International Journal of Engineering & Technology, 7 (2) (2018) 6-11

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Development of mobile adhoc network using leader Selection algorithm

S.Deepa [1]*, S.Kamal Raj [2], K.P.Sridhar [2]

[1] *Research Scholar, Department of Electronics and Communication Engg,Karpagam Academy of Higher Education,Coimbatore-21.*
[2] *Associate Professor, Department of Electronics and Communication Engg, Karpagam Academy of Higher Education, Coimbatore-21.*
**Corresponding author E-mail: deepaa.selva@gmail.com*

Abstract

Mobile ad-hoc network (MANET) is an interconnection of mobile devices without preexisting topology which form a communication network. QOS parameters like congestion control, confidentiality, output, delay, energy consumption, jitter, have to be improved based on the development of transmission technology, and real-time applications. MANETs are totally different from distributed COMPUTING systems. They are dynamic and self-organizing networks. A leader is needed to coordinate and organize tasks in MANET. The challenge is to own the proper election algorithm that chooses the correct leader based on numerous factors in MANET. The task of the leader is to keep up the quality of service (QOS) in the MANET. This paper explores QoS in MANET by using the leader of the network by correct election algorithm by improving the network lifetime, path stability, and reduce end to end delay.

Keywords: *Bully Algorithm; Distributed Systems; Election; Leader; QOS; Ring Algorithm; Throughput.*

1. Introduction

MANET has mobile devices which can alter its topology and location based on the mobility. It is also recognized as wireless ad hoc network. Since MANETs are portable they use wireless connections to connect to a variety of networks [1], [2]. There are distinct types of MANETs which include InVANET- Intelligent vehicular ad hoc networks that make use of artificial intelligence to challenge unexpected situations like vehicle collision and accidents. MANETs that sanctions effective communication with another vehicle or assists to communicate with roadside types of equipment are known as VANETs- Vehicular ad hoc networks, and another type facilitates to link fixed as well as mobile nodes called as iMANET-Internet-Based Mobile Ad hoc Networks [3], [4].
Every node operates autonomously as both router and host in MANET. If two different nodes want to transfer a message without radio range then multi hop routing is performed by MANETs. Firewall is not centralized in routing and security phase. The interconnected devices or nodes can join or leave the network anytime . So topology becomes dynamic in nature. When compared with wired links, the wireless links has lesser reliability, efficiency, stability and capacity. Due to mobility and spontaneous behavior of MANET minimum human intervention to configure the network is needed [5], [6], [7]. All nodes have identical features with similar tasks and facilities. Hence it forms a completely symmetric environment.
Challenges in MANETs
MANET environment have a few issues that include:

1) Reduced data rates due to limited radio band. So bandwidth has to be utilized efficiently by having low overhead.
2) The mobility of nodes makes frequent network topology changes and partition of networks that typically affects the intermediate nodes. The topology alteration breaks the path frequently.
3) Collisions easily affect MANETs that creates higher packet loss.

All the above said challenges are only present in wireless mobile nodes. In order to make MANET communication as reliable one with collision detection, link failure detection, identifying vulnerable node or path, isolation of affected nodes or path etc can be achieved by a leader node in the network. As and when the topology has been changed dynamically leader has to be selected within the network and his work is to maintain and monitor the network up to the node gets discarded from the network or the path is faded away [8], [9].

2. Existing work

The whole mobile network should be declared and every mobile node has its individual ID and virtual target node ID earlier than the configuration of the group. Intial part indicates the cluster formation, while a communication process performs, also to choose the cluster leader node and cluster member nodes of the specific cluster. Although choosing the cluster member nodes, these member nodes should be separate from remaining nodes. Present the Enhancement of Bee-Ad Hoc designing the multipath between Cluster Head, with virtual target nodes. Considering the Cluster head node transmits a data packet to attackers to reach the target node, whether the attacker is not able to search the destination within the group with the support of spy node then the spy is launching exterior the group is used to discover the target node. Previously the target node initiates the data is allowed among the chosen route. This process is previously executed on the earlier network. Except for the important difficulties in this communication, when the target node is exterior the group as initial the Cluster head node investigate the target node within the group with the support of attackers and spy, however, whether the base station

