International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 32 • 2017

Position Based Opportunistic Routing Protocol for Node Auto Configuration in MANETS

Vijayalakshmi Ambati[a] and Gandharba Swain[b]

[a-b]Department of Computer Science and Engineering, K.L. University,Vaddeswaram-522502, Guntur, Andhra Pradesh, India. Email: [a]vijayalakshmi.ambati2@gmail.com; [b]gswain1234@gmail.com

Abstract: Dynamic data transmission is an essential concept in present days to increase the operations in mobile ad hoc network configurations. Independent addressing protocol requires allocated and self-directed procedure to avoid address collisions in a dynamic network with recurrent partitions, and entering/exiting nodes. Filter based addressing protocol (FAP) for node auto-configuration configures nodes in real time using a allocated address database stored in filters that decreases the control load and makes the packet losses less and robust to network partitions. We proposed a multi-level approach called Position based Opportunistic Routing (POR) protocol which knows the network level objectives of the users and administrators and assemble the user requirements at run time. This approach gives more flexibility to clients. The quality of service is definitely improved. Our experimental result shows the dynamic node auto configuration in reliable data transmission.

Keywords: MANET, position based opportunistic routing, node auto configuration, AODV, clustering.

1. INTRODUCTION

Generally in IP networks, network administrator or Dynamic Host Configuration Protocol (DHCP) server can assign addresses to the hosts. In MANETs the network administrator or DHCP server does not configure the IP addresses. But MANET is a self configurable network i.e. the number of mobile hosts unite to form an arbitrary topology. So by using DAP (Distributed Address Pool) dynamically we can assign addresses to the host nodes i.e. newly joined nodes[1]. Depending on distributed administration and nodes similar functioning, the nodes that doesn't belong to the network wants to join the network by requesting the server in the MANETs using distributed dynamic host configuration protocol which ensures that no two nodes gets the similar IP address. At the time of configuration, the nodes will be assigned an unique IP address to avoid the IP mismatch [2],[3].

In MAN et. all the IP addresses will be stored in FAP. FAP utilizes filters to see that the IP addresses are store in a specified format, one among them is bloom filter. This bloom filter will store all the IP addresses in hash representation[4].Actually when MAN et. allocates the IP addresses to the host nodes dynamically there may be a chance in duplication of addresses. Through duplicate address detection (DAD) we detect the duplicate

addresses in MANET[5]. Host node address values are stored in bloom filters with hash representation in a sequential order. In FAP node identifier will check whether node has address or not. If any host node doesn't have IP address it will assign new address[6]. The sequence filters unique addressing scheme assigns the addresses to the nodes but also decrease the amount of overhead and increase packet delivery ratio. Hashing is used to detect the partitions and merging's[7].Routing protocols in MANETs are of two types, (i) proactive and (ii) on-demand. Proactive routing protocols are used for periodic neighbor discovery and for topology updates, which gives the route information to every node before transmitting the packets of data to the destination. Root request and route reply is used in On-demand protocol to find and maintain a route[8]. Due to the broadcasting AREQ messages, network merging will happen. Depending on the address signature of the host node, network merging & the node check, whether it is the new network or home network collisions. The host node removes colliding address from filter and then broadcast the message[9].

Quality of service (QOS) is used to achieve the efficient node auto configuration in network communication, we need to extend filter based addressing routing sequence protocol with energy oriented features. So in this paper we proposed Position Opportunistic Routing (POR) protocol to increase the energy of nodes and forwarding packet information to neighbor nodes using message authentication codes (MAC) interpretation in data transmission with different topology as shown in Figure 1.

