ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 6, August 2012

ROBUST AND FLEXIBLE IP ADDRESSING FOR MOBILE AD-HOC NETWORK

Pankaj Kumar, Vinod Kumar Mishra, Poonam Rautela
Department of Computer Science & Engineering,
B. T. Kumaon Institute of Technology,
Dwarahat, Almora, (Uttrakhand), INDIA

***Abstract*-Mobile Ad hoc Networks (MANETs) are expected to become more and more important in the upcoming years. In order to enable the establishment of IP services in MANets, IP address auto configuration mechanisms are required. In this paper, we review the existing solutions to interconnect MANETs, but find them lacking in robustness and flexibility. In a wired network, layer three address assignments is a task that is mostly performed by dynamic Host Configuration Protocol (DHCP), an easy to manage centralized network component that can be reaching by every node of the network by simply speaking or hearing through the wired media. In mobile ad hoc networks (MANETs) the wireless media infrastructure is a changing and dynamic environment where we cannot assure that every mobile node will be connected at a given time neither predict the topology or size of the network. IP address assignment is a difficult task in MANETs, in recent years several approaches have been proposed to solve this task, here we will present a review of them and discuss the main features of their solutions.**

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a self-organizing network of mobile hosts connected by wireless links. The mobile nodes are free to move to and fro and organize themselves randomly. The topology remains uncertain through the routing. In MANETs the wireless media infrastructure is a changing and dynamic environment where we cannot assure that every mobile node will be connected at a given time neither predict the topology or size of the network [1]. On the other hand, as soon as a node joins a MANET, it becomes part of the routing mechanism to exchange messages and performs actively routing tasks; hence there is not a sense of sub netting like in infrastructure network. For this reasons, IP address assignment is a challenge in MANETs. Traditionally, a user cans either configure the address of a host manually or the host can acquire its IP address dynamically through certain active addressing methods, such as, Dynamic Host Configuration Protocol (DHCP) [2]. Manual address configuration in most cases is inapplicable to MANET as it is a distributed type of network, and when it grows it is very difficult to manage all the used and unused IP addresses in the network. For unicast communication, each node should have a unique address. Therefore, it is required to distribute IP addresses uniquely and keep all the used and unused IP addresses in the network in a distributed manner [3]. Further, a node in a MANET is free to leave the network at any time. Therefore, it is also required to monitor the network so that the IP address of the departed node can used by others. As MANET is dynamic in nature, the network may get partitioned at any time and may also merge at a later time. Therefore, manual configuration may lead to contradiction of address, which may not be detected and also cannot be resolved. DHCP requires the presence of a centralized DHCP server which maintains the configuration information of all hosts in the network [3]. Since a MANET is devoid of any fixed infrastructure or centralized monitoring, this approach cannot be used.

II. RELATED WORK

For assigning an IP address, a standard IP addressing protocol should have the following objectives: -

Dynamic IP Address Configuration: Manual or static address configuration in most cases is inapplicable to MANETs. Due to unpredictable nature and dynamic topology of MANET the Dynamic Host Configuration Protocol (DHCP) is also inapplicable. Moreover, DHCP requires centralized administration. Therefore, a node should obtain an IP address from MANET dynamically.

Uniqueness: For correct routing and unicast communication, a node should have a unique IP address in the MANET. At any instant of time, there should not be more than one node with the same IP address in the network.

Robustness: MANET is highly dynamic and unpredictable in nature. Due to this, MANET may partition into several subnets and the partitions may combine later. Then there is a chance of address conflicts of the nodes in the network. The addressing protocol should resolve this address conflicts and also adapt the network partitions and merges.

Scalability: As the number of node increases in the network, the time taken to obtain an IP address or number of packet exchange during address allocation may increase exponentially. This is due to the fact that whenever a node intends to join a MANET, it sends one hop broadcast message to its nearby nodes. A node which is already in the MANET, after receiving this message, floods it throughout the network [4]. Therefore, if the total number of nodes in the network is n, then each node sends (n-1) messages and receives (n-1) messages in case joining of a new node. Therefore, communication complexity due to flooding is O ((n-1)*(n-1)), that is O (n^2) [1], [4]. Thus, the addressing scheme should not degrade its performance significantly as the number of nodes increases in the network.

Security: Without authentication, several types of security threats can be seen at the time of address allocation. Therefore, security is also a prime concern for the address allocation protocol of a MANET.