Copyright © 2018 Ms.S.Deepa et. al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

node is not available within the cluster, then the spy node need to travel arbitrarily outer the processing network [10].
A few of the spy nodes will unreasonably lose the energy for finding the target node in the network. This communication initiates, all the spy nodes need to start discovering the destination at the similar time period, so it obtains a maximum traffic, which should guide to the discharge of nodes in the network. The overload should be more it a guide to some packet latency in communication. Since for all the motivate the network does not be energy capable. Consequently to arrive over these issues, a recent inter-cluster packet sharing method is executed, which take the support of Edge Cluster Node, which constructs the mobile ad hoc network more efficient, and energy resourceful by the captivating concern of energy used for communication.
In this scheme have more significance has been specified in packet transmission from one cluster to another cluster, which the Cluster Head obtains the support of spy node is called as an edge Cluster Node, that is available at the border area of two clusters, it operates as packet sharing mediator through the clusters. While a communication is performed in the network Bee-AdHoc-C adopt an instance depending dynamic clustering scheme also apply a new scheme is called as group Header into a bee swarm for every Ad Hoc Network structure. The main dependability of group Header is used to claim that the node needs to be a cluster header node in a communication environment. Subsequent to the creation of the cluster also choosing the cluster head node, remaining cluster member nodes of the cluster and edge node are used the main process in cluster head, it is used to discover the destination node by the use of attacker, spy node, and an edge node of the cluster. On one occasion the Cluster head accepts single reply packets from any attacker, spy node have the important process of the Cluster head node is used to transmit the data packet to the base station node between the minimum distance route [11].
A recent algorithm is launched for performing communication in a Clustered Bee Ad-Hoc network is known as Improved Bee Ad Hoc-C. At this spot, the packet transmission rate is increased among the cluster to cluster by the use of edge Cluster Node. The Experimental result should be approved and the outputs are establishing to be efficient with respect to a normal Clustered Bee Ad Hoc Network environment. The output of Clustered Bee Ad Hoc Network is compared with considering various metrics are Energy Efficiency, End Packet latency, Transmission rate, Path discovery time, Packet Success Rate, Communication Overhead. All these metrics are calculated with respect to various packet sizes. Additionally, the communication is performed to discover the reply with respect to some various metrics. Additionally, this scheme performance is increased and provides the energy efficient with a maximum transmission rate by using the recent technique, it is used for on-demand path assigning among the source node, and a destination node in a Bee Ad Hoc mobile ad hoc network [12], [13].

3. Proposed work

The basic goal of the proposed work is to improve the quality of service in MANET for congestion control, monitoring and isolating the path or the node which is vulnerable to attack or already affected by the attacks. To achieve the goal the leader election algorithm has been implemented from congestion traffic network.
Proposed method contains two different election algorithms such as bully algorithm and ring algorithm have been adopted by which leader is selected and leaders work is to maintain the MANET. The quality of service parameters such as congestion control, finding the vulnerable node or path and isolation of such nodes have been used in communication process.
Bully Algorithm
Election algorithms are the technique used to select distinctive coordinator based on the idea that every node in the manet has a unique ID and every node is aware of all different nodes ID too. The goal of the bully algorithm is to seek out the non-crashed method with the best ID. A node initiates an election as and when it simply recovered from failure or it notices that the organizer has failed. Three kinds of messages are used such as Election, OK, and coordinator. Many nodes will initiate an election at the same time.

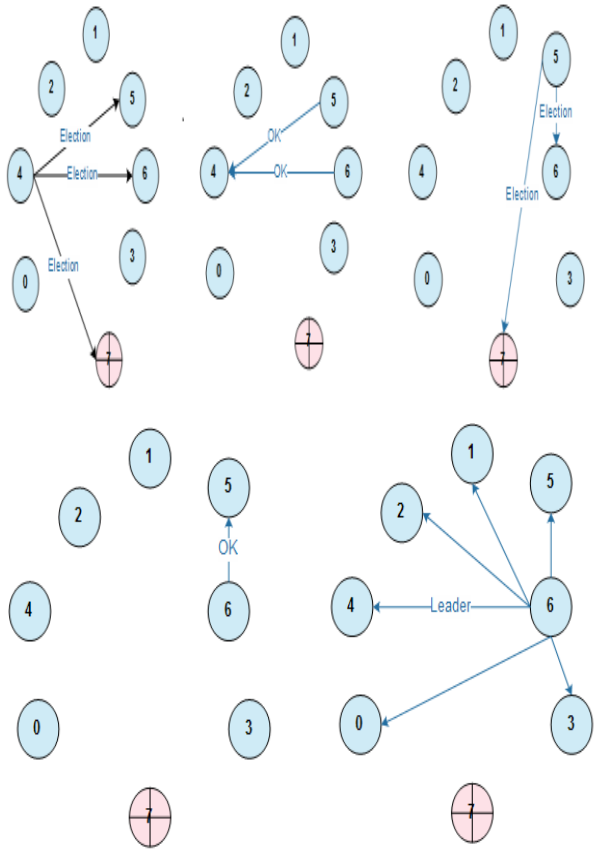

Fig. 2: Diagram of Bully Election Nodes.

