Fast Mobile Node Configuration Using Address Caching in Hybrid Wireless Network

Wooseong Kim°, YangWoo Ko*, Soojeon Lee* and Taeik Kang°

°LG Electronics, Seoul, Korea, {willie, tikang}@lge.com

*School of Engineering, Taejeon, Korea, {newcat, galgyeon}@icu.ac.kr

Abstract

Many small devices have wireless network interfaces that are used to receive or send data for intelligent services. Devices in pervasive computing environment may embed wireless interfaces for communication. Those devices may compose ad hoc network to communicate with others. Ad hoc network can be built without any infrastructure but it must merge with infrastructure network to let ad hoc nodes access a remote server through the Internet. Several configuration methods for host over ad hoc network without user's consciousness have been suggested so far. If an ad hoc network becomes larger, it will take long time for a newly joining node to configure itself with information from Zeroconf [1] or DHCP [2] server because the request should be transmitted through multiple hops. In this paper, we propose a distributed scheme in which each ad hoc node caches host configuration information temporarily to reduce traffic sent to original (Zeroconf or DHCP) server and to shorten message transaction delay between host and server.

Keywords

Ad-hoc network, Auto configuration.

1. INTRODUCTION

The Mobile nodes can communicate with each other using various wireless technologies in these days. Most of mobile nodes access a base station that allocates a wireless channel and is linked to wired network for transferring data to other segments or the Internet. Each base station has limited radio channels and fixed cell coverage. To improve these limitations of a cellular network, the peer-to-peer wireless communication technique such as ad hoc routing is necessary. Combination of cellular and ad hoc network is called the hybrid network. In a hybrid network, each node can access the Internet while utilizing enlarged network coverage through ad hoc routing.

When joining a new hybrid network, a mobile node should get a new IP address except cases such that IP address block allocated for the new network is same with that of most recently leaving network. To configure its network interface, a mobile node can access a DHCP server usually used in wired network.

There are several automatic host configuration methods, but they are useful only for either a cellular or an ad hoc network. When configuring the network interface of ad hoc nodes, there are several ways to get IP addresses. IETF (Internet Engineering Task Force) Zero conf working group suggests unique address configuration in link layer [4]. IP addresses used for this method are reserved for special purpose by IANA (Internet Assigned Numbers Authority). However when intermediate ad hoc routers partition a network, broadcast for detection of duplicated address allocation is not delivered to other sub networks. Therefore, those addresses are only unique within a single sub network. Some papers suggest IP allocation methods to enhance detection of duplicated address allocation and connectivity in ad hoc network. [6, 7]

A mobile node can get an IP address from a DHCP server usually attached to wired network. It broadcasts a DHCP message to the ad hoc network for address allocation. As the number of nodes increases, transaction time to handle address allocation increases because request and reply packets might be transmitted through multiple intermediate nodes. The overhead of packet flooding for address allocation will increase too. Previously suggested address allocation methods burden the hybrid network with frequent broadcasting packets for duplication detection and configuration.

We suggest a distributed caching mechanism in which each ad hoc node caches information for dynamic host configuration to reduce both delay in configuration and traffic over the network. In Section 2, we introduce related works. Our basic idea is presented in Section 3, and in Section 4, we describe the simulation model used and results from simulation. In section 5 and 6, we include future works and references.

2. RELATED WORK

2.1 Hybrid Network Overview

All We define a hybrid network as a heterogeneous network that is composed of a conventional cellular network and a peer-to-peer network. A conventional cellular network based on 802.11 infrastructure mode, CDMA or GPRS is a single hop wireless network. Each mobile node accesses a base station located at the center of each cell. Base station is fixed within wired network that is linked to the backbone. Cell coverage is limited by radio frequency and or transmission power. Thus many base stations are necessary to cover broad area and to manipulate lots of access requests. Each mobile node contends with others to occupy a radio channel and use network bandwidth of the cell. As the density of mobile nodes in a cell grows up, the probability of call drop and delay increases. Furthermore, mobile nodes also use the infrastructure network when they communicate with others joining in other cells. Especially the density of mobile nodes in a cell is different from the others according to the geographical characteristic and time line. Call drop probability becomes higher in hot spot than in cold spot. Cellular network that supports multi hopping is proposed to solve these problems [9, 10, 11].