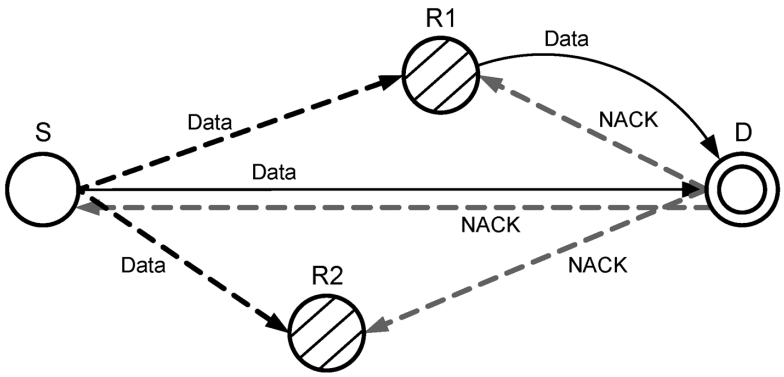

Figure 1: Co-operative data communication based on position with different locations

As shown in Figure 1, when the source initiated the transmission and forwarded the packet to the neighboring node, there may be chance of packet loss due to the unavailability of the nodes. This is taken care by using the POR protocol which routes the packet in the alternate route and see that the packet reaches the destination.

Remaining paper explanation is as follows. Section 2 describes the background approach for node auto configuration in ad hoc networks. Section 3 presents POR implementation for dynamic data transmission with quality of service in ad hoc networks. Section 4 gives experimental comparison results of both FAP and POR with data transmission. Section 5 summarizes the paper.

2. RELATED WORK

This section, discusses about FAP for dynamic data transmission with node auto configuration based on network address with load maintenance to merge different topologies in network communication. Filter based protocol performs frequent node selection by combining nodes which reduces the overload and solve the collision problem in ad hoc networks dynamic data transmission [10].Identifier sequence is a mechanism which is a part of FAP that helps in identifying the combination of nodes which causes conflicts in the network communication. FAP consists of sequence filters for node information storage and maintain different parameter representations. These sequence filters are extension versions of bloom filter for dynamic node address storage.

Step 1: Bloom Filter is a data structure for node information storage and maintains the unique sequence of addresses storage. IP address, port number sequences and protocol storage based on address range of array lists that are indexed with suffix and on bit information will be taken care by bloom filter mechanism. Procedure of the sequence filter shown in Figure 2.

Figure 2 represents array sequence with suffix numbers 0, 0, 1, 0, 0, 1, 1 with IP address 192.168.0.1 gateway allocation in different data communications. Sequence filter do not give false report to generate network simulation process based on node selection. So randomly data node value is generated in sequence filter with IP addresses. We select bloom filter to generate auto configurations in node simulation based on available address with respect to suffix with random node bit generation.

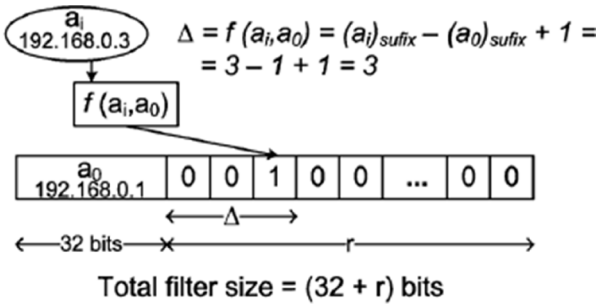

Figure 2: Bloom filter based on 256 address node storage

Step 2: Procedure of FAP: First, initialize the process that deals with node auto configuration with selection of nodes in network simulation. If more number of nodes combines together then host node gives beacon message to the server with in time intervals. Joining node uses HELLO and AREQ (address message request) with request sequence numbers as shown in Figure 3.

