International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 3, June 2022, pp. 2743~2755
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i3.pp2743-2755

Design and development of anonymous location based routing for mobile ad-hoc network

Swetha Mahendrakar Shaymrao[1], Pushpa Sothenahalli Krishnaraju[1], Thungamani Mahalingappa[2], Manjunath Thimmasandra Narayanappa[1]
[1]Department of Information Science and Engineering, BMS Institute of Technology and Management, Bengaluru, India
[2]Department of Computer Science, University of Horticulture, Gandhi Krishi Vigyana Kendra, Bengaluru, India

Article Info

Article history:

Received Oct 13, 2020
Revised Dec 29, 2021
Accepted Jan 19, 2022

Keywords:

Anonymous location-aided routing in suspicious MANET
Anonymous location-based efficient routing protocol
Authenticated anonymous secure routing
Optimal decided trust inference
Optimal tug of war partition
Strong secure anonymous location based routing

ABSTRACT

Mobile ad-hoc network (MANET) consists of wireless nodes interacting with each other impulsively over the air. MANET network is dynamic in nature because of which there is high risk in security. In MANET keeping node and routing secure is main task. Many proposed methods have tried to clear this issue but unable to fully resolve. The proposed method has strong secure anonymous location based routing (S2ALBR) method for MANET using optimal partitioning and trust inference model. Here initially partitions of network is done into sectors by using optimal tug of war (OTW) algorithm and compute the trustiness of every node by parameters received signal strength, mobility, path loss and co-operation rate. The process of trust computation is optimized by the optimal decided trust inference (ODTI) model, which provides the trustiness of each node, highest trust owned node is done in each sector and intermediate nodes used for transmission. The proposed method is focusing towards optimization with respect to parameter such as energy, delay, network lifetime, and throughput also above parameter is compared with the existing methods like anonymous location-based efficient routing protocol (ALERT), anonymous location-aided routing in suspicious MANET (ALARM) and authenticated anonymous secure routing (AASR).

Corresponding Author:

Swetha Mahendrakar Shaymrao
Department of Information science and Engineering, BMS institute of Technology and management
Doddaballapur Main Road, Avalahalli, Yelahanka, Bengaluru, Karnataka 560064, India
Email: swethams_ise2014@bmsit.in

1. INTRODUCTION

Mobile ad-hoc network (MANET) are mobile nodes that interact with each other impulsively over the air. MANET network keeps changing frequently because of the itinerant nature of its nodes. Due to this changing nature and nodes configuring by itself there is high risk in its security as shown in Figure 1 [1]. In MANET biggest problem is keeping the node secure which cannot be identified easily while routing. A main criterion of MANET is to provide unknown route for nodes [2]. Designing defeating protocols for such argumentative environments is an challenging task in MANETs due to misbehaving of nodes [3], [4] we need a fault tolerant and secure routing protocols to identify and to find routing in aggressive system, especially in the system where there is lot of duplication of nodes [5], [6].

In MANETs, most important part is hiding the nodes during communication. This can be achieved when nodes satisfy two conditions i) unidentifiability wherein source nodes and destination node should not exposes itself other nodes and ii) unlinkability wherein the motility and path of nodes from its start to end should be unable to be linked [7], [8]. Security is a very important in argumentative environments. As nodes

in the network are not trustable, at any time trustable node can become malevolent node and make other nodes also malevolent. As a result, mysterious communications (secure routing) will hide the node identifications and routes [9]. To protect node identity it needs to be continuously changing its identity with random numbers. A lot pf papers has been proposed earlier on anonymous routing [10], [11]. A direct method is mysterious routing wherein on-demand ad-hoc routing protocols, such as dynamic source routing (DSR) and ad-hoc on-demand distance vector (AODV) are used [12]. Mysterious routing protocol transfers the information very securely while compared with other techniques.

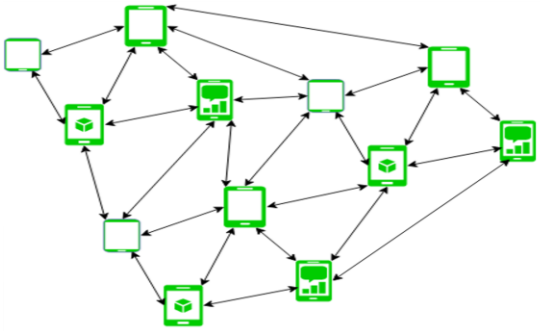

Figure 1. Simple structure of MANET

2. MOTIVATION

For security reason one method is that we go with mysterious path wherein no hacker identifies nor any other node identifies [13]–[16]. High security and privacy in MANET have been a major issue, while it comes in the field of defense and other such routing. Most of the communication system provides security in routing and data content. Mysterious communications should focus on anonymity in identity, location and route of the participating nodes. Mysterious communication between the MANET nodes are challenging as the nodes are free to move anywhere.

3. LITERATURE SURVEY

Zhang *et al.* [1] proposed protocol working on ant colony optimization (ACO) and physarum autonomic optimization (PAO) and introduced a bio-inspired hybrid trusted routing protocol (B-iHTRP). Initially perceptive ants were introduced using cross-layer perception into ACO. These perceptive ants would find route table in each zone and would find route to destination while B-iHTRP would utilize PAO to find best route from the existing different routes for multi–zone communication. Thus by utilizing ACO and PAO improved performance but they was high energy consumption when compared with distributed hash table (DHT) routing method.

Biswas *et al.* [2] has proposed a system wherein performance of secure routing better resource utilization and good throughput were gained but lacked in performance. According to his system packet transmission with great security with better resource utilization of mobile were involved along with neglecting black hole attacks. He ensured trust in every node based on most reliable route during transmission in the network which had stability based on mobility and pause time, remaining battery power.

Abid *et al.* [3] proposes a system which works on DHT-based routing. As per this routing nodes uses 3D structure to find relationship of node which again exploits 3D logical space by taking a statistics of each intermediate node. These nodes have algorithm assigned to it which runs to find its nearest logical identifier in the 3D logical space. Since it uses 3D structure which has multi-paths to destination node which helps it to measure and bounce back to its original path in case of node/link failure. Even though this proposed system has some great advantage when compared with other DHT routing protocol such as routing overhead, end-to-end delay, path-stretch values and packet-delivery ratio. But this is not workable for high traffic network because network lifetime is very low.

Taha *et al.* [4] proposes ad-hoc system based on multiple path distant vector protocol with fitness function (FF-AOMDV). According to these nodes find best possible path to reach from source to destination in multipath routing so as to reduce energy consumption. Even though this system is better than AOMDV and AOMR-LM in many of the network performance metrics and parameters but has a major problem within its internal module during malicious attacks during data transmission.

