Result Analysis of Virtual IP Address Configuration Protocol

Satinder Kaur
M.Tech Student
Amritsar College of Engineering & Technology, Amritsar, Punjab-India-143001

Tanu Preet Singh
Associate Professor, Dept. of CSE
Amritsar College of Engineering & Technology, Amritsar, Punjab-India-143001

ABSTRACT
Mobile ad-hoc networks are known to make as their own network without any defined infrastructure. They can be rapidly vanished and rebuild again. There are some set of applications for MANETs which are diverse, ranging from small static networks that are constrained with the sources of power, large scale mobile, and highly dynamic nature networks. The great success in the working of mobile adhoc network varies on the cooperation of nodes for providing best services to the other nodes. Since mobile ad hoc networks make it possible for the devices to join or leave the domain without required permission, node in the domain cannot considered to be trusted Conventional security approaches do not address all concerns of ad hoc networks since both benign and malicious parties have full admission to communicate with peers. The wireless channel is accessible to both legitimate network users and malicious attackers. Attackers may intrude into the network through the subverted nodes. In spite of the dynamic nature, mobile users can use this network for anytime, anywhere services as a security purpose and as they are in motion from one place to another.

In this research work, there are two techniques which are implemented: Generation of IP addresses virtually and Allocation of IP address virtually. In these techniques, research is based on implementation of virtual IP address on basis of above discussed algorithms. The technique proposes the methodology of allowing to generation and allocation of IP address virtually. The simulation results have demonstrated some important characteristic. This technique decreases the number of computations which are used in table i.e. every time there is no need to check from the table that whether this address is already allocated or not.

Index terms
IPv6; Foreign Agent; Home Agent; Mobile IP; Virtual IP.

1. INTRODUCTION

A MANET can be flexibly and simply deployed in almost adjustable with any kind of environment, but it has limited wireless connectivity and limited coverage to the MANET boundary. The growth of the Internet, its applications and services and the trends towards the fourth generation wireless network towards all IP based networks which results to the led of an increasing demand for activating mobile nodes which is connected to the internet and its uses of services and applications. Mobile IP protocols and IP micro mobility protocols activate the mobile nodes to access the Internet and change its access point without the lost of any connection. The mobile node should be in the coverage range of the access point and these nodes should have direct connection with that access point. So, with the cooperation between MANET routing protocols and the IP mobility protocol and connectivity with Internet to MANET nodes can be achieved. There are many solutions have been obtained by the researchers to enable the mobility with the use of IP addresses.

1.1 Mobile IP

As below Figure 1 show, the environment in the mobile IP, a mobile router or host can change its point of connection from subnet to subnet. If a mobile host is far from home when a corresponding Internet host sends an IP datagram for delivery to the mobile host's home network, the datagram will be forwarded or tunneled to the host's current foreign network. The home agent will encapsulate that datagram with an IP header with either the IP address of foreign agent's or the mobile host's collocated care-of address. In the implementation of that, the foreign agent de-encapsulates that datagram and forwards it to the mobile host. If the care-of address is already used, the mobile host will act as the endpoint of the tunnel and will do encapsulation locally. foreign agent and Home and agents advertise their services by periodically sending out Agent_Advertisement messages each other. A mobile host can send out an Agent_Solicitation message to look for local agents. With time to time, a mobile host must register the current care-of address with its home agent.

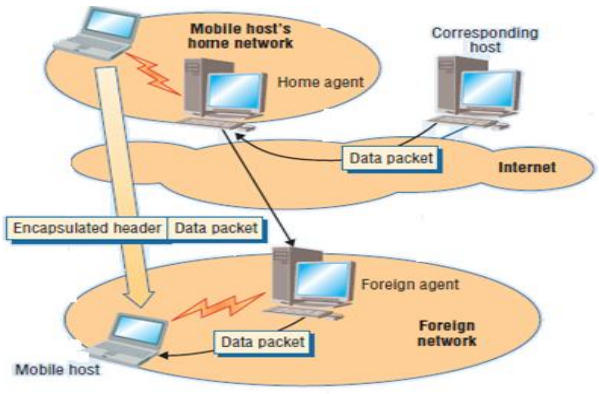


Figure 1 Environment of Mobile IP

The home agent keeps track of the configuring between care-of address and each residential mobile host's permanent addresses in a location dictionary. Other mobile IP extensions include smooth handoff [3] and an extension for IPv6[4]. In a Manet network, mobile hosts communicate with one another. A routing path consists of a sequence of wireless links that do not pass base stations. In this multihop configuration, each host of the mobile serves as a router. Manet routing protocols can be

