development was inspired by military applications such as battlefield supervision. In recent days such networks are utilized in several consumer and industrial applications, such as machine healthiness monitoring, industrial process monitoring and control etc.

WSN composed of thousands of sensor nodes. These sensing nodes are able to sense at least single environment phenomenon. Sensor nodes are battery motorized. Recharging or replacement of battery is not achievable in so many scenarios such as rescue operation, battlefield supervision and unmanned missions. Sensor nodes have to perform process like detection of certain object presence, object observation and tracking, data fusion, localization and event monitoring. This process of sensor nodes makes sensor nodes to create large quantity of

data and information. After generating large amount of information sensors has to transmit that collected information to base station or sink node. If WSN uses less energy to complete its task then lifetime of network will get increase. The reporting between sink node and source node utilizes energy based on the communication path, communication protocol type and number of hop counts between source nodes and sink node. This requires optimal path creation between source nodes and base station (i.e. sink node). This optimal path will get useful in efficient forwarding or transmission of information, reduction in consumption of power and communication problems in WSNs. Including optimal path creation, successful transmission and reception of information is also very important. During communication there are high chances of suspecting to network attacks such as

Denial of Service Attack (DoS), Node Capture Attack, and Eavesdropping attack etc. Blackhole attack is the one of the DoS attack. When source node wants to send information to the base station it transmits route requesting messages to all other nodes. Blackhole attack is also being part of network it accepts route request message and gives reply with route acknowledgement messages to ahead of all other nodes. Then it receives information to it from source nodes by falsely claiming the optimal path to the base station and it drops them continuously instead of forwarding packets. In our work we identifying optimal communication path between source node and base station using Dijikstra's technique and also we focus on blackhole node detection and solution to it.

## II. LITERATURE SURVEY

Xuxun Liu et.al [01] has presented node deployment strategy in WSNs. In this referred paper, to resolve grid-based and deterministic deployment problem deployment strategies for various sorts of requirements are presented. This strategy contains the deployment techniques. Primary one is cost based deployed technique, second one is transmission delay based technique. In this technique deployment cost profit, length of transmission path and transmission delay is evaluated and lost one is life time based technique in which extra nodes are deployed where really necessary. Aniket. A. Gurav et.al [02] has presented a shortest path selection scheme for WSNs using ant colony optimisation (ACO) technique. In this referred paper bio inspired ACO method is utilized for optimal path selection to communicate between source and destination nodes for packet transmission. To design this referred system, ACO considers number of hops, and path length for packet transmission.

P. Sathees Lingam et.al [03] has presented an energy efficient routing protocol for best path selection in WSNs. To reduce unnecessary flow of route request, new optimal path routing protocol is presented in this referred paper. This referred technique is analysed based on few parameters such as mean jitter, network throughput, packet delivery ratio and mean delay based on various routing protocols comparison. MarjanRadi et.al [04] presented a survey on multipath routing in WSN and its challenges. The main intend of this referred paper is to present multipath routing technique concepts and its related challenges and also basic inspiration to utilize this method in WSN. In addition to this complete categorization on the conventional routing protocols are presented.

HamidrezaSalarian et.al [05] has presented a mobile sink path selection technique for WSN. This approach hasbeen presented to overcome optimal path's drawback and challenges and to prevent creation of energy holes in WSN. To address the problem of optimal tour in rendezvous points new technique called weighted rendezvous planning (WRP) is presented, whereby every sensor node is defined a weight to its related hop distance from source to destination. This WRP technique is validated in computer simulation. And also it is demonstrated successful retrieval of sensed data in a given deadline. This WRP reduces consumption of energy by 22% and increases lifetime of network by 44% as compared conventional techniques. K. Venkataraman et.al [06] has presented survey on several attacks occurred in WSN. This referred journal paper presents several threats to WSN and the different advancements in network security. And also presented Different challenges involved in implementing those procedures.