Ejmaa *et al.* [5] came up with a method which is far better when compared with net charge per residue (NCPR) and AODV when made comparison with end to end delay, energy consumption network connectivity packet delivery ration and normal routing overhead. His protocol uses neighbor node connection dynamically and is named as dynamically connectivity factor routing protocol (DCFP). This routing protocol fetches data dynamically with neighbor nodes without the help of system administrator.

Smith *et al.* [6] in recent years many have used MANET due to its mobility and flexibility. These security protocols either protect routing or communication. But full protection has to be for both routing and communication. Keeping this as basis security using pre-existing routing for mobile ad hoc networks (SUPERMAN) framework was proposed. According to this framework protocols were allowed to do it's function keeping control over access, anonymity of node and secure communication. Simultaneously SUPERMAN frame work is compared with others to develop wireless communication security.

Shen and Zhao [7] designed a routing which separates network field dynamically into zones and then arbitrarily picks up next node to pass on the information. In this routing nodes are non-traceable and anonymity of routing is secured. His routing is based on Unidentifiable path based and efficient routing protocol (ALERT). ALERT has capability to hide the data initiator which in turn strengthens the source providing anonymity of Source node. This routing is also tough when it comes to timing attacks and intersection. At the end when data is transmitted to destination zone it provides complete K-anonymity.

4. PROPOSED SYSTEM

The proposal is for a intensely strong secure anonymous location based route (S2ALBR) method for MANET using best and most favorable partitioning and trust inference model both the methods optimize the network by considering the density of the node and divide the network has cluster [17]. The Figure 2 shows the structure of the proposed system. In S2ALBR method, initially separation of network is done into cluster zone using optimal tug of war partition (OTW) algorithm. Then we analyze the trustiness of each and every mobile node using optimal decided trust inference (ODTI) model. The trustiness is considered based on strong network parameter like received signal strength (RSS), mobility, and path loss and cooperation rate [18]. RSS is cost-effective metric used to estimates the distance between the mobile nodes for localization objectives. RSS is the most widely used benchmark because it is easy to measure and is directly related to the provision excellence [19], [20]. The RSS and cooperation rate values should be high or maximum, mobility, and path loss values should be low as much as possible.

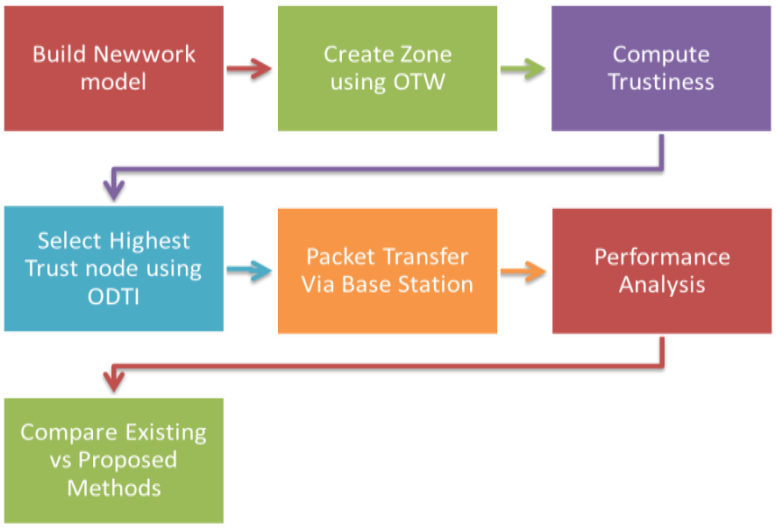

Figure 2. Structure of network model

The process of deserving and confidential node is optimized by the ODTI model, which provides the confidence in each node, and then it collects the highest deserving node as cluster head for the transmission and process the transmission with confidentially on each node in each cluster zones and intermediate nodes used for data transmission [21]. The proposed research focuses on the following objectives: i) to provide secure communication between mobile nodes, ii) to reduce parameters or minimize delay and energy used in

nodes, iii) to progress or maximize the throughput, system lifetime, and iv) comparing the above network parameter with the existing methods like anonymous location-based efficient routing protocol (ALERT), anonymous location-aided routing in suspicious MANET (ALARM) and authenticated anonymous secure routing (AASR).

5. METHOD

The NS2 is used to simulate the proposed S2ALBR protocol. The performance of the protocol is examined using various testing scenarios [22]. The nodes represented by varying number of attacker node and normal node. The S2ALBR protocol for MANET using optimal partitioning and trust inference model. The proposed work carries the following steps: i) creation of network model, ii) creation of cluster or zone using optimal tug of war partition method, iii) selection of trustiness node in sector, iv) routing scheme, v) performance analysis, and vi) comparison with existing methods.

5.1. Creation of network model

MANET consists many number of mobile nodes which exchanges its information with each other via wireless network. The Figure 3 shows the network model of 50 nodes. In the beginning step will create a 50 nodes as per the screen resolution. The node will be placed by reading the X and Y axis quadrants. In the similar way we can create a network of 100 nodes 200 nodes and for 500 nodes.

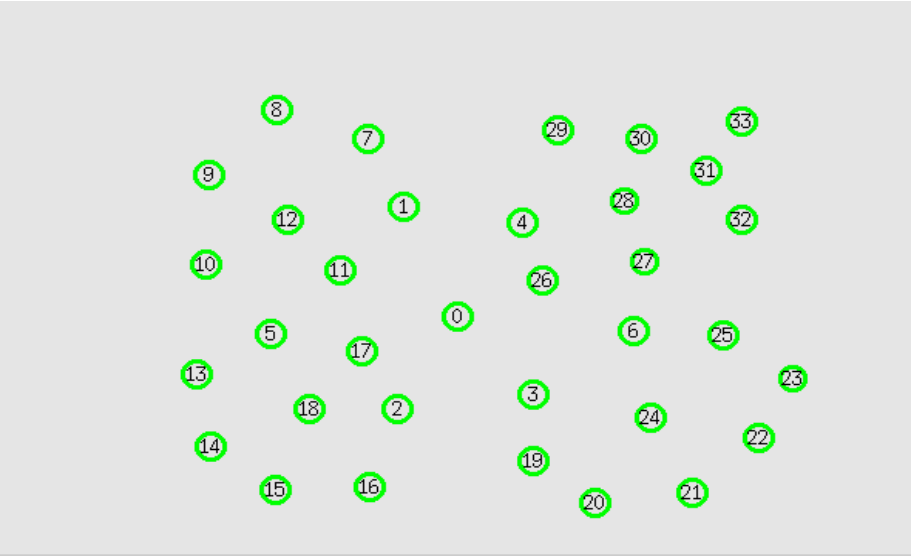

Figure 3. Network model

5.2. Creation of cluster or zone using optimal tug of war partition method

The cluster will be formed from nodes. To maintain the density of the node and to optimize the network load will use optimal tug of war process (OTW) as shown in Table 1. In this research work network area is considered has 1000*1000 m and 600 m of communication range of each node in the network model.