classified as reactive and proactive. A proactive protocol are as the destination-sequenced distance-vector (DSDV) protocol[5] constantly updates routing information to maintain a near-global view of the network topology. In contrast, reactive protocols are as dynamic source routing (DSR),[6] the zone routing protocol (ZRP),[7] the constant bit-rate (CBR) protocol, and ad hoc on-demand distance vector (AODV) routing conduct on-demand searches for a path. This approach is less costly than a proactive protocol when there is high host mobility.

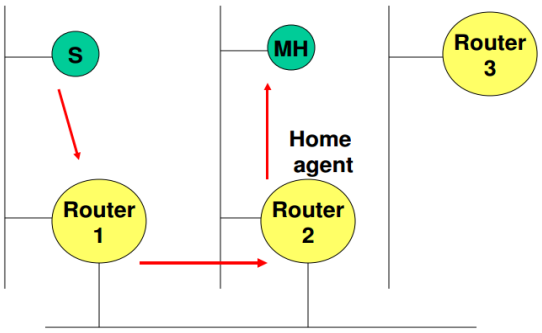


Figure 2 Communication between home agent and mobile host

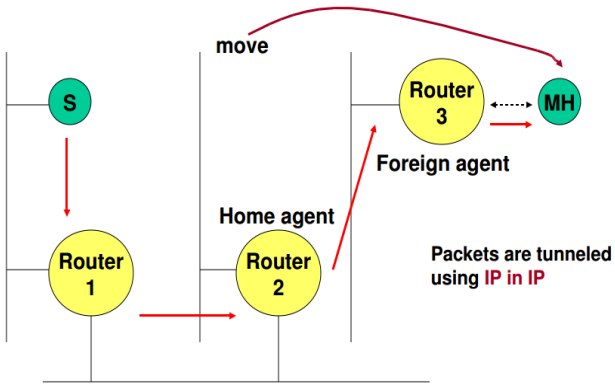


Figure 3 Communication between home agent, foreign agent and mobile host

2. COMPARISON BETWEEN IBA, RBA AND VBA

2.1. In ID based Auto configuration IBA, the IPv6 unicast address inherits from each IP address and it embed in 64bits Interface ID. The name of a node can be identified from its IP address. Every node except the leader node has two IPv6 multicast addresses because they automatically become a member of upper level node group and lower level node group. This information automatically or manually inputs to the node that considers as a PDA. IBA has at least a naming server in MANET, e.g. email addresses, SIP (Session Initiation Protocol) user names or site names such as 128-bits IP-addresses. The leader node works as a naming server.

Network Initialization of IBA. This mechanism is based on the fact in which the naming server knows whole IP address and name of all nodes. In order to collect that information on the naming server, initially every node except the leader node has to register its IPv6 address and name to the naming server. Each node sends a REGISTRARION REQUEST message to the naming server and it starts a REPLY TIMER after RANDOM BACK OFF to set waiting time in distributed ways among nodes. Its period is determined as a time value located between MIN-BACK OFF and MAX_BACKOFF. When the naming server receives REGISTRATION REQUEST message from a node, it transmits REPLY message to the sending node. During a REPLY TIMER period, if the node fails to receive a REPLY message from the naming sever, the REGISTRATION REQUEST message will send again and do REPLY TIMER reset. Above procedures repeat until that transaction is success or the number of retransmission of REGISTRATION REQUEST message goes to THRESHOLD TIMES.

