ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

MANAP: An Effective and Self-Configuring Protocol for Dynamic Node Addressing In MANETs

Pradyumna Rao D, Raghavendra T.S

2nd year M.Tech (CNE), Dept of Computer Science & Engg., Cambridge Institute of Technology, Bangalore, India

Asst. Professor, Dept. of Computer Science & Engg., Cambridge Institute of Technology, Bangalore, India

ABSTRACT: Mobile Ad hoc networks face serious drawbacks regarding the allocation of addresses to the nodes. This challenge is mainly because MANET nodes are primarily distributed and they do not have predefined infrastructure. The existing ad hoc network addressing protocols have not been completely successful in handling address collisions because of leaving and/or joining nodes, and frequently occurring network partitions. To overcome such undesirable scenarios, we propose an efficient protocol based on a distributed database containing addresses stored in filters. This approach will allow the network to be functional despite frequent network partitions and packet losses. We consider the cases such as initializing a network, merging of existing partitions and joining of new nodes in a network for evaluating the performance of our protocol. We can prove through simulation results that our protocol is highly efficient in handling the address collisions and reducing the control traffic load.

KEYWORDS: MANETs, distributed addressing, address collision

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are auto-configuring wireless ad hoc networks of mobile devices requiring no previously established infrastructure. Since MANETs lack a centralized administration[1], each node in the network will actively participate in routing, thus playing the role of an active router. Such a de-centralized and dynamic administration of MANETs have greatly contributed towards distributed applications such as Military/ Tactical MANET, internet based MANET (iMANET), Vehicular Ad hoc networks (VANET), disaster recovery and so on.

Since the nodes in a MANET are free to move in any direction, the network is subject to frequent partitions. The mobility of the nodes can cause them to join or leave a network which often results in the disordering of the MANET control. Due to the absence of a centralized administrative server, MANET initialization is also a challenge.

Since each node in a MANET acts as a router, each node needs a unique network address. But the address allocation to these mobile nodes are not as simple as in centrally administered networks. The distributed and self organizing nature of MANET nodes is always a bottleneck in address assignment.

We propose an effective protocol called MANET Node Addressing Protocol (MANAP). In our proposed protocol, we extend the functionalities of the Filter-based Addressing Protocol (FAP)[2]. This protocol makes use of filters which are used to store a highly distributed database containing already assigned addresses in the network. We propose a new kind of filter called Linear filter along with the Bloom filter. These filters ensure unambiguous address allocation for the nodes which are joining the network. They also detect the address collisions of the nodes whenever two or more partitions merge. Hence our proposed protocol allows the mobile nodes to check the duplication of addresses. In order to diminish the storage overload of filters, we propose the usage of a unique Partition identification Code (PARCODE). The filter is hashed and the resultant hash value is the PARCODE. Hence the nodes can easily identify the network partitions and thus avoid the address collisions. The simulation results prove that the proposed protocol achieves a very low communication overhead, low storage requirement and low latency.

The remainder of this paper contains the following sections: We discuss the related work in section I. Proposed algorithm and pseudo code are detailed in section II and section III respectively. Section IV depicts the simulation results. Finally we conclude the paper and discuss about the future scope of this paper in section V.