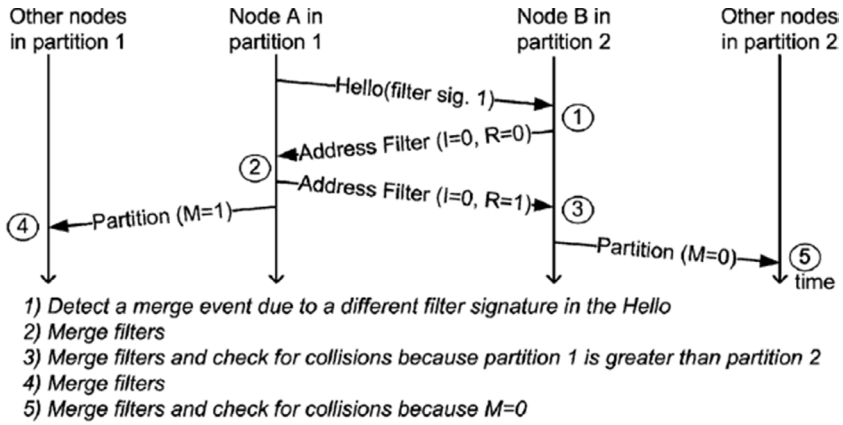

Figure 3: Partitioning based node detection to utilize formal data presentations

Figure 3 shows combination of different nodes. Before combining the nodes server detects the distance between every node. Collision occurs due to the node combines so after this process server selects the partition node in filter sequence. After initialization, each node starts hello packet which contain filter sequence numbers based on signatures in broadcast message data representation. FAP requires synchronous sequence filter with node integration to avoid false positives in network communication to detect merge nodes in network location. After completion of merging the node releases data to other nodes in sequence process. FAP fails similar auto node configuration in network data progression to increase quality of service maintenance.

3. PROPOSED WORK

We extend the robustness of FAP communication in distributed large node representation to avoid merging strategy and decreasing of time. This approach is as follows.

Step 1: Triggering is a mechanism where the initializing node triggers the data to the neighboring node which helps in boosting the packets. Data packet forwarding from source node to intermediate node to implement multi path routing in sequential protocol implications. Based on some graphical data presentations shown in Figure 4.

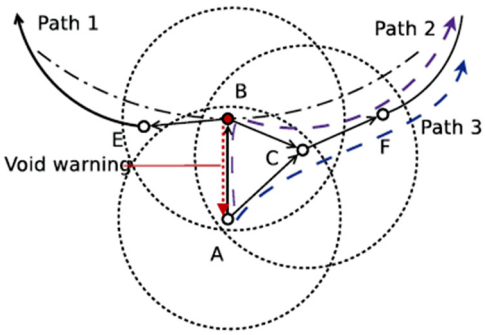

Figure 4: Potential paths around network partitions

As shown in Figure 4, A-B-E path is available for data forwarding to other nodes in routing communication. Path 2 is better than path 3 with message communication. After storage of path and node information in network it will be easy to send data from one node to another node. It is better storage data representation.

Step 2: Virtual Destination: During joining node communication, selective node provides multicast communication, whenever route exploited with different paths. Through the opportunistic routing protocol with virtual destination we can select more number of paths in data communication. When we construct the virtual destination node from all source nodes we can avoid handling procedures by using trigger data.

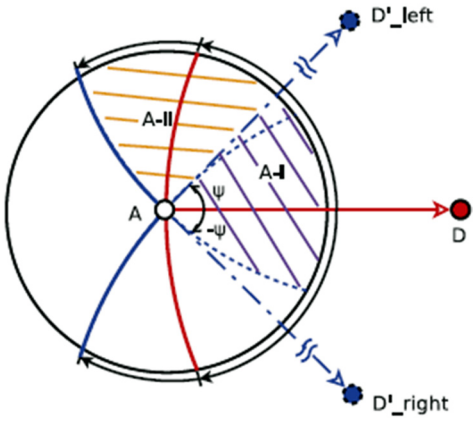

Figure 5: Potential node forwarding to handle virtual selection

Step 3: Greedy Forwarding: To handle miscommunication in data forwarding via intermediate node we are using virtual destination and path selection identifier. Through virtual destination we can send the data correctly shown in Figure 5. Greedy heuristics analysis performs hop-by-hop data forwarding packets in network communication. Source send information to next node in selection procedure, then it automatically detect whether the node present or not.

