 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

Secure and Conflict-Free Address Allocation Scheme in MANET

[1]Avinav Pathak, [2]Anju Shukla, [3]Akash sharma
[1,2,3]IIMT Institute of Engineering & Technology, Meerut, India

Abstract
A Mobile ad-hoc Network (MANET) consists of a set of mobile nodes communicating with each other via wireless links. Due to rapid change in topology of MANET, address allocation is not possible through centralized servers. So some auto configuration schemes are proposed. In this paper we proposed conflict free address allocation scheme. We also proposed some security procedures that should be followed by a requester node and cluster head for efficient allocation of address.

Keywords
MANET, Auto-Configuration, Address Allocation, Trust Value Computation

I. Introduction

A Mobile Ad hoc Network (MANET) [1] is an independent self organizing network in which each node functions as both an end host and a router. This form of wireless network is created by mobile nodes without any existing or fixed infrastructure. The formed network can be changed without the need of any system administrator dynamically. In MANET, topology changes rapidly because nodes are free to move independently. For communicating among nodes, each node needs an identity. So a unique address is assigned to each node so that packet can be routed and delivered to the final destination correctly. But researchers assume the nodes that are participating in routing are already configured. Dynamic allocation and management is very difficult. In MANET, static address allocation is not possible because nodes topology changes very frequently as nodes are free to move any time and at any place. So in MANET, nodes cannot rely on centralized servers. Here we have proposed a distributed dynamic address allocation protocol for assigning address to a requesting node.

Security of MANET is also the major concern because nodes can join and leave the network at any time. So before granting permission to join the network, network must ensure whether coming nodes are trustworthy or not. So for enhancing security of MANET, we have proposed a secured procedure for joining the new node in a MANET.

II. Related Work

Mohsin and Prakash [2], propose a stateful protocol which use Multiple Disjoint Allocation Tables. In [3], this protocol is called the Buddy protocol. In this approach every node has a disjoint set of IP addresses that can be assigned to new nodes, is said that as node owns these pool of IP addresses hence no quorum is required to make a decision. This approach uses a proactive scheme for dynamic allocation of IP addresses in MANETs. A node that does not have an IP address broadcasts request messages to locate initiator neighbors using its hardware address. Requester chooses the initiator that responds first and send it a acknowledgment message. An initiator can have one or multiple blocks of IP addresses, the second case happens when neighbor nodes leave the network and release gracefully their corresponding blocks, also nodes can depart abruptly and a synchronization mechanism solves the leaking IPs. An initiator with one block divides its set of available IP addresses into two disjoint subsets, one for keep and the other to assign. On the other hand an initiator with multiple blocks will assign one of these blocks to requester. In both cases initiator also sends its IP address table. Then the requester configures itself taking the first address from the received block and keeps the rest for future requesters. The process finishes when initiator receives a successful configuration message from requester. This approach discusses three solutions for nodes with no free IP addresses to allocate. This protocol employs the approach described in MANETconf to solve network partitioning.

Vaidya [4] proposes a stateless protocol which uses a DAD mechanism integrated with the routing protocol. This mechanism is called weak DAD (WDAD) and requires modification of the routing protocol packets format to add a key. This key is generated during node autoconfiguration and its purpose is to identify the node i case of an IP duplicate conflict arise where more than one node selected the same IP address. As WDAD is integrated with the routing protocol, it can continuously detect duplicate addresses by simply checking if two address-key pairs have the same address.

In most networks, including MANETs, each node needs a unique identifier to communicate. It may be argued that the MAC address or the home IP address of the node should be sufficient for this purpose. However, use of the MAC address as a unique identifier has the following limitations [5]:

- MANET nodes are not restricted to using network interface cards (NICs) with a 48-bit IEEE-assigned unique MAC address. In fact, the TCP/IP protocol stack should work on a variety of data-link layer implementations. So, if this approach were to be employed, specific implementations would be required for each type of hardware.
- The uniqueness of a MAC address cannot always be guaranteed, as it is possible to change the MAC address using commands like ifconfig.
- There are known instances of multiple NIC cards from the same vendor having the same MAC address [6-7].