Dr.DeepaliVirmani et.al [07] has presented a trust based technique to identify blackhole assault in WSN. In the blackhole attack node all the data are continuously dropped which results in reduction of network efficiency and wastage of unnecessary battery life. In this referred paper exponential trust based technique is presented for malicious node detection. Streak counter is implemented to store the number of consecutive packets dropped for each node which helps in detecting malicious node. Mohammad Wazid et.al [08] has presented blackhole attack finding and avoidance technique in WSN. Blackhole is kind of DoS attack and it is very tough to notice and avoid in WSN. In blackhole attack, attacker receives all the data from source node and reprograms a node in the network to block the packet instead of forwarding it to other nodes. As a result any information that enters to blockhole node will not reach destination. In this system initially blackhole attack is measured based on the network parameters followed by the presentation of new method for recognition and avoidance of Blackhole attack in WSN.

K. Rohila et.al [09] has presented Dijikstra's optimal path technique for road network. In road network applications, optimal path challenges such as drive guiding system and city emergency handling. That challenges are rectified through shortest path utilizingdijikstra's technique in the referred system. The main objective of the novel is to provide low cost implementation. This technique is implemented using applets in a java programming language.

Ojekudo et.al [10] has presented an application of dijkstra's method to solve shortest route problem. In the transport sector and information sector network examination is an important tool for the flow of energy and matter. This research paper addresses dominion paints nig problems in transporting their goods from manufacture plant to sale stores by presenting shortest path analysis using dijikstra's technique. Tora software was utilized in this analysis. Ismail Butun et.al [12] has presented a survey on intrusion identification systems (IDSs) in WSN. Initially, IDSs detail information is provided. Then brief survey about IDSs is presented for Mobile Ad-Hoc networks and also applicability of those IDSs in WSNs is presented. Thirdly, proposed IDSs for WSN are presented. After this, comparison of each system with their advantages and drawbacks are analysed. At last, IDSs guidelines that are related to wireless networks are presented.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

## III. METHODOLOGY

The implementation architecture of the proposed system is presented in Figure 1.The proposed diagram mainly consists of four blocks such as Network Initialization, Select Sink Location, create Constraint Region and Shortest Path. Initially in the network initialization block, network is created by initializing the nodes in the form of mountain road path. After network initialization, sink location is selected which is to be at the centre of network system. Then constraint region is created. Actual path is created from starting point of the constraint region to sink (i.e. Base Station) based on high hops b/w source and sink nodes. Two nodes are selected as source nodes in the constraint region and followed by shortest path is created using Dijikstra's technique. After creating shortest path, source nodes sends route request messages to all router which are in shortest path and receives route acknowledgments messages followed by information packets are transmitted from source to sink node through optimal shortest path. Including shortest path creation, black hole detection and solution for that also presented. If blackhole detected means Creation of other optimal shortest path is presented to transmit packets from source to sink.

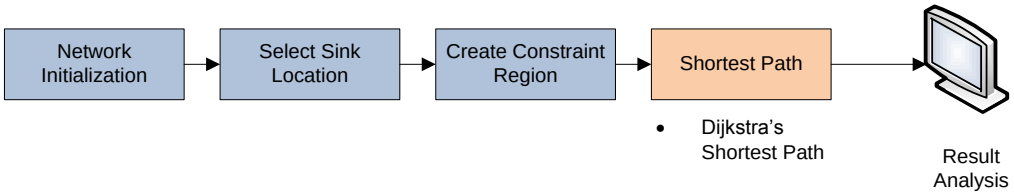



Figure 1: Block Diagram of the Proposed System

### 3.1. Network Initialization

We assume that the scenario of mountain roads with a few zigzag and long paths forms a square network, in which $N = n \times n$ grid points are considered with a uniform length of each grid, as shown in Figure. 2. The nodes created in thesquare network by assigning initial parameters (Energy, Distance etc.) to each node.

