

Mobility and Internet Connectivity in Mobile Ad Hoc Networks

Jahanzeb Farooq

Department of Computing Science
Umeå University, Sweden
int04jfq@cs.umu.se

Abstract. A mobile ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure. Some of the nodes in an ad hoc network may want access to an external network, such as Internet, while still moving around. Special ad hoc routing protocols have been developed that provide for mobility among the nodes within an ad hoc network. Mobile IP, a modified version of IP, allows a mobile node to move between different networks without any interruption in network connectivity and ongoing communications. This paper discusses how ad hoc routing and Mobile IP can be integrated to provide Internet connectivity to the nodes in a mobile ad hoc network.

1 Introduction

Mobile wireless networks can be classified into two categories: infrastructure and infrastructure-less or ad hoc networks, as shown in Fig.1.

In an infrastructure wireless network, a node can connect to a central gateway, also known as the base station or access point. The gateway is fixed and acts as a router to the other nodes. Communications among the nodes can only be achieved through the fixed gateway [1].

In infrastructure-less networks there is no fixed gateway. Mobile nodes communicate with each other directly. This means the node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may not be within direct wireless transmission range of each other. An ad hoc routing protocol is used that allows nodes to discover paths through the network to other nodes. Since the mobile nodes in the network dynamically establish routing among themselves, a network can be setup on ad hoc basis [1]. Infrastructure-less networks, therefore, are also called Mobile Ad hoc NETWORKS(MANET) [2].

Mobile ad hoc networks turn the dream of getting connected “anywhere and at any time” into reality. Some typical applications include requirement of network in disaster area or in military operations. In these situations an ad hoc network can be established with the help of groups of people with laptops at a place where no network services are present or have been destroyed because

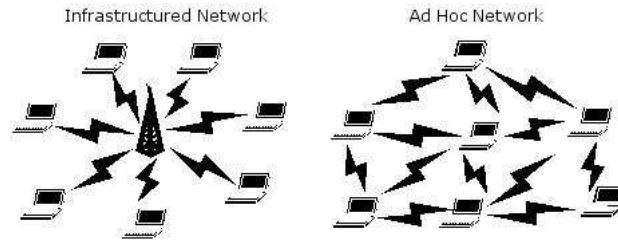


Fig. 1. Infrastructured vs. Ad Hoc Networks

of some disaster, e.g. a hurricane or an earthquake. This is one of the many examples where ad hoc networks are very useful.

As mobile nodes in an ad hoc network can freely move around, there are frequent changes in network topology. Two nodes that have had a direct route between them might not be able to communicate after a short period of time as one or both of them will have changed their locations. The greatest problem for routing in ad hoc networks thus arises because of highly dynamic topology. Traditional routing protocols used in wired networks react too slowly to these changes or generate too many updates to reflect changes in topology. Furthermore, this highly dynamic topology results in broken routes, which in turn result in packet losses. Asymmetric and redundant links make routing in ad hoc networks even more difficult. Special routing protocols are required for ad hoc networks to provide solutions for these problems.

Ad hoc networks can be connected to an external network such as Internet or LAN to facilitate the users with the resources provided by the external network. In this scenario, routers, or one or more nodes in the ad hoc network, called gateways, connect the rest of network with the external network. Here Mobile IP [3] comes into action.

Mobile IP is an extension of existing Internet Protocol (IP) to accommodate mobility. It allows a mobile node to change its location (or network) without the need to re-establish the network connections or to terminate any ongoing communication [4].

Since nodes in an ad hoc network are mobile, they may desire to move between different networks while still maintaining the network connection. Integration of Mobile IP and ad hoc networks enables mobile nodes, as well as gateways, to move between networks while retaining the connectivity to the external network.

This paper discusses two issues; the mobility and connectivity of individual nodes within the ad hoc network, and, the mobility and connectivity of the ad hoc network with respect to other networks, specifically the Internet. Special ad hoc routing protocols have been developed to provide solutions for mobility within the ad hoc networks, while integration of Mobile IP with these ad hoc routing protocols provides the connectivity with external networks, here, the Internet.