Table 1 IP Addresses and Name Table of Name Server

Name	Parent Name	Level	IP Address(U)	IP address (M)
B1-0	UNDEFINED	0	FE80::ID_{B1}	F200::B1-0
C1-0	B1-0	1	FE80::ID_{C1}	F200::B1-0,F200::C1-0
C2-0	B1-0	1	FE80::ID_{C2}	F200::B1-0,F200::C2-0
C3-0	B1-0	1	FE80::ID_{C3}	F200::B1-0,F200::C3-0
C4-0	B1-0	1	FE80::ID_{C4}	F200::B1-0,F200::C4-0
. . .	. . .	. . .	. . .	. . .

2.2. In Role Based Autoconfiguration RBA, The most different feature from IBA is that there is no naming server in this protocol. It means that every leader node is in charge of managing IP address of lower level nodes. This information automatically or manually inputs to the node that considers as a PDA. The group ID in IPv6 multicast address is from node's Interface ID. Every node except the leader node has two IPv6 multicast addresses because they automatically become a member of upper level node group and lower level node group.

Network Initialization of RBA. Every node of a sends REGISTRATION REQUEST message to the upper level node and starts REPLY TIMER after RANDOM BACK OFF time between MIN BACK OFF time and MAX_BACK_OFF time. When the timer expires, REGISTRATION REQUEST message sends again and reset REPLY TIMER until the number of retransmission of REGISTRATION REQUEST message goes to THRESHOLD TIMES. When a node receives REGISTRATION REQUEST message from lower level nodes, then it becomes ready to send a VERIFICATION messages for synchronization. After that, it sends a REPLY message to the sender node.

Table 2 IP Addresses and Name of the leader Node

Node	Relation	Level	IP Address (U)	IP Address (M)
UNDE FINED	Parent	UNDE FINED	UNDEFINED	UNDEFINED
11000	Child	1	FE80::11000	F200::10000,F200::11000
12000	Child	1	FE80::12000	F200::10000,F200::12000
13000	Child	1	FE80::13000	F200::10000,F200::13000
14000	Child	1	FE80::14000	F200::10000,F200::14000

2.3. Virtual ID Based Auto configuration: In the IP-based network, the assignment of IP address to mobile devices or the mobile nodes is the most important parameter of network configuration. A mobile device cannot participate in communications which is unicast until it is assigned a free IP address and the corresponding subnet mask. One of the most important resources is the set of IP addresses that are assigned to the network. When a new node wants to join a network, it has to be assigned an IP address as part of its initialization. For assigning an IP address to nodes one should meet the following requirements:

1. There should be no conflict in IP address assignment, i.e., at any given instant of time there should not be two or more nodes with the same IP address.
2. An IP address is assigned only for the duration the node stays in the network. When the node activate in the network and communicate with the other node, its IP address should become available for assignment to other nodes.
3. A node should be denied an IP address only when the whole network has run out of its available IP addresses. In other words, if any of the nodes has a free IP address, this address should be assigned to the requesting node.
4. The protocol should handle network partitioning and merging. When two different partitions merge, there is a possibility that two or more nodes have the same IP address. Such duplicate addresses should be detected and resolved.

5.The protocol should make sure that only authorized nodes are configured and granted access to network resources.

In Virtual ID Based Autoconfiguration, whenever a node needs a IP address, it will generate an IP address virtually and allocate that IP address to the particular nodes. I have removed the concept of dynamic allocation of IP address. In dynamic allocation of IP address whenever node needs an IP address, while allocating an IP address to that particular node firstly it has to be checked that whether this IP address is already allocated or not. If it is already allocated it can be replaced with some other IP address. This process also maintains a table for storing the IP address when there are multiple IP addresses to single node and every time it is checked from the table whether this IP address is in the table or not, if it is in the table it means it is already allocated and some other objects has to be chosen. So if come to this research work it is totally based on virtual generation and allocation of IP address. Every time whenever node needs an IP address It will generate an IP address which is not already generated and allocate that IP address virtually to the mobile nodes

Table 3 Comparison between IBA, RBA and VBA

Parameters	IBA	RBA	Current Approach(VBA)
Latency	Low	Medium	Minimum
Failure Ratio	Less	Moderate	Minimum(fluctuations)
Join Ratio	Less	Moderate	Less
Network Size	All types	All types	All types with optimization

3. ALGORITHM FOR GENERATING MOBILE IP IN VBA

3.1 Algorithm:

Step A: while node_ traversed(true)