Any node P can begin an election

- P transmit Election messages to all nodes which are currently interconnected in the network with higher IDs and awaits for OK messages
- If no OK messages are received, P becomes coordinator and transmit Coordinator messages to all nodes with lower IDs
- If it receives an OK, it decline out and waits for a Coordinator Message
- If a node receives an Election message immediately sends Coordinator message if it is the node with Highest ID
- If not, returns an OK and starts an election if a node receives a Coordinator message, it treats Sender as the leader.

To find the vulnerable node
Step 1: After the leader node has been elected in the MANET when the network or the topology is created the leader nodes operates to find the vulnerable node or route during communication.
Step 2: Affected node can be identified with broken link separation, the node with higher traffic, that particular node which transfers packets to the single location for a long period of time

Fig. 3: Vulnerability Detection.

Step 3: The leader nodes are used to find the vulnerable node or path with all the above-mentioned constraints also separating that node from all other mobile nodes, and significant for all the mobile nodes in the network about the vulnerability. Then all other nodes cannot send their packets through the vulnerable node.

Congestion control by leader

The primary role of the elected leader is to find the congestion in the network that is high traffic and letting know to the other nodes so that other nodes won't transmit packets via such congested node.

The leader node periodically sends a sense packet to each node in the round-robin fashion and waits for an acknowledgment. If the leader does not receive any acknowledgment within the timeout period, then the leader can identify that the node is in congestion. Then the leader will notify other nodes about congestion and reduces congestion in the congested node since no packet is sent via congested node for a long time period.

4. Implementation and result analysis

The execution of the proposed model is simulated using ns2 simulation, In this a node starts at a random position, and waits for the pause time, It moves to a different random position with a speed chosen between 0 m/s and therefore the maximum simulation speed. The TUI value is about to five seconds that has been found optimum in previous experiments for networks wherever the nodes have a maximum speed of up to twenty m /s with a transmission range of 250 meters. The performance metrics are obtained through ensemble averaging by simulation, the network with a special mobility and connection pattern. The performance of the proposed scheme is evaluated based on the metrics like throughput, Packet Loss By malicious node. To enhance the quality of service the identified vulnerable tunnel will provide information on concerning wormhole to remaining nodes in the network.

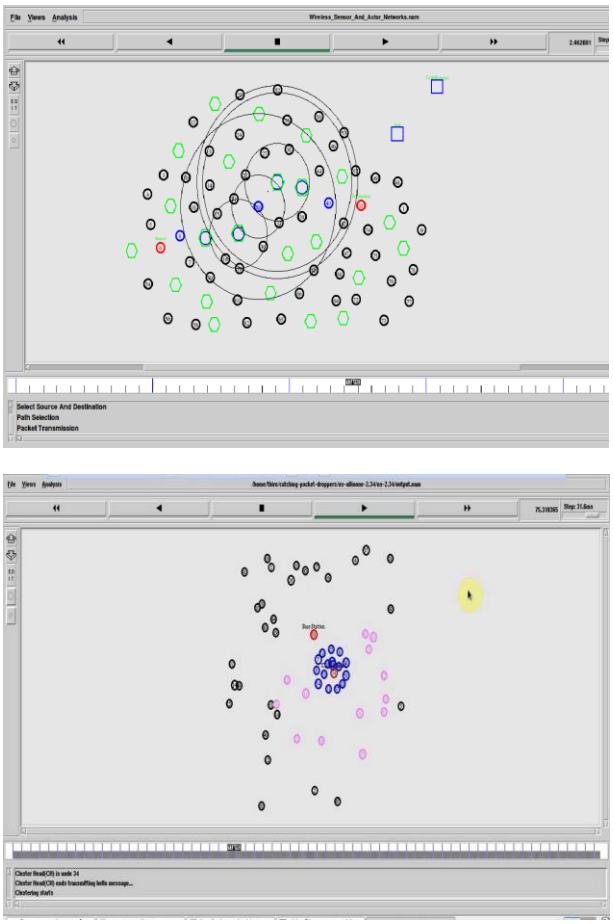

Fig. 4: Proposed Lsa.

