ANALYSIS AND DESIGN OF PROTOCOL FOR ENHANCED SELFISH ROUTING SCHEME

Raman Kumar

Department of Computer Science and Engineering
I K Gujral Punjab Technical University, Kapurthala, Punjab, India
er.ramankumar@aol.in

Abstract

The proposed routing mechanism in this paper has modified the conventional hello request and reply mechanism to include a new feature called power status. This feature keeps a node aware about the power status of neighboring nodes. Thus, the neighbor table of a node, in the proposed routing protocol, will have an additional entry in form of power status of the neighboring node. The knowledge about the power status of the neighbors helps a node in avoiding a node which is very low in power and may drop the packet in selfish manner to save the energy. A node in the ad hoc network can have five power statuses: very low, low, medium, high, very high with their ordinal values as 0, 1, 2, 3, 4 respectively.

***Keywords*:** Average Power left per node, Average Throughput and Average no. of hop count for successful transmission

1. The Main Text

The Communication in an ad hoc network is a multihop communication wherein a source node communicates with a distant node using intermediate nodes to save the power. Thus, the major activity in an ad hoc network environment is to find a suitable route such that the delivery of the message is ensured beyond doubt. The route should be so chosen that all the nodes in the path are trustworthy, non-malicious, unselfish and the hop count is minimum.

The first receiver of the message to a distant node is some immediate neighbor of the source node. Therefore, it is necessary that every node in the ad hoc network must be aware of its immediate neighbors at every moment. To remain aware about its neighbor nodes, a node in the network keeps on broadcasting hello requests on the periodic basis and keeps on receiving the hello replies as well. Using these hello request and replies a node in the ad hoc network constructs and maintains a table of its neighbors known as neighbor table. Since the nodes in the ad hoc networks are mobile the neighbor table keeps on changing with time. Our proposal begins with the format for hello request packet as shown in Figure.1.

Packet Type	Source Address	Power Status

Figure 1 Hello Request Packet

The hello request packet has three fields, namely packet type, source address and power status. The packet type field denotes that it's a hello request packet, source address field is the identifier of the node in the network which generated the hello request and power status field indicates the current status of the power of the node issuing the hello request. There is no destination address in this packet as hello request is a broadcast mechanism.

Hello reply is multiple unicast mechanism wherein a node responds to the node from which it has received a hello request. The format of hello reply packet is shown in the Figure 2.

Packet Type	Source Address	Destination Address	Power Status

Figure 2 Hello Reply Packet

It has four fields: packet type, source address, destination address and power status. The packet type field here is hello reply, source address field contains the identification of the node from which the reply packet originated, destination address field is the identification of the node to which the packet sent and the power status field provides the current power status of the sender node.

2. Designing the Routing Protocol

The aim of the routing protocol is to find out the path without any selfish node i.e. the nodes whose energy is low may not be the part of the route from source to destination. The strategy used in routing protocol design is as follow:

This protocol takes following inputs from the user: -

- Area of the network
- Number of nodes that a network contains
- Transmission radius or range that is used to find out the neighbor list of each node
- Source node and destination node

After having the following information, a neighbor list is generated. First source node send the hello request packets to all its neighbors, then all the nodes who received the hello request packets send the unicast hello reply packets to the source node by using this neighbor list source address checks whether the destination node is in its vicinity or not, if the destination node is in its vicinity then it directly unicast the packet to the destination node otherwise we apply the Roulette wheel mechanism to find out the destination node by using the neighbor list. The process goes on until the hop count maximum limit exceeds or the packet reaches to the destination.
The following parameters were recorded:

- Average Power left per node
- Average Throughput
- Average no. of hop count for successful transmission

3. Simulations and Results

The simulation process involved the capturing of the results from a arbitrary ad hoc network in two ways: In the first way (referred to as normal routing in this thesis) a node with the lower energy was considered for the route formation. In the second way (referred to as proposed protocol). The nodes with the lower energy were not allowed to participate in the route formation process. A comparison was made and it was found that the proposed protocol is quite effective. This Protocol was designed in C++ in which an area of 35*35 sq. unit's size was chosen. The nodes were distributed randomly in the given area and following performance metrics results were recorded in an output file.