1. *Maintain routing_table(RREQ,RREP's)*
2. *Maintain list of home IP's (i.e. permanent IP).*
3. *Maintain on load IP's (i.e. temporary IP).*
4. *check_conflict()*

End of step A loop

```
check_conflict()
{
    If node_path<IP(true)
    {
    generate new_IP()
    }
    else
    {
check IP_match()
transmit_exit()
    }
    }

    node_path_IP(Boolean)
    {
If(node_id(i)_IP == node_id(i+1)_IP)
            {
            generate_new_IP()
            }
            Else
            {
            Transmit data()
            }
}

Generate_new_IP()
{
```

1. *found network class*
2. *check of allocated IP's*
3. *count= lost IP generated*
4. *new IP=count(lost)*
5. *allocate IP*
6. *exit*

}

4. SIMULATION RESULTS

The Simulation Analysis for generating IP address are as follows:

Basically every node has its own IP address. While sending data if any node has conflict of same IP address it will resolve that conflict and remap that IP address. In figure 4, it shows that conflict arise in NODE2 to NODE 4 i.e. both nodes has same IP address

The Concept behind this is that every node has two IP addresses one is Home IP's which is permanent and other one is load IP's which is temporary so this approach is working on this temporary IP whenever any received conflicts i.e. if more than one node has same IP address, It automatically generates new IP address so that node can communicate easily with the other node. The main advantage of this researched work is that it did not need to maintain any table to store the IP addresses as compare to the ID Based Autoconfiguration (IBA) and Role Based Autoconfiguration (RBA).So by doing this it saves lot of time. Below are the snapshots of arising conflicts between nodes and remapping new IP address.

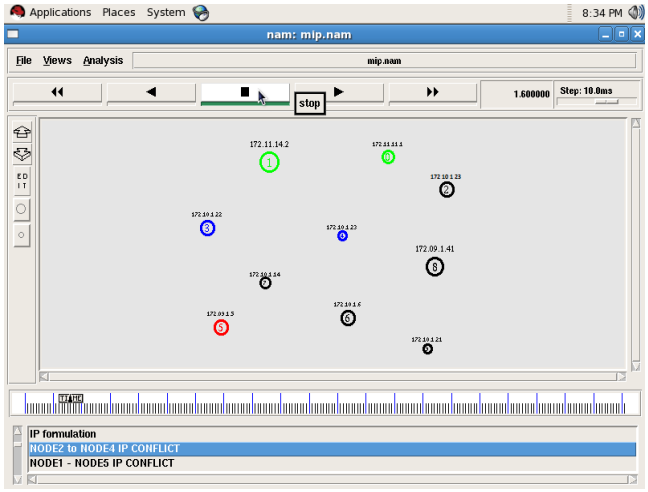


Figure 4 Conflicts arise between node 2 and node 4

In Figure 5 It shows the remapping of IP address and resolving conflicts between node 2 and node.