Path Stability: Figure 5 shows path stability is estimated by considering the stabilty of the routing path, during packet transmission time with the amount of packet sent by all node details are stored in the routing table. In proposed LSA method is used for path stability is improved compared to existing method Energy Efficient routing EET [14, 15].

$$Path\ Stability = radio\ range * number\ of\ packet\ sent$$

Table 1: Speed (M/S) Vs. Path Stability (%)

Speed (m/s)	Path Stability (%)	
	Existing EET	Proposed LSA
20	44	78
40	45	79
60	46	80
80	48	81
100	49	82

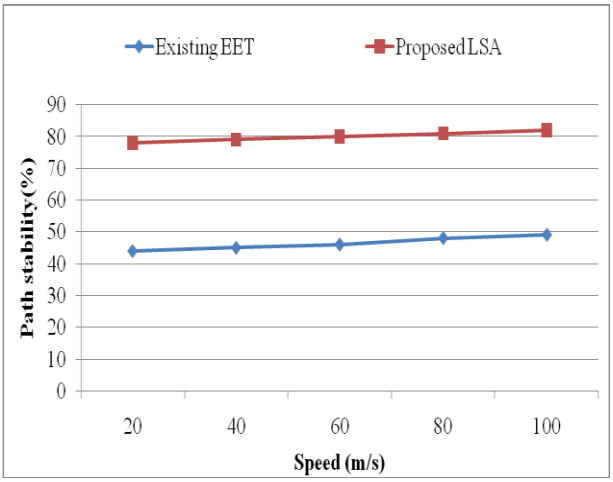

Fig. 5: Graph for Speed (M/S) Vs. Path Stability (%).

Analysis the result from the table. For instance, From the Table 1, it was observed that , increase in the speed of the network, the path stability of the network increases. Further, for tuning of 100 m/s , the proposed network able to achieve better path stability with 82%.

End to End Delay: Figure 6 shows end to end delay is calculated by the time taken to transmit packet from start point to end point, track the location information also analyze timer. In proposed LSA, end to end delay is minimized compared to existing method Energy Efficient routing EET [16].

$$Delay = End\ Time - Start\ Time$$

Table 2: Nodes vs. End-To-End Delay (Sec)

Nodes	End to end Delay (sec)	
	Existing EET	Proposed LSA
20	9.40	6.13
40	10.48	7.23
60	11.62	8.31
80	12.84	9.52
100	13.23	10.58

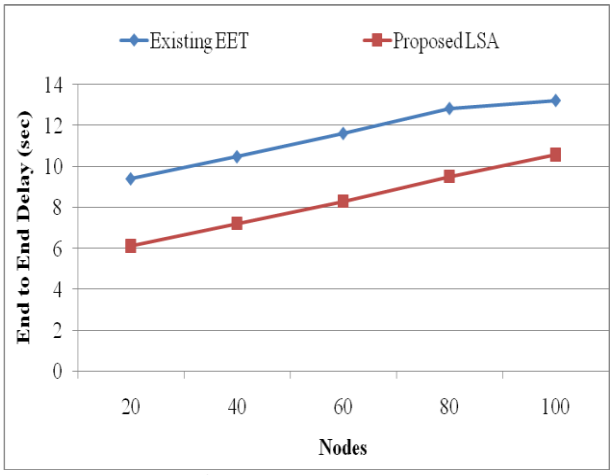

Fig. 6: Graph for Nodes vs. End-to-End Delay (Sec).

Analysis the result from the table. For instance, From the Table 2, it was observed that, increase in the number of node, the end to end delay is increased. In nodes 100, the proposed network capable to obtain minimum delay with 10.58(sec).

