An Effective and Modified approach for Distance Vector Routing Protocol to increase the Throughput and Security

Simarjot Kaur[1] **Dr.Neeraj Sharma[2]**

[1]Research scholar

[2]Head of Department CSE

Department of Computer Science Engineering, CEC Landran (Mohali)

Abstract— **Wireless Sensor Networks consists of small devices or nodes which communicates over wireless links without using any fixed infrastructure. So for better data transmission between the source and destination efficient routing protocols must be required. Generally routing protocols like DSDV,DSR, DVR determines the best path or route for data transmission on the basis of distance only. These protocols do not consider parameters like throughput, trust(surety) of node, security of data during transmission. In this paper we study a modified approach for Distance Vector Routing protocol which finds the best route for data transmission not only upon the distance but also considers other parameters like throughput of nodes, surety and security of nodes which improves the packet delivery ratio during transmission.**

***Index Terms*—Wireless Sensor Networks, Distance Vector Routing, Throughput, Surety**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consists of thousands of sensor nodes which are communicating with each other over wireless links in a network of dynamic topology. In WSNs as there is no fixed topology so nodes can freely move in a network and interfere with each other. In this each node contains the information about its all neighboring nodes. The main problems in WSNs are changing network topologies, Interference among nodes, secure transmission of data etc. The area of WSNs grows day by day and used in many fields. like in home networks, medical and health fields, industrial applications like detection of nuclear and explosive materials.

A. Routing

Routing is the process of selecting the best route for data transmission between sender and receiver. Many routing protocols were established for routing purpose which are divided into two categories like topology and position based. Topology is further divided into three categories Proactive, Reactive and Hybrid.

The main aim of each routing protocol is to find the appropriate path for forwarding of data packets. Some algorithms like Ad Hoc On demand Distance Vector Routing protocol (AODV), Destination Sequenced Distance Vector (DSDV), Distance Vector Routing (DVR) protocol were established. These were generally based on the concept of finding the shortest path on the basis of distance only. For successful transmission of data we don't consider distance as a main factor for finding the best path.

B. Distance Vector Routing (DVR)

Distance Vector Routing protocol generally maintains a vector in which the distance of source node to all other neighbor nodes must be manipulated. The node with shortest distance must be selected as the next node. This process further repeats for selecting all other nodes in a path.

Any router which uses the DVR protocol must knows-

a) Distance to destination node

b) Direction in which traffic should be directed.

Here each node knows how to reach the next node and the cost to reach there. This protocol generally requires periodically updates of routing tables.

Example of DVR-

a) Interior Gateway Routing Protocol (IGRP)

b) Routing Information Protocol (RIP)

C. Problems with DVR

a) Updating of routing tables.

b) Generally considers the shortest paths which are based on the neighboring nodes. Hence, all nodes in a network must not be included.

c) Paths must be find on the basis of distance only. No other parameters like security, throughput, trust value of nodes must be included.

In this paper we proposed a modified approach for distance vector routing protocol in which other factors like throughput, surety, security of data during forwarding must be included for reliable transmission of data. Implementation process is carried out in MATLAB environment and results of this approaches better than previous approach in case of parameters like throughput, surety and packet delivery ratio. Route for data transmission is selected by comparing the throughput, surety level and distance values and then keys must be provided to sender and receiver for creating a dedicated link so as to achieve the security.

II.LITERATURE SURVEY

Amith Khandakar represents a paper in 2012 which defines the Procedural Comparison of DSR, AODV and DSDV Routing protocols which is based on performance metrics like Packet Delivery Fraction, End to end delay between source and destination,Normalized Routing load while the number of nodes varying, speed and pause time during transmission. This approach does not consider other quality of service parameters.

Rajesh Sharma in (2013) proposed a paper Dynamic Source Routing Protocol (DSR).The Dynamic Source Routing protocol (DSR) is an efficient routing protocol which must be designed specifically for use in multi-hop wireless ad hoc networks**.** DS provides the network which is self-organizing and self-configuring, without the need for any existing fixed network infrastructure.This protocol consists of mainly two mechanisms Route Discovery and Route Maintenance, which work together for discovering and maintaining of source routes to all possible destinations. The main emphasize in this this research is to provide a better solution on the basis of reputation method to solve any routing issues raised by some misbehaving nodes in a network.