Mobile nodes can directly communicate with each other in the form of peer-to-peer such as the ad hoc network. It reduces the traffic in the base station. Furthermore iCAR [10] proposes ad hoc relaying stations which relay the traffic of nodes in a hot spot to a cold spot base station. Therefore the burst traffic of hot spot can be distributed among neighbor cells. This load balance scheme reduces call drop/block probability and network congestion. MADF [11] has a local channel to current base station and a forward channel to a neighbor cell. A mobile node uses the forward channel when the average delay exceeds a threshold value. So cell coverage can be extended by the ad hoc node relay without an additional base station. For example, when Joe leaves a building while using his portable computer, the base station in the building cannot reach his device and connections will be broken. In case of the hybrid network, if another user who has an ad hoc wireless interface is staying in the middle of the base station and Joe, he can receive data through the intermediate ad hoc node using ad hoc routing.

To approach a wireless packet network [12], we analyzed the unique characteristics of each wireless network. Cellular network is better in terms of mobility and location based flow control such as route reservation. Peer-to-peer communication using ad hoc routing shows better performance in terms of delay, power consumption and throughput but it tends to be unfair and vulnerable to node mobility. There is a significant trade-off between the conventional cellular network and the ad hoc network. Therefore the hybrid network can act as a mediator between the cellular and the ad hoc network.

2.2 Mobile Nodes Configuration Method

2.2.1. At Cellular Network

Most of cellular networks use conventional methods such as DHCP [2] for host configuration. It is managed in a centralized way to make administration easier. Normally a base station manages configuration information such as IP addresses in a pool and allocates them to mobile nodes. In case of using a DHCP server, a mobile node requests to the DHCP server individually. A DHCP server designed for wired network also can be used for mobile nodes in a wireless network. First, a mobile node broadcasts a DHCP DISCOVERY message to search an available DHCP server in a sub network. The DHCP server receives DISCOVERY messages from clients and responses with OFFER messages that include configuration parameters. Then the mobile node selects one of the OFFER messages that have arrived. Secondly, the mobile node as a DHCP client sends a DHCP REQUEST message for address allocation to the DHCP server and receives ACK or NACK message from the server. When the mobile node moves to another sub network, it broadcasts a DHCP discovery message to the network to initiate configuration. Thirdly, after the mobile node receives an ACK message from the DHCP server, it can configure its network interface, naming server address, default gateway and so on. Normally it checks whether the allocated IP address is duplicated or not. But that procedure can be omitted for reducing the total time of host configuration.

2.2.2. At Ad Hoc Network

MANET [3] is a stand-alone network. So each node has a unique IP address in the network and it can be configured with a private or specific IP address block. Zeroconf IETF working group defines configuration categories such as IP interface configuration, naming, IP multicast address allocation and service discovery. [4] Zeroconf is not just for a wireless network. Zeroconf solution can be applied to a single network segment for allocating a unique IP address to an ad hoc node on the same link. Actually it generates a link local IP address using a pseudo random number generation algorithm. It is assumed that each node can communicate with each other using link local broadcast and multicast. However, in MANET, there may be many intermediate nodes that route packets to the next hop. So link local broadcast cannot guarantee sending of a packet to all MANET nodes, because intermediate nodes that act as routers may block packets with link local IP addresses. It means this scheme cannot resolve the IP address duplication problem.

PMWRS [6] solution is proposed by Perkins et al. Basic idea is detecting a duplicated IP address by using an ad hoc routing protocol. It uses an address request and an address reply similar to reactive routing protocol. Therefore, if an ad hoc network uses the proactive routing protocol, the ability of protocol operation is significantly impacted. It also uses the 169.254/16 link local address block that is registered by IANA. If a router receives packets that have link local IP addresses as their destinations, it would discard them. It also uses a timer waiting for an address reply message for duplication detection. But a small amount of time period is not enough for transferring data to all nodes in the ad hoc network.

MANETconf [7] proposes a two-phase address allocation procedure using a surrogate. When new host enters an ad hoc network, it selects one of the near nodes as a surrogate node, which is called as an initiator. The initiator sends an address request message to all nodes over the ad hoc network on behalf of the new node. Allocation of IP addresses proceeds in two phases. First, a request for address marks the status of IP allocation as "middle of progress". After receiving a reply, the initiator sends a confirm message about the request to all nodes. To synchronize the allocation table, network gives a priority to each IP address. If concurrent requests are made for an address, an allocation order is set by the initiator's address priority. It means there must be a fixed IP address pool and each node knows the priority policy. In addition, the address request and reply procedure over all ad hoc nodes makes a lot of traffic flooding. If the size of IP pool becomes larger, the address list management would become a big burden.