Packet Delivery Ratio: Figure 7 shows Packet delivery ratio is measured by the packet received from packets sent at a specific rate. The speed of the node is constant in the sensor network; the simulation rate is fixed at 100. In proposing LSA scheme Packet delivery ratio is higher should compared with existing method Energy Efficient routing EET [17-18].

$$PacketDeliveryRatio = (Numberofpacketreceived/Sent) * speed$$

Table.3: Nodes vs. Packet Delivery Ratio (%)

Nodes	Packet Delivery Ratio (%)	
	Existing EET	Proposed LSA
20	35	77
40	36	78
60	37	79
80	38	80
100	40	81

Analysis the result from the table. For instance, From the Table 3, it was observed that, increase in the number of nodes, the packet delivery ratio of the network is improved. In nodes 100 , the proposed network able to achieve efficient packet delivery ratio 81%.

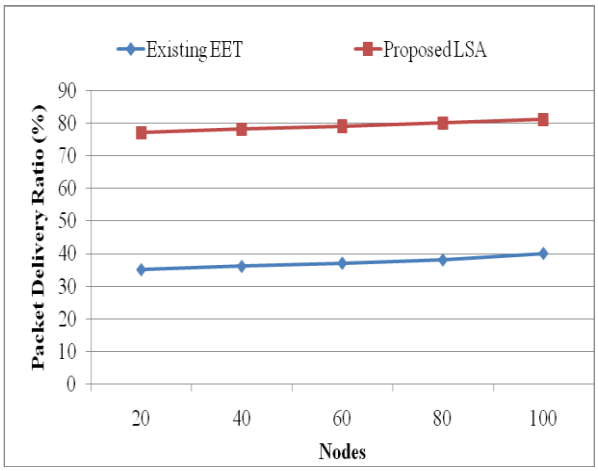

Fig. 7: Graph for Nodes vs. Packet Delivery Ratio.

Network Lifetime: Figure 8 shows that the lifetime of the network is calculated by using the entire network communication process, a resource utilized to make best packet transmission. In proposing LSA scheme Network Lifetime is improved should compared with existing method Energy Efficient routing EET [19-20].

$$NetworkLifetime = lengthofenergyusage/overallenergy$$

Table 4: Nodes vs. Network Lifetime (%).

Nodes	Network Lifetime (%)	
	Existing EET	Proposed LSA
20	28	82
40	29	83
60	30	84
80	31	85
100	32	86

Analysis the result from the table. The Table 4, it was observed that, increase in the number of node, the network lifetime is increased. In nodes 100, the proposed network is used to achieve maximum network lifetime 86%. [21].

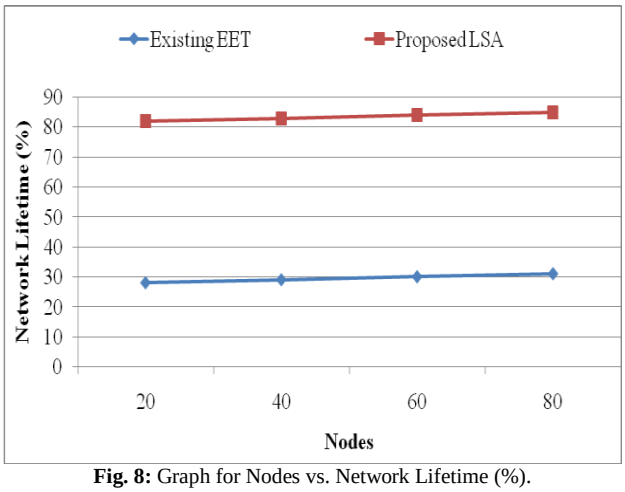

Fig. 8: Graph for Nodes vs. Network Lifetime (%).

Energy Consumption: [22] Figure 9 shows energy consumption; it evaluates total energy used for starting node to ending node for the communication process. In proposing LSA scheme, virtue-based authentic nodes are used for packet transmission, so energy consumption is minimized compared to existing method Energy Efficient routing EET. [23].

$$EnergyConsumption = InitialEnergy - FinalEnergy$$

Table. Five: Speed (M/S) Vs. Energy Consumption (Joules)

Speed (m/s)	Energy Consumption (J)	
	Existing EET	Proposed LSA
10	168	129
20	174	136
30	181	141
40	189	148
50	196	157