Junling Lu,Xiaoming Wang proposed a paper Interference Aware Probabilistic Routing for WSNs in 2012 which adopts a probability theory and proposed a probabilistic routing algorithm which gives better results than AODV algorithm according to packet delivery ratio, jitter, throughput. The time and space complexity, correctness have also been examined during simulation.

Rajeshwar Singh in (2011) represents a paper "Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks" in which ad hoc routing protocols like DSR and DSDV have been implemented by considering a 500m x 500m terrain area which describes the throughput and packet delivery fraction for these protocols. Simulation is done by using the NS-2 simulator which shows that DSR is better than DSDV protocol according to performance.

Rabeb.F in 2012 proposed a paper "An extensive comparison among DSDV, DSR and AODV protocols in Wireless Sensor Network" in which two classes of routing algorithms are defined, first one is the flat and the second class is of the hierarchical algorithms. In this paper we study class flat and compare many routing protocols and their performance during simulation. Simulation is performed by using NS2 simulator. Performance metrices like throughput, loss rate and end to end delay must have been examined.

Zehua Wang,Yuanzhu Chen,Cheng li in 2014 proposed a paper " PSR: A Lightweight Proactive Source Routing Protocol for Mobile Ad Hoc Networks" in which proactive source routing protocol proposed which maintains information about the network topology than distance vector routing protocol Performance of PSR is better than DSDV,DSR protocols.

Nandkumar P. Kulkarni in (2011) proposed a paper"Performance Evaluation of AODV, DSDV & DSR for Quasi Random Deployment of Sensor Nodes in Wireless Sensor Networks" in which a new deployment technique known as Quasi Random Deployment (QRD) for WSNs must be implemented in order to increase the lifetime of network and energy efficiency. Implementation is done on NS2 simulator. Three protocols like AODV, DSDV and DSR must be assumed for deployment process. AODV protocol gives better performance than DSDV protocol.

III. PROBLEMS WITH EXISTING SYSTEM

Routing is the process of selecting best paths in a network. Previously routing was only dependent on the distance between the nodes. Many algorithms were used for routing like AODV, DSR, DSDV etc. but they all considered only distance factor for deciding the best path. But since there are many other quality of service parameters on the basis of which best path could be decided like bandwidth, energy and security. Algorithms were designed to consider these parameters but these algorithms considered only one of the factor and the other factors were ignored or either two of the parameters like distance and energy or distance and bandwidth were taken into consideration for routing. The other major factors that need to be kept in view while routing are security and surety of the code transmission. It should be made sure during routing that the data or the code that is transmitted should be received successfully at the other end. Security is of prime concern today, one never wants that the information transmitted changes or some part of information is lost so the security of the code cannot be left unconsidered because if successful transmission is must for a good system, secure transmission is also one of the challenges. So protocols needs to be designed that consider number of quality of service parameters like distance, energy,

bandwidth along with the surety and security of data transmitted during routing. During routing, along with the selection of best path, success and security of the transmission of code should also be guaranteed. A new algorithm is to be designed that not only takes in account the quality of service parameters but also the factors of security and surety in consideration while selecting the best path for routing. This will improve the routing process and the reliability and the lifetime of the system can be improved.

IV.METHODOLOGY

Routing is the process of choosing the best path among the number of available paths. The factors to be considered while routing for taking out the best path are distance, bandwidth, energy, as well as the security and the surety of the data to be transmitted.

A new work is proposed i.e. algorithm is designed that considers all parameters like distance, bandwidth, trust value or the surety level and energy while routing. The distance between the neighboring nodes is found and then bandwidth and energy constraints are considered, keeping in view the values of all these, the best path is selected and the routing is done. For security purpose, keys are designed in this system. Each node is assigned a unique key that changes after every 5 seconds, when distance between the neighboring nodes is found and the best path is selected, the keys of the neighboring nodes are matched, the matching should be at least 70 percent accurate. When the keys of both the neighboring nodes match with 70 % accuracy, the transmitter node sends a unique key to the next node and with that unique key a dedicated link is formed between the two nodes. This dedicated link forms a secure link among the nodes and now the data can be transmitted securely without the any external disturbance, no other node can interrupt the data during transmission and no malicious node can interfere in the link. This procedure is repeated each time two nodes link with each other and this way whole path for routing is selected and is secured using dedicated link formed using keys. This proposed work is believed to be better, efficient and secure than the conventional algorithms. The new designed algorithm improves PDR, the security of the system is improved and the immunity to external attacks of the system is improved.