5.3. Selection of trustiness node in sector

In the proposed model entire system is gathered to form sectors. Sectors are nothing but grouping of nodes based on its positioning as shown in the Figure 4. Once sectors are being created they calculate distance between current node and source node which then starts grouping based on nearest distance [23]–[25]. In the sectors node trustiness is computed by every node is calculated by the parameter like received signal strength (RSS), mobility, path loss and cooperation rate and is called as ODTI method or model, which provides the trustiness of each mobile. Then selects the highest trust degree owned node in each sector as intermediate node for data transmission, which form a non-traceable mysterious route. The selection of trustiness node in each sector done by ODTI model as shown in the Table 2. The proposed ODTI algorithm variants for the two strategies and analyze the computation complexity [26].

Table. 1 Tug-of-war optimization algorithm

Partition using Tug-of-war optimization algorithm	
1	Begin
2	Initialize number of mobile nodes, variables and range of variables
3	Generate population of variable by random solutions
4	While do
5	Compute the objective function
6	Define the weights of groups
7	Sort the solutions and save best one
8	For each group i
9	For each group j
10	If ($W_i < W_j$)
11	Move group I towards group j
12	Close if
13	Close for
14	Compute total displacement of group i
15	Compute total displacement of group j
16	Use the side constraints handling technique
17	Compute the new objective functions
18	Close if
19	Close while
20	Close
Return: optimal partitioning	

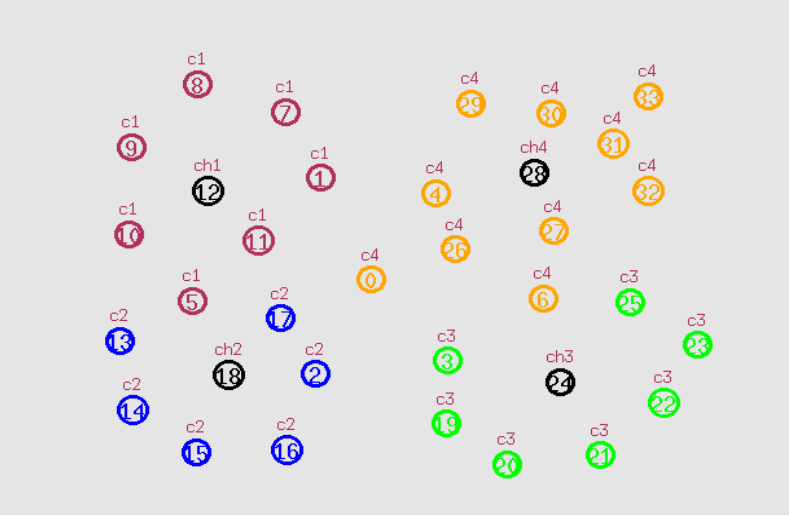

Figure 4. Creation of sector

Table 2. Trust computation using ODTI model

Trust computation using ODTI model	
1	Begin
2	Initialize number of mobile nodes, number of constraints and threshold
3	While do
4	Compute the RSS (K1)
5	Compute the mobility (K2)
6	Compute the path loss (K3)
7	Compute the path cooperation rate (K4)
8	Compute the fitness function
9	Define best and worst solutions
10	For each node i
11	Trust degree=K1+K2+K3+K4
12	Threshold=Min (K2+K3) U Max (K4+K1)
13	If (Trust degree>Threshold)
14	Trust degree=optimal solution
15	Close if
16	Close for
17	Close while
18	Close
Return: optimal trust value	

5.4. Routing scheme

The routing will happen between cluster to cluster through cluster head, that is intra and inter cluster communication [27], [28]. Intra cluster is within the cluster and inter cluster is between the two clusters. The routing in the network is established by selecting a secure trustable node with high trust degree knows as header node and this selected header node is responsible to transmission of data in each sector as shown in Figure 5.

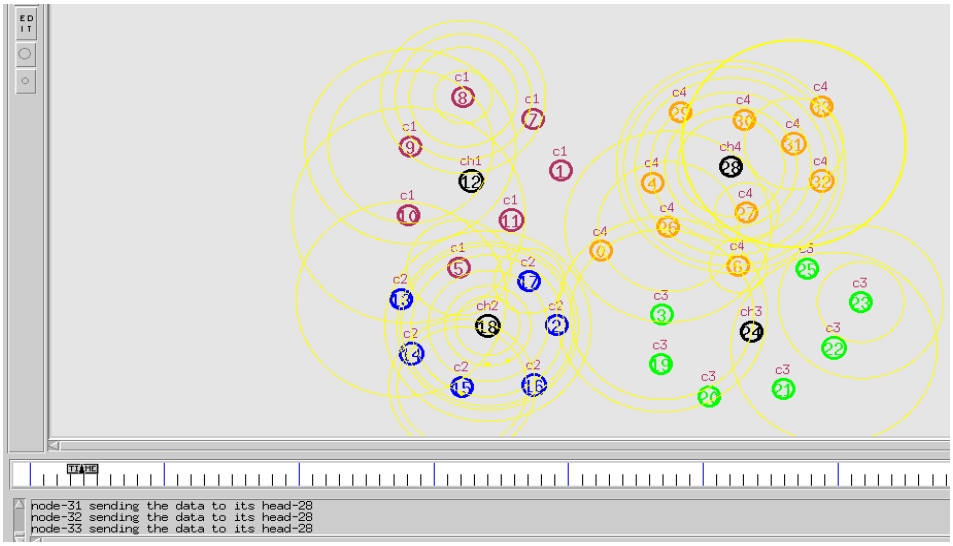

Figure 5. Routing in proposed model

5.5. Performance analysis

Finally, the performance of the proposed intensely strong secure anonymous location based routing (S2ALBR) method is done for the major network parameters with minimizing energy consumption, Delay maximizing network lifetime and throughput with varying the number of nodes and for attackers. Figures 6-9 shows the graph for the proposed methods S2ALBR for energy consumption, Delay, network lifetime and throughput for the number of nodes 50, 100, 150, 200 and 250 nodes. Figures 10-13 shows the graph for the proposed methods S2ALBR for energy consumption, Delay, network lifetime and throughput by varying the attackers 5, 10, 15, 20 and 25 with respect to nodes. The performance analysis S2ALBR method is given below with respect to number of attacker 5, 10, 15, 20 and 25.

