ISSN:2249-5789
Bini M Issac et al , International Journal of Computer Science & Communication Networks,Vol 4(5),160-164

ID Based Addressing Scheme for Node Autoconfiguration in Ad Hoc Networks

Bini M Issac[#1], Deepu Benson[*2]

[#]*PG Scholar,*[*]*Assistant Professor*

Amal Jyothi College of Engineering, Kanjirappally

[1]binimissac@cs.ajce.in
[2]deepubenson@amaljyothi.ac.in

***Abstract*— The TCP/IP protocol allows the different nodes in a network to communicate using a unique IP address. In wired or wireless networks with infrastructure, there is a server or node acting as such which correctly assigns the IP addresses, but in Ad hoc networks there is no such centralized entities or mechanism to do this function. So address assignment is a key challenge in Ad hoc networks due to the lack of centralized entity and lack of infrastructure. So, a protocol is needed to perform the network configuration automatically and in a dynamic way, as if they were servers that manage IP addresses. The goal of this study is to develop a protocol for IP address auto-configuration with less address conflicts. Also, a bloom filter is implemented in each node to check the address conflicts efficiently. Simulations were done in NS-2 to test the performance of the proposed protocol. A comparative study was then conducted. The proposed scheme was compared with the randomized approach. The different parameters such as number of address conflicts, average end to end delay, average throughput, control load are analyzed and a comparison is made between two protocols. Results from the simulation experiments show that ID based addressing scheme outperforms randomized approach in all the metrics evaluated-number of address collisions, average throughput, average end to end delay and normalized routing load .**

Keywords- Ad Hoc Networks, IP Address, Simulation, Birthday Paradox, Bloom Filter

I. INTRODUCTION

An Ad hoc network is a decentralized type of wireless network mode where wireless devices communicate with each other directly, without the aid of a central access point device. The network is Ad hoc because it does not rely on a preexisting infrastructure. Here, every node participates in routing by forwarding data for other nodes. So which all nodes can forward data is made on the basis of network connectivity. These devices should ideally be within close range of each other. The term “ad hoc" tends to imply “can take different forms" and can be “mobile, stand alone, or networked". Ad hoc implies that the network is formed in a spontaneous manner to meet an immediate demand and specific goal. Ad hoc networks are formed spontaneously and they can dynamically handle the joining or leaving of nodes in the network. Mobile nodes are capable of roaming independently. They are autonomous units.

A. Motivation

Like in wired networks, nodes in ad hoc networks cannot take part in any type of communication unless they are configured with an address. Although routing protocols assume the existence of unique node addresses, the question of how to provide them remains open. The autonomous nature of ad hoc networks requires the presence of an address auto configuration mechanism with less address conflicts. In these networks, such a mechanism has to cope with a highly dynamic environment and uncertain network structures.

B. Problem Definition

Unlike wireless networks with central access points and DHCP servers, stateless mobile ad hoc networks are completely decentralized and possess no central infrastructure. In addition, due to the limited range of a mobile node, a node normally has no complete view of the network. Thus it is necessary to have auto configuration algorithms, i.e. algorithms for assigning a unique address to a node upon connection to an ad hoc network that works under these constraints. These addresses have to be unique in a certain scope to avoid packets being sent to wrong nodes. A task of particular difficulty is the address uniqueness test: as the nodes normally do not have a complete view of all participating nodes in the network, they cannot determine a duplicate address conflict. So far, there are several possible solutions for this problem, but none of these has been standardized.

II.RELATED WORK

Address auto configuration proposals that do not store the list of allocated addresses are typically based on a distributed protocol called Duplicate Address Detection (DAD). In this protocol, every joining node randomly chooses an address and floods the network with an Address Request message (AREQ) for a number of times to guarantee that all nodes receive the new allocated address. If the randomly chosen address is already allocated to another node, this node advertises the duplication to the joining node sending an Address Reply message (AREP). When the joining node receives an AREP, it randomly chooses another address and repeats the flooding process. Otherwise, it allocates the chosen address. This

proposal, however, does not take into account network partitions and is not suitable for ad hoc networks.