II. RELATED WORK

Since the MANETs are distributed in nature, there is no centralized administrative entity to monitor the configuration of the network nodes. Hence there is always a high probability of address collision by newly joining nodes, as shown in the birthday paradox[3]. This birthday paradox guarantees the detection of address replication with high probability. The paper [4] discusses the Duplicate Address Detection (DAD) which is the basis for address auto configuration in distributed networks. Here the allocated addresses are never stored unlike in the proposed protocol. In this protocol, each newly joining node chooses an IP address and broadcasts this address using an IP address query (IPQRY) message, so that all other nodes in the network are notified about this address. If any other node in the network has the same IP address as the joining node, it alerts the joining node regarding the address collision by replying with an IP address duplication (IPDUP) message. The paper[5] discusses in detail about handling the network partitions in a MANET. In this paper each partition is assigned a unique network identifier (NID). Each newly joining node repeatedly broadcasts a configuration request (CREQ) message until a neighbour responds with a hello message. Then the neighbour sends the necessary configuration parameters to the joining node which is then identified by the {IP address, NID} pair. The paper[6] proposes to enhance the detection performance of a partition merge through MANETconf protocol. According to MANETconf, each node in a MANET maintains two lists : Allocated_List and Allocated _Pending_List. When a new node arrives at a MANET, it repeatedly broadcasts the address request message to its neighbours. One neighbour responds to the address request message by choosing am address which is then broadcasted to the whole MANET by the responder. This chosen address is then added to the Allocated_Pending_List until the responder gets positive replies from all the nodes. Once it is confirmed that the chosen address is not assigned any other node, that address gets allocated to the joining node. Then the address is removed from the Allocated_Pending_List and added to Allocated_List, and then it is again broadcasted to all the nodes so that they too can update the lists.

III. PROPOSED WORK

The aim of the proposed MANAP is to efficiently auto-configure the addresses of the MANET nodes by resolving address duplications in case of node joining or partition merging events. To accomplish these goals, address filters are maintained at all the nodes across the network. We propose to use two kinds of filters :

(a) Bloom Filter
(b) Linear Filter

Bloom Filter: The Bloom filter is a probabilistic data structure that is used to test whether an element is present in a set or not[7,8]. We consider the bloom filter to consist of a x-bit vector to represent a set S={s_1,s_2,s_3,...s_y} of y elements. All the x-bits are initially set to 0. A set of hash functions f_1,f_2,...f_k are fed with the elements of set S and the output of the hash functions are distributed evenly over the x-bit vector. Then, all the hash functions are used to hash every element si ϵ S whose output is represented by a bit which is set to 1 in the x-bit vector. We can check if an element s_i ϵ S by verifying whether all the bits in the vector corresponding to the locations $f_1(s_i)$, $f_2(s_i)$,...$f_k(s_i)$ are set to 1 as shown in Fig 1. The element s_i is not considered to be in the filter even if at least one bit is set to 0.

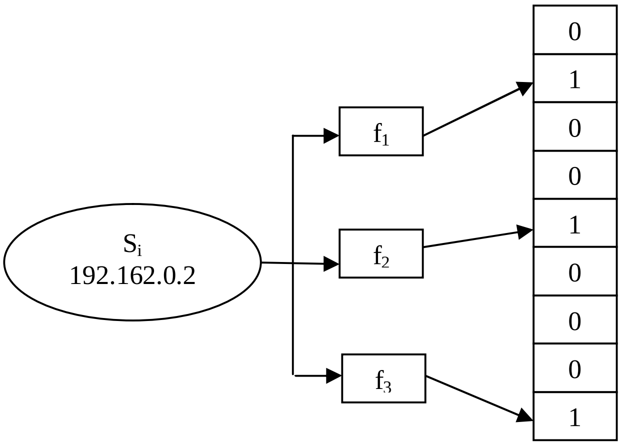

Fig 1. Bloom Filter with k=3 and x=9

We can obtain the probability of a specific bit in the vector is 0 even after y elements are inserted, explained by Mitzenmacher and Broder. This probability can be given by the following expression:

$$P_{(0)} = [1-1/x]^{(k,y)}$$

We can also find the probability of the false positives which is the probability that all the k-bits representing an element which is not inserted, are set to 1. In other words, this probability $P_{(+ve)}$ can be given by the following expression:

$$P_{(+ve)} = [1-P_{(0)}]^{k}$$

Thus the $P_{(+ve)}$ increases with the increase in the number of elements in S, or with the decrease in the vector size x.