A. Average Power left per node
B. Average Throughput
C. Average no. of Drop count

The following assumptions were made in measuring average power:
1. The node looses 4 units battery in multicasting and broadcasting while transmitting a packet.
2. The node looses 1 units of its battery power while receiving.
3. The node loses 1 unit battery power in unicasting while transmitting the packet.
4. Each node is assigned 150 units of power

This protocol was designed in C++. It takes the following parameters as input:

- Number of nodes
- Transmission radius of each node

The following output was recorded:

A. Average Power Left per Node

The protocol designed selects random source and destination every run. Each execution of program involved 100 runs. The average power left per node after all the 100 execution was recorded in an output file.

Table 1 Average Power left per node in Normal Routing Protocol

Transmission range	No. of nodes=15	No. of nodes=20	No. of nodes=25	No. of nodes=30
5	102.59	96.3	100.16	117.86
6	91.26	100.94	112.4	108.7
7	80.67	89	102.59	94.73
8	100.33	85.05	78.08	78.53
9	80.33	91.34	73.5	77.16
10	56.33	69.4	58.36	50.7
11	45.53	56.45	48.84	60.93
12	42.34	37.1	43.84	58.1
13	26.67	42.55	47.56	40.17
14	37.94	33.95	54.48	42.64
15	28.6	29.05	28.16	37.3

Table 2 Average Power left per node in Proposed Selfish Routing Protocol

Transmission range	No. of nodes=15	No. of nodes=20	No. of nodes=25	No. of nodes=30
5	70.8	72.19	79.44	71.63
6	55.86	50.9	58.44	73.76
7	45.46	53.95	57.68	61.57
8	43.4	52.25	48.08	50.87
9	26.87	49.3	53.56	41.16
10	33.8	36.35	48.95	34.7
11	35.34	46.78	34.16	41.2
12	34.8	29.15	34.52	39.1
13	29.8	21.4	26.92	29.4
14	22.8	38.8	34.68	31.5
15	15.33	19.35	28.2	33.06

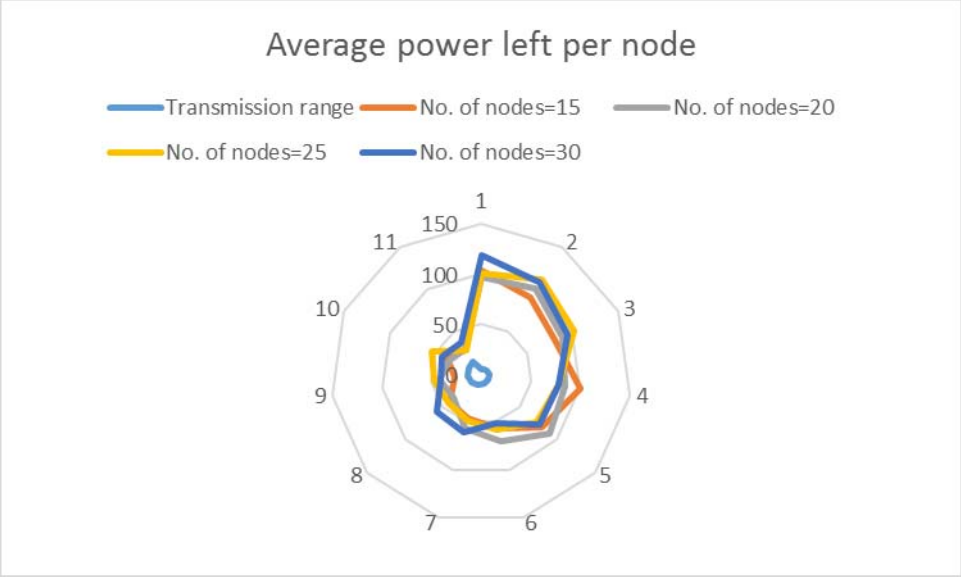

Figure 3 (a) Average Power left Vs Transmission Range for Normal Routing Protocol