Other proposals use routing information to work around the addressing problem. Weak DAD [3], for instance, routes packets correctly even if there is an address collision. In this protocol, every node is identified by its address and a key. DAD is executed on the 1-hop neighbourhood, and collisions with the other nodes are identified by information from the routing protocol. If some nodes choose the same address and key, however, the collision is not detected. Moreover, Weak DAD depends on modifying the routing protocols.

Some other protocols proposed needs additional data structures to run the addressing protocol. MANETconf [4] is a stateful protocol based on the concepts of mutual exclusion of the Ricart Agrawala algorithm. In this protocol, nodes store two address lists: the Allocated list and the Allocated Pending list. A joining node asks for an address to a neighbour, which becomes a leader in the address allocation procedure. The leader chooses an available address, stores it on the Allocated Pending list, and floods the network. If all MANETconf nodes accept the allocation request and positively answer to the leader, then the leader informs the allocated address to the joining node, moves the allocated address to the Allocated list, and floods the network again to confirm the address allocation. After receiving this message, each node moves the address from the Allocated Pending list to Allocated list. MANETconf handles address reallocation, but partition detection depends on periodic flooding. Therefore, this protocol incurs in a high control overhead.

III. PROPOSED PROTOCOL

C. *BasicIdea*

ID Based addressing scheme was inspired by the notion that it is difficult to guarantee uniqueness of allocated addresses without DAD. This is a hybrid protocol which uses a distributed allocation table for IP address lookup. This protocol takes into account the device MAC address for IP address configuration. Every NIC has a hardware address known as a MAC, for Media Access Control which is unique. MAC addresses are linked to the hardware of network adapters. A MAC address is given to a network adapter when it is manufactured. The MAC address is a string of six sets of two-digits or characters, separated by colons. The first three octets identify the manufacturer. MAC address is 48 bits in length. These 48 bits are taken and hash functions are applied and the 48 bits are reduced to 8 bit address suffix. This address suffix is then appended to the available range of addresses for Ad hoc network and individual IP addresses are configured to the nodes based on each device MAC address. The address conflict detection is performed using bloom filter. Each node stores in a compact way the set of allocated IP addresses in bloom filters.

D. *Network Model*

Every new node that wishes to join the Ad hoc network needs to have a unique IP address during its connection. The address assignment is the responsibility of each node. It is assumed that atleast one node in the network knows the IP address block from which the IP addresses are to be assigned to the nodes in the Ad Hoc network. For this allocation, the IP address block 192.168.123.0 to 192.168.123.254 is used in this implementation. The address block information can be propagated to other nodes joining the network during the assignment process.

E. *Network Model*

The network initialization procedure deals with the autoconfiguration of the initial set of nodes. Two different scenarios can happen at the initialization: the joining nodes arrive one after the other with a long enough interval between them, called gradual initialization, or all the nodes arrive at the same time, called abrupt initialization. For, the implementation purpose, the abrupt initialization is considered in this work.

The proposed protocol uses Hello, AREQ and AREP messages. The Hello message is used by a node to advertise its current association status and partition identifier. The AREQ message is used to advertise that a previously available address is now allocated. Each AREQ has an identifier number, which is used to differentiate AREQ messages generated by different nodes, but with the same address.

In the proposed protocol, a node trying to join the network listens to the medium for a period. If the node does not receive a Hello message within this period, then it starts the network, acting as the initiator node. An initiator node may start the network alone, or with other initiator nodes. Otherwise, if the node receives a Hello message, then the network already exists and the node acts as a joining node. An initiator node chooses an address that corresponds to the hashed MAC address, considering the address range defined by the bits of the network prefix, creates an empty address filter, and starts the network initialization phase. In this phase, the node floods the network a number of times with AREQ messages to increase the probability that all initiator nodes receive the AREQ message. If there are other initiator nodes, they also send their AREQ times, advertising their chosen addresses. After waiting a period without listening to AREQs from other initiator nodes, in case they exist, the node leaves the initialization phase and inserts on the address filter all the addresses received with AREQs.