The home IP address of the mobile node may not be usable as a unique identifier at all times. The home IP address may not be permanent, for example when the node acquires an IP address during boot up through DHCP and releases it when it leaves the network. It is possible that two nodes belonging to the same home network, at different times, may join the MANET with the same home IP address. Moreover, even if a node owns a unique home IP address, it needs a unique care-of IP address in the MANET if it is to be addressable from the Internet.

The main assumption of ad hoc routing protocols is that all anticipating nodes do so in good faith and without maliciously disrupting the operation of the protocol.

III. Proposed Work

The objective of this protocol is to assign a unique IP address to every new node joining the MANET. The new node that will join the network is called a requester. The configured node which is responsible for assigning an IP address to requester is called an allocator.

A. Initiation Phase

In this phase, it is assumed that the MANET starts with a single node. We call this node the Initiator of the network and the configuration of the very first node is called as MANET initialization. For ease of understanding, it is assumed that at least the first node in the MANET knows the IP address block from which the IP addresses are to be assigned to the nodes in the MANET. The new proposed protocol can be equally applied to general IPv6 address space. The address block information is then propagated to other nodes that will join the network during the assignment process. The term "broadcast" in the paper stands for local broadcast.

B. Broadcast Phase

When the Initiator begins its operation in MANET mode, it broadcasts a message requesting an IP address (fig. 1). As there are no other MANET nodes in the neighborhood previously, the Initiator will not receive any response. The Initiator will then re-broadcast its request message for a constant number of times after which it assigns itself the first IP address from the IP address block and forms its free ip set from the remaining addresses.

This free ip set is an ordered set containing addresses that have not been used by any node in the network. After MANET initialization, every time a new node (requester) requests an IP address, one of the existing MANET nodes (allocator) which is in the communication range of the requester initiates address allocation process for the requester.

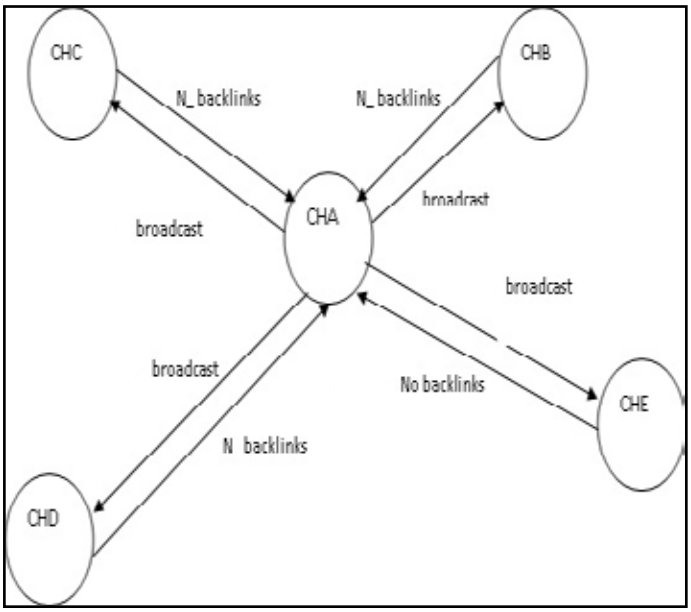

Fig. 1: Broadcast Phase

If the allocator has a non-empty free ip set, it allots the second half of the addresses from its free ip set to the requester.

C. Ring Search Phase

After nodes initialization and allocation has been completed the MANET now performs an expanding ring search whereby it propagates the request through the network. If the allocator finds a node (say node A) with a non-empty free ip set during the expanding ring search, it will then allot half of the addresses from node A's free ip set to the requester. The requester configure itself with the first address from the alloted address block and forms its free ip set with the remaining addresses in the block. There is a small issue with this technique i.e., during the expanding ring search, the allocator might fail to find a free IP address either because of the two reasons: (i) all IP addresses have been assigned to nodes currently in the MANET or (ii) some nodes have left the MANET without releasing their IP address and/or free ip set (leaked-addresses). In the first scenario, no new node can be admitted (without expanding the address block range) as the MANET has reached its maximum size.