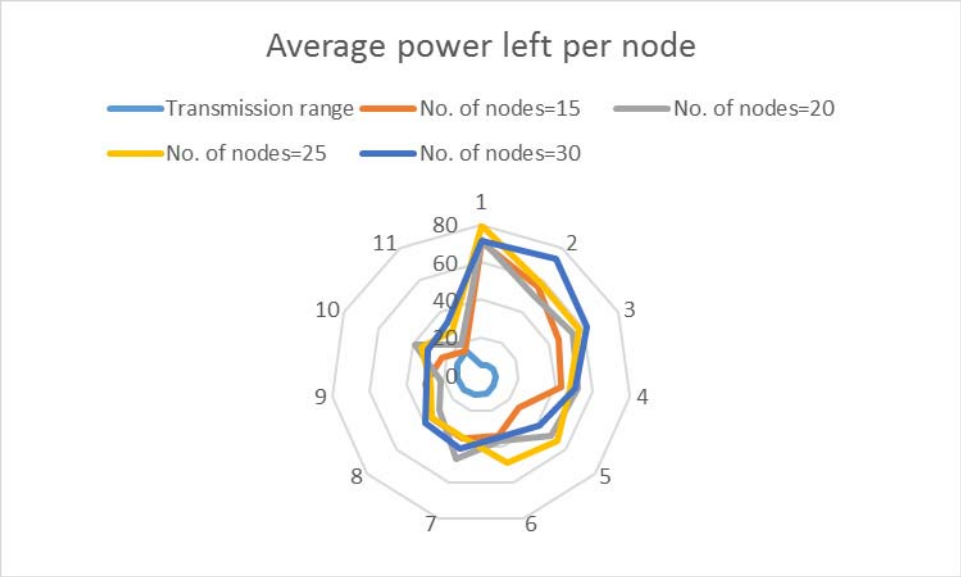

Figure 3 (b) Average Power left Vs Transmission Range for Proposed Selfish Routing Protocol

B. Throughput

It may be defined as the number of successful transmission to the total number of transmissions. The average throughput increases as the transmission range increases since the information regarding neighbouring nodes gets increased.

Table 3 Average Throughput in Normal Routing Protocol

Transmission range	No. of nodes=15	No. of nodes=20	No. of nodes=25	No. of nodes=30
5	0.32	0.74	0.71	0.69
6	0.62	0.92	0.74	0.85
7	0.64	0.86	0.85	0.97
8	0.74	0.86	0.9	0.89
9	0.8	0.78	0.92	0.96
10	0.69	0.92	0.91	0.74
11	0.64	0.84	0.78	0.88
12	0.7	0.6	0.85	0.62
13	0.76	0.55	0.66	0.77
14	0.58	0.5	0.75	0.66
15	0.5	0.69	0.57	0.68

Table 4 Average Throughput in Proposed Selfish Routing Protocol

Transmission range	No. of nodes=15	No. of nodes=20	No. of nodes=25	No. of nodes=30
5	5	0.28	0.75	0.66
6	6	0.63	0.65	0.73
7	7	0.54	0.73	0.73
8	8	0.58	0.64	0.75
9	9	0.59	0.61	0.55
10	10	0.45	0.51	0.65
11	11	0.35	0.55	0.59
12	12	0.51	0.49	0.6
13	13	0.59	0.54	0.52
14	14	0.47	0.56	0.5
15	15	0.49	0.53	0.49

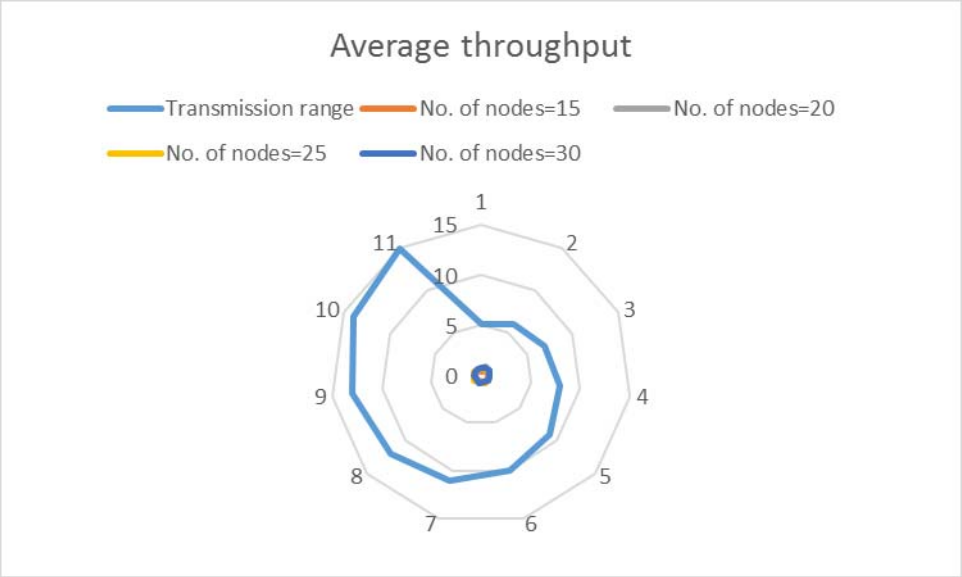

Figure 4 (a) Average Throughput Vs Transmission Range for Normal Routing Protocol