A new protocol which is to be designed should have certain objectives so that it can be better than the conventional protocols and can be used in future for the efficient and effective working of the system. The objectives of the new system designed are as follows:

1. The concept of security to be introduced in the algorithm. So that reliability of the system is not questioned afterwards.
2. The data rate is to be made faster by considering bandwidth as one of the factor for routing process.
3. The surety level based data rate should be set higher so that the system can be considered reliable for future use.
4. A new protocol is to be introduced that considers all the quality of service parameters for deciding the path of routing like distance, energy and bandwidth along with the surety and security of the data to be transmitted.

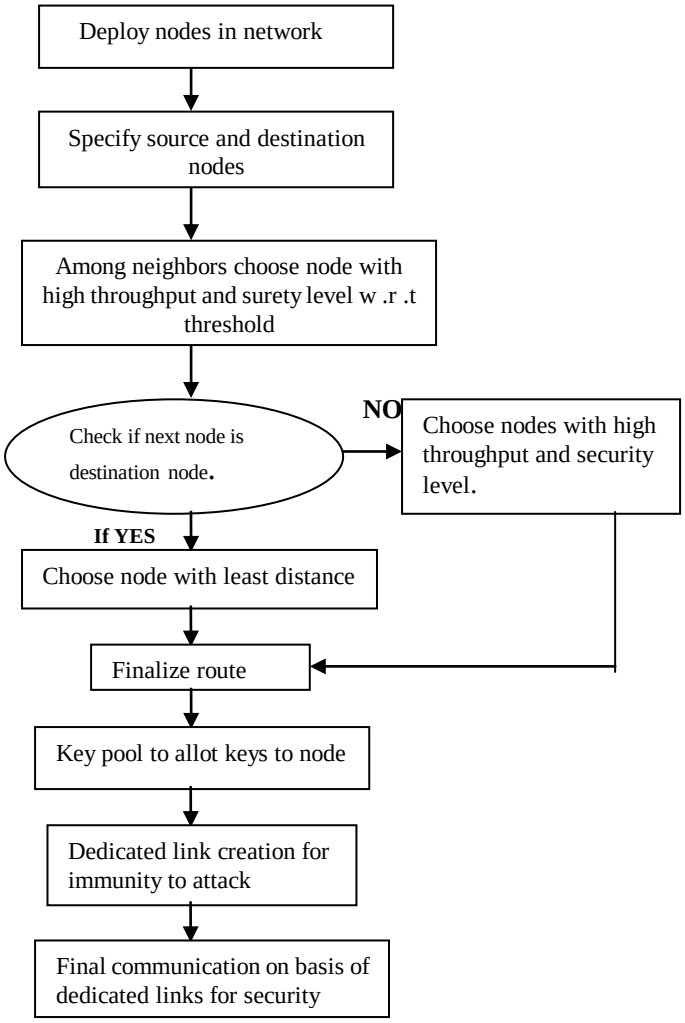


Fig 1:-Implementation Flow Chart

The methodology of the process which takes in account all the factors of routing is described below:

1. The network in which routing is to be done will consider some number of nodes. The first step in this will be the deployment of nodes in the network.

2. Source node is the node from which transmission will take place and the destination node is the node at which reception takes place or we can say that is the last node up to which data has to be transmitted. So the next step will be deciding the source node and the destination node. Source node will send the data to the destination node, and the data transmitted will cover all the deployed nodes in the network and will at last reach the destination node.

3. Now, the data transmission will start from the source node, after selection of the source node the neighbor nodes will be calculated as per the range defined. The neighbor node will be that node which will have the least difference from the source node.

4. The nodes having the least difference from the source node will be selected as neighbor nodes and then among those neighbor nodes the node having high throughput and high surety level with respect to the threshold value will be selected.

5. Then the neighbor node selected will be checked whether it is destination node or node. The next step will depend on whether neighbor node is the destination node or not.

6. If the next node is the destination node then the node with the least distance will be chosen because the routing is considered best when it have to travel the least distance.

7. After choosing the node with the least distance the route will be finalized.

8.If the next node is not the destination node then the node with high throughput and security level will be selected.