In the second case, the leaked-addresses have to be reclaimed and assigned to new nodes joining the network.

D. Address Reclamation Phase

Address reclamation is done as follows:

1. The allocator determines the addresses of the nodes that failed to respond during the expanding ring search (call this set the missing addresses set). The allocator performs a network-wide broadcast targeted towards these addresses.
2. The nodes in the network, on hearing this broadcast message, respond with a message indicating a conflict if their IP address is among the broadcast addresses. If the allocator receives messages indicating conflict, it removes the corresponding IP address from the missing addresses set.
3. The addresses in the resultant missing addresses set are then declared as free IP addresses. One of these addresses is assigned to the requester. The rest of the free IP addresses are re-distributed among the existing nodes in the network to form their free ip sets. Concurrent reclamation operations are serialized based on the priorities of the allocators .

E. Proposed Security Procedures for the MANETS

In order to make the address allocation scheme a secured and authentic one we employ certain secured allocation techniques that can be beneficial for the hassle free communication.

The following steps are undertaken to make the security mechanism a feasible one:

STEP 1. We can consider the new node that wants to join the cluster as N_Node. This N_Node will be granted a communication ticket by the cluster head for transferring the messages in the cluster.

STEP 2. This ticket or token will then be exchanged with the neighbor nodes present in the cluster. The lifetime of the granted token to the N_Node will be for 5 seconds. A new node(n) can request for a token only limited no. of times(i.e. k=3).

STEP 3. After the request has been made and accepted by the CH, the cluster nodes reply by accepting the authentic token of the N_Node and in return they supply a "Member key" which is asymmetrically encrypted. After this, each member of cluster has a member key of its own. When the new node wants to communicate with any node in cluster the exchange takes place by transferring the token and the Mem_key .This procedure is authentic as every member has its unique Mem_key and this is copied and transfer to the new node by the previous member of the cluster.

STEP 4: Next we check the previous Path History of the incoming new node to figure out whether the node is purely valid or invalid. The criteria is that more the no. of back links a node is possessing to join the cluster better will be its priority to join the cluster else the node is rejected. This makes our security more enhanced.

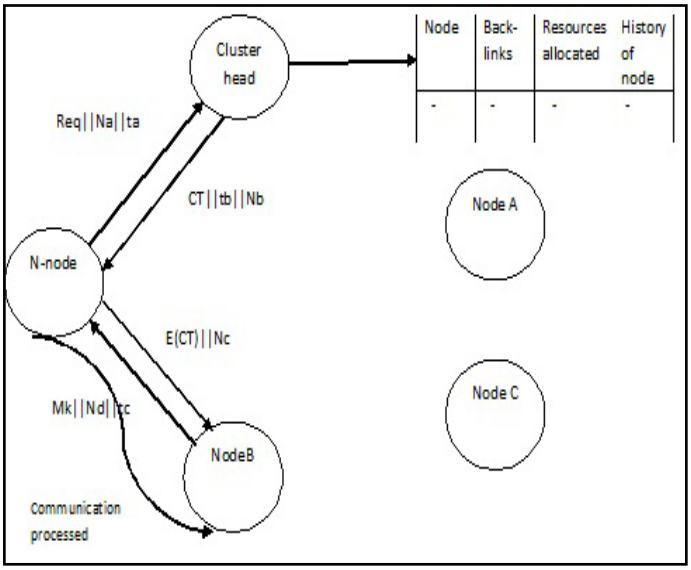

Fig. 2: Authentication Procedure

In this way no new node can communicate without the permission of Cluster Head and the permission of the member node.

1. Algorithm

The proposed algorithm is classified in two phases as described below-

2. Node Authentication

When a new node wants to join the cluster, it requests for a token that will allow the node to communicate with other member nodes. The criteria for its allocation are the dynamic generation of the ticket for cluster member communication. When a new node gathers the valid ticket it is then allowed to communicate with the members of the cluster. To make this procedure more authentic we have introduced the concept of asymmetric encryption. This scheme allows the new node to exchange data with the cluster member by using private member key exchanged with the ticket of new node. Thus making communication secure.