F. *Address Configuration Procedure*

ID Based Address configuration protocol takes into account the device MAC address for IP address configuration. MAC address which is 48 bits in length is taken and consecutive bits xor-ed to form an 8-bit address suffix. This address suffix is then appended to the available range of addresses for Ad hoc

network and individual IP addresses are configured to the nodes based on each device MAC address. So each node will be configured with the address suffix corresponding to the hashed MAC address. Figure.1 and Figure.2 shows the address configuration procedure.

Figure.1 Formation of Address suffix

Figure.2 Address Formation

G. Bloom Filter Implementation

The Bloom filter is a compact data structure used on distributed applications. The Bloom filter[8] is composed of an m-bit vector that represents a set A=a1; a2; a3..:an composed of n elements. The elements are inserted into the filter through a set of independent hash functions, whose outputs are uniformly distributed over the bits. First, all the bits of the vector are set to zero. After that, each element is hashed by each of the hash functions, whose output represents a position to be set as 1 on the m-bit vector. To verify if an element belongs to A, we check whether the bits of the vector corresponding to the positions are all set to 1. If at least one bit is set to 0, then A is not on the filter. Otherwise, it is assumed that the element belongs to A. There is, however, a false-positive probability that an element be recognized as being in A. This may happen when the bits at the positions are all set by previously inserted elements. Fig.3 shows a bloom filter. Similarly bloom filters can be implemented for IP addresses.

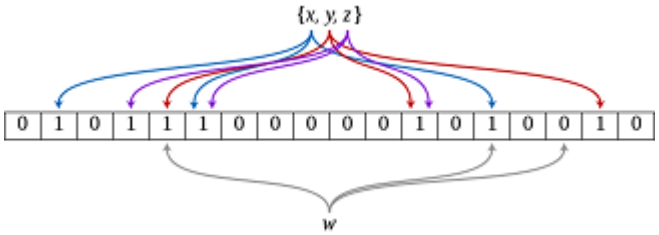

Figure.3 Bloom Filter

Also, the protocol is implemented using the randomized approach for performance comparison. The drawback of the Randomized approach is the larger number of address collisions. Here the nodes selects random IP address. A node floods Route Requests (RREQs) for the selected IP address. If no Route Reply (RREP) is received within a timeout period, the node retries for RREQ a number of times. At the end of all the retries, if no response is received, the chosen IP address is assumed to be free. The node assigns itself that IP address. Here the latency is the timeout value multiplied by RREQ retries. This approach requires the routing protocol to have a "route discovery" phase. For this protocol implementation, appropriate random number generators are used. There is a chance for more than one node taking the same address as random numbers are not a good choice. So duplicate address detection is done using bloom filters. The bloom filter is built using the selected IP addresses and this filter is present in all nodes. So each node can easily check whether an address is already allocated or not. The address collision rate is high in randomized approach due to Birthday paradox problem.

IV . SIMULATION RESULTS

The method described previously are implemented and simulated in NS-2.35 running on Ubuntu Linux operating system to produce the results discussed below. Those results and an analysis were documented. To generate a graph output AWK scripts are used to pipe out the desired outputs from trace files. The Network Animator (NAM) is one of the most important components in NS-2 that visualize the animation of the network and its behavior. It monitors for the network information such as node locations, node movements, traffic, and topology. The Xgraph is a trace file analyzer for NS-2 to generate graphs showing the metrics of network performance.

The table I shows different simulation parameters and table II shows the different parameters values considered for simulation.

TABLE I. SIMULATION PARAMETERS

Parameters	**Environment**
Maximum node speed	100.00
Interface queue	DropTail/PriQueue
Radio propagation	Two Ray Ground
Network interface	Wireless physical
MAC protocol	IEEE 802.11
Antenna model	Omni Antenna
Routing protocol	AODV

TABLE II. SIMULATION PARAMETER VALUES

Parameters	**Values**
Simulation Time	20s
Simulation Area	1000 x 1000

Number of Nodes	10, 20, 30, 40, 50
Recorded parameters	Average end to end delay, Normalized Routing load, Average throughput

The number of nodes used for simulation is 10, 20, 30, 40, 50. The same parameter values are used for simulation of both scenarios - ID based addressing protocol and the randomized approach. As a result of simulation, a trace file is generated for each simulation and that is analyzed for calculating the various parameters such as average throughput, average end to end delay and routing load. A comparative study is then made using the resulting trace files of both protocol simulations. The different values obtained from the simulation results are described below.