9. After the selection of the node on the basis of next node being the destination node or not. The route will be finalized.

10. Then a key pool is selected to allot keys to nodes, this key pool is to provide security to the system as a unique key will be assigned from this key pool to the nodes which will prevent malicious nodes from attacking the node.

11. The two neighboring nodes after the final selection of the path will be assigned unique keys for dedicated link creation that will provide immunity from external attacks to the node.

12. The final communication link will be set up on the basis of dedicated links for security.

V..IMPLEMENTATION AND RESULTS

For implementation process, MATLAB is used .Below figures describes the implementation results in MATLAB environment in which throughput, surety level are defined.

A.Selection of Source and Destination Node

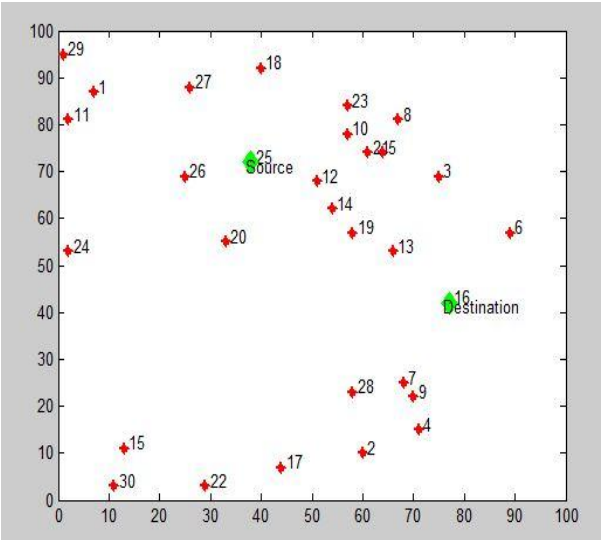


Fig 2:- Source and Destination nodes

The figure 2 shows the source and destination nodes. Firstly we assign 30 modes in a particular network area among which 25 node is the source node and 16 is the destination node. Source and destination nodes are represented by green color and other nodes are represented by red color.

B.Route selection

Figure 3 represents the path for transmission of data between source and destination in which the next node for data transmission is selected by considering various parameters like throughput,surety and distance.Next node is selected not only upon the distance factor.

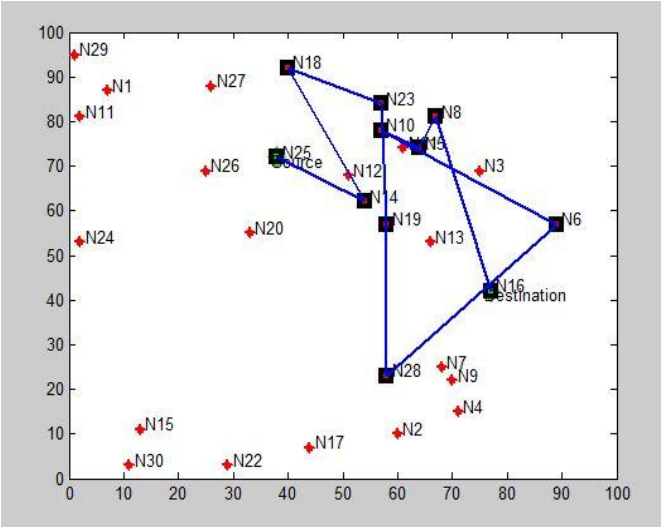
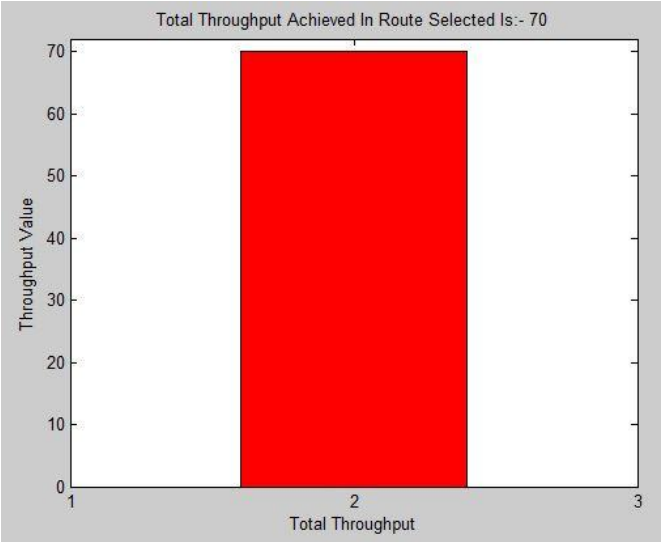


Fig 3:- Route or path selection for data transmission

C.Throughput

Figure 4 repesents the total throughput achieved in the selected route.Throughput can be assigned manually or randomly.Value of throughput achieved in this route is 70.