The major security threats [4] associated with dynamic IP address configuration in MANET are as follows: In *Address Spoofing Attack*, an IP address of a host can be spoofed by a malicious host to hijack the network traffic. *Address Exhaustion Attack:* an attacker may claim as many IP addresses as possible for exhausting all valid IP addresses to prevent a newly arrived host from getting an IP address. False *Address Conflict Attack:* an attacker may transmit address conflict messages falsely so that victim host may give up its current address and seek a new one. *False Deny Message Attack:* an attacker may continuously transmit false deny messages to prevent a newly arrived host from getting an IP address. In the paper, U.Gosh & Raja [1] proposed an ID based secure distributed dynamic IP configuration scheme for address allocation which do not require the need for broadcasting messages over the entire MANET during the address assignment process. With the help of the proposed scheme, each host in the MANET can generate a unique IP address for a new authorized host. It also generates a node ID (node_id) as a node identifier, which is evaluated using its IP address and also a public key. Thus, a node can be identified by the unique tuple node_id, IP addressing [3], [4], which adds a node authentication feature in addition to identification. The proposed scheme gives an improved solution to the problems that may arise due to host failures, message losses, mobility of the hosts and network partitioning/ merging.

III. Present approaches

In this section we present the address allocation agent based Addressing of mobile multi-hop ad-hoc networks. The goal was to develop a fast and reliable addressing scheme for ad-hoc networks. To achieve this target, the following requirements were identified

Unique: all client nodes of an ad-hoc network should get unique IP-addresses.

Simple: The addressing should be performable by each and every node. A node performing addressing service is called Address-allocation-agent (AAA).

Multi-hop: if there is any node is not reachable that node can access address using neighbor node. The addressing of nodes, those cannot reach the address-allocation-agent directly, must be possible.

Robust: Against network partitioning and merging of ad-hoc networks.

Adaptive: the approach shall be able to accommodate to fast topology changes of adhoc networks:

- If no address-allocation-node is present in an adhoc network, one of the nodes has to become the address-allocation-agent.
- If several address-agents are available in an ad-hoc network, the number of the addressing agents should be reduced to one.

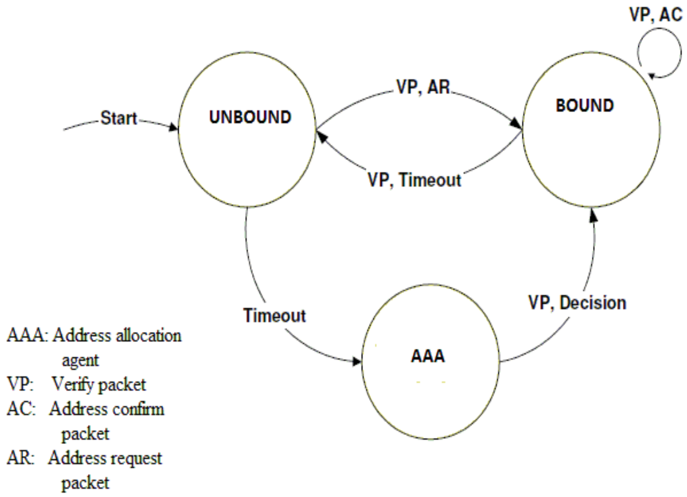

VP, AC
Start
UNBOUND
VP, AR
BOUND
VP, Timeout
Timeout
VP, Decision
AAA
AAA: Address allocation agent
VP: Verify packet
AC: Address confirm packet
AR: Address request packet

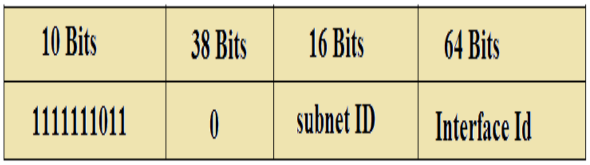
Fig.1 (State graph of a node in address allocation agent Based addressing)

A. State Graph of a Node

A node is in one of three states (see fig 1). After start, a node is in state Unbound, i.e. it does not have a valid address. From this state, the node can switch to two other states. If the ADDRESS_ALLOCATION_AGENT_DISCOVERY timer expires, the node switches to the address-allocation-agent (AAA) state and itself becomes an AAA. Otherwise, if the node receives a Verify-Packet (VP), it responds with an Address-Request (AR) packet; the node switches to the Bound state, i.e. it has a valid IP-address. A node remains in state Bound while it receives Verify-Packets from the AAA and responds with Address-Confirm (AC) packets, and leaves the state bound either by not receiving a Verify-Packet or by not responding to a Verify-Packet. The AAA state is only left if another address-allocation-agent is also present in the ad-hoc network and the node loses the election for AAA.