Linear Filter: This is the proposed filter which stores the addresses according to the linear order of the addresses. The first address in the address list is concatenated with a vector of size q-bits. We call the concatenated address as the leader element (s_0) and the vector size (q-bits) represent the address range. We consider the suffix of each address in the list which is represented by a single bit. Each of the address suffix can be indexed by δ, which gives the distance between leader suffix $s0_{suf}$ and the present element suffix si_{suff}. If a bit indicates 1, then the address suffix represented by that bit belongs to the filter. In the opposite case, then the address is not said to be in the filter. Since the representation of each available address is deterministic, the concept of false positives and false negatives does not exist.

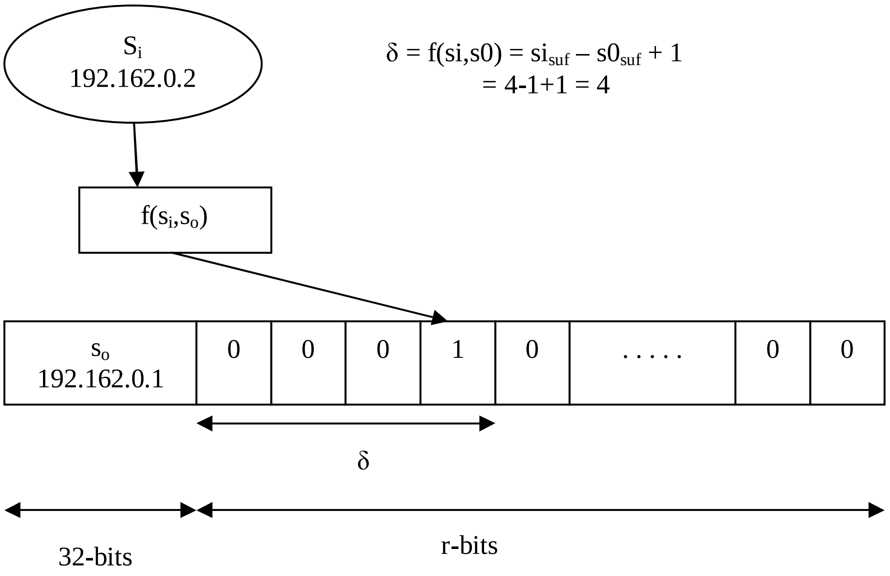

Fig 2. Linear filter

The representation of the linear filter is as shown in the above figure.

IV. PSEUDO CODE

```
Step 1: Node $n_o$ arrives at a network at current time $T_C$
Step 2: $n_o$ listens to the network for a time period $T_W$
Step 3: If $T_C > (T_C+T_W)$ and Hello_message_received=false
                Make $n_o$ as the initiator $n_i$;
                Form the network;
        end if
Step 4: else if $T_C <= (T_C+T_W)$ and Hello_message_received from initiator $n_i$=true
                Make $n_o$ as the joining node $n_j$
Step 5:         $n_i$ randomly chooses an address $A_o$
                $n_i$ broadcasts address request message MREQ advertising $A_o$ to all other initiators $N_M$ times
                Other initiators broadcast MREQs advertising their chosen addresses $A_i$ $N_M$ times
Step 6:         $n_i$ receives MREQs from other initiators
Step 7:         $n_i$ compares $A_i$ s with $A_o$
Step 8:         if $A_i$= $A_o$
                     goto Step 5
                end if
Step 9:         else
                     Assign $A_o$ to $n_j$
                end if
       end if
```

V. SIMULATION RESULTS

The proposed MANAP was implemented in ns 2 simulator. In the simulation results, we try to compare and analyze the efficiency of MANAP, DAD, DAD with partition detection (DAD-PART) and MANETconf. Efficiency is measured by considering the parameters like average delay and control overhead.