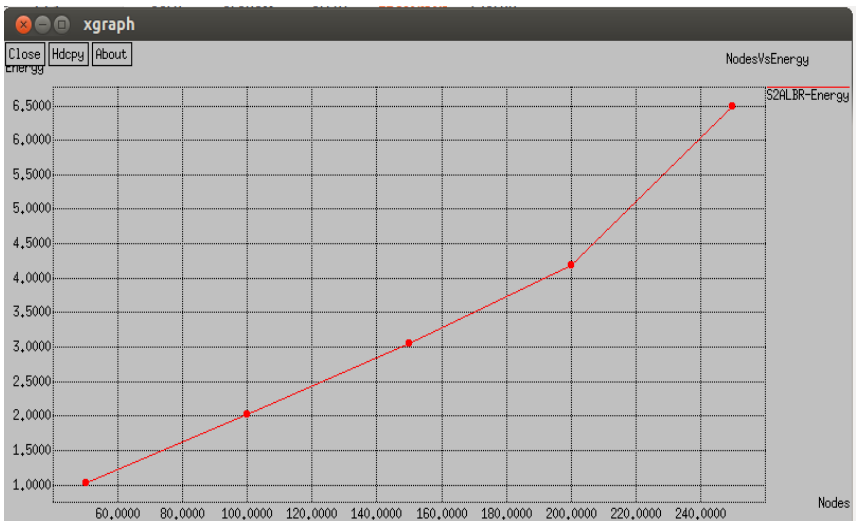

Figure 6. Energy consumption graph of S2ALBR method

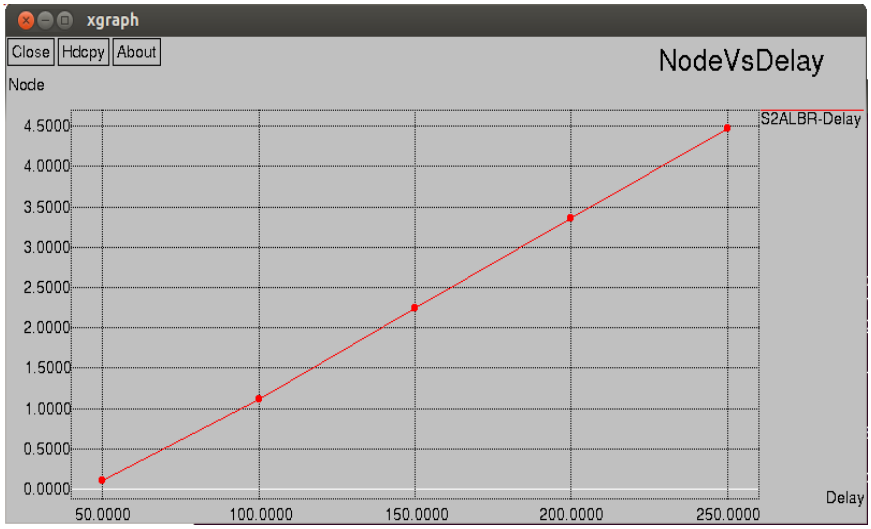

Figure 7. Delay graph of S2ALBR method

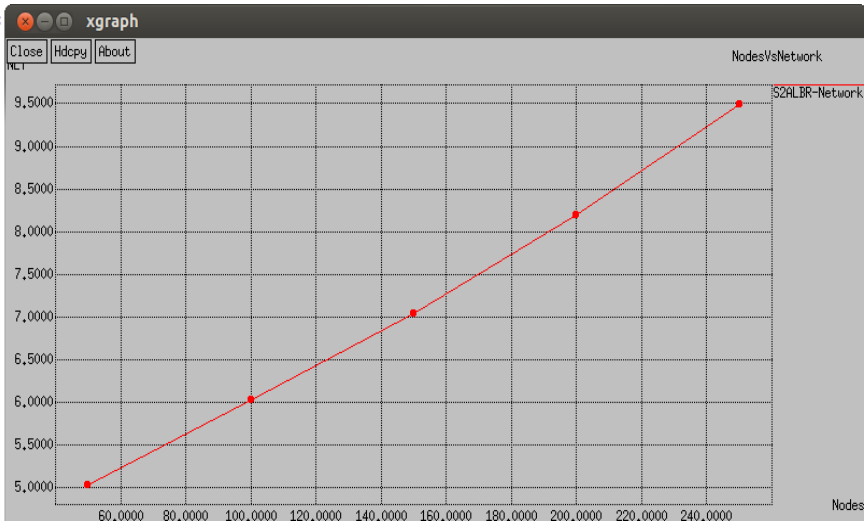

Figure 8. Network lifetime graph of S2ALBR method

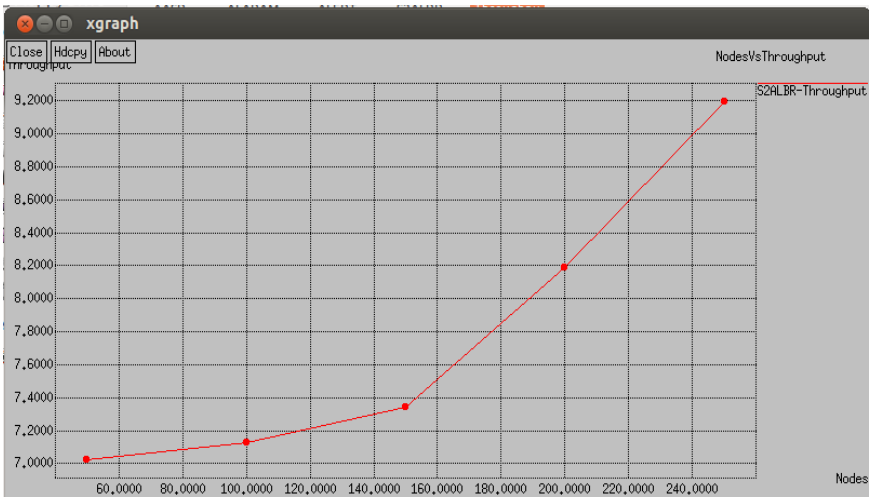

Figure 9. Throughput graph of S2ALBR method

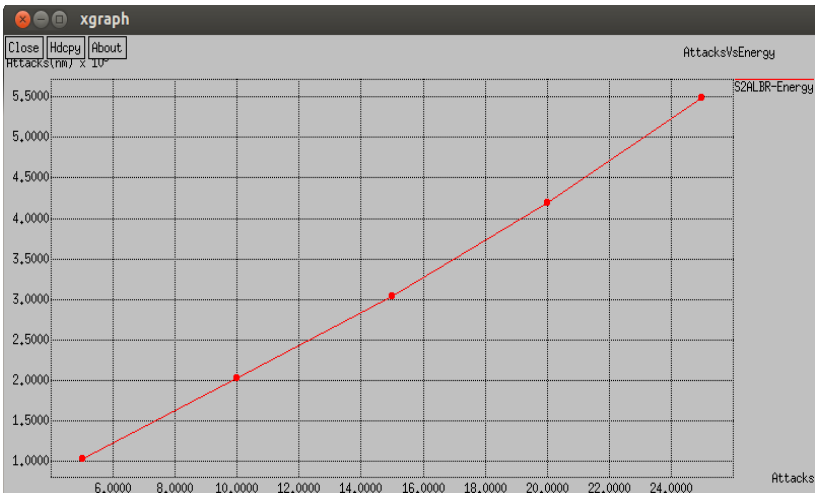

Figure 10. Energy consumption graph of S2ALBR method w.r.t attack

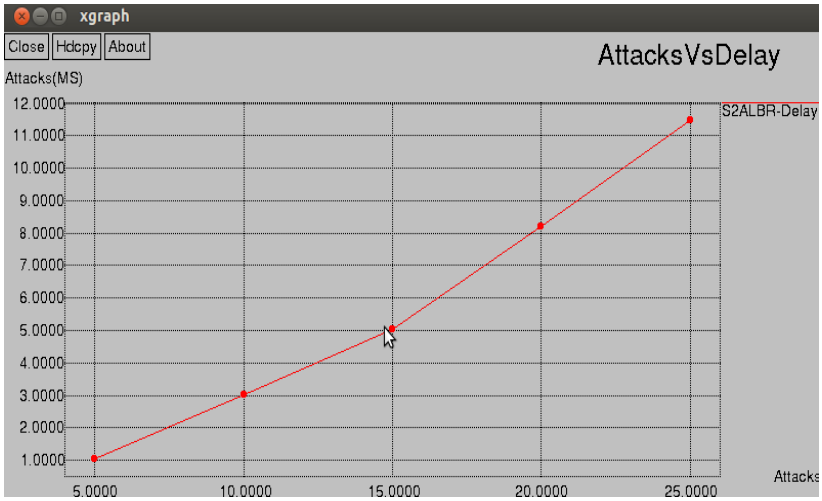

Figure 11. Delay graph of S2ALBR method w.r.t attack

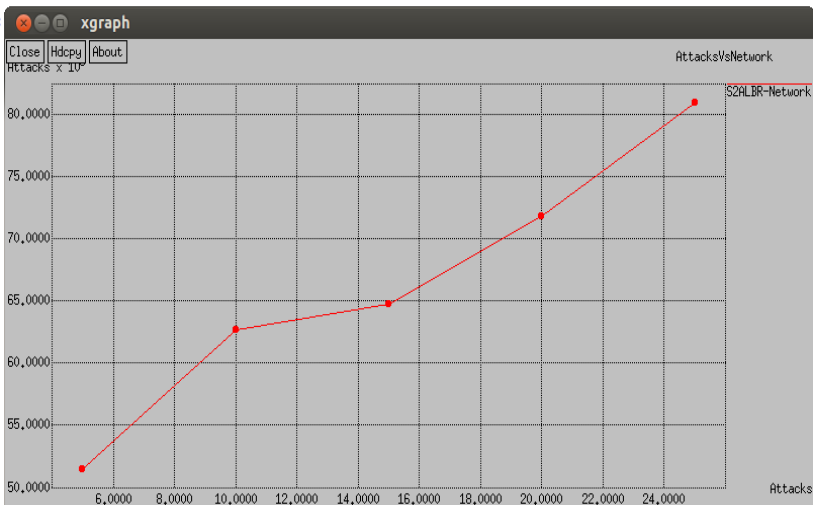

Figure 12. Network lifetime graph of S2ALBR method w.r.t attack

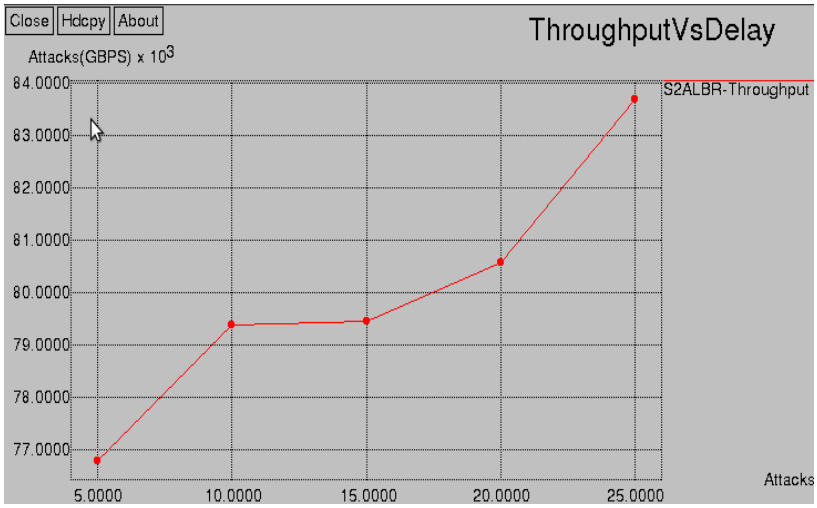

Figure 13. Throughput graph of S2ALBR method w.r.t attack

5.6. Comparison with existing methods

5.6.1. Comparison-number of nodes

By varying number of nodes from 50 to 250 randomly the performance metrics of proposed and previous routing protocol is given in Figures 14-17. The delay was minimized from 29% to 5% respectively and shown in Figure 15. Then energy was increased from 8% to 10% and graphical results shown in Figure 14. The network lifetime and throughput also increased as Compared with the ALERT, ALARAM and AASR as result shown in Figures 16 and 17.

5.6.2. Comparison-number of attacker

In this test, by vary the number of attacks as 5, 10, 15, 20 and 25 with respect to the number nodes given in Figures 18-21. The performance evaluation and the result comparison of proposed S2ALBR protocol and existing ALERT [7], ALARM [8] and AASR [9]. Delay of proposed S2ALBR protocol is 30.08% lower than ALERT, 37.1% lower than ALARAM and 41% than AASR as shown in Figure 19. Energy consumption of proposed S2ALBR protocol is 28.12% lower than ALERT, 35% lower than ALARAM and 37.34% than AASR as shown in Figure 18. Network lifetime of proposed S2ALBR protocol is 31.2% higher than ALERT, 19.5% higher than ALARAM and 17.3% higher than AASR as shown in Figure 20. Throughput of proposed S2ALBR protocol is 41.2% higher than ALERT, 36.7% higher than ALARAM, 32.2% higher than AASR as shown in Figure 21.