B. *Address construction*

We propose to use IPv6 site local addresses. Site local addresses are unicast addresses which can be routed within a site. Site local addresses have the following format [5]:



10 Bits	38 Bits	16 Bits	64 Bits
1111111011	0	subnet ID	Interface Id

For us only the subnet ID and the interface ID are interesting. The interface ID is worldwide unique and is derived from the MAC-address, its construction is described in [6]. The subnet ID is specific for an ad-hoc network and it is generated by the address-allocation-agent. The address-allocation-agent generates it from its own MAC-address, so it is also unique. If a node requests an IP address for a certain ad-hoc network, the AAA creates a new IP address, which is derived from its own MAC address and from the MAC-address of the requesting node (see fig 2).

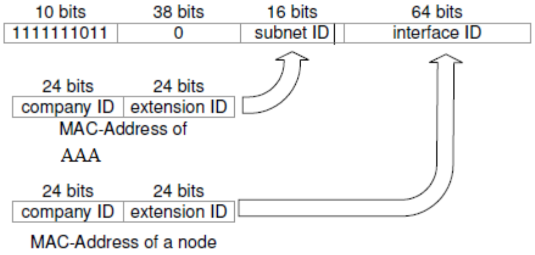


Fig.2 (Address construction)

C. *Addressing of Nodes*

The main component of the address-allocation-Agent-Based Addressing is the AAA, which is responsible for the addressing within an ad-hoc network. The functionality of an AAA can be performed by every node. The AAA maintains an Address-List (AL) of all nodes in the adhoc network. The address-list contains the mapping of MAC-addresses to IP-addresses and further information. The AAA periodically sends Verify-Packets which contain the address list and a time stamp. Every node receiving a Verify-Packet checks whether or not it is included in the address-list. If the node wants to remain in the ad-hoc network it will send an Address-Confirm packet to the AAA. A new node requests an address by sending an Address-Request packet to the address-allocation-agent. A node will be removed from the address-list if the AAA does not receive a packet from the node before the ADDRESS_CONFIRM_ TIMER expires.

D. *Election of the Address-allocation-Agent*

A new node waits ADDRESS ALLOCATION AGENT DISCOVERY time units for a Verify packet. If it does not receive a packet within this time, it assumes that no AAA is available and therefore switches to AAA state. Subsequently it sends a Verify- Packet. If several address-allocation -gents (AAA) exist in an ad-hoc network the number should be reduced to one, i.e. all other address-allocation-agents (AAA) switch to state Bound. This reduces the overhead of the address administration and provides for uniqueness of the addresses. This is performed as follows. If address-allocation-agent AAAk receives a Verify-Packet from another address-allocation-agent (AAA) it computes the number of nodes in its AL and the number of nodes in the received AL. AAAk leaves the AAA-state if the number of nodes in its AL is less than the number of nodes in the received AL. If the numbers of nodes are equal, the decision is based on the MAC-address (network interface ID). The address-allocation-gent with the smaller MAC-address remains the address-allocation-agent and the other node leaves the AAA state.

E. *Addressing of Ad-Hoc Networks*

In this scenario a new ad-hoc network shall be established and therefore all nodes need an address. At the beginning of the simulation none of the nodes has an address. At time t = 0 the address server becomes active and the nodes can request addresses. This is similar to a cold start of a computer farm. One node performs the job of the address server (S), which serves the other nodes (C) (fig3). We discuss two cases:

1. **Single-Level:** all nodes can reach the address server directly; therefore the packets do not need to be relayed. This case is similar to a meeting with few participants in which each

participant uses its notebook. One of the notebooks could perform the job of the address server.

2. Multilevel: not all nodes can reach the address server directly; therefore some packets have to be relayed by intermediate nodes (fig4). Nodes in same level can communicate directly. In some approaches there are special nodes (R) which are responsible for relaying packets between levels.

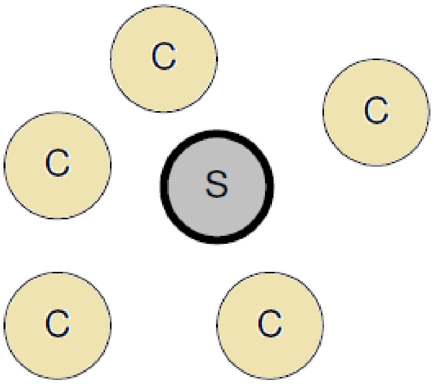


Fig.3 (an adhoc network in which all nodes can reach each other)

We used the both variants of this scenario to investigate the suitability of the approaches for multi-hop ad-hoc networks.