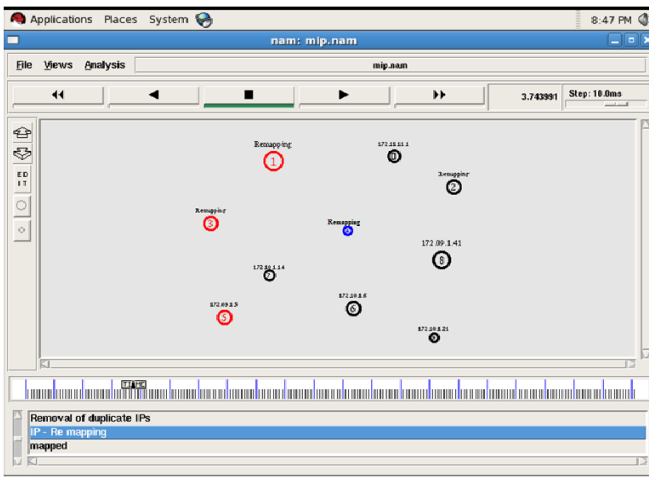


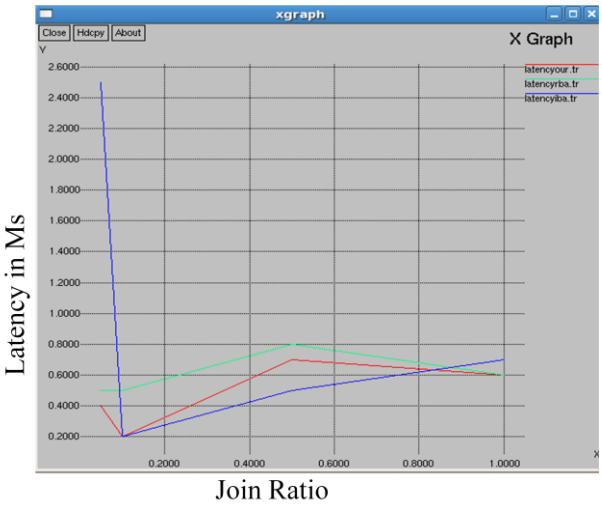
Figure 5 Remapped IP address

Figure 6 shows the removal of duplicate IP address and mapping the new IP address

Figure 6 Allocation of new IP address

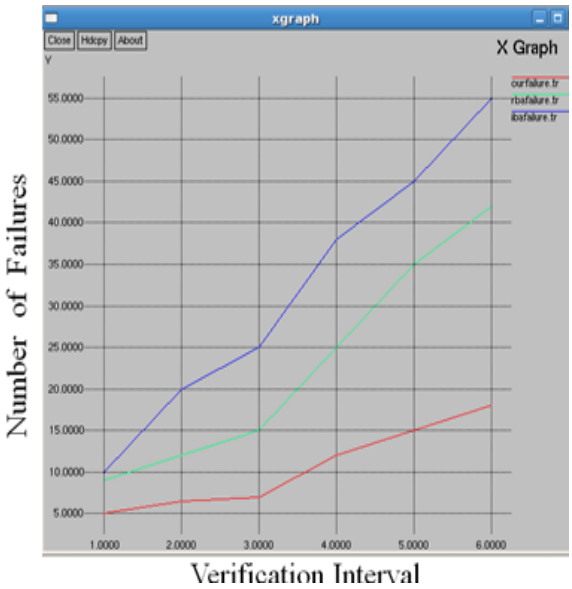
The Performances of these nodes can be checked with the help of following parameters. These Parameters are : Latency, Node Failure Ratio, Join Ratio and Network size. The graphs of these parameters with comparison with previous one are as follows:

4.1. Latency: In a network, latency, or it can be say delay, is an expression of how much time it takes for a packet of data to get from one designated point to another. In the Graph 1, it shows that how much time is taken in this approach and previous approaches to send the packets from one node to another.



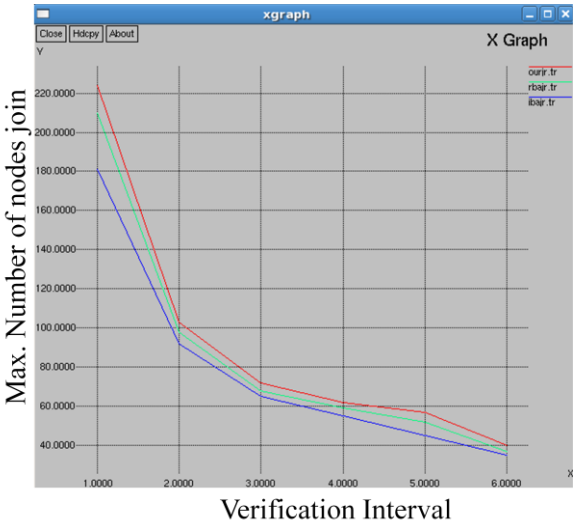
Graph 1 shows Latency Value of current and previous approach

4.2. Node Failure Ratio: In the node failure Ratio, it defines how many nodes fails to send packet from one to another or in other words say how many nodes fails due to some technical reason in the network. In the graph 2, it shows that node failure ratio of this approach and the previous approaches.