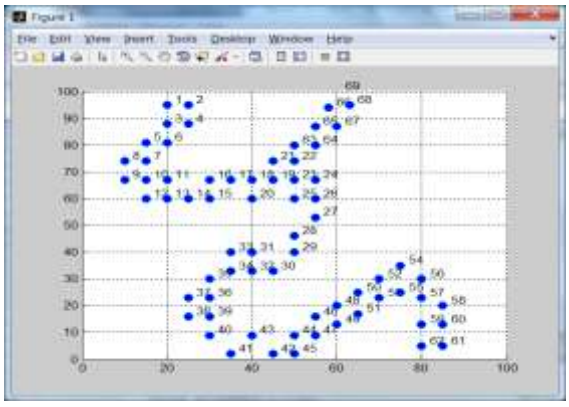


Figure 2: Network Initialization Model

3.2. Sink Location and Constraint Region

Sink is also referred as base station or destination. It collects the information from all other sensor nodes. Here sink node is selected and created at the centre of the network followed by constraint region is created. Constraint region is a circle centred on the sink node and it is represented in Figure 3. Actual path is created from the starting nodes (i.e. node 12 and node 54) of the constraint region to sink node which contain high hops and it is represented in Figure 4. The actual path is represented in red colour line as shown in Figure 4. The number of hops from starting node 12 to sink node is 9 and from starting node 54 to sink node is 11.

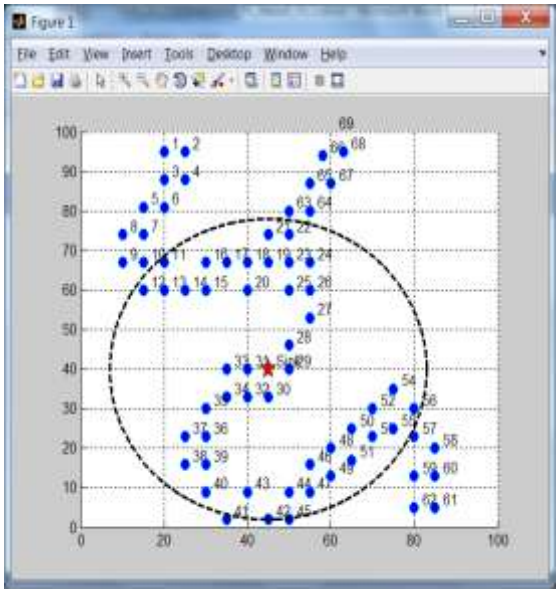



Figure 3: Sink and Constraint Region Selection

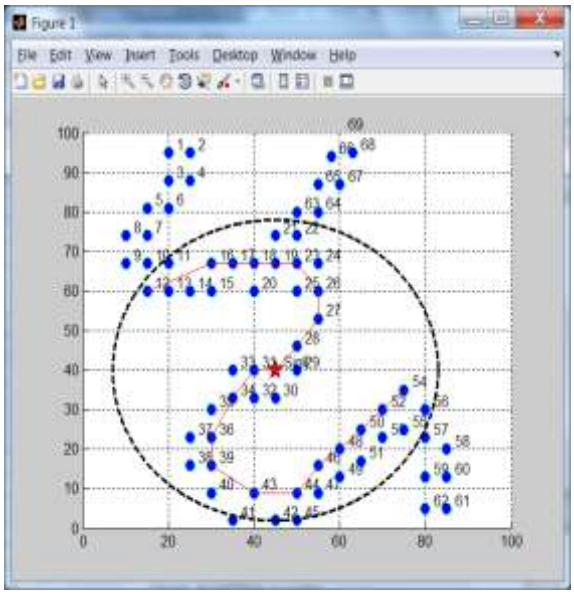



Figure 4: Hop Count Computation

3.3. Shortest Path Creation

Shortest path creation is the important process to transmit information from source to destination successfully. Successful delivery of packets with less transmission delay and energy are the important parameters in networking communication. By creating optimal path we can achieve less transmission delay and energy. In this block, initially starting nodes are selected as source node, then shortest path is created from source nodes to sink node using Dijikstra's technique. In Figure 5, dark red colour line represents the shortest path created. The implementation and detailed description about Dijikstra's technique is presented in below section:

3.3.1. Dijikstra's Shortest Path Algorithm

Dijikstra technique is introduced by EdsgerDijstra in 1956. He is a ductch computer scientist. This technique is published in 1959. Dijkstra's technique is a graph based searching technique that resolves the single source shortest problem. It will be applied on positive weights graph. This technique is often utilized in routing. This technique is utilized in shortest path finding with less cost. Dijikstra's technique contains many variants but, the most used and common one is for shortest path finding from vertex to all the vertices in the graph. The steps involved in this technique are presented below:

a. Set each and every vertices distance to infinity except source vertex, and then set the source distance to 0.
b. Push the source vertex in a minimum priority queue in the form (Ex: distance, vertex), as the comparison in the min-priority queue will be according to vertices distances.
c. Pop the vertex with the minimum distance from the priority queue (at initial the popped vertex is equal to source).
d. Update the distances of the connected vertices to the popped vertex in case of "current vertex distance + edge weight < next vertex distance", then push the vertex with the new distance to the priority queue.
e. If the popped vertex is visited previously, just continue without utilizing it.
f. Apply the same technique again until the priority queue is empty.

Figure 5 represents the shortest path creation.

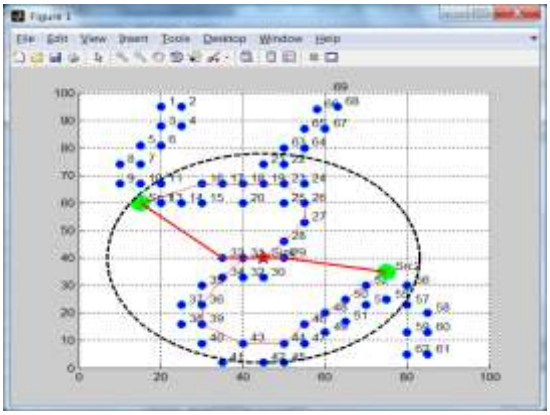


Figure 5: Shortest Path Creation

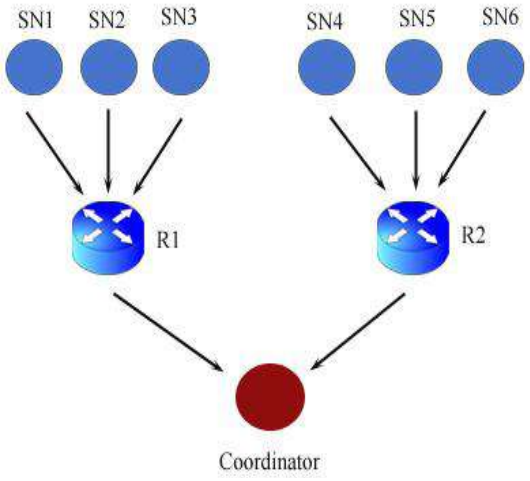
After shortest path creation route request message will be sent to other routers which are in optimal path by source nodes and route acknowledgement message will be inward by source nodes. After route-request-acknowledgment packet will be transmitted from source to destination. After creating shortest path, successful delivery of packets is also very important. In network communication there are lot of attacks which lost the data. Hence in the proposed paper with shortest path creation, Blackhole discovery and its solution also presented. The brief information about blackhole assault, attack detection and solution to it is presented in below section.