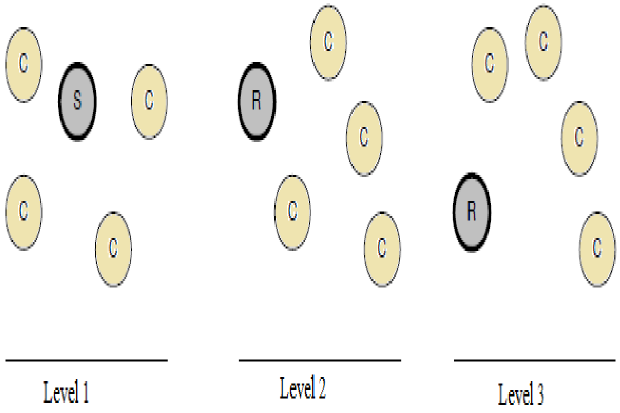


Fig.4 An adhoc network consisting of several levels

F. *Union of Ad-Hoc Networks*

This scenario analysis several adhoc network creating a new compound networks. The nodes of the origin networks move uniformly together until they build only one network (fig 5). In the new network, some of the nodes have to be readdressed. After the integration, only one address server should be active to issue unique addresses. An example for this scenario is given by a meeting of two work groups, which worked alone, but want now discuss together. Both groups create a new big group.

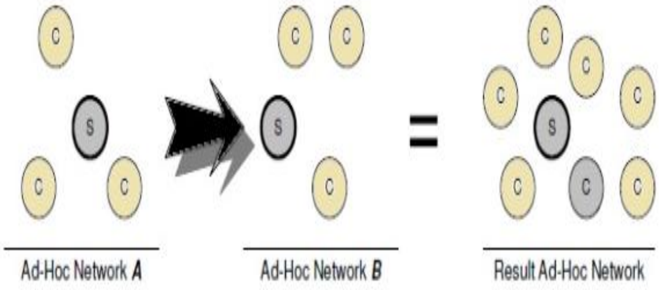


Fig.5 (union of two adhoc networks)

G. *Splitting of Ad-Hoc Networks*

This scenario is the counterpart of the last scenario. One ad-hoc network splits into several smaller ad-hoc networks. Each new network needs its own address server which supports its nodes (fig 6). An example from reality could be the splitting of a work group to several task groups, which have to perform special tasks. We used the both scenarios to investigate the adaptation and robustness of the approaches. We consider sets of ad-hoc networks, which can dynamically build new ad-hoc networks.

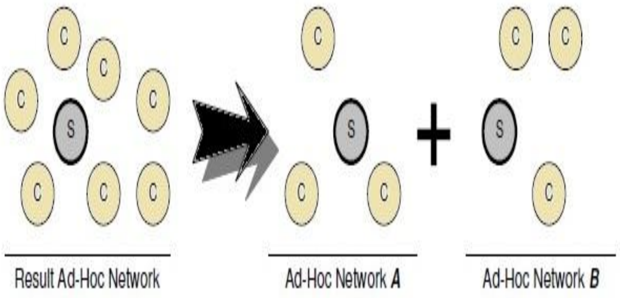


Fig.6 (Splitting of adhoc network)

IV. SIMULATION RESULTS ANALYSIS

In this section we present our simulation results. The discussion of the results is set up similar to the discussion of section 4. The graphs presented are based on the median of 10 simulations.

A. Addressing of an Ad-Hoc Network

The results of this section are based on simulations with up to 50 nodes uniformly distributed among the individual levels. In case of only one level, all nodes are able to communicate directly without multi-hop communication. In case of several levels, only the nodes on the same level can communicate directly. The traffic between two nodes, on different levels has to be relayed by intermediate nodes. We measured the time to address all nodes in a certain ad-hoc network.

B. DHCP

In the simulations with DHCP there are 40 nodes and one DHCP-server. In the cases of several levels there is also a DHCP-relay in each level. Fig 7 shows the results with 1, 2, and 3 levels. To address all 40 nodes of one level, DHCP needs a maximum time of 30 seconds. The time increases with the number of nodes in the network.

