*THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE*

# A Review on FAP in Mobile Adhoc Networks

**M. Harini**
Department of Computer Science and Engineering, GPCET, Kurnool, India
**M. Sri Lakshmi**
Assistant Professor, Department of Computer Science and Engineering, GPCET, Kurnool, India
**Dr. S. Prem kumar**
Ph.D, M. Tech, Professor and Head of the Department, Department of CS & ITGPCET, Kurnool, India

***Abstract:***
*Mobile adhoc networks do not have fixed infrastructure. Nodes keep on joining and leaving the network dynamically. Assigning addresses for mobile nodes is a challenging task. The difficulty is even raised due to channel fading, partitions in network and dynamic joining and leaving of the nodes. Address collisions are quite a common problem in mobile adhoc networks. Autonomous addressing protocols are used here which indeed need a distributed self-organized mechanism. The model under discussion uses filters to maintain a distributed database of addresses to configure mobile nodes in adhoc networks. It also aims at reducing control load and is resistant to packet losses and network partitions.*

***Keywords:*** *Mobile adhoc networks, filters, network partitioning*

**1. Introduction**

Mobile adhoc networks connect mobile devices in an infrastructure less fashion without wires and configure themselves continuously. Mobile nodes are free to move on in the network as per their wish and have frequently changing links. But every node acts as a router for the information which it is not concerned with. Building a MANET means providing each node with the necessary information for routing the traffic. These networks may operate by themselves or may get connected to larger internet. This makes it a dynamic, autonomous topology. Now-a-days, many distributed applications prefer mobile adhoc networks as there is no centralized administration. Mobile adhoc networks are based on dynamic multihop topologies for communication and do not have any previous infrastructure. In addition, network partitioning is a significant problem which unfortunately is not properly taken care of. Mobility of nodes, channel fading and many other issues disturb the control over the distributed network. Initialization of network is also not an easy task due to the lack of servers. Achieving multihop routing and full connectivity makes a unique addressing network essential. Self-management makes it even more complex. Further, DHCP and NAT do not serve the distributed nature, partitioning and merging of the network. As a solution, we present the FAP model which uses filters to address the above mentioned issues. Distributed database containing the currently allocated addresses is maintained in filters in a compact fashion. To design a filter-based protocol, we use two filters called a Bloom filter and a Sequence filter. This scheme ensures not only the univocal address configuration of the nodes joining the mobile network and address collision detection after partition merging. This is a simple way because every node has the knowledge of the already assigned addresses. Also, to easily detect network partitions, a hash of the filter is provided as the partition identifier. High storage overhead is avoided by using filters which are distributed. Neighbours with different filters are easily detected with less control overhead which may cause address collisions. The addressing method is vigorous because all the nodes share the common allocated address list. The scheme reduces the message overhead and the number of trials made before an address is allocated.

**2. History**

Various addressing schemes are used but with many drawbacks. The birthday paradox error depicts that the random numbers create high probability of address collisions. Another scheme is hardware-based and assigns $IPv_6$ network addresses for the nodes depending on the MAC address of the device. This necessitates hashing MAC address if the number of bits in the address suffix is too small. This is also vulnerable to high address collisions. Other proposals that do not store the previously allocated addresses use Duplicate Address Detection (DAD) which is a distributed protocol. This scheme allows a new node to choose a random address and flood the network with Address Request (AREQ) Message for many times so that all the other nodes know the new address and if any node has the same allocated address, then it replies with an Address Reply (AREP) message to inform about the duplication. But this does not take any notice of network partitions. An extension would be the usage of Hello messages and partition identifiers, which are random numbers that are changed whenever a network partitioning is identified or a partition merge occurs. Some schemes use routing information to solve addressing problem where every node is identified by its address

and a key. But collisions are likely to occur when the nodes choose same address and key. Weak DAD protocol, Dynamic Address assignment Protocol (DAP) and other protocols are also not suitable for the mobile nature of adhoc networks.