Figure 5 represents the individual throughput of nodes which are considered in selected route.



.Fig 4:-Total Throughput achieved in selected route

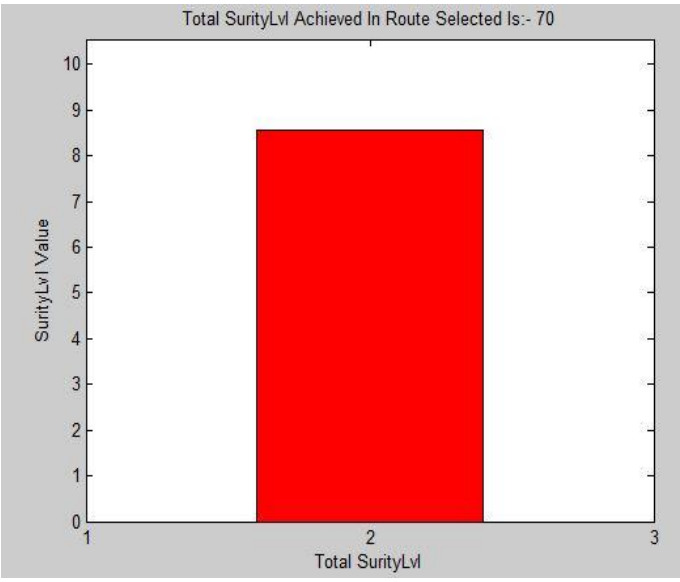


Fig 6:- Total surety level achieved in selected route

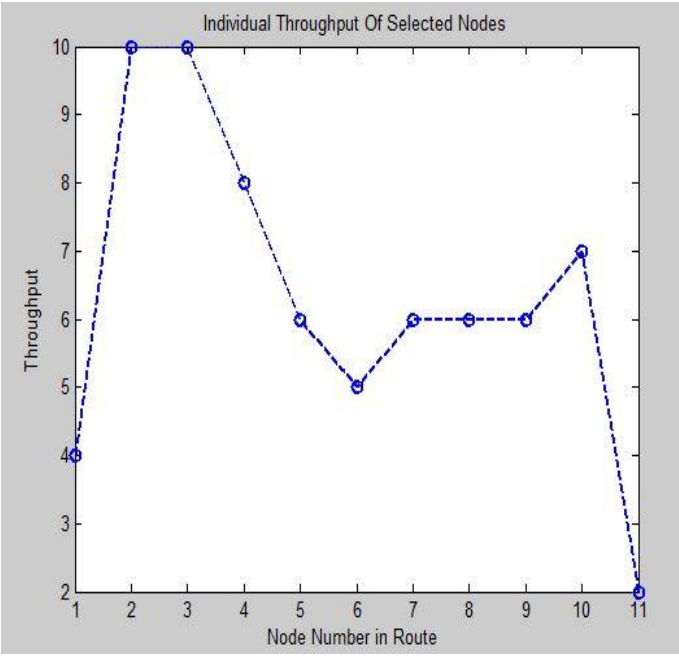


Fig 5:- Individual throughput of selected nodes

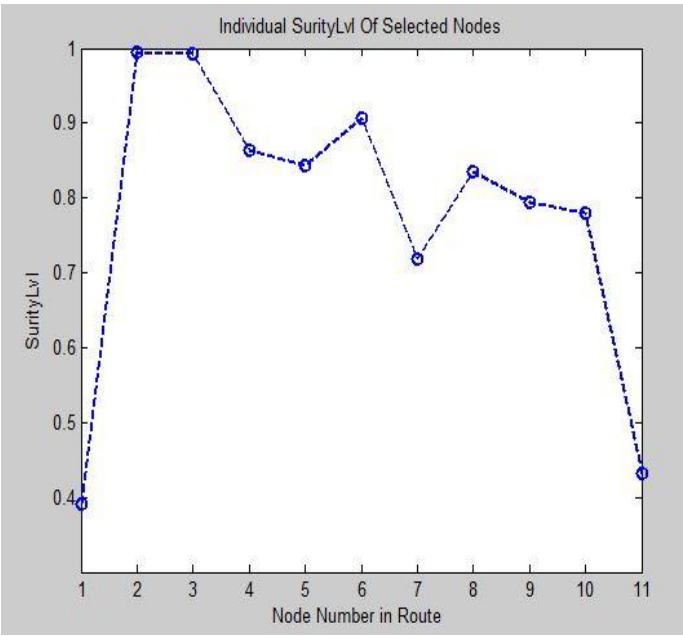


Fig 7:- Individual surety level of selected nodes

D.Surety Level

Figure 6 represents the total surety level achieved in the route which describes the data drop rate of nodes. Here the value of surety level is 70.The node with minimum data drop rate must be selected as the next source node.

Figure 7 represents the individual surety level of nodes which are considered in desired route.With this new approach trust rate of nodes also increases which minimizes the data drop rate and data is transferred with more accuracy.