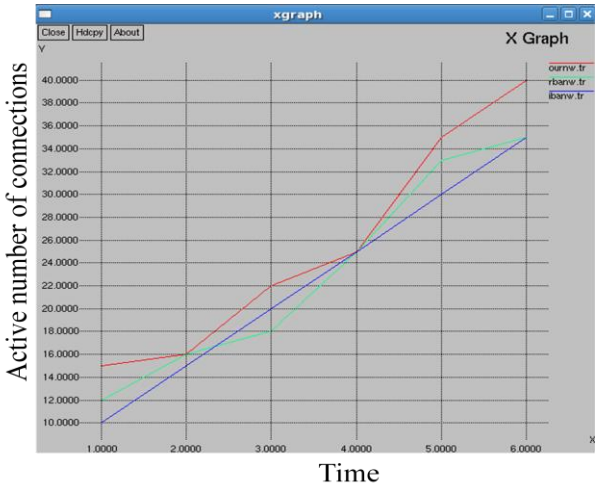
Graph 2 shows Node Failure Ratio of current and previous approach

4.3. Join Ratio: Node Join Ratio means that how many nodes want to join in the network or how many nodes have joined with the other nodes. The more the number of nodes joined with the other nodes in the network, more communication will happen in the network. Graph 3 shows joining of nodes in this approach with the previous ones.



Graph 3 shows Join Ratio of current and previous approach

4.4. Network Size: Network size depends on the number of nodes join in the network. Graph 4 shows the active number of connections with time.



Graph 4 shows Network Size of cuurent and previous approach

5. CONCLUSION

Mobile IP generation is weak in terms of algorithmic approach, thus, making it an over head task that takes large computations in terms of generating IP. In this research work, there are two techniques which are to be implemented: Generation of IP addresses virtually and Allocation of IP address virtually. In this research work it has been implemented virtual IP address on basis of above discussed algorithms. The technique proposes the methodology of allowing to generation and allocation of IP address virtually. The simulation results have demonstrated some important characteristic. This technique decreases the number of computations which are used in table i.e. every time there is no need to check from the table that whether this address is already allocated or not.

This technique also helps to decrease latency time, delays and number of overheads. Number of resources can also be shared easily if anybody are using virtual mobile nodes. And it also helps to less wastage of memory while allocating mobile IP. While doing this it will increase the quality of service for sending data from one node to another and less ratio of packet loss. The overall conclusion is that allocation of virtual mobile IP, is best choice to allocate IP address to the mobile nodes on a network to achieve Quality of Service (QoS) and less loss of packets .There has been improvement in terms of network overheads as overheads decreased with implementation of virtual Mobile IP with AODV that further optimize the performance of network structure.

6. FUTURE WORK

Using virtual mobile IP improves the overall performance of transfer of data in the network therefore it is recommended to use in several areas of research areas which are neglected due to time constrained. Further research in this area of Mobile IP could be explored. The work reports in this research are limited to mobile IP.

In Future, work can be done regarding routing on basis of secure automatic IP identification, generation and allocation. IP identification also increases the reliability in the area of secure connections. As Future work can also be carried to optimize the network by carrying packet monitoring that will evaluate number of nodes joining and leaving the particular group.

This is can also be in future that spoofing can be done while allocating the IP address.

7. REFERNCES

[1] Suman Deswal and Sukhbir Singh," Implementation of Routing Security Aspects in AODV", International Journal of Computer Theory and Engineering. Vol. 2, No. 1, February, 2010.

[2] A Rajaram, Dr.S.Palaniswami." Detecting Malicious Node in MANET Using Trust Based Cross-Layer Security Protocol" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2), 2010.

[3] C.E. Perkins and K-Y. Wang, "Optimized Smooth Handoffs in Mobile IP," Proc. 4th IEEE Symp. Computers and Communications (ISCC 99), IEEE CS Press, 1999, pp. 340-346.

[4] C.E. Perkins and D.B. Johnson, "Mobility support in IPv6," Proc. 2nd Ann. Int'l Conf. Mobile Computing and Networking (Mobicom 96), ACM Press, 1996, pp. 27-37.

[5] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination- Sequenced Distance-Vector (DSDV) Routing for Mobile Computers," Proc. ACM SIGCOMM '94 Conf. Communications Architectures, Protocols and Applications, ACM Press, 1994, pp. 234-244.