3.3.2. Black hole node Detection and Solution

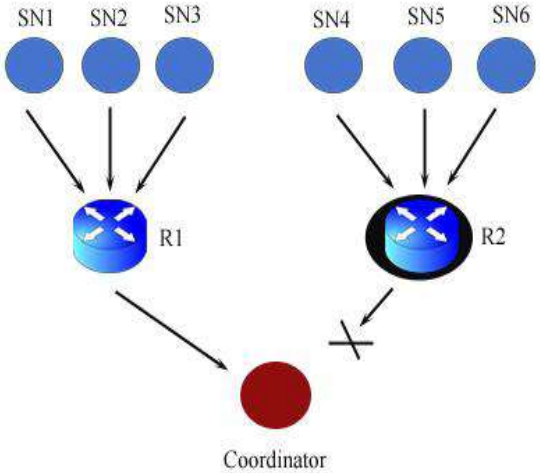
Blackhole is a critical attack against the routing protocol in the sensor network. In this attack, malicious affected node misleads other nodes by simply indicating a false route to sink or destination node. The black hole simply receives route request messages and sends route responses, later it receives packets but instead of forwarding those packets to other node,blackhole node drops them continuously. Blackhole assault scenario is presented in Figure 6

In Figure 6, 'a' represents normal flow of packets. In this scenario six sensor nodes (SN) are there, two router node i.e. R1 and R2 and coordinator. If this sensor nodes sense any environmental phenomenon, it converts that information and transmits processed information to R1 and R2 node. SN1, SN2 and SN3 sensor nodes are reporting to R1 router, SN4, SN5 and SN6 sensor nodes are reporting to R2 router. R1 and R2 router sends received data to coordinator.'b' represents the blackhole attacking scenario. In this scenario, SN1, SN2 and SN3 sensor nodes transmits sensed information to router R1 and SN4, SN5 and SN6 transmits to R2. Router R1 sends received data to coordinator node but router R2 will not transmits data to coordinator node because it is blackhole node. It absorbs all the information from other node without sending it to further node. Due to blackhole attack, the transmission delay gets increases it results poor network performance. Hence considerable work for blackhole detection and its solution is important.

In the network to detect blackhole node backward node verification is performed. In which each and every node is compared with its previous node, if both two nodes contain equal number of packets then a single pulse is created to show that all packets presented. This step is repeated with previous node until to detect the blackhole node which holds the high data packets than the current network mode. After successful identification of blackhole node, there must necessary to estimate alternative best solution so that all packets must reach the sink node without any delay and data loss. The functional steps involved in this are presented in Algorithm 1.




a). Normal flow of Packets




b). Blackhole attacking scenario

Figure 6: BlackHole Node Illustration

***Algorithm 1 : Blackhole Identification***

*Step 1:* *Network Creation with* ***'ni'*** *number of nodes.*

*Step 2:* *i.e.* $i = 1, 2, \ldots . n$

*Step 3:* *Consider* ***Source node*** *'S1 & S2' send a messages to* ***sink node*** *'S'*

*Step 4:* ***Node*** *'S1 & S2' broadcast* ***RREQ messages.***

*Step 5:* ***Wait*** *for network response for* ***'t' time.***

*Step 6:* ***CollectRREP messages****.*
*Step 7:* ***Estimate*** *shortest path*
*By* ***Dijikstra's Algorithm***

*Step 8:* ***Set packet delivery ratio i.e.*** $p = t_1$***;***
*Step 9: Transmit data packets* ***in*** $t_1$ ***time***
*Step 10:* ***if*** *neighbour node or* ***'D's received packets at*** $p = t_1$***.***
*Step 11: Continue the data transmission*
*Step 12:* ***else***
*Step 13:* ***for*** *i = 1: no. of nodes*
*Step 14: Refer back travel*
*Step 15: Compare the node packets*
*Step 16:* ***if*** *equal*
*Step 17: Activate positive pulse*
*Step 18:* ***else***
*Step 19: Conform the blackhole assault*
*Step 20:* ***Go to*** *routing table*
*Step 21: Select another optimal routing path*
*Step 22:* ***Reroute the packets to node 'S'***
*Step 23:* ***end if***
*Step 24:* ***end for***
*Step 25:* ***Repeat***
*Step 26:* ***end if***
*Step 27:* ***end algorithm***

Figure 7 represents the packet transmission. The pictorial representation of blackhole attack and another optimal path creation is depicted in Figure 8 to Figure 11. In Figure 8 large black colour node is the blackhole node. Figure 9 and Figure 10 represents the blackhole presence and another optimal pathing dialog boxes. Figure 11shows the other optimal path creation which is represented in pink colour. Figure 12 presents dialog box which is created after successful packet transmission.