The remainder of this paper is organized as follows. Section 2 presents an overview of ad hoc routing and ad hoc routing protocols that serve a solution to mobility among the nodes within the ad hoc network. Section 3 discusses mobility management and an overview of Mobile IP. Section 4 discusses integration of ad hoc networks with Mobile IP to provide connectivity of ad hoc networks with the Internet, and some proposed architectures. Finally, section 5 concludes the paper.

2 Ad hoc Routing

An ad hoc mobile network is a collection of mobile nodes that are changing their location dynamically and arbitrarily. While in wired or wireless networks with infrastructure support all nodes in the network can be reached, this is not always the case in ad hoc network. A destination node might be out of range of a source node transmitting data. Routing is required to find a path between source and destination. Therefore in ad hoc networks, each node must be able to forward data to other nodes, in other words a node may act like a router. As nodes change their locations dynamically, this results in continuously changing topology.

One of the first ad hoc wireless networks was the packet radio network started by ARPA in 1973. It used a variant of Distance Vector routing algorithm that is not efficient in modern ad hoc networks where the number of nodes can be large and there are dynamic changes in network topologies due to mobility [1].

In a Distance Vector routing algorithm, each node periodically sends routing information to only its directly connected neighbor nodes, and provides them with routing information from itself to all other nodes in the network. It is called Distance Vector algorithm because each node maintains a vector of distances to all other nodes in the network. If some change occurs in routes to a mobile node's neighbors, the algorithm requires long time to update routing tables of all nodes in the network, a process known as *convergence*. On the other hand, in Link State algorithm, each node sends routing information to all other nodes, and knows cost of each route to each node in the network. This requires a large number of messages to send to all nodes in the network. In contrast to Distance Vector algorithm, routing tables are only updated when some change occurs in the network [5].

Distance Vector and Link State based routing protocols that are used in wired networks had not been designed keeping in mind the mobility in ad hoc networks. Most of them proved inefficient when applied to ad hoc networks. Traditional Distance Vector and link state based protocols, such as OSPF (Open Shortest Path First) and RIP (Routing Information Protocol) that are used in Internet, completely fails or performs very poorly when used in ad hoc networks because of their dynamic nature [1]. The greatest problem for routing in ad hoc networks thus arises because of highly dynamic nature of ad hoc networks; as number of nodes varies and routes break and establish frequently, periodic updates are

required in routing tables to keep them consistent with the most recent state of the network.

Another problem for routing in ad hoc networks is asymmetric links. If node A receives packets from node B, this does not assure anything about the quality of connection in reverse. Node B may receive nothing, or have a weak or even stronger link to node A depending on the characteristics of medium. This also results in situations where route in one direction is very long compared to the route in the reverse direction, e.g. node A has a one hop route to node B which may only have a longer multiple hops route in reverse. Yet another problem is redundant routes between nodes which makes routing decisions in ad hoc network even more difficult [1]. More efficient protocols are therefore required for ad hoc networks that can sustain the mobility of nodes.

Next section discusses two different approaches for ad hoc routing protocols to solve the problems associated with traditional routing protocols.

2.1 Proactive vs. Reactive Routing

One of the most important aspects of ad hoc routing is whether nodes in an ad hoc network should maintain routes to all other nodes, or instead keep track of only the nodes to which it wants to send packets. In principle, a node in an ad hoc network does not need to maintain a route to another node until it wants to send packets to that node, or if that node is the first node along the path to some other node to which it wants to send packets.

In ad hoc networks, protocols that keep track of routes to all other nodes have the advantage that as a node wants to send packets, it can start with minimal delay because the routes to the destination node are pre-calculated. Such protocols are called *proactive* because they store route information even before it is needed. They are also called *table driven* protocols because routes are already residing in the route table and can be immediately selected from there [6]. On the negative side, in order to keep track of broken routes periodical updates are required that consumes time and bandwidth. Moreover, as discussed in previous section, in ad hoc networks with large number of mobile nodes and high mobility rates, it is very expensive for proactive routing protocols to maintain and update large number of routing information.