A. *Number of Address collisions*

No address collision is detected with the ID based addressing scheme using up to 50 MAC addresses. The efficiency of this method depends on the uniqueness of the device MAC address. However if two different MAC addresses hash to the same value, there is a chance for address collision. But atleast two address collisions occurs with five successive simulations of randomized approach. The address collision rate is high in randomized approach due to Birthday paradox problem . Random approach is not a good choice since always there is a chance for duplicates in random selections.

B. *Average Throughput*

Average Throughput is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet. When comparing the average throughput of both protocols by varying the number of nodes, ID based addressing protocol has better performance than the randomized approach.

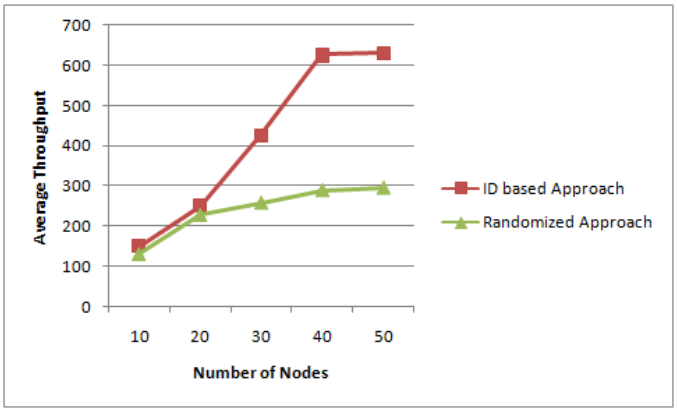

Figure.4 Average Throughput - ID Based Addressing scheme versus Randomized approach

Figure.4 shows the throughput versus number of nodes graph of both ID based approach and distributed approach using the values obtained from simulation. It is found that, throughput increases with increase in number of nodes. The throughput of ID based addressing scheme is very high compared to randomized approach. But when the number of nodes reaches 50, the throughput stays steady in both approaches.

C. *Average Throughput*

End-to-end delay is the time taken by a packet to route through the network from a source to its destination. The average end-to-end delay can be obtained computing the mean of end-to-end delay of all successfully delivered messages. Therefore, end to-end delay partially depends on the packet delivery ratio. As the distance between source and destination increases, the probability of packet drop increases. The average end-to-end delay includes all possible delays in the network i.e. buffering route discovery latency, retransmission delays at the MAC, and propagation and transmission delay. The lower value of end to end delay means the better performance of the protocol.

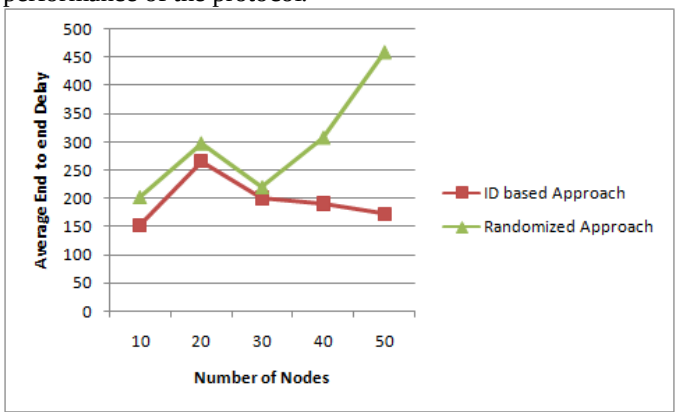

Figure.5 Average End-to-end delay - ID Based Addressing scheme versus Randomized approach

Figure.5 shows the delay versus number of nodes graph for both approaches. It is observed that the end to end delay increases with the number of nodes upto 20 nodes. Then the end to end delay begins to decrease. Both approaches have almost same delay when the number of nodes reaches 30. After that, for ID based approach the end to end delay goes on decreasing which is desirable. But in the case of Randomized approach, the delay goes on increasing which is not desirable in the network. The end-to-end delay should be minimum in any network.