E.Comparison Graphs between old and new approach

Figure 8 represents the comparison between the throughput of old approach in which priority is given to the shortest path and new approach in which throughput considers as a main parameter than distance. The red bar represents the proposed work and blue bar represents the old work.

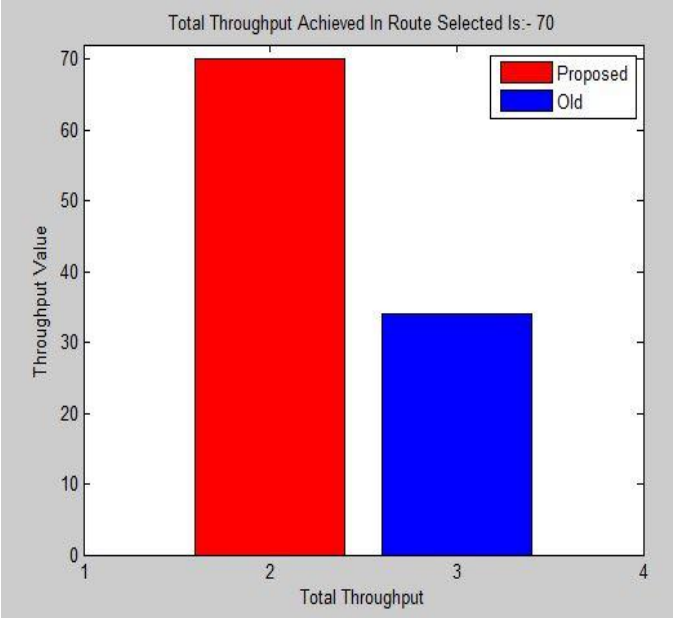


Fig 8:-Throughput Comparison

Similarly, figure 9 represents the comparison of surety level of proposed and old work.

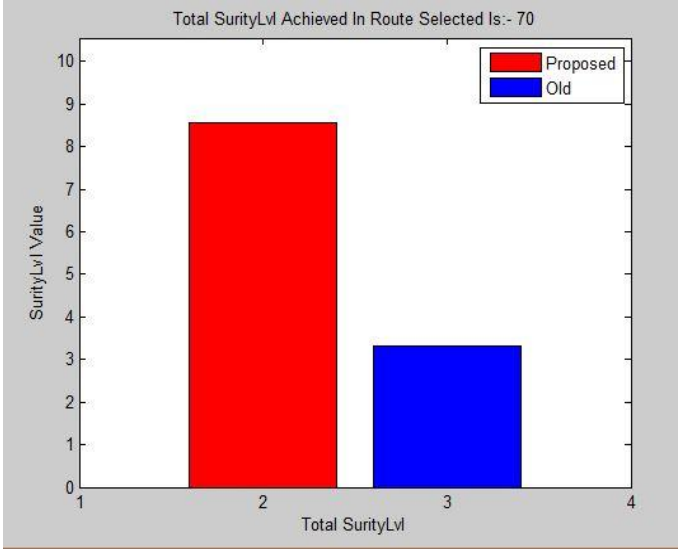


Fig 9:- Surety Level Comparison

F.Packet Delivery Ratio

For security purpose unique keys must be assigned to the source and destination. If keys are matched then a dedicated link must be created between both nodes and data packets must be delivered. Figure 10 represents the comparison between packet delivery ratio of old and new approach.