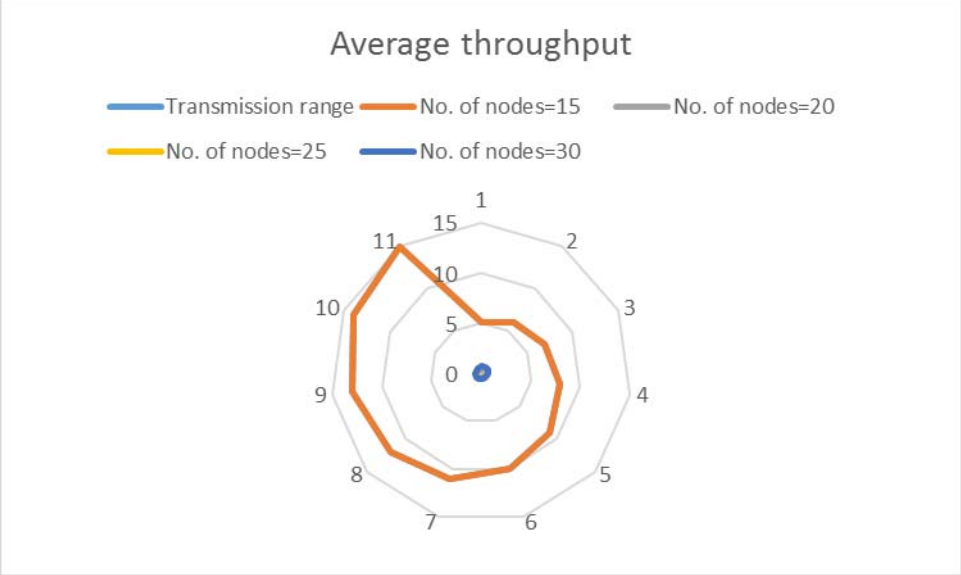

Figure 4 (b) Average Throughput Vs Transmission Range for Proposed Selfish Routing Protocol

C. Drop Rate

It may be defined as the no. of times the intermediate node drop the packet due to its selfish behavior.

Table 5 Average Drop Rate in Normal Routing Protocol

Transmission range	No. of nodes=15	No. of nodes=20	No. of nodes=25	No. of nodes=30
5	0	0	0	0
6	0	0	0	0
7	0	3	0	0
8	0	2	3	2
9	4	0	1	0
10	7	1	6	11
11	12	1	8	6
12	10	13	8	20
13	9	16	20	7
14	13	13	4	13
15	12	14	10	8

Table 6 Average Drop Rate in Proposed Selfish Routing Protocol

Transmission range	No. of nodes=15	No. of nodes=20	No. of nodes=25	No. of nodes=30
5	7	4	6	5
6	19	16	6	6
7	18	11	8	20
8	13	14	9	12
9	15	12	11	17
10	22	15	8	12
11	20	10	14	12
12	15	20	10	15
13	9	12	14	9
14	10	13	15	15
15	13	16	15	9