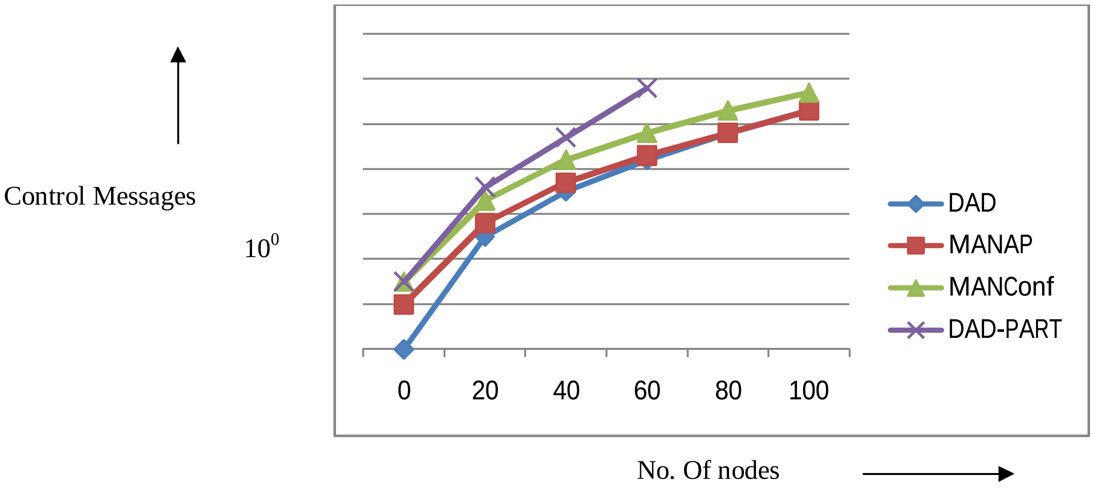

Fig 3(a). Control overhead according to no. of nodes

Fig 3(a). plots the number of control messages against the number of nodes for various protocols. As per the results, DAD-PART suffers the greatest overhead as compared to other three protocols. The DAD protocol achieves very less control overhead than MANAP when the number of nodes in the MANET is in between 0 and 60. However, as the number of nodes in the network starts exceeding 60, the MANAP marginally takes the lead in reducing the control overhead. It can be noticed very clearly from the above graph that as the number of nodes approaches 100, the control overhead difference between MANAP and DAD protocol is very less. That is, the MANAP slightly overtakes the DAD protocol in reducing the overhead when the node count nears 100.

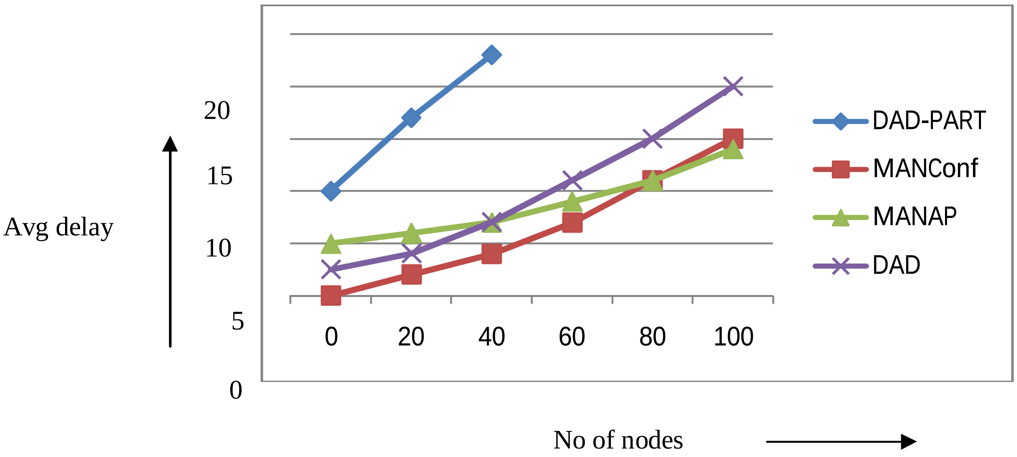

Fig 3(b). Average delay versus no of nodes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

Fig 3(b). plots the average delay against the number of nodes for various protocols. As per the results, DAD-PART has the highest average delay. Hence it is not the ideal protocol for MANET node address allocation. If the number of nodes are less, MANAP has the second highest delay. As the number of nodes approaches 80, the delay is lowest for MANAP. Thus, the MANAP may not prove to be an optimal choice to reduce the average delay in MANETs when the number of nodes are less than 80. But it is very efficient for the networks with the number of nodes exceeding 80.