As a result, on-demand, or reactive, protocols have been designed that search for a route only when desired by the source node. A node that requires sending packets to another node initiates a route discovery process and this process is completed once a route is found or all possible routes have been examined. This is relatively less costly than a proactive protocol when the node mobility is high, however, the route discovery process for an unknown destination node will cause considerable delay in starting the communication [7].

In addition, it is possible to adopt a hybrid approach, where nodes proactively maintain routes to the nodes within a local neighborhood, while reactively sending out route queries for distant destination nodes [6].

Some popular proactive and reactive routing protocols are examined in following sections.

Destination-Sequenced Distance Vector (DSDV) The DSDV [8] is a proactive routing protocol based on Distance Vector algorithm. DSDV uses hop-by-hop routing; that is, each node maintains only the route to the next node and not the entire route.

In DSDV, each node maintains a route table that contains all routes to each of the reachable nodes. Each route is assigned a sequence number by the destination node [6]. The sequence numbers enable the nodes to distinguish expired routes from new ones, thereby avoiding the formation of routing loops [9].

Routing tables are periodically broadcasted to all nodes in the network, such that each node advertises a monotonically increasing even sequence number for itself [10]. When a node receives new routing information, it is compared to the information already available in its route table. A route with a more recent sequence number is chosen. If two routes have same sequence numbers, the route with a “better” metric is chosen, where metric is a selection criteria e.g. number of hops in the route. The newly chosen route is advertised to the neighbor nodes and its metric is incremented by one hop [6]. When a node A finds that its route to a node D has broken, it advertises it to D with a sequence number one greater than its sequence number for the route that has been broken (making an odd sequence number) and a “bad” metric, called an *infinite-metric*. This helps any node B routing packets through A determining that the route to node D has broken, thereby stopping routing through A until node B receives a route to D with a higher sequence number [10].

Temporally-Ordered Routing Algorithm (TORA) TORA [11] is a reactive routing protocol based on a “link reversal” algorithm. In link reversal algorithm, a node transmits packets in the reverse order, i.e. to the previous node in the route, whenever it does not have a better outgoing route. The algorithm of TORA can be described in terms of water flowing downhill through tubes between the nodes, where tubes represent routes between the nodes and the water in the tubes represents the packets flowing towards the destination node. If water flowing from node A to B becomes blocked such that there is no way for it to flow out of node B, the height of B is set to a height greater than that of its remaining neighbor nodes, such that the water flows back to the node A. Thus, TORA uses a “height” metric in a similar way “number of hops” metric is used in DSDV [10].

TORA is very efficient in highly dynamic mobile networks and provides multiple routes to a destination [9]. On the negative side, it suffers from loops in routes because of its link reversal algorithm. Consider a node A routing packets to node C through node B. If node B’s link to C breaks, B will reverse its link to A, transmit an update message to its neighbors to notify the change, and begin routing packets to C through A. Until node A receives the update message, packets to C will loop between A and B [10].

Dynamic Source Routing (DSR) DSR [12] is a reactive protocol that uses source routing rather than hop-by-hop routing. In source routing each packet

to be sent includes in it the complete ordered list of nodes through which the packet must pass [10]. Each node maintains a route cache that contains routes to all the nodes of which the node is aware. When a node wants to send packets to some destination node, it first checks its route cache, if it does not have a route to the destination, it initiates route discovery by broadcasting a *route request* packet that contains the address of the destination node. Each node receiving the packet checks whether it knows a route to the destination. If it does not, it adds its own address to the packet and forwards the packet to the next node. A *route reply* packet is generated when the packet reaches either the destination itself, or an intermediate node which contains a route to the destination. By the time it contains in the packet the sequence of hops taken [9].

Thus, in source routing, intermediate nodes do not need to maintain up-to-date routes in order to forward the packets since the packets themselves already contain all the routing information. Source routing, along with the on-demand nature of the protocol, eliminates the need for the periodic route advertisement present in other protocols [10]. On the negative side, DSR suffers from the overhead of information carried in the route caches and packets.