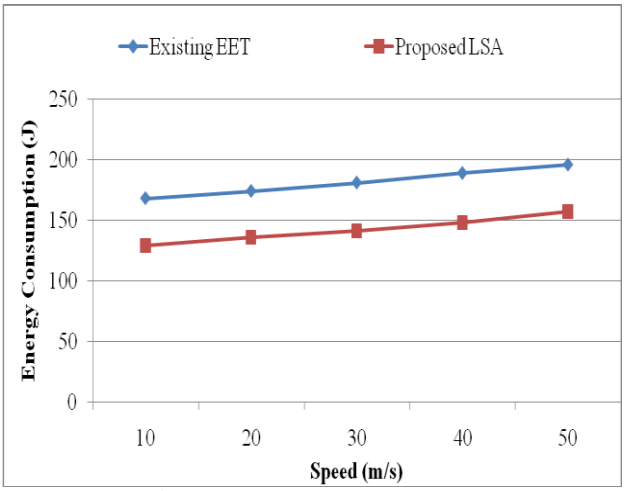

Fig. 9: Graph for Speed (M/S) vs. Energy Consumption (Joules).

Analysis the result from the table. The Table 5, it was observed that , increase in the speed of network nodes, the energy consumption is increased. In nodes 100, the proposed network is used to offer lesser energy consumption with 157J.

Packet drop rate: Figure 10 shows that Packet loss of all transmissions on the network is planned by nodes loss the packet because of data packet overload, so go for the leader selection algorithm, it offers the traffic free packet sharing. In proposing LSA scheme Packet loss rate is reduced when compared with existing method Energy Efficient routing EET.

$$Packet\ drop\ rate = \left(Numberofpacket\frac{lossed}{Sent}\right) * 100$$

Table.6: Nodes vs. Packet Drop Rate (%).

Nodes	Packet drop rate (%)	
	Existing EET	Proposed LSA
20	65	28
40	66	29
60	67	30
80	68	32
100	69	33

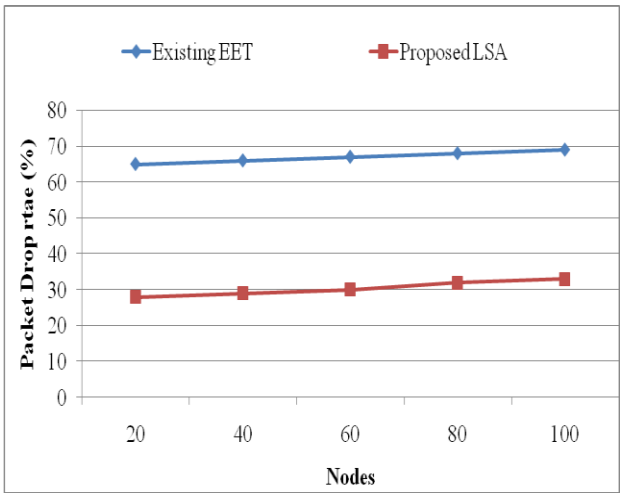

Fig. 10: Graph for Nodes vs. Packet Drop Rate (%).

Analysis the result from the table. The Table 6, it was observed that, increase in the number of node, the packet drop rate is increased. In nodes 100 , the proposed LSA network is used to provide lesser packet drop rate 33%.

5. Conclusion

The purpose of the proposal is to maintain quality of service in MANET with the parameters of congestion control and vulnerability identification with the help of leader or coordinator. First step of the proposal is to elect the leader as and when the topology is created in the MANET, since it has the dynamically modifying topology. Then leader node operate as to find the intruder node or routing path and finding the congestion and eliminating them from the network to sustain quality of service. In this proposal two quality of service parameters have been used such as congestion control and vulnerability detection, it improves the network lifetime 86%, path stability 82%, also it reduce end to end delay at 10.58 (sec) but in future it can be verified with different QoS parameters.

References

[1] Brahma, M., Kim, K.W., Abouaissa, A. and Lorenz, P., 2005. A load-balancing and push-out scheme for supporting qos in manets. Telecommunication Systems, 30(1), pp.161-175. https://doi.org/10.1007/s11235-005-4323-2.

[2] Bricard-Vieu, V. and Nasser, N., 2006, November. WSN16-1: A Weighted Clustering Algorithm Using Local Cluster-heads Election for QoS in MANETs. In Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE (pp. 1-5). IEEE. https://doi.org/10.1109/GLOCOM.2006.982.

[3] Dagdeviren, O. and Erciyes, K., 2008. A hierarchical leader election protocol for mobile ad hoc networks. Computational Science–ICCS 2008, pp.509-518. https://doi.org/10.1007/978-3-540-69384-0_56.