Step 4: Path Acknowledgement: If trigger node detect forwarding node in various circumstances. It finds all the routes finally select one suitable route for communication, in order to decrease redundancy to control messages.

Finally we select automatic route for data transmission to increase packet delivery ratio with different throughput calculations in ad hoc networks. The destination node takes data from trigger node with sequence numbers stored in hop representation.

4. RESULTS AND DISCUSSION

In this section, we observe performance of the POR in mobile Adhoc network communication. To implement this architecture in ad hoc networks, we use NS-3 simulator for network construction with different node configurations compared with FAP in data transmission. Common simulation parameters for implementing network communication are shown in Table 1.

Table 1
Simulation parameters

Parameter	*Simulator Value*
Protocol	IEEE 802.16
Propagation sequence	Two or more ground sequence
Transmission distance	350 m
Mobility sequence	Randomly generate bit rates
Nodes for simulation	200
Time	200s

This proposed work is compared with the existing work by 3 metrics, (i) packet delivery ratio (ii) delay presentation and (iii) execution time. Packet delivery ratio means multiple of packets will be received by destination with different parameters in node simulation based on source node selection. Delay presentation means when sender node sends the data to the receiver node sometimes the data will take time to reach destination due to the link breaks and collisions, this will be consider as delay. Execution time is calculated based on multiple packets transferred from sender node to receiver node.

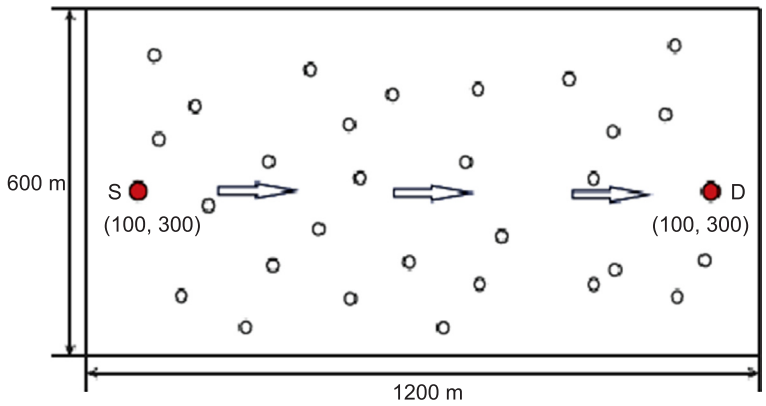

Figure 6: Network topology simulation based on different parameters

As shown in the above Figure 6, nodes were constructed with static structure with respect to node forwarding in data delivery formations from source node to destination (shows in red color sequences). Based on nodes configuration, packet delivery in network progression contains effective packet delivery with respect to FAP.

The comparison between FAP and POR is shown in Figure 7. POR has high packet delivery ratio compared to FAP. FAP has low packet delivery ratio.POR has been shown in red color.