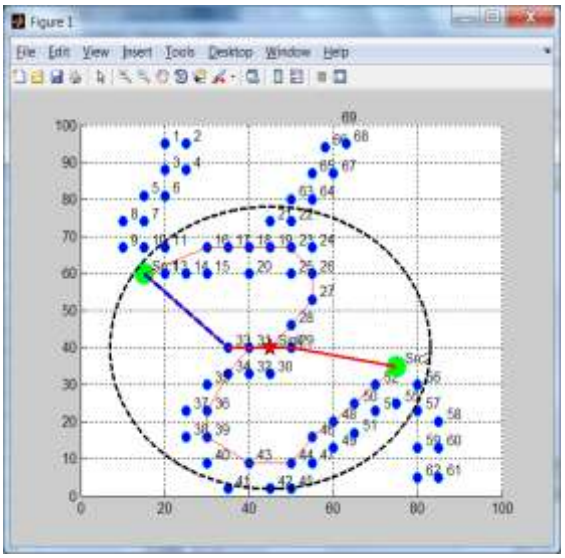



Figure 7: Packet Transmission

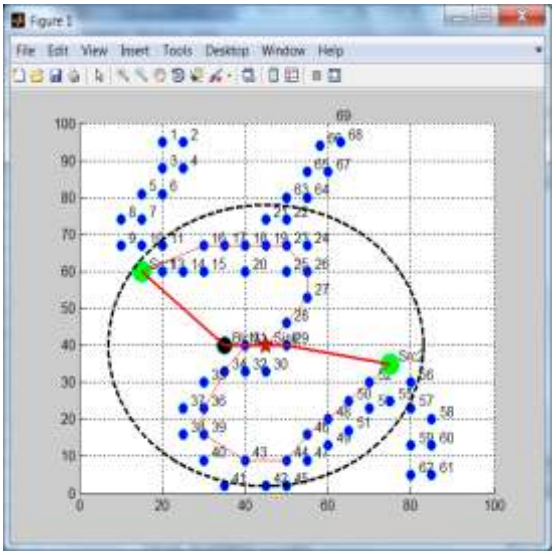



Figure 8: Blackhole Node Identification


Figure 9: Blackhole Detection

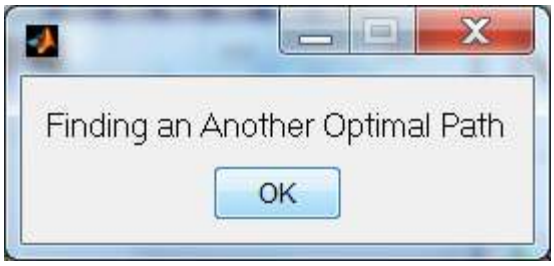



Figure 10: Finding another Optimal Path

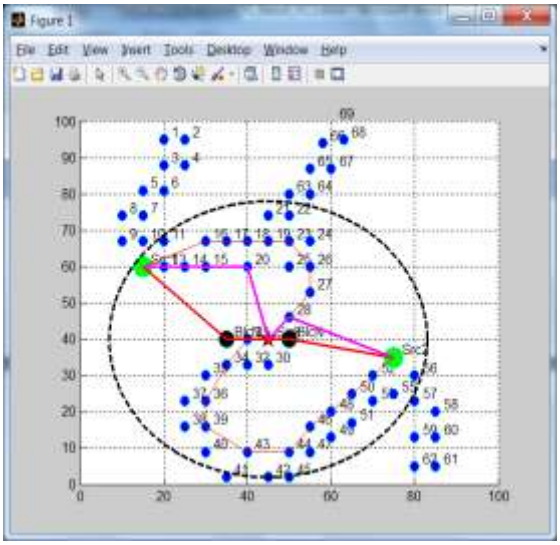



Figure 11: Successful Packet Reception at Sink Node

Figure 12: Another Optimal Path Creation.