D. *Routing Load*

Routing load is the number of routing packets transmitted per data packet delivered at the destination. The routing load increases as the number of nodes increases.

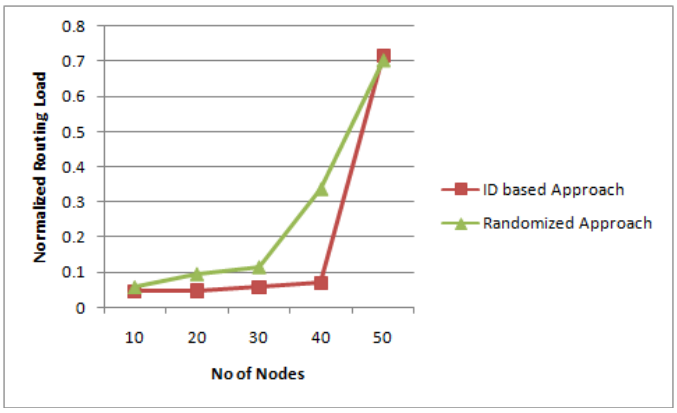

Figure.6 Normalized Routing load - ID Based Addressing scheme versus Randomized approach

Figure.6 shows the comparison graph of Normalized routing load of both ID based approach and the randomized approach. From the graph, it is clear that the routing load increases as the number of nodes increases. Also, the routing load for Randomized approach is greater than that of the ID based approach. This is because of the larger number of route requests generated in the case of randomized algorithm.

V. CONCLUSION

Lack of manual management in Ad hoc networks means that automatic configuration is highly desirable. Automatic configuration of nodes in wireless Ad hoc network will help in reducing administration efforts by users and network administrators. Initial investigation into this area identified the need for achieving high levels of address uniqueness without affecting the performance. It is found that randomized addressing is not a good choice. ID based approach reduces the address collision rate and it has better performance parameter values. Simulation experiments were done in NS-2 to test the performance of the protocol and the various parameters were evaluated. Bloom filters helps to detect the address collisions effectively.

REFERENCES

[1] Natalia Castro Fernandes, Marcelo Duffles Donato Moreira, and Otto Carlos Muniz Bandeira Duarte An Effcient and Robust Addressing Protocol for Node Autoconfiguration in Ad Hoc Network" ,IEEE/ACM Transactions on Networking, VOL. 21, NO. 3, JUNE 2013

[2] C. E. Perkins, E. M. Royers, and S. R. Das, IP address autoconfiguration for ad hoc networks," Internet draft, 2000.

[3] N. H. Vaidya, Weak duplicate address detection in mobile ad hoc networks," in Proc. 3rd ACM MobiHoc, 2002, pp. 206216.

[4] S. Nesargi and R. Prakash, MANETconf: Configuration of hosts in a mobile ad hoc network,"in Proc. 21st Annu. IEEE INFOCOM, Jun. 2002, vol. 2, pp.10591068.

[5] Mohsin, M. and Prakash, IP Address Assignment in a Mobile Ad-hoc Network",Proceedings of IEEE MILCOM 2002, Anaheim, CA, Oct. 2002.

[6] Y. Hsu, C. Tseng, Prime DHCP:A prime numbering address allocation mechanism for manets", in: IEEE Communicatons, August 2005

[7] Hongbo Zhou, Lionel M. Ni, Matt W. Mutka:Prophet address allocation for large scale MANETs",IEEE Transaction 2003

[8] MB Mutanga , TC. Nyandeni, P. Mudali, S Xulu, MO Adigun,Wise-DAD AutoConfiguration for Wireles Multi-hop Networks"

[9] Teerawat Issariyakul, Ekram Hossain, Introduction to Network Simulator NS2-springer,2009

[10] Greis M, Tutorial for the network simulator NS from :http://www.isi.edu/nsnam/ns/tutorial/,September 30, 2009