3. Malicious Check

In this phase we have planned to improve the security of the cluster node by checking the back links of the incoming new node which will guarantee the authentic behavior of the node. After this if the node is found valid (the criterion is satisfied), it is allowed to join the cluster. This ensures certain amount of security element in our proposed work.

Cluster Head Token (Tk), Cluster Member Key (MEM_Key), No. of times token is requested =k(k=no. of new nodes), n=total nodes in the cluster, CH=cluster head.

(i). Node_ Authenticate

```
{
n= no. of new nodes;
k=0;
mem=member nodes;
t=0;                                    //lifetime of token
while(k<4)
{
N_Node = cluster;
for(t=0;t<4;t++)
{
  Generate Ticket=Tk;
 If(tk==1)
   {
      N_node=Mem_key;
       exchange of data takes place;
    }
  else
   {
    place request;
}
}
k++;
}
}
```

(ii). Malicious_Check();

```
{
   N-Node=n;
  No. of back links=x;
 Trusted link value=g;
 If(x>g)
{
  CH=N_Node;                    // accept the new node(N_Node);
}
else
{
 CH=0;                          // reject the new node(N_Node);
}
return;
}
```

IV. Conclusion

This paper proposes a mechanism for conflict free address allocation in MANET. So address confliction is not possible, because each node has a specific range of address blocks. We also discuss about the security of MANET by using asymmetric encryption technique by which any malicious node cannot enter in cluster that enhances the security of MANET.

References

[1] Mobile Ad-hoc Networks (MANET), [Online] Available: http:// www.ietf.org/html.charters/manet-charter.hml

[2] M. Mohsin, R. Prakash,"IP Address Assignment in a Mobile Ad Hoc Network", Proc. IEEE MILCOM 2002, Anaheim, CA, Oct. 2002.

[3] C K Toh,"Ad-Hoc Mobile Wireless Networks", Prentice Hall Publishers isbn=0130078174), 2002.

[4] N. H. Vaidya,"Weak Duplicate Address Detection in Mobile Ad Hoc Networks", Proc. ACM Mobi Hoc 2002, Lausanne, Switzerland, June 2002, pp. 206–16.

[5] Mansi Thoppian, Ravi Prakash,"A Distributed Protocol for Dynamic AddressAssignment in Mobile Ad-Hoc Networks".

[6] Cisco,"Duplicate MAC addresses on Cisco 3600 series", May 1997, [Online] Available: http://www.cisco.com/warp/public/770/7.html

[7] S. Nesargi, R. Prakash,"MANETconf: Confi guration of Hosts in a Mobile Ad Hoc Network", Proceedings of INFOCOM 2002, 2002.

Avinav Pathak is pursuing his M.Tech in Computer Science from IIMT Engineering College, Meerut. He has received his Bachelor's degree in Computer Science and Engineering with Honors from Vidya College of Engineering (UPTU), Meerut. He is working as Assistant professor in IIMT Institute of Engineering and Technology, Meerut. He has been a keen researcher in his field and has published various research papers in reputed journals. He has also attended seminars and workshops on current technologies nationally.

Anju Shukla received her Master in Computer science from Shobhit University, Meerut in 2012 and, Bachelor in Information Technology from Uttar Pradesh Technical University (UPTU) in 2009. She has done Post Graduate Diploma in Software Development from International Institute of Information Technology (IIIT) Bengaluru in 2010. She is working as Assistant Professor in IIMT Institute of Engineering & Technology, Meerut and teaching undergraduate students. She has attended several seminars, workshops and conferences and, published several research papers in Conferences and Journals of repute.

Akash Sharma received his Master's degree in Information Technology from Karnataka State Open University in 2011 and Bachelors degree in Computer Science and Engineering from MIET, Meerut (UPTU) in 2002. He is working as Assistant Professor in IIMT Institute of Engineering and Technology, Meerut and teaching undergraduate students. He has attended national seminars on various upcoming technological trends and is keen researcher in his field.