## IV. EXPERIMENTAL RESULTS

The experimental outcome of the proposed system is presented in this section. This simulation is performed in MATLAB. The functional flow of the proposed system is present in Figure 13. To increase the lifetime of the network this simulation is performed. Network is initialized in 100m*100m respectively. The nodes are

initialized with initial parameters such as initial energy, transmission energy and receiver energy. Initial energy of each node is 100J, transmission energy for each node is 0.16J and reception energy for each node is 0.08J. This simulation is performed in MATLAB. Initially after initializing the network, sink and constraint region are selected. Based on these parameter shortest path is created from source to sink node using Dijikstra's technique. Then blackhole node attack recognition and its solution are presented. After blackhole discovery and another optimal path is created and packets are rerouted to destination through that another optimal path. The proposed system gives 41 maximum transmission rounds. Compare to existing method NDSPC method [11] our proposed method giving better performance. All the packets are successfully receiving at destination node. Hence it gives 100% packet deliver ratio. Figure 14 and Figure 15 shows the network lifetime comparison and packet delivery ratio respectively.

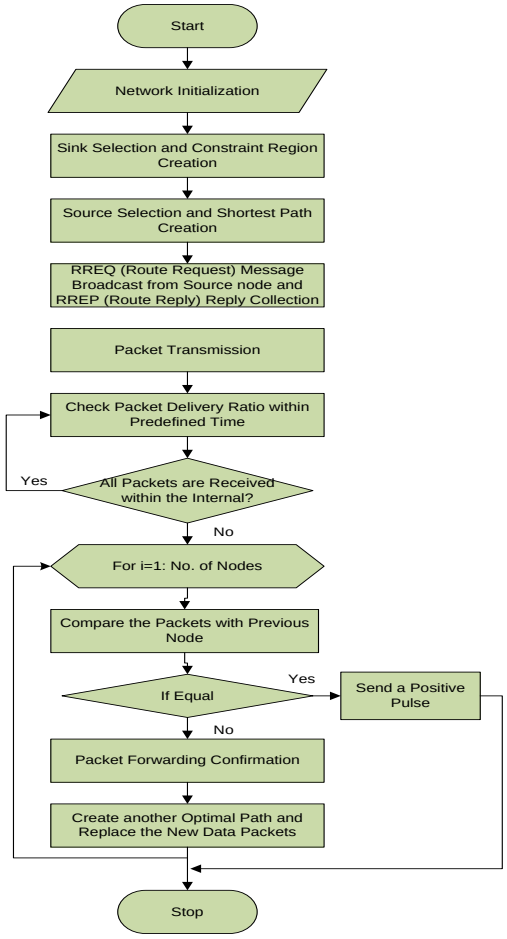



Figure 13: Functional Flow of the Proposed System

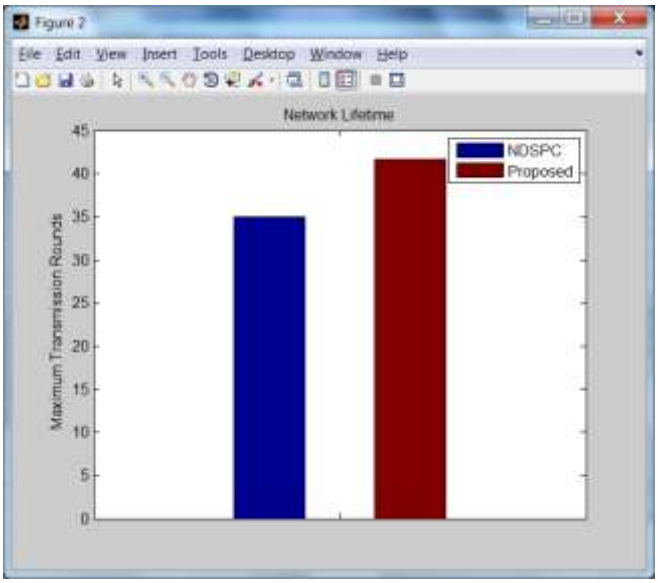



Figure 14: Network Lifetime Comparison


Figure 15: Packet Delivery Ratio

## V. CONCLUSION

Compare to network communication in WSN, mountain roads networks are zigzag and creates longest path. In network communication, successful transmission of data with less delay and energy consumption is very important, but if network has longest path means it's not possible. So, optimal or shortest path creation is required and also successful transmission of packets or information very important. In the proposed system Dijikstra's technique based shortest path creation is presented and blackhole attack node detection and its solution also presented in this paper. Results are examined through network parameters such as packet delivery ration, network life and also compared with existing NDSPC method it shows better performance in proposed system compare to existing method.