[6] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, C.E. Perkins, ed., Addison-Wesley, 2000, pp. 139- 172.

[7] Z.J. Haas and M.R. Pearlman, "ZRP: A Hybrid Framework for Routing in Ad Hoc Networks," Ad Hoc Networking, C.E. Perkins, ed., Addison-Wesley,2000, pp. 221-253.

[8] K. Weniger, "Passive duplicate address detection in mobile ad hoc networks," in IEEE WCNC, (Florence, Italy), February 2003.

[9] Thoppian, M. R.; Prakash R.;, "A distributed protocol for dynamic address assignment in mobile ad hoc networks,"Mobile Computing, IEEE Transactions on , vol.5, no.1, pp. 4-19, Jan. 2006

[10] Ghosh, A.; Talpade R; Elaoud M.; Bereschinsky M.;, "Securing ad-hoc networks using IPsec," Military Communications Conference, 2005. MILCOM 2005. IEEE , vol., no., pp.2948- 2953 Vol. 5, Oct. 2005

[11] Jung, Y.C.; Peradilla M.;, "Tunnel Gateway Satisfying Mobility and Security Requirements of Mobile and IP-Based Networks," Journal of Communications and Networks, vol. 13, no. 6, pp. 583-590, Dec. 2011

[12] C.E.Perkins, J.T. Malinen, R.Wakikawa, E.M.Belding-Royer and Y.Sun,"IP Address Autoconfiguration for Ad Hoc Networks, draft-ietfmanetautoconf- 01.txt," Internet Engineering Task Force, MANETWorking Group, July 2000.

[13] N.H.Vaidya, "Weak duplicate address detection in mobile ad hoc networks", tech. rep., University of Illinois at Urbana-Champaign, January 2002.

[14] K.Weniger, "Passive Duplicate Address Detection in Mobile Ad Hoc Networks", in Proc. of IEEE WCNC 2003, New Orleans, USA, March 2003.

[15] S.Nesargi and R.Prakash, "MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network," in Proceedings of IEEE INFOCOM, volume 2, pages 23-27, New York, USA, June 2002.

[16] M.Mohsin and R.Prakash, "IP Address Assignment in a Mobile Ad Hoc Network," in Proceedings of Military Communications Conference (MILCOM 2002), volume 2, pages 856-861, Anaheim, California, USA, October 2002.

[17] J.P.Sheu, S.H.Tu and L.H.Chan, "A Distributed IP Address Assignment Scheme for Ad Hoc Networks," in Proceedings of the 2005 11th International Conference on Parallel and Distributed Systems (ICPADS'05), volume 1, pages 439-445 Vol. 1, July 2005.

[18] R. Droms. Dynamic host configuration protocol. RFC 1531,Oct. 1993.

[19] S. Thomson and T. Narten. IPv6 stateless address autoconfiguration. RFC 2642, Dec. 1998.

[20] S. Cheshire, B. Aboba, and E. Guttman. Dynamic configuration of link-local IPv4 addresses. Internet Draft: draftietf-zeroconf-ipv4-linklocal-13.txt, Feb. 2004.

[21] M. Mohsin and R. Prakash. IP address assignment in a MANET. In IEEE Milcom, Anaheim, California, USA,2002.

[22] S. Nesargi and R. Prakash. MANETconf configuration of hosts in a MANET. In IEEE Infocom, New York, USA, 2002.

[23] C. Perkins, J. Malinen, R.Wakikawa, E. Belding-Royer, and Y. Sun. IP address autoconfiguration for ad hoc networks. Internet Draft: draft-ietf-manet-autoconf-01.txt, Nov. 2001.

[24] C. E. Perkins, J. T. Malinen, R. Wakikawa, E. Belding-Royer, and Y. Sun. IP address autoconfiguration for ad hoc networks. IETF Internet Draft, draft-ietf-manet-autoconf-01.txt, Nov. 2001.

[25] C. E. Perkins, E. M. Royer, and S. R. Das. Ad hoc ondemand distance vector (AODV) routing. draft-ietf-manetaodv- 06.txt, July 2000.