VI. CONCLUSION AND FUTURE WORK

We proposed and analyzed the MANAP, which is self-configuring and dynamic in nature. It is very well suited for MANETs which encounter frequent network partitions and have leaving and/or joining nodes. The proposed protocol uses address filters to store the available addresses which highly reduces control load and address duplications. Also our protocol is very much robust, given the continuously changing topologies of MANETs. The filter signature produced by filter hashing provides better unique representation of nodes in a MANET. Even the protocols such as DAD has a low control overhead, but it can not be efficient in case of network partitions. Hence it is reasonable to conclude that the MANAP is best suited for the node addressing in MANETs.

But the MANAP is not suitable for MANETs with a low node count as it is evident from the simulation results plotted in the previous section. Hence, in the future, we would like to optimize the performance of our proposed protocol even when the network has a low number of nodes..

REFERENCES.

1. N. C. Fernandes, M.D.Moreira, and O. C. M. B. Duarte,"A self-organized mechanism for thwarting malicious access in ad hoc networks ", in Proc 29th IEEE INFOCONF Miniconf., pp 1-5, April 2010.
2. N.C.Fernandes, M.D.Moreira, O.C.M.B. Duarte ,"An efficient filter-based addressing protocol for autoconfiguration in mobile ad hoc networks", in proc 28th IEEE INFOCOM, pp 2464-2472, April 2009.
3. B.Parno, A.Perrig, V.Gligor, "Distributed detection of node replication attacks in sensor networks", in proc.IEEE symp security privacy, pp 49-63, May 2005.
4. C.E.Perkins, E.M.Royers,S.R.Das, "IP Address autoconfiguration for ad hoc networks", Internet Draft, 2000.
5. Z.Fan, S.Subramani, "An address auto configuration for IPv6 hosts in a mobile ad hoc network", Comput. Commun., vol 28, no. 4, pp 339-350, March 2005.
6. S. Nesargi and R. Prakash, "MANETconf: Configuration of hosts in a mobile ad hoc network", in *Proc*. 21st Annu. IEEE INFOCOM, vol. 2, pp. 1059–1068, Jun 2002.
7. M. D. D. Moreira, R. P. Laufer, P. B. Velloso, and O. C.M. B. Duarte, "Capacity and robustness tradeoffs in Bloom filters for distributed applications", IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp 2219-2230, Dec. 2012.
8. L. Fan, P. Cao, J. Almeida, and A. Z. Broder, " Summary cache: A scalable wide-area web cache sharing protocol", IEEE/ACM Trans. Netw., vol 8, no. 3, pp 281-293, June 2000.

BIOGRAPHY

Mr. Pradyumna Rao D is a student of Computer Science and Engineering department in Cambridge Institute of Technology, Bangalore, affiliated to VTU. He is pursuing his final year of M.Tech in Computer Networks Engineering. He received his Bachelor of Engineering degree from Jawaharlal National College of Engineering, Shimoga. He is currently working as a research assistant under the guidance of Asst. Prof. Mr. Raghavendra T.S.

Mr. Raghavendra T.S is currently Assistant Professor in the Department of Computer Science and Engineering at Cambridge Institute of Technology. He has received B.E and M.Tech degrees affiliated to VTU. He is also a trainer in Wipro Academy of Software Excellence (WASE). His areas of expertise are Computer Architecture and Microprocessors.