Ad Hoc On-Demand Distance Vector (AODV) AODV [13] is a reactive protocol that is a combination of both, DSR and DSDV. It borrows source routing and on-demand route discovery from DSR, and sequence numbers from DSDV [10].

In contrast to DSDV, AODV minimizes the number of broadcasts by creating routes only when they are required. When a node wants to send packets to some destination node and does not already have a route to that destination, it initiates a *path discovery* process by broadcasting a *route request* (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a route to the destination is found [9]. The RREQ packet contains the most recent sequence number to the destination node. A node receiving the RREQ packet replies with a *route reply* (RREP) packet only if it has a route to the destination whose destination sequence number is greater than or equal to that contained in the RREQ [9]. The RREP packet contains the number of hops in the route to the destination and the most recent sequence number for destination [10]. The sequence numbers are used to distinguish old routes from new ones, thereby ensuring that routes are loop-free [9].

2.2 A Performance Comparison of Proactive and Reactive Routing Protocols

In a study of comparison, Broch, Maltz, Johnson, Hu and Jetcheva [10] concluded that each of these protocols performs well in some cases yet has certain drawbacks in others. DSDV performed very well, delivering over 92% packets when node mobility and movement speeds were low, but the ratio dropped to 70% as mobility increased. TORA delivered between 90% and 95% of the packets in scenarios with up to 20 transmitting nodes. But as the transmitting nodes

increased to 30, the performance dropped to 40% and significant fraction of packets was lost, mainly because of routing loops.

DSR and AODV performed equally well, delivering over 95% of the packets regardless of mobility rate. The use of source routing in DSR increases the routing overhead information required by the protocol. AODV though eliminates source routing overhead but still suffers from high overhead because of its Distance Vector algorithm. For this reason, AODV proved more expensive than DSR at high rates of mobility.

Comparing the overheads associated with each protocol, DSR exhibited the least overhead, TORA had the most, and AODV required about 5 times the overhead of DSR. While DSR, TORA and AODV are reactive protocols, their overhead dropped as the mobility rate dropped. DSDV, on the other hand, exhibited constant overhead with respect to mobility rate.

2.3 Hierarchical Routing

The protocols described in previous section only perform well with small number of nodes and fail in conditions where number of nodes is large and mobility is high. For larger networks, nodes are grouped in clusters such that different routing protocols can be utilized in clusters independent of each other. This provides a scalable and efficient solution. In a cluster, one or more nodes can be declared as *clusterheads*, which act like gateways and are responsible for routing packets to and from the cluster. The communications between clusters take place through these gateways. This form of routing is called hierarchical routing [1]. By using clusters, nodes typically remain within the cluster and hence the chances of nodes leaving the cluster are very low. If the topology within a cluster changes, only the nodes within the cluster are informed and updated with new routing information. Nodes in other clusters only need to know how to reach the cluster through the clusterhead. Clusters can be combined to form bigger clusters, called super clusters, building up a larger hierarchy.

Next section examines one of the hierarchical routing protocols.

Clusterhead Gateway Switch Routing(CGSR) CGSR is a hierarchical routing protocol based on Distance Vector algorithm. Compared to other Distance Vector based routing protocols, the hierarchical nature of CGSR helps to reduce the size of routing tables [1]. More specifically, CGSR uses DSDV as the underlying routing protocol, and hence has much of the same problems as DSDV suffers from. However, it modifies DSDV by using a hierarchical clusterhead-to-gateway routing approach to route packets from source to destination. Gateways are nodes that are within communication range of two or more clusterheads. A packet sent by a node is first routed to its clusterhead, and then the packet is routed from the clusterhead to a gateway to another clusterhead, and so on until the clusterhead of the destination node is reached.

All nodes participate in a clusterhead selection algorithm in order to select a node as the clusterhead within the cluster. Frequent clusterhead changes result in

repetitive use of clusterhead selection algorithm which causes delays and routing protocol performance can be badly affected. Therefore, instead of performing clusterhead selection every time a clusterhead changes, a Least Cluster Change (LCC) clustering algorithm is used. Using LCC, clusterheads only change when two clusterheads come into contact, or when a node moves out of contact of all other clusterheads [9].