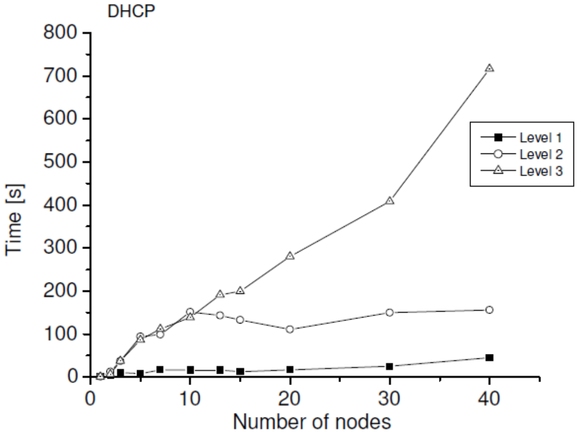


Fig.7 (DHCP address allocation)

The DHCP server has to response to more address requests from the clients.

With 2 levels, the time increases up to 125 seconds. Time increases for up 10 nodes, and then remained stable. The quadruplicating of the time is caused by the DHCP-relay, which appears like a bottleneck. All address queries from the second level are relayed by the DHCP-relay. With 3 levels, the time needed for the addressing increases up to 600 seconds. The repeated quadruplicating of the needed time is caused by the second DHCP relay. DHCP seems to be not adequate for addressing of nodes which are several levels away.

If the DHCP-server rejects an address query of a node, the DHCP-relay is informed, which in turn informs the node. The client has now two possibilities, either it can directly send a new address query, or it re-initializes itself and then sends a new address query.

C. Address-allocation-Agent Based Addressing

In the simulations with the agent-based addressing up to 50 nodes distributed over up to 5 levels were involved. Fig8 shows the results. The time needed for addressing the whole network with up to 3 levels is below 2 seconds. The time for 1 and 2 levels with up to 30 nodes is below 1 second. From the graph it is evident that the time increases up to 2 seconds, if there are more than 30 nodes. This is caused by the increased network load created by flooding. The time for 4 levels is 3-4 seconds. With 5 levels the observation repeats by 4-5 seconds. The times of level 3, 4, and 5 are high at the beginning and become lower. The reason for this is that with fewer nodes only infrequent request packets from the clients reach the address server. With more nodes the phenomenon does not appear and therefore does not affect the performance. From fig8 it is obvious that the time needed for addressing is linear increasing with the number of levels. In the agent-based case there are no central nodes at each level. All nodes are permitted to relay packets. Therefore, packets reach the address server over the shortest path as well as over the longest path. The disadvantage of flooding is here an advantage, because dropped address requests are received after a short time again by the address server. In contrast to DHCP this approach results in a high network load, a disadvantage. But nothing else is transmitted in this phase this is not too severe.

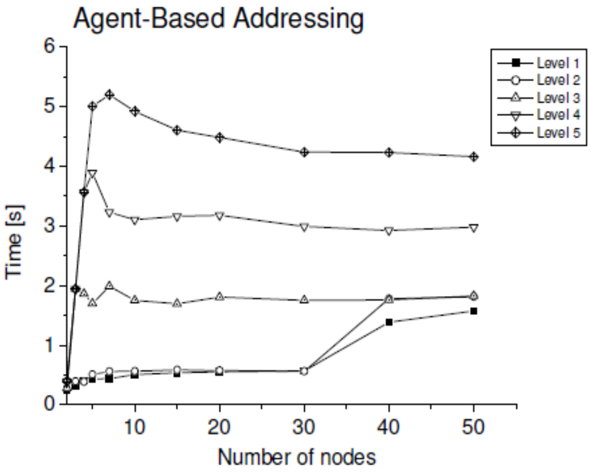


Fig 8 Address-allocation-based addressing (AAA)

V. Brief Summary of the Results

A. DHCP

To deploy DHCP for the addressing of ad-hoc networks, a DHCP-server and if several levels exist one DHCP-relay in each level is needed. According to our results, DHCP is suitable for the addressing of an ad-hoc network with only one level. The performance of DHCP is poor in an ad-hoc network consisting of several levels [7]. DHCP is also not able to recognize the splitting and merging of ad-hoc networks. Additionally the complexity of the DHCP-server and DHCP-client is also a disadvantage.