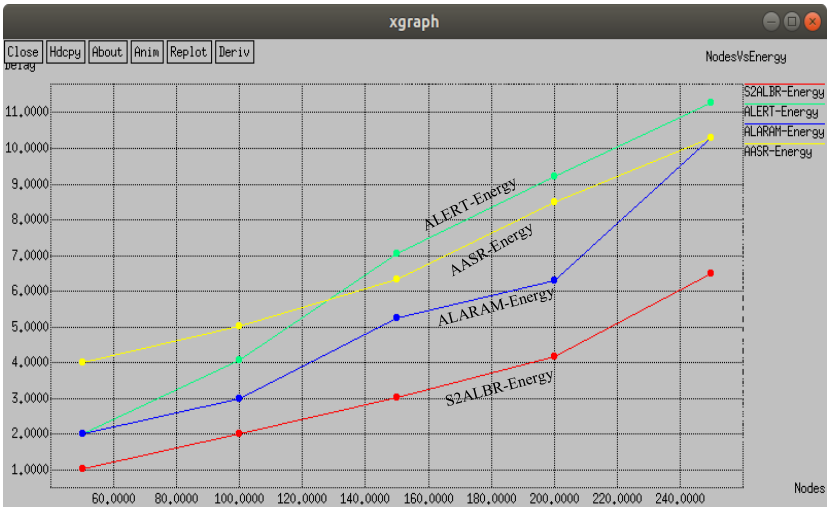

Figure 14. Energy consumption graph

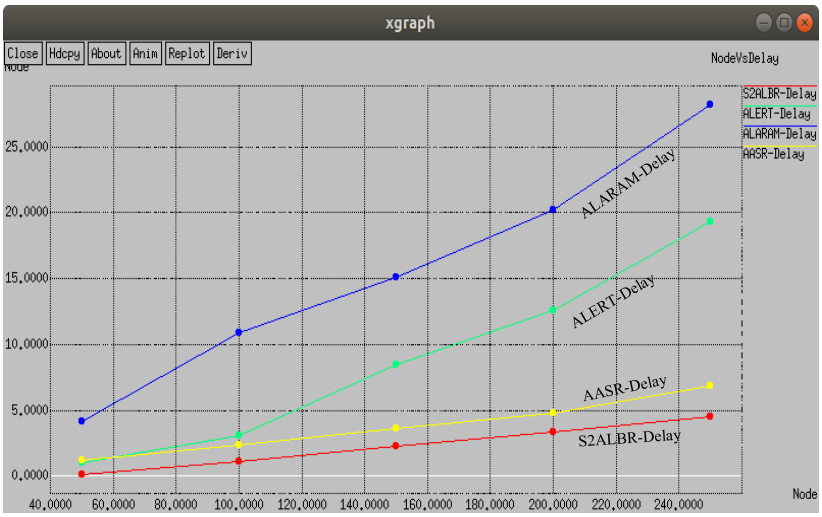

Figure 15. Delay graph

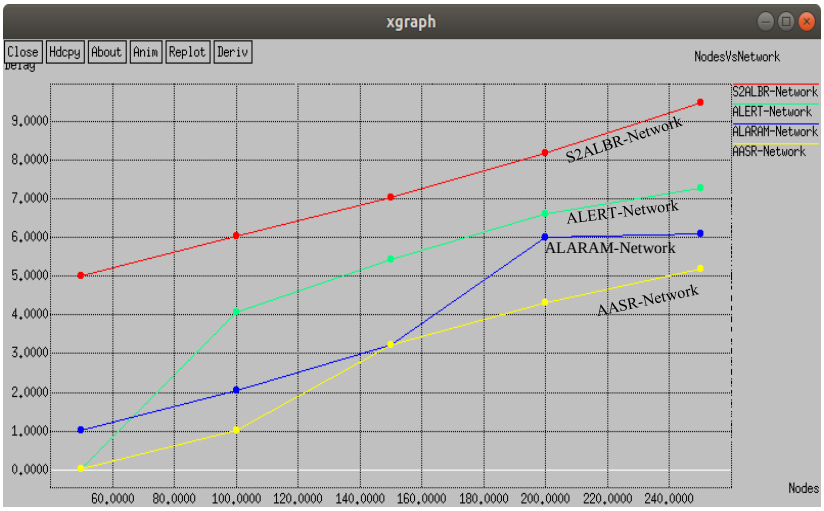

Figure 16. Network lifetime graph

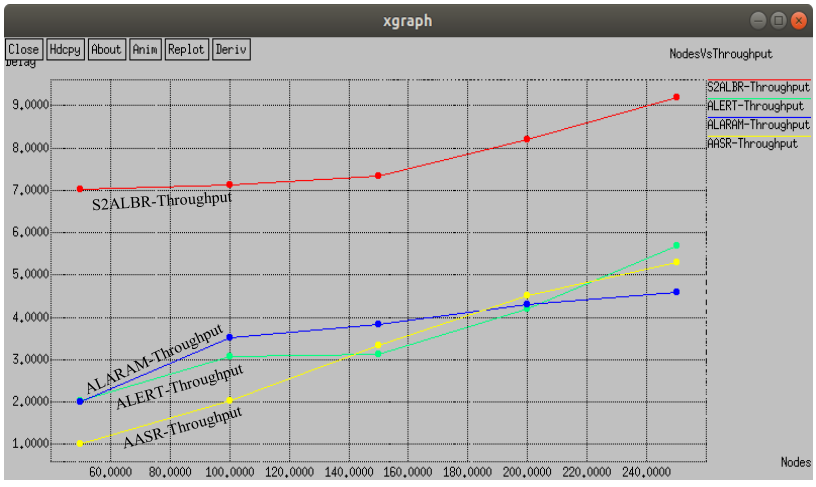

Figure 17. Throughput graph

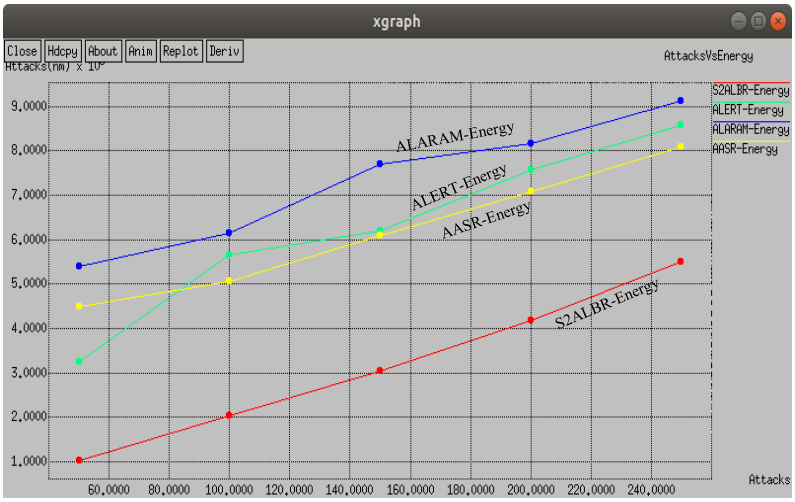

Figure 18. Energy consumption graph

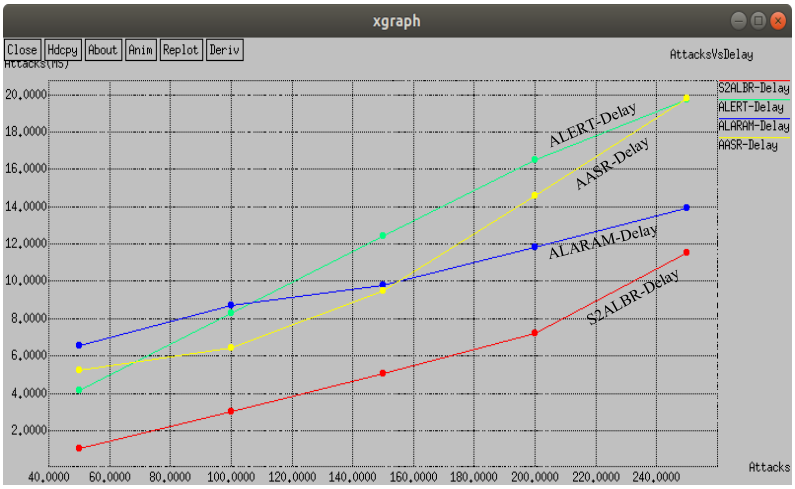

Figure 19. Delay graph

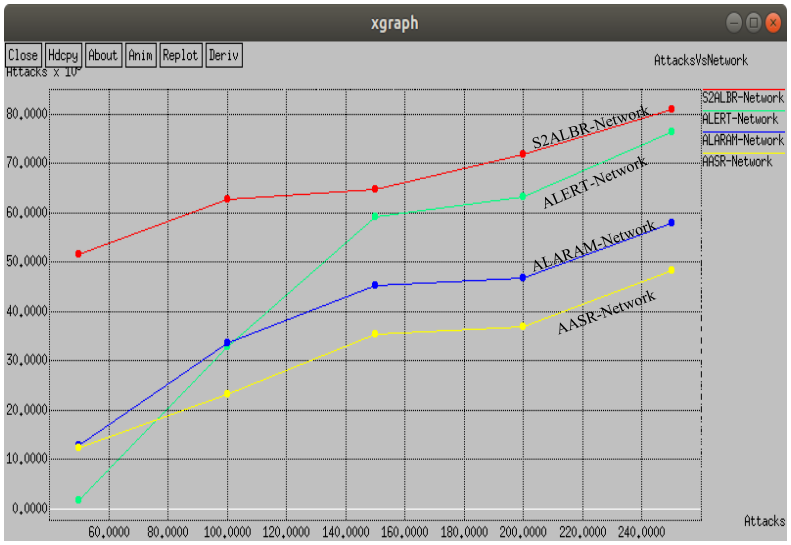

Figure 20. Network lifetime graph

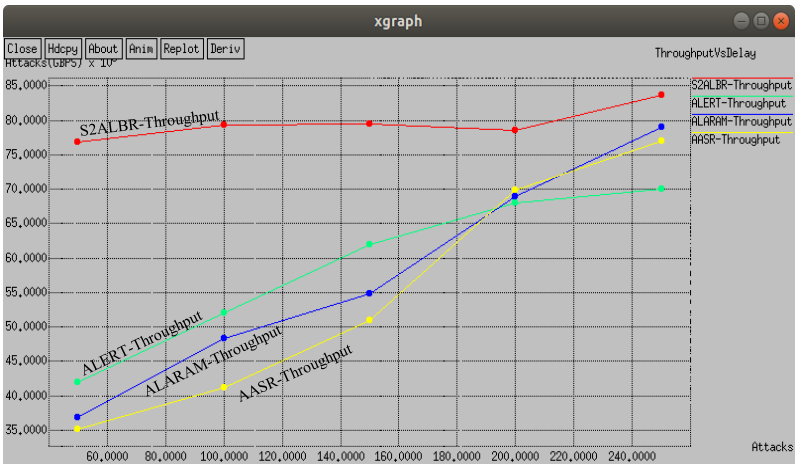

Figure 21. Throughput graph

6. CONCLUSION

S2ALBR method is used for the selection of strong secure trusted node in each sector and this trusted node is responsible for the communication between the intermediate nodes, the proposed work is to reduce the network parameter like delay, energy consumption in the network and maximize the throughput, network lifetime in network and the said method S2ALBR is checked with the existing technique ALERT, ALARM and AASR and by this we can justify proposed method is better one. In future the work can be enhanced by using soft computing-based techniques, and location-based routing in telecommunications.

REFERENCES

[1] M. Zhang, M. Yang, Q. Wu, R. Zheng, and J. Zhu, "Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs," *Future Generation Computer Systems*, vol. 81, pp. 505–513, Apr. 2018, doi: 10.1016/j.future.2017.07.030.

[2] S. Biswas, T. Nag, and S. Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET," in *2014 Applications and Innovations in Mobile Computing (AIMoC)*, Feb. 2014, pp. 157–164, doi: 10.1109/AIMOC.2014.6785535.