Each node maintains a “cluster member table” which contains the address of clusterhead for each mobile node in the network. These tables are periodically broadcasted to all other nodes. In addition, each node also maintains a routing table which is used to determine the next hop in order to reach the destination. If a node wants to send packets, it first checks its cluster member table and routing table to determine the clusterhead along the route to the destination. Once clusterhead is known, it then checks its routing table to determine the next hop that can be used to reach the clusterhead. [9].

With increasing number of nodes in clusters, congestion around the clusterheads also increases. Moreover, because of the centralized nature of protocol, failure of clusterhead can bring the whole cluster down. In environments with high mobility rates, it is difficult to maintain and organize individual clusters [1].

3 Mobility Management

There is a difference between mobility and portability from network layer’s point of view [5]. If a mobile node (e.g., a laptop or notebook computer) is moved from one place to another such that its network connections are shut down and re-established at the new point of attachment to the network, then this is referred to as portability or nomadcity [4]. Mobility, on the other hand, allows a mobile node to maintain the network connections while moving around, therefore neither the applications running on the system nor the network connections need to be re-established [14].

Routers base their routing decisions on the network prefix portions of the destination IP addresses [5]. The IP address is divided into two portions, network address and the host address (or node address). The Network address, also called network prefix, defines the network to which the IP address belongs. The IP addresses of nodes within the same network thus share the common network prefix. The node address portion of the IP address identifies a specific node in the network [5]. Thus, packets from node A sent to node B are routed toward the router which connects the networks of node A and B together, where the network of node B is determined by the network prefix portion of IP address of destination node, B [5]. If the node B is mobile and has moved to another network, means that it is not located in the network where its network prefix shows it is supposed to be located, then packets sent to it from any other node will be undeliverable. This means that such a node is unable to communicate with any other nodes [4].

One solution to this problem is that if a node is moving from one network to another, it should obtain a new IP address such that the network prefix portion of the new IP address reflects the network in which the node is currently residing [4]. This solution does work for nomadicity but not for mobility. As defined earlier, mobility is the ability of a node to change its point-of-attachment from one network to another while maintaining the network connections and without terminating the active applications. But because of the architecture of higher layers, IP address cannot be changed without terminating the connections and active applications. The protocols TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) residing in transport layer just above the network layer relies heavily on IP addresses to identify the end hosts participating in the communication. They simply terminate the connections to a destination node whose IP address has been changed. Thus, all ongoing communication between a mobile node and any other nodes will also be terminated, with new connections being initiated by the mobile node at its new address. In other words, changing a mobile node's address as it moves does not solve the problem of mobility [4].

3.1 Mobile IP

Mobile IP solves the following two problems discussed above [4]:

- if a node moves from one link to another without changing its IP address, it will be unable to receive packets at the new link; and
- if a node changes its IP address when it moves, it will have to terminate and restart any ongoing communications each time it moves.

Mobile IP allows a mobile node to move among networks while still retaining its permanent IP address, thereby maintaining the network connectivity and any ongoing communications [4].

Mobile IP defines the following functional entities:

Home Network (HN): The network the mobile node belongs to.

Home Agent (HA): A router on a mobile node's home network that maintains location information for the mobile node and forwards packets to the node while the node is away from its home network.

Foreign Network (FN): Any network other than the home network of mobile node.

Foreign Agent (FA): A router on the mobile node's visited (foreign) network. The foreign agent cooperates with the mobile node's home agent to deliver packets to the mobile node.

Care-of Address (COA): A temporary address assigned to the mobile node that reflects its current network, and used to deliver packets destined to it.

Mobile IP allows mobile nodes that enter a foreign network to register with a foreign agent and obtain a care-of address (COA). This COA allows the mobile node to send and receive data packets from the networks other than its home network [14].