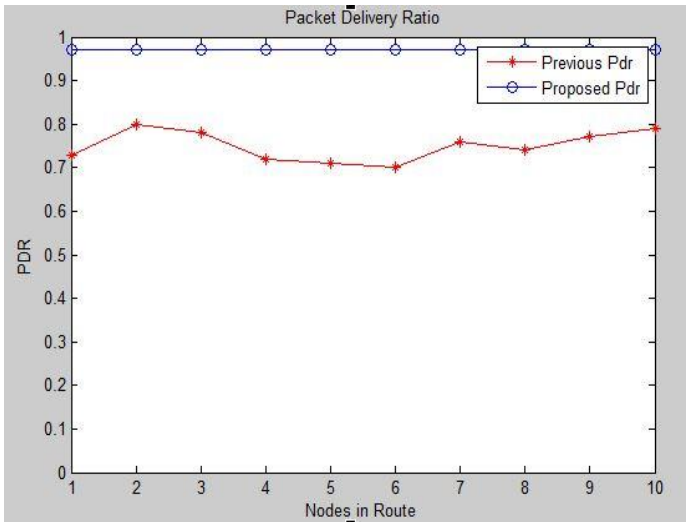


Fig 10:-PDR of previous and new approach

Packet delivery ratio of new work represented by blue curve which is greater than 90 and old work is represented by red curve which is upto 75.

G. Total distance covered by route

Figure 11 represents the total distance covered form source to destination by selecting a particular path.

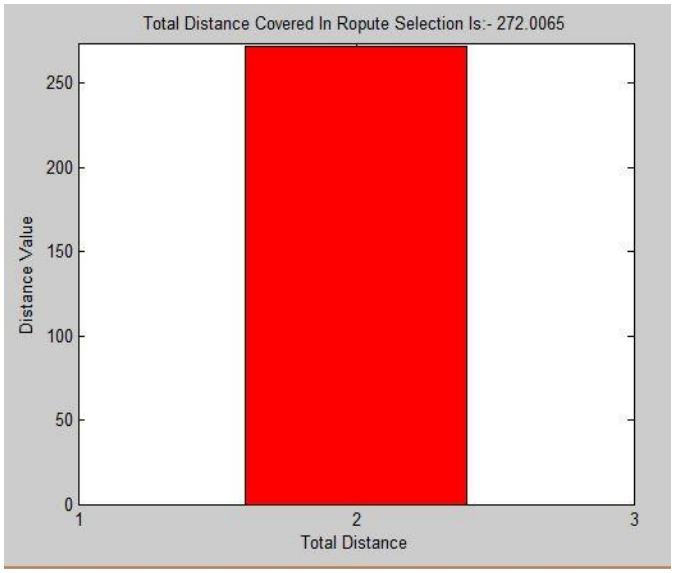


Fig 11:-Total Distance covered in a selected route

VI. CONCLUSION AND FUTURE SCOPE

There are many routing protocol like DSR , DVR , DSDV, AODV for finding the efficient route for data transmission between sender and receiver generally on the basis of shortest distance or path .In this paper a modified approach of distance vector routing protocol is defined in which many

parameters like throughput, surety or trust value of nodes, security must be considered for selection of best path among sender and receiver for data transmission. Distance is also considered for finding the route but the efficient route is selected by considering the throughput, surety and security of data. For future work ,we can implement the same protocol by considering these parameters as well as distance on the Flying Ad Hoc Networks (FANETs) which is an upcoming research area in which the nodes are not stationary. We can also implement this technique in case of swarm intelligence like in PSO(Particle Swarm Optimization).