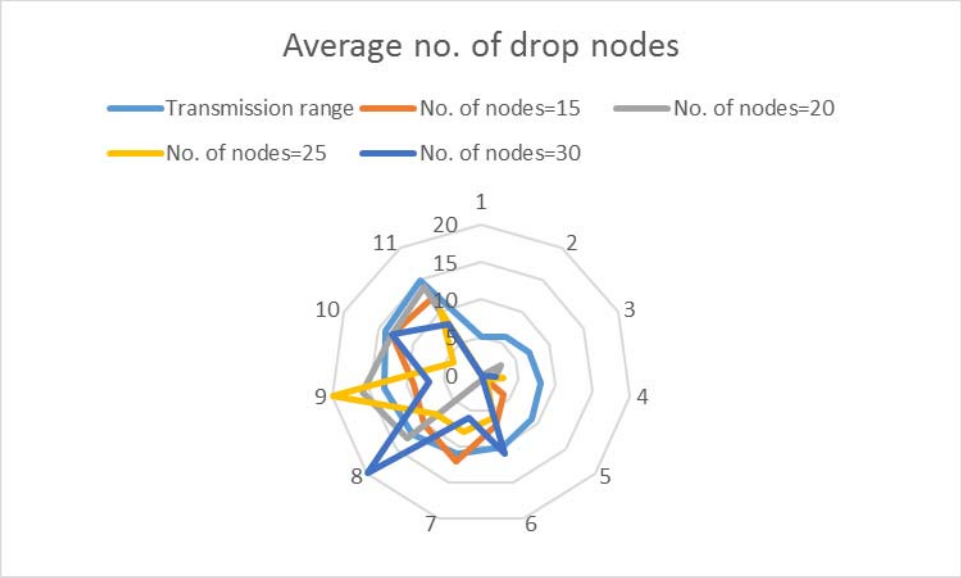

Figure 5 (a) Average Drop Rate Vs Transmission Range for Normal Routing Protocol

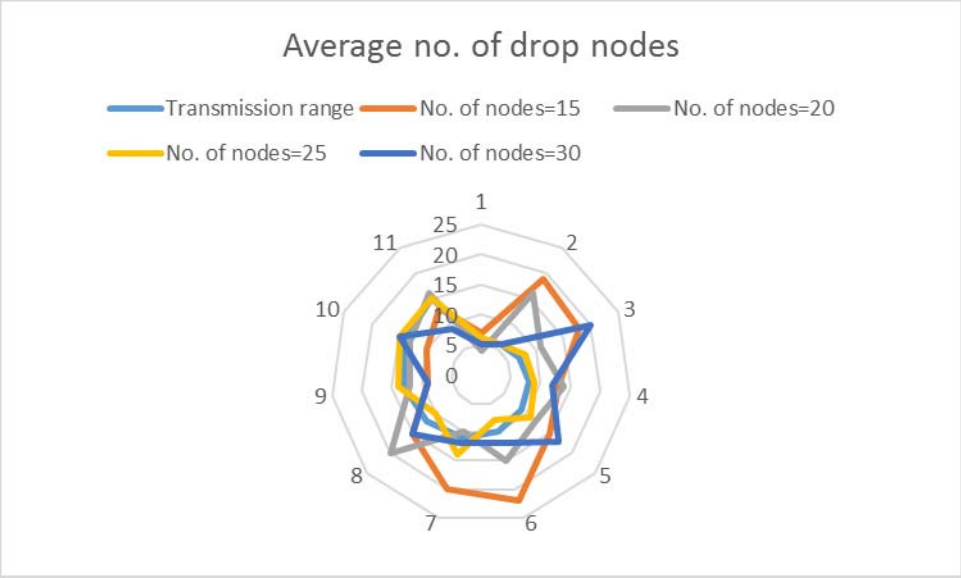

Figure 5 (b) Average Drop Rate Vs Transmission Range for Proposed Selfish Routing Protocol

Table 7 (a) Percentage of Node having Energy more than 20 for Normal

Transmission range	No. of nodes=15	No. of nodes=20	No. of nodes=25	No. of nodes=30
5	15	20	25	30
6	15	16	25	27
9	11	11	21	25
11	12	18	12	26
13	8	13	18	22
15	8	9	11	14

Table 7 (b)Proposed Selfish Routing Protocol

Transmission range	No. of nodes=15	No. of nodes=20	No. of nodes=25	No. of nodes=30
5	9	14	22	25
6	13	10	12	22
9	9	14	16	15
11	9	11	13	19
13	8	12	15	13
15	8	10	11	16