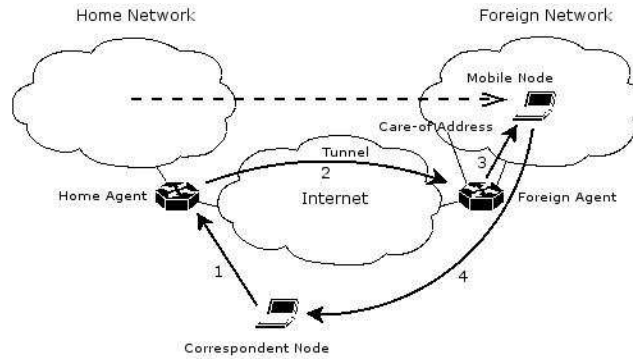


Fig. 2. Architecture of Mobile IP

Once a mobile node has received a COA that address must be registered with the home agent. After the registration has been done, the home agent delivers all packets destined to the node to its COA instead of its home address [14]. The whole procedure is illustrated in Fig.2.

As a mobile node moves into a foreign network, the first step is to find a foreign agent. The process of finding a foreign agent is called *Agent Discovery*. There are two methods for *Agent Discovery*. In the first one, home agents and foreign agents advertise their presence by periodically broadcasting special messages called *Agent Advertisements* which are received by all nodes in the network. Mobile nodes examine these messages and determine whether they are connected to their home or a foreign network. If a mobile node is in a foreign network, it receives message from the foreign agent responsible for that network, and thereby registers with it.

In the second method, a mobile node that does not want to wait for the Agent Advertisement messages can itself broadcast an *Agent Solicitation* message, indicating that it wants to register with a foreign agent. An agent receiving this message sends an Agent Advertisements message directly to the mobile node. As the mobile node finds a foreign agent, it gets a COA from the foreign agent and registers it with its home agent. Registration can be done either by the foreign agent who then registers the COA with the home agent, or directly by the mobile node itself. After receiving the COA of mobile node, the home agent advertises its reachability to the home address of the mobile node. Thus, after registration with the home agent, any node, referred to as Correspondent Node (CA), that wants to send packets to the mobile node, sends them to home agent of that node. Home agent in turn then forward packets to the COA. This indirect delivery of packets is called *tunneling*. There can be two possibilities for the location of COA. It can be the address of foreign agent in the network in which mobile node is currently residing, then it is called *foreign agent COA*, or it can be a temporary address assigned to the mobile node, termed as *colocated COA*. If it is the address of foreign agent (foreign agent COA), on receiving packets from

the home agent, foreign agent delivers them to the destination mobile node. The mobile node then can send packets directly to the correspondent node or it can be done via tunneling in reverse order [4].

4 Ad Hoc Networks and Internet Connectivity

Most of existing research limits mobile ad hoc networks to stand-alone isolated networks. Such networks are not suitable for applications that require access to services from other networks. With advancement in technology when portable devices, such as laptops, cellular phones and PDAs (Personal Digital Assistants) are widely in use, a portable device can provide many wireless interfaces, such as WLAN (Wireless LAN), GPRS (General Packet Radio Service), PHS (Personal Handy phone System) and Bluetooth. Users with portable devices equipped with these facilities want connectivity to Internet to benefit with its unlimited resources.

As illustrated in Fig.3, in order to provide Internet connectivity to the nodes in an ad hoc network, routers or one or more nodes in the ad hoc network can serve as gateways to an external network, where the external network can be an infrastructured network such as LAN, Internet or a cellular network, or even an infrastructure-less network such as another ad hoc network.

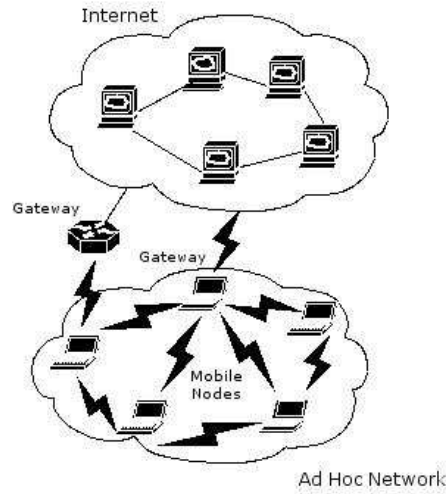


Fig. 3. Internet Connectivity in Ad Hoc Networks

As a solution, an integration of Mobile IP and ad hoc networks is implemented, such that Mobile IP enables nodes to move between different gateways