[3] S. A. Abid, M. Othman, N. Shah, M. Ali, and A. R. Khan, "3D-RP: A DHT-based routing protocol for MANETs," *The Computer Journal*, vol. 58, no. 2, pp. 258–279, Feb. 2015, doi: 10.1093/comjnl/bxu004.

[4] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq, and T. Saba, "Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function," *IEEE Access*, vol. 5, pp. 10369–10381, 2017, doi: 10.1109/ACCESS.2017.2707537.

[5] A. M. E. Ejmaa, S. Subramaniam, Z. A. Zukarnain, and Z. M. Hanapi, "Neighbor-based dynamic connectivity factor routing protocol for mobile ad hoc network," *IEEE Access*, vol. 4, pp. 8053–8064, 2016, doi: 10.1109/ACCESS.2016.2623238.

[6] D. Hurley-Smith, J. Wetherall, and A. Adekunle, "SUPERMAN: security using pre-existing routing for mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2927–2940, Oct. 2017, doi: 10.1109/TMC.2017.2649527.

[7] H. Shen and L. Zhao, "ALERT: an anonymous location-based efficient routing protocol in MANETs," *IEEE Transactions on Mobile Computing*, vol. 12, no. 6, pp. 1079–1093, Jun. 2013, doi: 10.1109/TMC.2012.65.

[8] K. El Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," *IEEE Transactions on Mobile Computing*, vol. 10, no. 9, pp. 1345–1358, Sep. 2011, doi: 10.1109/TMC.2010.256.

[9] W. Liu and M. Yu, "AASR: authenticated anonymous secure routing for MANETs in adversarial environments," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4585–4593, Nov. 2014, doi: 10.1109/TVT.2014.2313180.

[10] Remya S and Lakshmi K S, "SHARP: secured hierarchical anonymous routing protocol for MANETs," in *2015 International Conference on Computer Communication and Informatics (ICCCI)*, Jan. 2015, pp. 1–6, doi: 10.1109/ICCCI.2015.7218121.