Comparison Graph of Percentage of Node having Energy more than Threshold Energy

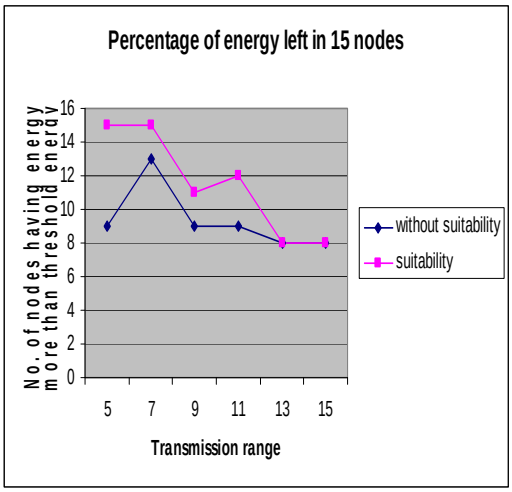

Figure 6(a)

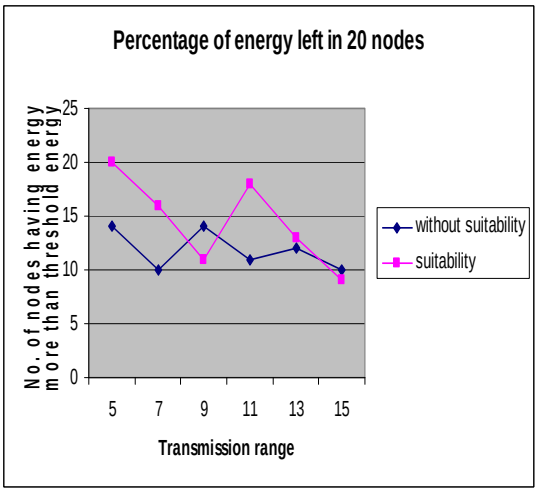

Figure 6(b)

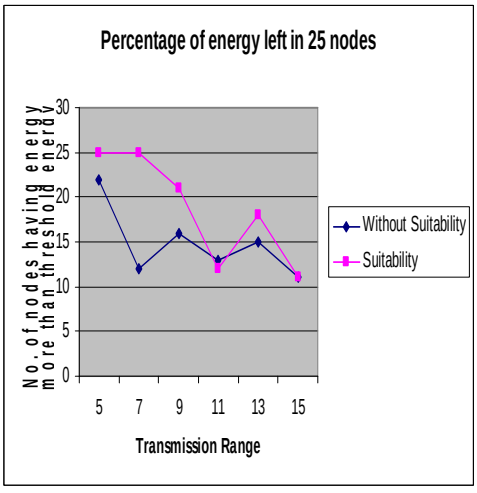

Figure 6(c)

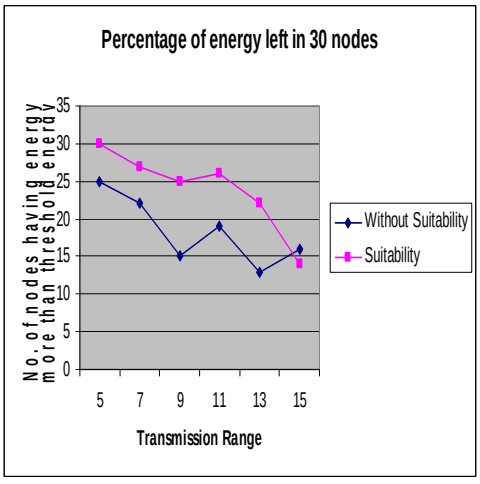

Figure 6(d)