**3. Related Work**

Centralized addressing schemes are not suitable for mobile adhoc networks because there are no servers. Further, simple distributed schemes are vulnerable to duplicated addresses which may result in high probability of address collisions. In view of the problems involved in the above mentioned schemes, another way is needed. One such way is the Filter-based Addressing Protocol. The objectives of small storage allocation and less control overhead are achieved through the usage of small filters and a mechanism precisely distributed for the updation of state information of the dynamic nodes in the mobile adhoc networks. Unlike the previous proposals, we use filter signature, i.e; the hash of the filter to identify the network partition in the place of random numbers which is very helpful in detecting and merging the partitions. The key concepts to be known in this metod are:

- FAP
- Bloom Filter
- Sequence Filter

*3.1. FAP*

Filter-based Addressing Protocol (FAP) deals with the achievement of dynamic auto configuration of mobile nodes in the network and collision resolution with low control load even in the case of joining and merging events. For this, a distributed compact filter is used to store currently allocated address set which is present at every node to simplify node joining that occurs very often. Also address collisions are resolved with reduced control overhead. The filter signature is a significant facet of our proposal that makes network merging event detection easy which is prone to conflicts usually.

*3.2. Bloom Filter*

It is a compact data structure based on hash functions which is used in distributed applications.

$$V= \{v1, v2, v3,.....v_n\}$$

*3.3. Sequence Filter*

Based on the sequence of addresses, it compacts the addresses and stores the data. It is created by concatenating the initial element, i.e; the first address of the address sequence with the address range size, an n-bit vector. Each address suffix is represented by one bit that gives the distance between the initial element and the current element. There are no false-positives, or false-negatives in sequence filters as every available address is represented by its respective bit.

*3.4. Selection of Filter*

The best type of filter is determined by the network features and the false-positive and false-negative rates of the filter. Bloom filter does not exhibit false-negative. But false-positive is possible. Hence, its size is not determined by the address range but by the maximum number of participant nodes in the mobile network. But the sequence filter is deterministic whose size is confined to the address range and address size. Thus there is no possibility of false-positives or false-negatives. The address range size is the number of bits in the address suffix. Both the filters follow opposite ways in the case of their sizes: Bloom filter's size is confined to the address range size and increases with the number of nodes active in the network while the size of Sequence filter is constant to the number of nodes in the network and raises with increase in address range size, making the bloom filter suitable for extensive address ranges and sequence filter for the larger number of active nodes in the network. The below figure shows the difference:

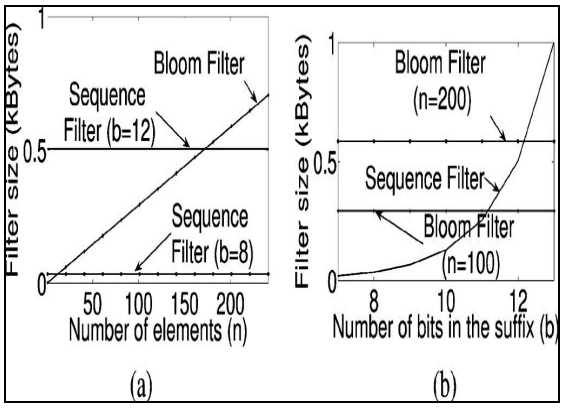


*Figure 2*

*3.5. Scheme of FAP*

3.5.1. Building the network

Initialising the network is nothing but auto configuring the initial nodes in the network. Usually, addressing protocols assume that there is a long interval between the entries of the upcoming nodes. FAP uses both gradual and non-gradual ingresses through Hello and AREQ messages. The joining node initially listens to the medium for a particular time and if it does not listen to any Hello messages, then randomly chooses an address with respect to the bits of the network and begins the initialization of the network. The node floods the network with AREQ. After timeout, it stops listening to AREQs and inserts all the addresses received with AREQs into the address filter. Then it sends Hellos with the filter signature, i.e.; the hash of the filter. If an AREQ with the same address chosen by the node is received, then it waits for a while and then sends another AREQ. Here the waiting interval reduces the probability of choosing the same address again as another node that decreases the network control load eventually.