These address allocation methods are designed only for an ad hoc network. It mostly focuses on duplication detection of a self-generated address or a randomly selected address from a specific address block. Those kinds of addresses guarantee uniqueness only within the same link and are not usable in a public network. For using them, an additional function is needed such as network address translation.

2.2.3. At Hybrid Wireless Network

For implementing a hybrid network, we must bind a cellular network and an ad hoc network. A hybrid network can support multiple-hop routing by utilizing each host as a relay. Peer communication does not need to use a base station in the hybrid network. It just sends a message using an ad hoc routing in the local area. We can consider application of both configuration methods to the hybrid network.

First, a mobile node can set up itself using an ad hoc node configuration method. But address block reserved for link local address cannot be used in the public network. So a router will drop out packets tagged with those addresses. To avoid this problem, a gateway can translate those addresses into public addresses. But it has problems with supporting address transparency to end-to-end applications. Each ad hoc node can configure itself with a network prefix, which is advertised by the router or a foreign agent of mobile IP. An address is made of a network prefix and a host identifier that is generated randomly by the ad hoc node. [13] But there are still disadvantages already commented at ad hoc network configuration like flooding and duplication detection.

Second, a mobile node can take services used for a cellular network using DNS and DHCP server. When a mobile node initiates configuration using a DHCP server in infrastructure, it broadcasts a DISCOVERY message to neighbor nodes. General configuration procedure using DHCP makes data flooding over ad hoc network. So whenever a mobile node requests address allocation or releases address, a broadcast must occur. It causes network congestion over ad hoc network and bottleneck at base station. In addition, it also takes more time than single cellular network due to multiple hopping. To reduce packet flooding, the DHCP relay function is used at each ad hoc node [8]. When a mobile node sends an IP allocation message to a DHCP server, intermediate nodes between the request node and DHCP server can play a role as a DHCP server. It can reduce control traffic for searching a route to the DHCP server since each relay node already knows the address of the DHCP server. A mobile node that needs an IP address can locate the DHCP server using broadcast to neighbor nodes. Neighbor nodes relay DICOVERY and OFFER messages on behalf of the request node.

When route to the DHCP server fails, intermediate node invokes route discovery procedure. Route often changes because of the nodes' frequent movement in ad hoc network. In hot spot, user moves frequently and DHCP request may increase. Route request flooding for IP allocation still exists in ad hoc network and it takes more time to request address allocation through multiple intermediate nodes. It causes handoff delay problem when mobile node moves between two hybrid networks. As opposed to ad hoc network, configuration service is centralized into single system and is manageable in wired network. For example, service policy can be easily applied to mobile nodes so duplication control mechanism is not necessary. But we must resolve configuration delay problem and packet flooding for configuration on a hybrid network.

We propose a decentralized model for the configuration of the nodes in a hybrid network. It can reduce the traffic in the hybrid network. The main goal of the new model is to reduce the configuration delay.

3. BASIC IDEA

We propose a scheme to configure a host's network interface by using the configuration information distributed among ad hoc nodes in a hybrid network. In related works, ad hoc nodes normally use private IP addresses or address block allocated by IANA with the duplication detection. These approaches are only applicable to a stand-alone network that is not connected to the public network like the Internet. A public address generation scheme with a network prefix advertised by a sub network router is suggested in [13]. But this method also cannot avoid the duplication detection procedure, which takes most part of the address allocation delay, since two or more host identifiers can be generated as the duplicated one. Other approaches are based on the broadcast service of infrastructure like DHCP. These methods broadcast DHCP messages to ad hoc network basically. To reduce network traffic occurred by address allocation, the DHCP relay function could be used on the assumption that mobile nodes have the relay functionality. A configuration procedure using the DHCP relay function takes time for request message to hop multiple intermediate nodes. The configuration delay is a critical problem while users of an ad hoc network might execute time-critical applications such as real-time video service or voice over IP. A node may request a care-of address for mobile IP service or new IP address from the sub network when it comes to a new sub network. In this case, service can be stopped while new configuration is being set up. It can decrease the quality of service. We distribute available addresses among ad hoc nodes.