Figure 6(a)- 6(d): No. of Nodes having Energy more than Threshold Energy

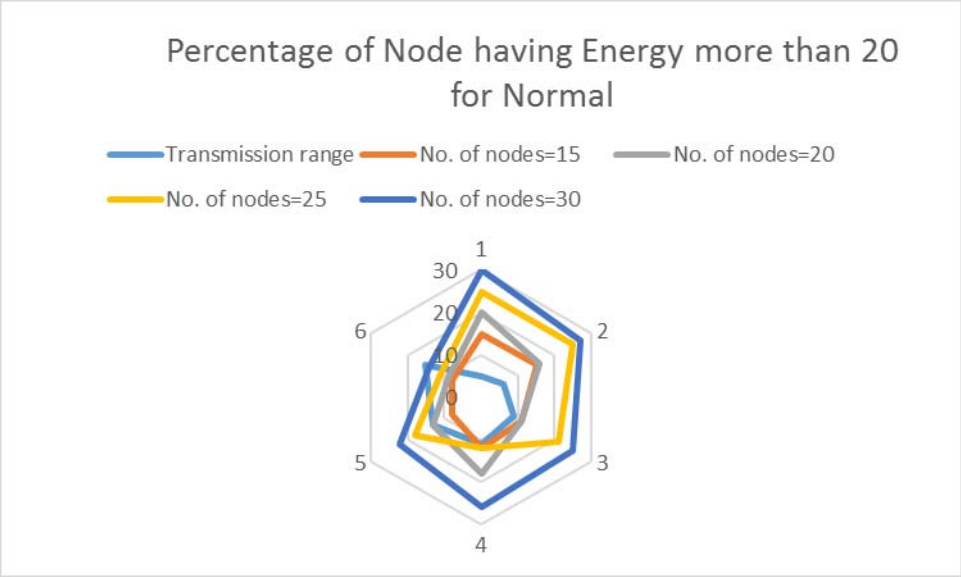

Figure 7 Percentage of Node having Energy more than 20 for Normal

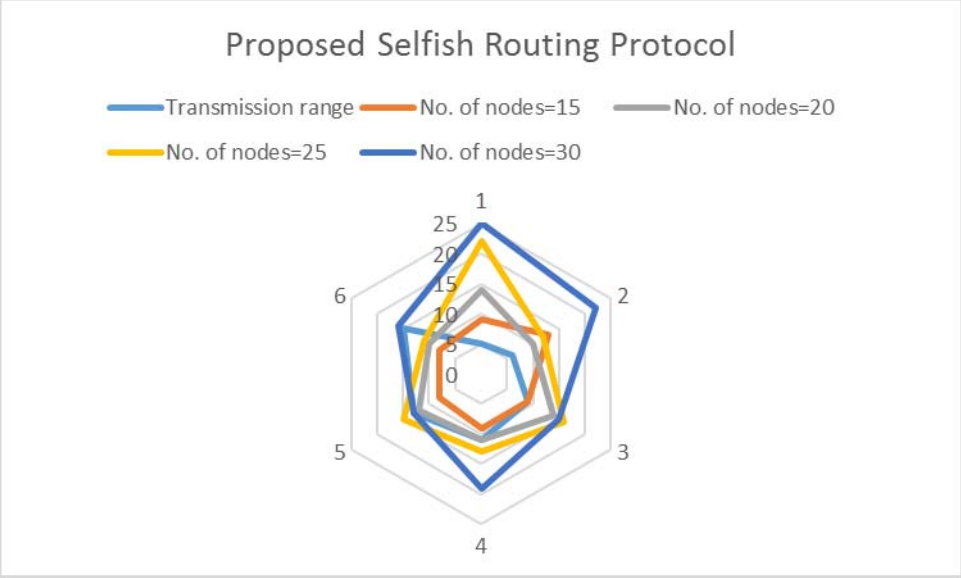

Figure 8 Proposed Selfish Routing Protocol

Discussion about Results

The power consumption in transmitting a packet is directly proportional to the distance between the source and destination, more is the distance more is the power consumed and lesser is the effective network life time.

4. Conclusion

In this work a new routing protocol has been implementing for ad hoc network. The proposed protocol is power aware keeping in view the power constraint of nodes being used in ad hoc network. To test the performance of the protocol a program has been designed in C++. This implementation in C++ used to check the performance of the protocol under various conditions. This performance has been illustrated in the forms of the graphs and tables in this research paper. The results are quite satisfactory indicating that the proposed protocol has feasible implementation.

5. Future Scope

The testing of the protocol in the present work has been done in environment where conditions are standardized. However, to check the actual applicability of protocol it is mandatory to check this protocol under an industrial standard environment. So, that actual rating of a proposal can be made. Such an environment implemented using standard software's like NS2/NS3 and Qualnet. However, to test a protocol in NS2/NS3 and Qualnet the C++ code of the protocol be physical augmented. The implementation of the protocol in C++ has accomplished this task. Now, the future work is to customize more on this implementation to create it augmentation compatibility with NS2/NS3 or Qualnet. Then the proposed protocol can be tested for more standardized conditions.

Acknowledgments

The author also wish to thank many anonymous referees for their suggestions to improve this paper.

References

[1] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks," Proc. 22nd Ann. Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2003), IEEE Press, 2003, pp. 1976-1986.

[2] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02), IEEE Press, 2002, pp. 78-87.

[3] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, September 2002, pp. 12-23.