3.5.2. Detection of collision while node entry and partition merging

The joining node sends an Address Filter (AF) message to a node already in the network in order to join the network. The recipient node checks the bit I for 1.If so, it sends an AF with bit R set to 1.Then the joining node stores the address filter and chooses a random address. It floods the network with AREQ messages. All the recipient nodes insert the new address in their filters and update the filter signatures. This avoids address collisions. Another issue is collision in partition merging. Nodes assign addresses based on the remaining node addresses in their partition only. Hence nodes in different partitions may have the same addresses. Problem arises when the partitions merge. A node checks the filter signature on the arrival of a Hello message. If it is different, then it means that the sender is from different address set. During the event of partition merging the nodes exchange the filters of the partitions through AFs. Then both the partitions are flooded with the Partition message. All the nodes in first partition update their filters with the other partition data. All the nodes check for address collisions with the nodes from other partition. If there is one, then the node randomly chooses a new address and sends AREQ to all other nodes. If there are no collisions, then the filters are updated with the new AREQ addresses at all the nodes. Thus collisions in partition merging are detected and resolved.

3.5.3. Departure of Nodes

A departing node floods the network with the notification to the other nodes so that its address is made available for the joining nodes. Then the other nodes remove the departing node address from the address filter. Otherwise, the available address space would become inadequate after a number of successive unnotified node departures.

**4. Conclusion**

We discussed the Filter-based Addressing Protocol (FAP) which solves the problems of address collisions, channel fading and network partition in mobile adhoc networks. It uses less control overhead and is resistant to message losses which is a common issue in adhoc networks. The hash of the filter used as partition identifier better represents the set of nodes in the partition as it reflects the change in the set of nodes.

**5. References**


1. N. C. Fernandes, M. D. Moreira, O. C. M. B. Duarte, “A self-organized mechanism for thwarting malicious access in adhoc networks”, in Proc. 29th INFOCOM Minoconf., San diego, CA, Apr. 2010, pp. 1-5.
2. D. O. Cunha, O. C. M. B. Duarte and G. Pujolle, “A cooperation aware routing scheme for fast varying fading wireless channels”, IEEE Commun. Lett., vol. 12, no. 10, pp. 794-796, Oct 2008.
3. N. C. Fernandes, M. D. Moreira and O. C. M. B. Duarte, “An efficient filter-based addressing protocol for auto configuration of mobile adhoc networks”, in Proc. 28th IEEE INFOCOM, Rio de Janeiro, Brazil, Apr. 2009, pp. 2464-2472.
4. Z. Fan and S. Subramani, “An address auto configuration protocol for $IPv_6$ hosts in a mobile adhoc network”, Comput. Commun., vol. 28, no. 4, pp. 339-350, Mar. 2005.
5. C. E. Perkins, E. M. Royers and S. R. Das,”IP address autoconfiguration for adhoc networks”, Internet draft 2000.
6. S. Thomson and T. Narten, “$IPv_6$ stateless address autoconfiguration”, RFC 2462, 1998.
7. S. Nesargi and R. Prakash, “MANETConf: Configuration of hosts in a mobile adhoc network”, in Proc 21st Annu, IEEE INFOCOM, Jun. 2002, vol. 2, pp. 1059-1068.
8. B. Parno, A. Perrig and V. Gligor, “Distributed detection of node replication attacks in sensor networks”, in Proc. IEEE Symp. Security Privacy, May. 2005, pp. 49-63.
9. H. Kim, S. C. Kim, M. Yu, J. K. Song and P. Mah, “DAP: Dynamic address assignment protocol in mobile adhoc networks”, in Proc. IEEE ISCE, Jun. 2007, pp. 1-6.
10. M. Fazio, M. Villari and A. Puliafito, “IP address auto configuration in adhoc networks: Design, implementation and measurements”, Comput. Netw., vol. 50, no. 7, pp. 898-927, 2006