## REFERENCES

[1]. Xuxun Liu, "A Deployment Strategy for Multiple Types of Requirements in Wireless Sensor Networks", IEEE Transactions on Cybernetics, Vol. 45, No. 10, pp. 2364-2376, 2015.

[2]. Aniket. A. Gurav and Manisha J. Nene, "Optimal Path Identification using Ant Colony Optimisation in Wireless Sensor Network", AIRCCJ, pp. 223–232, 2013.

[3]. P. Sathees Lingam, S. Parthasarathi and K. Hariharan, "Energy Efficient Shortest Path Routing Protocol for Wireless Sensor Networks",International Journal of Innovative Research in Advanced Engineering (IJIRAE), Vol. 4, No. 6, 2017.

[4]. MarjanRadi, Behnam Dezfouli, Kamalrulnizam Abu Bakar and Malrey Lee, "Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges", Sensors, Vol. 12, No. 1, pp. 650-685, 2012.

[5]. HamidrezaSalarian, Kwan-Wu Chin and FazelNaghdy, "An Energy-Efficient Mobile-Sink Path Selection Strategy for Wireless Sensor Networks", IEEE Transactions on vehicular technology, Vol. 63, No. 5, pp. 2407-2419, 2014.

[6]. K. Venkatraman, J. Vijay Daniel and G. Murugaboopathi, "Various Attacks in Wireless Sensor Network: Survey", International Journal of Soft Computing and Engineering (IJSCE), Vol. 3, No. 1, pp. 208-212, 2013.

[7]. DrDeepaliVirmani, ManasHemrajani, and ShringaricaChandel, "Exponential Trust Based Mechanism to Detect Black Hole Attack in Wireless Sensor Network", arXiv preprint arXiv, pp. 1401.2541, 2014.

[8]. Mohammad Wazid, AvitaKatal, Roshan Singh Sachan, R. H. Goudarand D. P. Singh, "Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network", In Communications and Signal Processing (ICCSP), IEEE,pp. 576-581, 2013.

[9]. K.Rohila, P.Gouthami and Priya M, "Dijkstra's Shortest Path Algorithm for Road Network", "International Journal of Innovative Research in Computer and Communication Engineering", Vol. 2, No. 10, 2014.

[10]. Ojekudo, Nathaniel Akpofure, Akpan and Nsikan Paul**,** An application of Dijkstra's Algorithm to Shortest Route Problem "IOSR Journal of Mathematics", Vol. 13, No. 3, pp. 20-32, 2017.

[11]. Xuxun Liu, "Node Deployment Based on Extra Path Creation for Wireless Sensor Networks on Mountain Roads", IEEE Communications Letters, Vol. 21, No. 11, pp. 2376-2379, 2017.

Ismail Butun, Salvatore D. Morgera, and Ravi Sankar., "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", IEEE communications Surveys & Tutorials, Vol. 16, No. 1, pp. 266-282, 2014.