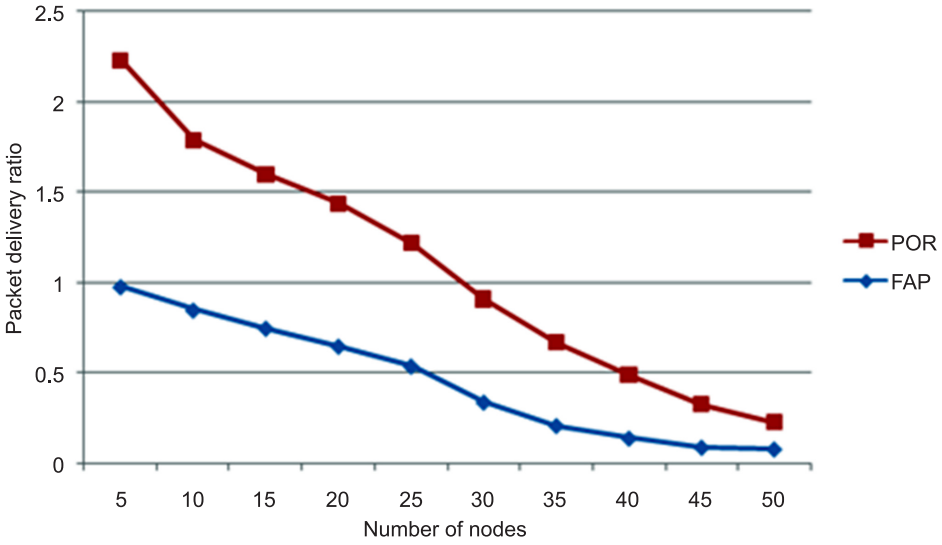

Figure 7: Packet delivery ratio process with respect to dynamic data transmission

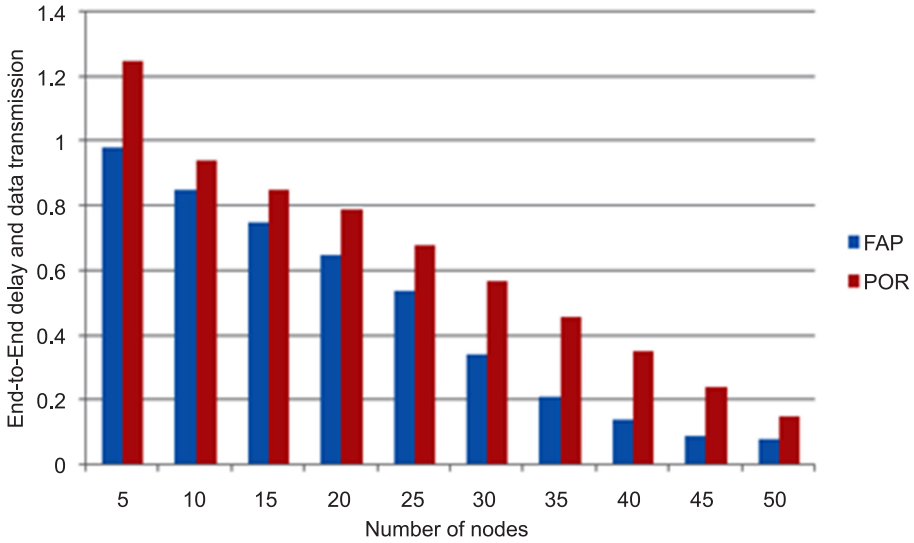

Figure 8: End-to-end communication in network simulation

As shown in Figure 8, POR delivers the data without any loss of packets to destination. As compared to FAP it is more effective to deliver the data end-to-end data transmission.

By observing Figure 9, POR gives better Packet delivery ratio and low execution time in data transmission. Our application efficiently handles node auto configuration in dynamic data transmission.

5. CONCLUSION

In this paper, we detect the problem of effective and authentic data delivery in dynamic mobile ad hoc networks because of continuously changing network topology. So, we proposed Position based Opportunistic Routing (POR) protocol to maintain node auto configuration in dynamic data transmission. POR performs stateless communication in dynamic data transmission of geographic routing with broadcast nature of implementation in wireless network communication. In node selection, we define selective node configuration due to link failure problem in network communication. If any link breaks during data transmission then the proposed POR protocol helps in recovering