[4] Ding, S., 2008. A survey on integrating MANETs with the Internet: Challenges and designs. Computer Communications, 31(14), pp.3537-3551. https://doi.org/10.1016/j.comcom.2008.04.014.

[5] Hoang, V.D., Shao, Z. and Fujise, M., 2006, June. Efficient load balancing in MANETs to improve network performance. In ITS Telecommunications Proceedings, 2006 6th International Conference on (pp. 753-756). IEEE. https://doi.org/10.1109/ITST.2006.289010.

[6] Jhaveri, R.H., Patel, S.J. and Jinwala, D.C., 2012, January. DoS attacks in mobile ad hoc networks: A survey. In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on (pp. 535-541). IEEE. https://doi.org/10.1109/ACCT.2012.48.

[7] Lochert, C., Scheuermann, B. and Mauve, M., 2007. A survey on congestion control for mobile ad hoc networks. Wireless communications and mobile computing, 7(5), pp.655-676. https://doi.org/10.1002/wcm.524.

[8] Mamatha, G.S. and Sharma, D.S., 2010. Network Layer Attacks and Defense Mechanisms in MANETS-A Survey. International Journal of Computer Applications, 9(9).

[9] Mehta, S., Sharma, P. and Kotecha, K., 2011, December. A survey on various cluster head election algorithms for MANET. In Engineering (NUiCONE), 2011 Nirma University International Conference on (pp. 1-6). IEEE.

[10] Mohapatra, P., Li, J. and Gui, C., 2003. QoS in mobile ad hoc networks. IEEE Wireless Communications, 10(3), pp.44-53. https://doi.org/10.1109/MWC.2003.1209595.

[11] Baskar, S., Pavithra, S., &Vanitha, T. (2015, February). Optimized placement and routing algorithm for ISCAS-85 circuit. In Electronics and Communication Systems (ICECS), 2015 2nd International Conference on (pp. 958-964). IEEE.

[12] Baskar, S., &Dhulipala, V. S. RELIABILITY ORIENTED PLACEMENT AND ROUTING ANALYSIS IN DESIGNING LOW POWER MULTIPLIERS.

[13] Chandra, M. E. H., & Scholar, P. G. (2014).ENHANCED DECODING ALGORITHM FOR ERROR DETECTION AND CORRECTION IN SRAM.

[14] Maheswari, M. U., Baskar, S., &Keerthi, G. M. High Speed Finite Field Multiplier GF (2 M) for Cryptographic Applications.

[15] Raghupathi, S., &Baskar, S. (2012).Design and Implementation of an Efficient and Modernised Technique of a Car Automation using

Spartan-3 FPGA. Artificial Intelligent Systems and Machine Learning, 4(10).
[16] Souihli, O., Frikha, M. and Hamouda, M.B., 2009. Load-balancing in MANET shortest-path routing protocols. Ad Hoc Networks, 7(2), pp.431-442. https://doi.org/10.1016/j.adhoc.2008.04.007.
[17] Sudhan, S.K.H.H. and Kumar, S.S., 2016. Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9(44).
[18] Tang, K., Obraczka, K., Lee, S.J. and Geria, M., 2002, October. A reliable, congestion-controlled multicast transport protocol in multimedia multi-hop networks. In Wireless Personal Multimedia Communications, 2002. The 5th International Symposium on (Vol. 1, pp. 252-256). IEEE.
[19] Wu, K. and Harms, J., 2001. QoS support in mobile ad hoc networks. Crossing Boundaries-the GSA Journal of University of Alberta, 1(1), pp.92-106.
[20] Mohapatra, S., & Siddappa, M. (2016, October). Improvised routing using Border Cluster Node for Bee-AdHoc-C: An energy-efficient and systematic routing protocol for MANETs. In Advances in Computer Applications (ICACA), IEEE International Conference on (pp. 175-180). IEEE.
[21] Cai, X., Duan, Y., He, Y., Yang, J., & Li, C. (2015). Bee-sensor-C: an energy-efficient and scalable multipath routing protocol for wireless sensor networks. International Journal of Distributed Sensor Networks, 11(3), 976127. https://doi.org/10.1155/2015/976127.
[22] Tikhe, K., & Sohni, N. (2016, September). PF-RBF based energy efficient target tracking routing algorithm for WSN. In Automatic Control and Dynamic Optimization Techniques (ICACDOT), International C onference on (pp. 532-537). IEEE.