[4] J. Mackar and S. Corson, RFC 2501, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF 1999.

[5] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," ACM Mobile Networks and Applications Journal, Special Issue on Routing in MobileCommunication Networks, pp. 183-197, October 1996.

[6] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networks,"Mobile Computing, ed. T. Imielinski and H. Korth, Kluwer Academic Publishers, pp. 153-181,1996.

[7] C-K. Toh, "A Novel Distributed Routing Protocol To Support Ad-Hoc Mobile Computing, "Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on Computers and Communication, pp. 480-486, March 1996.

[8] Raman Kumar, Harsh Kumar Verma and Renu Dhir, "Cryptanalysis and Performance Evaluation of Enhanced Threshold Proxy Signature Scheme Based on RSA for Known Signers", Mathematical Problems in Engineering, Vol. 2013, Article ID 790257, 24 pages, 2013.

[9] Raman Kumar and Nonika Singla, "Cryptanalytic Performance Appraisal of Improved CCH2 Proxy Multisignature Scheme", Mathematical Problems in Engineering, Vol. 2014, Article ID 429271, 13 pages, 2014.

[10] Raman Kumar, Harsh Kumar Verma and Renu Dhir, "Analysis and Design of Protocol for Enhanced Threshold Proxy Signature Scheme Based on RSA for Known Signers", Wireless Personal Communications – An International Journal - Springer ISSN: 0929-6212 (Print) 1572-834X (Online), Volume 80, Issue 3 (2015), Page 1281-1345.

[11] Raman Kumar and Karan Verma, "ANALYSIS AND DESIGN OF SCALABLE AND EFFICIENT KEY MANAGEMENT USING ELLIPTIC CURVE CRYPTOGRAPHY", 3rd International Conference on Electrical, Electronics, Engineering Trends, Communication, Optimization and Sciences (EEECOS–2016), SASI Institute of Technology and Engineering, Tadepalligudem, West Godavari District, Andhra Pradesh, India, pp. 302-325, 1st - 2nd June 2016.

[12] Raman Kumar and Gurpreet Singh, "ANALYSIS AND DESIGN OF AN OPTIMIZED SECURE AUDITING PROTOCOL FOR STORING DATA DYNAMICALLY IN CLOUD COMPUTING", International Conference on Processing of Materials, Minerals and Energy (PMME–2016), PACE Institute of Technology and Sciences, Ongole, Andhra Pradesh, India, pp. 1-7, 29th - 30th July 2016.

[13] Reena and Raman Kumar, "Effect of Randomization for Privacy Preservation on Classification Tasks", In Proceedings of the International Conference on Informatics and Analytics (ICIA-16), ACM, New York, NY, USA, Article 41, 5 pages, 25th - 26th August 2016. DOI: http://dx.doi.org/10.1145/2980258.2980345.

[14] Raman Kumar and Manisha Sharma, "DESIGN AND ANALYSIS OF SECURE ROUTING PROTOCOL FOR MOBILE ADHOC NETWORK", International Conference on Current Research Topics in Power, Nuclear, Fuel and Energy (PNFE–2016), st. peters engineering college, Hyderabad, India, pp. 1-12, 25th - 27th October 2016.

[15] Raman Kumar and Sandeep Thakur, "PERFORMANCE ANALYSIS OF SECURE MULTI-SERVER PASSWORD AUTHENTICATED KEY AGREEMENT SCHEME USING DISCRETE LOGARITHM MAPPED ELLIPTIC CURVE CRYPTOGRAPHY", International Conference on Current Research Topics in Power, Nuclear, Fuel and Energy (PNFE–2016), st. peters engineering college, Hyderabad, India, pp. 1-10, 25th - 27th October 2016.

[16] Dhiraj Soni and Raman Kumar, "Multimedia Cloud Computing Security an Evolving Trend: Rudimentary EssentialsComputing", International Journal of Advanced Trends in Computer Applications, (IJATCA), Vol. 2, Issue 7, pp. 19-25, 20th January 2016.

[17] Dhiraj Soni and Raman Kumar, "Multimedia Data Security Based on RSA and MD-5 Algorithm for Downloading and Uploading in MATLAB Environment", International Journal of Advanced Computronics and Management Studies, (IJACMS), Vol. 1, No. 1, pp. 47-51, February, 2016.