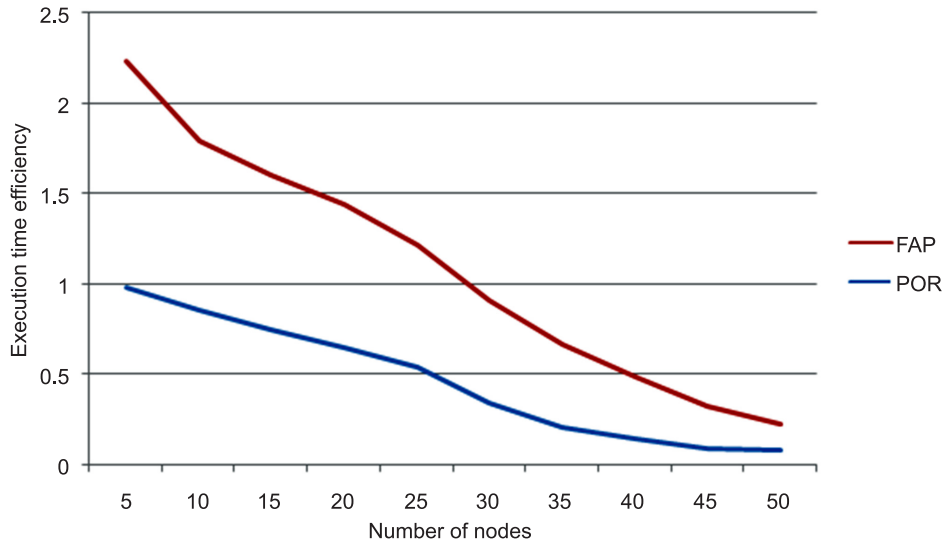

Figure 9: Execution time efficiency with respect to data transmission

the route in no time. Due to the position based opportunistic protocol (POR) routing hierarchy in next hop selection for data transmission will be increased. Through our simulation results, we achieve effectiveness, scalability and productivity of the POR protocol with high packet delivery ratio and throughput.

REFERENCES

[1] H. Kim, S. C. Kim, M. Yu, J. K. Song, P. Mah, DAP: Dynamic address assignment protocol in mobile ad-hoc networks, In Proceedings of IEEE International Symposium on Consumer Electronics, doi: 10.1109/ISCE.2007.4382219,2007.

[2] N. C. Fernandes, M.D.D. Moreira, O. C. M. B. Duarte, Aself-organized mechanism for thwarting malicious access in ad hoc networks, In Proceedings of INFOCOM, doi: 10.1109/INFCOM.2010.5462232, 2010.

[3] S. Nesargi, R. Prakash, MANET conf: configuration of hosts in a mobile ad hoc network, In Proceedings of INFOCOM, doi: 10.1109/INFCOM.2002.1019354,2002.

[4] D.P. Rao, T.S Raghavendra, MANAP: an effective and self-configuring protocol for dynamic node addressing in MANETs, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, No. 5, pp. 4419-4424, 2014.

[5] N.H. Vaidya, Weak duplicate address detection in mobile ad hoc networks, In Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing,pp.206-216, 2002.

[6] N.C. Fernandes, M.D.D. Moreira, O.C. M.B. Duarte, An efficient filter-based addressing protocol for autoconfiguration of mobile ad hoc networks, In Proceedings of IEEE INFOCOM,doi: 10.1109/INFCOM.2009.5062174, 2009.

[7] R. S. Madhavi, K. Sekar, Unique address assignment and dynamic configuration of node traffic of MANETs, International Journal of Innovative Research in Computer and Communication Engineering,vol.2, No. 4,pp.202-208,2014.

[8] S.C. Kim, J.M. Chung, Message complexity analysis of mobile ad hoc network address autoconfiguration protocols, IEEE Transactions on Mobile Computing, Vol. 7, No. 3, pp. 358-371, 2008.

[9] D. Suganthi, S. Ravimaran, Collision free address assignment for nodes in ad hoc networks using FAP, International Journal of Advanced Research in Computer Science and Electronics Engineering,vol.3, No. 6, pp. 327-332, 2014.

[10] N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, An efficient and robust addressing protocol for node auto configuration in ad hoc networks, IEEE/ACM Transactions on Networking, Vol. 21, No. 3, pp. 845-856, 2013.