3.1 Mobile Node Ability

Each ad hoc node has the DHCP server functionality that offers an IP address allocation (and possibly configuration information) and relays requests to other DHCP servers. From now on, to avoid misunderstanding of terms, we denote the DHCP server of infrastructure as the main DHCP server. Ad hoc nodes manage the path to default gateway for connectivity to Internet by use of an ad hoc routing protocol. That path is the same with the DHCP relay route to the main server, since the main DHCP server can be accessible by the gateway. Each ad hoc node has an address pool. When booting up, mobile nodes already have addresses used before in their pools, they send DHCP request message to the main DHCP server to extend expiration time of the using addresses. Each ad hoc node relays address allocation request to the main DHCP server. If an intermediate ad hoc node has proper addresses in its pool, it replies to the node that requested configuration information on behalf of the main DHCP server. An ad hoc node passes its own address and cached addresses to a specific node when they leave network, only if possible.

3.2 Address allocation Procedure

Until a number of ad hoc nodes are saturated in a sub network, ad hoc nodes may frequently request configuration information to the main DHCP server. In this case, each ad hoc node plays a role of the DHCP relay, which is exactly same with the related work [8] scenario. When a new ad hoc node comes in a sub network, it broadcasts a DHCP discovery message to neighbor nodes within one hop distance by setting TTL value as one. Neighbor nodes that receive the discovery message reply with the DHCP offer message, which contains one of addresses in their caches. Then the new ad hoc node chooses one of the offer messages and sends the DHCP request message to the ad hoc node. Any others that do not receive request message ignore the allocation and revoke the offered address. Neighbor nodes that cannot offer IP address relay the discovery message to other nodes. In some cases, it relays the discovery message to the main DHCP server that is located in the infrastructure network through several intermediated DHCP relays in the ad hoc network.

We assume the number of ad hoc nodes become increasing in an ad hoc network as time goes by. At that time, the message transaction between ad hoc nodes and the main DHCP server decreases, as a new comer can receive configuration information from neighbor nodes. Before leaving a network, an ad hoc node releases its IP address to one of the neighbor nodes. A neighbor node that receives the IP address release message caches the information instead of relaying it to the main DHCP server.

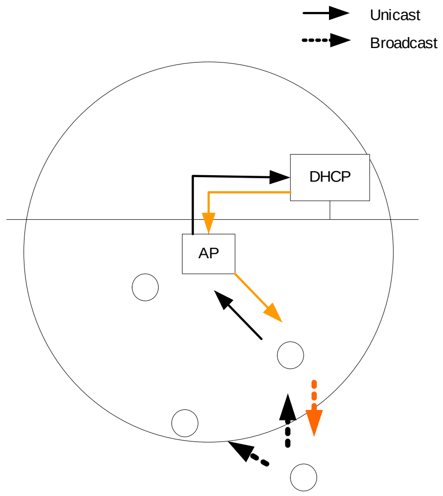

Fig 1 Beginning stage

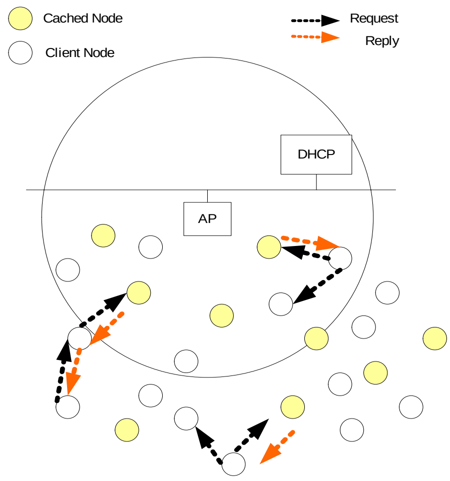

Fig.2 Middle Stage

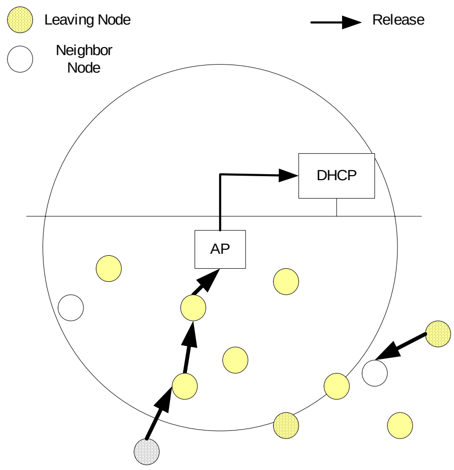

Fig.3 End Stage

3.3 Abrupt failure of an ad hoc node

We assume that an ad hoc node releases addresses to a neighbor node before it leaves network in most cases. But sometimes, it can disappear without any notification to the network due to the power off, unknown terminal failure and so on. We must revoke those lost addresses that the leaving ad hoc node had. The main DHCP server manages address resources using lease timer. The network operator sets the timer value properly to meet the requirements and the characteristics of the network. For example, when the number of nodes is larger than the number of available addresses, it is efficient to set the lease time shorter. In this case, the request to extend the lease time is made frequently. If the timer expires, the main DHCP server can allocate it to a new ad hoc node

3.4 Consistency of Cached Configuration Information

In our scheme, all nodes participate in the management of address resources. Therefore, the consistency of cached information among participating nodes should be preserved to avoid malfunctions. Most of the address conflict problems are due to the duplicated addresses. We prevent this problem using two simple schemes.