REFERENCES

[1]Aditi Sharma, July 2014, "Performance Comparison of AODV and DSDV Routing Protocols in Mobile Ad Hoc Networks"
[2] Sumitha J., 2014, "Routing Algorithms in Networks"
[3] G.Asha, S.Durgadevi, November 2014, "The comparison between routing protocols based on lifetime of wireless sensor networks"
[4]Alahdal, Tariq A., and Saida Mohammad. "Performance of standardized routing protocols in ad-hoc networks." Computing, Electrical and Electronics Engineering (ICCEEE), 2013 International Conference on. IEEE, 2013
[5]Adel.S.El ashheb, (2012), "Performance Evaluation of AODV and DSDV Routing Protocol in wireless sensor network Environment ", *International Conference on Computer Networks and Communication Systems*, PCSIT vol.35, pp. 55-62.
[6]Seema, Reema Goyal (2013) A Survey on Deployment Methods in Wireless Sensor Networks,
[7]Amith Khandakar (2012) Step by Step Procedural Comparison of DSR, AODV and DSDV Routing protocol, Mobile Ad hoc network is network where nodes communicate without any central administration or network infrastructure.
[8]Vibha Yadav (2009) Localization S Cheme For Three Dimensional Wireless Sensor Networks Using Gpsenabled Mobile Sensor Nodes,
[9]Rajesh Sharma(2013) Dynamic Source Routing Protocol (DSR), The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes.
[10]Amit N. Thakare(2010) Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks,
[11]Parul Kansal(2010) Compression of Various Routing Protocol in Wireless, Wireless Sensor Networks have emerged as an important new area in wireless technology.
[12]Matthias Ringwald, Kay Romer, Deployment of Sensor Networks: Problems and Passive Inspection,
[13]Rajeshwar Singh (2011) Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks
[4]Pallavi Sahu, Sunil R. Gupta(2012) Deployment Techniques in Wireless Sensor Networks in this paper, we study coverage with connectivity properties in large wireless sensor networks (WSN).
[15]Bikash Rath(2009) Implementing And Comparing DSR And DSDV Routing Protocols For Mobile Ad Hoc Networking,
[16]Guoyou He, Destination-Sequenced Distance Vector (DSDV) Protocol, An ad hoc network is a collection of mobile nodes forming an instant network without fixed topology.
[17] Perkins CE, and Bhagwat P, (1994), "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Proceedings of ACM SIGCOMM, pp. 234–244
[18]C. E. Perkins and E. M. Royer, "Ad Hoc On-demand Distance Vector Routing", In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, 1999, 90-100.
[19] Valid Nazari Talooki, and Jonathan Rodriguez, "Quality of Service for Flat Routing Protocols in Mobile Ad-hoc Network,"ICST,7-9 September 2009.
[20] Abhishek Gupta , Samidha D Sharma, 2014, "A Survey on Location Based Routing Protocols in Mobile Ad-hoc Networks"
[21] Zehua Wang, FEBRUARY 2014, "PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks"
[22] Priyanshu and Ashish Kumar Maurya, may 2014, "survey: comparison estimation of various routing protocols in mobile ad-hoc network"
[23] [16] Gupta P, Kumar P R. The capacity of wireless networks. IEEE Transactions on Information Theory, 2000, 46(2): 388-404.
[124] Tan H, Lou T, Wang Y, Hua Q, Lau F C M. Exact algorithms to minimize interference in wireless sensor networks. Theoretical Computer Science, 2011, 412(50): 6913-6925.
[25] Teo J, Ha Y, Tham C. Interference-minimized multipath routing with congestion control in wireless sensor network for high-rate streaming. IEEE Transactions on Mobile Computing, 2008, 7(9): 1124-1137.
[26] Mohammad reza soltan aghaei, A hybrid algorithm for finding shortest path in network routing, Journal of Theoretical and Applied Information Technology © 2005-2009 **(2009)**
[27] Taehwan Cho, A Multi-path Hybrid Routing Algorithm in Network Routing, International Journal of Hybrid Information Technology, **5(3), (2012)**

Simarjot Kaur presently is a PG scholar in Department of Computer Science, Chandigarh Engineering College, Punjab Technical University, Landran, Mohali. She received the B-Tech Degree in Computer Science Engineering from Punjab Technical University, Jalandhar, India in 2013. Her research area of interest is networking.

Dr. Neeraj Sharma received his B-Tech degree from MDU, Rohtak in 2001 and M.tech degree from MDU, Rohatk in 2007. He received PHD degree from NIMS University, Jaipur in 2012. Presently, He is a Head of Department (CSE) in Chandigarh Engineering College, Punjab Technical University, Landran, Mohali. His research area of interest is Wireless Ad-Hoc Network, Wireless Sensor Network, Software Define Network, MANETs.