[11] S. M. Shaymrao *et al.*, "Strong secure anonymous location based routing (S2ALBR) method for MANET," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 3, pp. 4349–4356, 2021, doi: 10.17762/turcomat.v12i3.1726.

[12] H. Moudni, M. Er-rouidi, H. Mouncif, and B. El Hadadi, "Secure routing protocols for mobile ad hoc networks," in *2016 International Conference on Information Technology for Organizations Development (IT4OD)*, Mar. 2016, pp. 1–7, doi: 10.1109/IT4OD.2016.7479295.

[13] S. Othmen, F. Zarai, A. Belghith, and L. Kamoun, "Anonymous and secure on-demand routing protocol for multi-hop cellular networks," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, May 2016, pp. 1–6, doi: 10.1109/ISNCC.2016.7746093.

[14] U. R. Bhatt, N. Nema, and R. Upadhyay, "Enhanced DSR: an efficient routing protocol for MANET," in *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, Feb. 2014, pp. 215–219, doi: 10.1109/ICICICT.2014.6781282.

[15] S. Mohapatra and P. Kanungo, "Performance analysis of AODV, DSR, OLSR and DSDV routing protocols using NS2 simulator," *Procedia Engineering*, vol. 30, pp. 69–76, 2012, doi: 10.1016/j.proeng.2012.01.835.

[16] Y. Wang, M. Motani, H. K. Garg, Q. Chen, and T. Luo, "Multi-channel directional medium access control for ad hoc networks: A cooperative approach," in *2014 IEEE International Conference on Communications (ICC)*, Jun. 2014, pp. 53–58, doi: 10.1109/ICC.2014.6883294.

[17] A. Jenniefer and J. R. Jose, "Techniques for identifying denial of service attack in wireless sensor network: a survey," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 6, pp. 7247–7249, 2014.
[18] Xin Ming Zhang, En Bo Wang, Jing Jing Xia, and Dan Keun Sung, "A neighbor coverage-based probabilistic rebroadcast for reducing routing overhead in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 3, pp. 424–433, Mar. 2013, doi: 10.1109/TMC.2011.277.
[19] S. Liu, Y. Yang, and W. Wang, "Research of AODV routing protocol for ad hoc networks," *AASRI Procedia*, vol. 5, pp. 21–31, 2013, doi: 10.1016/j.aasri.2013.10.054.
[20] H. Kaur, M. Bala, and V. Sahni, "Study of blackhole attack using different routing protocols in MANET," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 2, no. 7, pp. 3031–3039, 2013.
[21] S. A. Abid, M. Othman, and N. Shah, "Exploiting 3D structure for scalable routing in MANETs," *IEEE Communications Letters*, vol. 17, no. 11, pp. 2056–2059, Nov. 2013, doi: 10.1109/LCOMM.2013.091113.131256.
[22] W. Quan, J. Guan, C. Xu, S. Jia, J. Zhu, and H. Zhang, "Content retrieval model for information-center MANETs: 2-dimensional case," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2013, pp. 4422–4427, doi: 10.1109/WCNC.2013.6555290.
[23] S. K. Guirguis and O. S. .Saaid, "Evaluating the performance of secure routing protocols in mobile ad hoc networks," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 1, no. 9, pp. 710–716, 2012.
[24] Z. Wan, K. Ren, and M. Gu, "USOR: an unobservable secure on-demand routing protocol for mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 5, pp. 1922–1932, May 2012, doi: 10.1109/TWC.2012.030512.111562.
[25] N. Shah, D. Qian, and R. Wang, "MANET adaptive structured P2P overlay," *Peer-to-Peer Networking and Applications*, vol. 5, no. 2, pp. 143–160, Jun. 2012, doi: 10.1007/s12083-011-0115-5.
[26] I. Panda, "A survey on routing protocols of MANETs by using QoS metrics," in *International Journal of Advanced Research in Computer Science and Software Engineering*, 2012, vol. 2, no. 10, pp. 120–129.
[27] S. Bali, J. Steuer, and K. Jobmann, "Capacity of ad hoc networks with line topology based on UWB and WLAN technologies," in *2008 Wireless Telecomunications Symposium*, Apr. 2008, pp. 17–24, doi: 10.1109/WTS.2008.4547538.
[28] S. Sampalli *et al.*, "Routing intrusions on mobile ad hoc networks: Test bed and vulnerability analysis," in *2007 15th Int. Conference on Software, Telecommunications and Computer Networks*, 2007, pp. 1–5, doi: 10.1109/SOFTCOM.2007.4446072.

BIOGRAPHIES OF AUTHORS

Swetha Mahendrakar Shaymrao completed her B.E from Adichunchanagiri Institute of Technology (AIT) Chikkamagaluru and M.Tech from RV Institute of Technology (RVCE) Bangalore, in the year 2008 and 2013 respectively. Currently pursuing Ph.D under Visvesvaraya Technological University (VTU), Karnataka, India. Her area of research is Network Security, wireless sensor networks and ad-hoc networks and working tools are NS2 and NS3. She has published more than 25 technical papers in various National & International Conferences and more than 9 papers in reputed Journals and she has 13 years of teaching experience. She can be contacted at email: swethams_ise2014@bmsit.in. Researcher Id-N-9617-2017.

Pushpa Sothenahalli Krishnaraju has received her Ph.D. in wireless sensor Network from Vinayaka Mission University in the year 2017 and her master from Bangalore University, in the year 2004, Bengaluru. She is currently a Professor and Head of the Department of Information Science and Engineering at BMS Institute of technology and Management, Bengaluru. She has published more than 40 technical papers in various National and International Conferences and more than 18 papers in reputed Journals and she has 18 years of teaching experience. She can be contacted at email: pushpask@bmsit.in. Researcher Id- N-9599-2017.

Thungamani Mahalingappa has received her Ph.D. in Pattern Recognition from Centre for Manufacturing Research and Technology Utilization (CMRTU) R.V. College of Engineering, Bangalore in the year 2014 and her master from Dr. M G R Educational and Research Institute University, Chennai. She has published more than 40 technical papers in various National and International Conferences and more than 12 papers in reputed Journals and she has 16 years of teaching experience. She can be contacted at email: thungamani_k@rediffmail.com.

Manjunath Thimmasandra Narayanappa has received her Ph.D. in data warehouse and data mining from Bharathiar University in the year 2015. He is currently a Professor in Department of Information Science and Engineering at BMS Institute of technology and Management, Bengaluru. He has published more than 50 technical papers in various National and International Conferences and more than 30 papers in reputed Journals and he has 10 years of Industry and teaching experience. He can be contacted at email: manju.tn@bmsit.in**.** Researcher Id- N-9391-2017.