B. Auto-Configuration

The approach of auto-configuration works fast and reliable. In contrast to the other both techniques, auto-configuration does not need any central node. The chosen addresses are flooded in the network to check if they are occupied [8]. The addressing of ad-hoc networks with auto-configuration is easily realizable. In the current version [8] the approach has several weaknesses, which need fixing. The uniqueness of the used IP-addresses in the whole network is not guaranteed. The addresses are tallied only once, when a new node enters or connected to the network and chooses an IP-address [9]. Furthermore, the approach does not define any mechanisms for the recognition of splitting and merging of ad-hoc networks. A malicious node, which responses to every address query, is able to perform a denial of service attack. In addition, the flooding of the address queries creates very high network load.

C. Address-allocation-Agent (AAA) Based Addressing

The Address-allocation-agent based addressing fulfills the requirements from section 3. It is suitable for addressing of ad-hoc networks, since it solves the problem as fast as reliable. In contrast to the other methods, the address-allocation-agent based addressing is able to recognize the splitting and merging of ad-hoc networks the uniqueness of the used addresses is also guaranteed by the addressing-agent. Furthermore, the approach supports dynamic adaptation of the number of address-allocation-agents. A disadvantage of the approach is the additional load for the addressing.

VI. Conclusions

Mobile ad-hoc networks are highly dynamic because of node mobility, i.e. all nodes are mobile and can move freely. In ad-hoc networks there are no special nodes which are always reachable. Thus, these types of networks need distributed and adaptive solutions. In this paper we presented the Agent-Based addressing, a new dynamic addressing scheme for mobile ad-hoc networks. Furthermore, we evaluated and discussed two other approaches, a well known approach from the literature, DHCP, and a new approach from the current discussion, Auto Configuration. The analysis of all approaches was based on selected scenarios, which reflect typical situations of future ad-hoc networks. The results have shown that current approaches are not well suited for ad-hoc networks, because they do not consider adequately the dynamics of ad-hoc networks. The approach of auto-configuration is very interesting, but the current version has many weaknesses. The Agent-Based addressing fulfills the requirements for a dynamic addressing scheme. The approach is simple, robust, and adaptive. It is also able to recognize the splitting and merging of adhoc networks. This yields higher efficiency, since the overhead is reduced. A weakness of the approach is the additional high network load. Addressing is a very important part of network communication. Thus, this issue needs more research work. Open questions include: scalability, protection against attacks and the reduction of overhead. Furthermore, there is a need for mechanisms to connect ad-hoc networks to the internet. Mobile-IP could play an important role in this area.

References

[1] Uttam Ghosh, Raja Datta “A secure dynamic IP configuration scheme for mobile ad hoc networks”, Ad Hoc Networks, Volume 9 Issue 7, Pages 1327-1342, September, 2011.

[2] R. Droms, Dynamic Host Configuration Protocol, RFC 2131, March 1997.

[3] M. Taghiloo, M. Dehghan, J. Taghiloo, M. Fazio, New approach for address auto-configuration in MANet based on virtual address space mapping (vasm), in: International Conference on Information and Communication Technologies: from Theory to Applications (IEEE ICTTA 2008), Damascus, Syria, 7–11 April 2008.

[4] M. Tajamolian, M. Taghiloo, M. Tajamolian, Lightweight secure IP address auto-configuration based on vasm, in: 2009 International Conference on Advanced Information Networking and Applications Workshops, Waina 2009, pp. 176–180.

[**5**]S. Nesargi, and R. Prakash, Manetconf: Configuration of hosts in a mobile ad hoc network. In Proc. of IEEE INFOCOM 2002, June 2002.

[6] N.H. Vaidya, Weak duplicate address detection in Mobile Ad Hoc Networks, Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc02), June 2002, pp. 206–216.

[7] R. Hinden and S. Deering. IP version 6 addressing architecture, RFC 2373. http://www.ietf.org/rfc/rfc2373.txt, July 1998. IEEE. Guidelines for 64- bit global identifier (eu- 64) registration authority oui/tutorials/EUI64.html, May 2001.

[8] IEEE. Guidelines for 64- bit global identifier (eu-64) Registration authority. http://standards.ieee.org/regauth /oui/tutorials/EUI64.html, May 2001.

[9] Jung-Soo Park, Yong-Jin Kim, and Sung-Woo Park. Stateless address auto configuration in mobile ad hoc networks using site-local address, draft-park-zeroconf-manet-ipv6-00.txt. http://www.ietf.org/internetdrafts/draft-park-zeroconf-manetipv6-00.txt, July 2001.