First, an ad hoc node that leaves network passes its own address and cached addresses to a single neighbor node. The leaving ad hoc node broadcasts pseudo release message to neighbor nodes. When the leaving node receives acceptance message(s) from the neighbor nodes, it releases its own address and cached addresses to only one of those neighbor nodes. So there exists only one copy of address in an ad hoc network. It effectively removes the duplication detection procedure. But the same addresses can exist in the network when the timer of a cached address is expired at the main DHCP server because the main DHCP server can allocate corresponding address to a new ad hoc node. And another ad hoc node gives the same address to the other. It makes address conflicts without a duplication detection procedure. So we acknowledge that our scheme also needs a duplication detection mechanism by the main DHCP server such as defined in the general DHCP process.

Second, ad hoc nodes, which have cached addresses, must request the timer extension of their own address and cached addresses to the main DHCP server. It reduces the time of sending the request message to the main DHCP server by updating all addresses simultaneously. A request message contains an address lists to update and the lease time. The ad hoc nodes checks expire time of addresses cached and request extension of expire time to main DHCP server against all of addresses if there were one about to expire. After updating the lease time, the lease time of all addresses is same. And an ad hoc node periodically updates timer. A few addresses expired can be handled by the duplication detection. If there were conflict before allocating the address to the ad hoc node, the main DHCP server would extend lease time of address.

In our scheme, it is possible for ad hoc nodes to receive configuration information faster than the ordinary DHCP relay because they can receive configuration information from the neighbor ad hoc nodes within one hop distance when the neighbor nodes have cached addresses. Even at the worst case, delay is no longer than that of the normal DHCP service. It is not guaranteed that a surrogate node, which relays address request to the main DHCP server, is always staying near a new ad hoc node. It means a new ad hoc node may retry to request an address. Moreover our scheme needs no route request for searching the path to the main DHCP server in case of receiving information from neighbor nodes. It also does not invoke release message broadcast when node leaves network. It just gives its own or cached IP addresses to a specific neighbor node. If every nodes use the main DHCP server for requesting and releasing the configuration information, wired and wireless resources of infrastructure are wasted by configuration traffic.

We can reduce the traffic by trying to localize the configuration within the ad hoc network. Each node manages available IP addresses to allocate other nodes and expiration time of addresses. And each node has different cached IP address information and does not need the control messages for keeping consistency among the ad hoc nodes. Furthermore when the main DHCP server on infrastructure goes down, there is no problem to configure a new comer in the network. Our scheme is tolerable in failure by distributing configuration information. After the main DHCP server was recovered, address configuration information is automatically updated by periodic request from caching ad hoc nodes.

4. SIMULATION

4.1 Simulation model

We use NS-2 simulator for the simulation. The scenario is like below;

- *Region size : 500m x 500m*
- *Number of nodes : 30 ~ 50*
- *Total time : 2,400 seconds*
- *Average lifetime : 50seconds*
- *Leave mode*
  - *OFF : DIE = 9 : 1*
  - *OFF : Leaving with notification*
  - *DIE : Leaving without notification (to simulate abrupt power off or failures)*

4.2 Implementation

For test the validity of our scheme, we implemented our scheme and DHCP with flooding using ns-2. We implemented ad hoc routing agent in ns-2 pass IP broadcast packets to upper layers by modifying the source code of AODV routing protocol. Therefore, ad hoc nodes can send and receive IP broadcast packets.

The integration of automatic configuration services with routing protocols and the proper mixture of broadcast and unicast for configuration are also necessary.

All details of our scheme and DHCP with flooding are implemented. We found that in the real implementations of DHCP there are several improvements and optimizations that are not specified in the [2]. Some of features in our scheme, such as extension of expiration time, are not implemented, because those features are not crucial parts of distributed cache based configuration.

4.3 Analysis of results

We tested our scheme and DHCP (with flooding) using the same scenario file generated by modified version of setdest, which is included as an independent application of ns-2. In this scenario, there are 637 configuration tries. Overall test results are summarized in the following table.

	Successful configuration	Total number of packets (transmitted + received)	Total number of dropped packets by duplication checks
Our scheme	371	2,038,598	936,291
DHCP	382	2,111,443	976,719

The success rate of configuration with our scheme is slightly (around 3%) lower than the rate with DHCP. This may be due to the fact that in our scheme, local caching server that offered IP addresses for configuration could become unreachable more frequently before the configuration process is finished. These cases may happen when the offering caching node may be off or intermediate nodes are off or moved, or too many requests are made against the node, which has a very limited cache buffer. In DHCP environment, since the configuration relies only on the "fixed" and "always-on" DHCP server, the possibility of failed configuration due to the movement or off the node is zero.

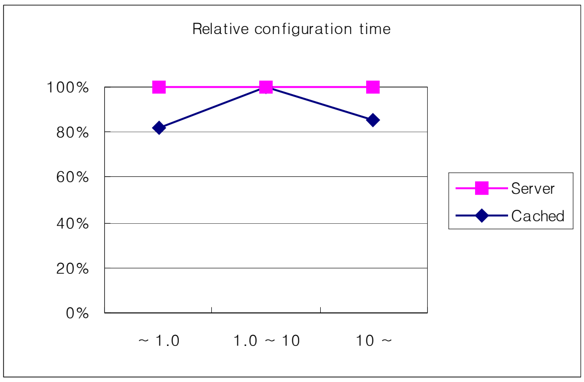

Fig. 4 Relative Configuration Time

The number of total and duplicated packets with our scheme is about 4% less than that with DHCP. This is because the node with cached IP addresses sends replies instead of forwarding the request packets with IP broadcast. The overhead of packet transmission can be more reduced with proper use of unicast.. (Note: The current implementation of our scheme and DHCP does not use unicast at all to simplify the implementation and the fair comparison.)

We also compared configuration delays from the server and from the cache nodes. With the current scenario data, 59 out of total 371 configurations (about 16%) of total configuration are done by addresses from the caching nodes. As shown in the above graphs, the configuration delay with caching nodes is about 10% faster.

5. REFERENCES

[1] A. Williams, "IP Requirement for Automatic Configuration of IP Hosts", draft, IETF, Sep. 2002.

[2] R. Droms, "Dynamic Host Configuration Protocol", RFC2131, IETF, Mar. 1997.

[3] C. Perkins, "Ad Hoc Networking", Addison-Wesley, 2001.

[4] S. Cheshire, B. Aboba, E. Guttman, "Dynamic Configuration of IPv4 Link Local Addresses", draft, IETF, Aug. 2002.

[5] U. Jonsson et. al, "MIPMANET-Mobile IP for Mobile Ad Hoc Networks", MobiHoc, 2000.

[6] C. Perkins, et. al, "IP Address Auto configuration for Ad Hoc Networks", draft, IETF, Nov. 2001.

[7] S. Nesargi, R. Prakash, "Configuration of Hosts in a Mobile Ad Hoc Network", Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. In Proceedings of IEEE INFOCOM, 2002.

[8] M.J. Miller, W.D. List, N.H. Vaidya, "A Hybrid Network Implementation to Extend Infrastructure Reach", Technical Report, Jan.2003.

[9] Y. Lin, Y. Hsu, “Multihop Cellular: A New Architecture for Wireless Communications”, In Proceedings of IEEE INFOCOM, Mar. 2000.

[10] H. Wu, C. Qiao, S. De, and O. Tonguz, “Integrated Cellular and Ad Hoc Relaying Systems: iCAR”, IEEE Journal of Selected area in Communications, Oct. 2001

[11] X. Wu, S. Chan, and B. Mukherjee, “MADF: A Novel Approach to Add an Ad-Hoc Overlay on a Fixed Cellular Infrastructure”, in Proceeding of the IEEE WCNC, Sep. 2000.

[12] H. Hsieh, R. Sivakumar, “Towards a Hybrid Network Model for Wireless Packet Data Networks”, In Proceedings of IEEE INFOCOM, 2002

[13] Y. Sun, E. Belding-Royer, and C. Perkins, “Internet Connectivity for Ad hoc Mobile Networks”, International Journal of Wireless Information Networks special issue on Mobile Ad hoc Networks, 9(2), April 2002.