while maintaining the connectivity and ad hoc routing protocols provide connectivity among the nodes within the ad hoc network. In other words we can say that Mobile IP provides *macro* mobility and ad hoc routing protocols provide *micro* mobility [15]. *Micro* mobility, also called Intra-Domain mobility, is the movement of a mobile node within its own network, while *macro* mobility, also called Inter-Domain mobility, is the movement of mobile node between different networks.

Next section discusses the integration of Mobile IP and ad hoc networks and some of the proposed architectures.

4.1 Integration of Ad Hoc Networks with Mobile IP

In order to be able to communicate with Internet hosts, each mobile node must find a gateway, called *Gateway Discovery*, and obtain an address with the prefix of that gateway. With this new globally routable address, packets can be received from and sent to the Internet. When a mobile node moves and selects a different gateway, it configures a new address with the new prefix. In summary, a mobile node obtains its globally routable address in following steps. Basically, it (1) has a initial IP address (home address) which is routable in the ad hoc network, (2) discovers reachable gateways in its surrounding (3) selects one gateway out of the set of reachable gateways, and (4) forms a globally routable IP address with the prefix of the selected gateway [15]. This is achieved by Mobile IP as described in section 3.1.

In a similar way used to find foreign agents, gateway discovery is achieved either in a proactive or reactive way. In proactive approach, also called *passive discovery*, periodical gateway advertisements are sent to all nodes in the ad hoc network from the Internet Gateways. In the reactive approach, also called *active discovery*, solicitation and advertisement messaging between a mobile node and the Internet Gateway takes place. Once a mobile node discovers an Internet Gateway, it can connect to the Internet through the gateway.

As a mobile node receives gateway discovery advertisements, useful extension can be achieved if it can forward the advertisements to neighbor nodes that are located beyond the range of the gateway. Typically, a gateway has a larger transmission range than a mobile node, which results in a disadvantage of the passive discovery method: it is not necessarily guaranteed that a mobile node receiving a gateway discovery advertisement from the gateway does also have path to the gateway. In practice, both active and passive discovery methods can be combined and run in parallel. This leads to a *hybrid* gateway discovery method. If a mobile node receives more than one gateway discovery advertisements at once from different gateways, it selects one gateway according to a certain criteria e.g. strength of received signal from the gateway, number of hops between the node and the gateway [15].

As shown in Fig.3, connectivity of ad hoc network with Internet makes a heterogeneous network. In the link layer at the ad hoc network side, standard wireless technologies are used, such as the Wireless LAN standards IEEE 802.11, HIPERLAN/2, or Bluetooth. On the Internet side typical link layer protocols are

used [15], such as Ethernet, Token Ring, ATM(Asynchronous Transfer Mode) or FDDI(Fiber Distributed Data Interface) [5]. In the network layer, ad hoc networks use one of the ad hoc routing protocols described in section 2. On the Internet side standard Internet routing protocols are used [15], which includes RIP(Routing Information Protocol), OSPF(Open Shortest Path First) and BGP(Border Gateway Protocol) [5]. In the transport layer, ad hoc networks use improved version of TCP, modified for wireless networks. The gateway contains protocols for both the Internet and the wireless ad hoc network. For routing, usually two different routing tables are used, one for Internet and one for ad hoc network. The gateway may also contain functionality of translating between usual TCP and TCP for wireless networks [15].

Next section discusses some purposed architectures for the integration of ad hoc networks and Mobile IP.

Some Proposed Architectures by the Researches One of the methods for connecting ad hoc networks with the Internet has been specified by Sun, Royer and Perkins in [17] and Wakikawa, Malinen, Perkins, Nilsson and Tuominen in [18]. It presents a method for enabling nodes within an ad hoc network to obtain Internet connectivity when one or more nodes is within direct transmission range of a foreign agent or more specifically an Internet Gateway (IG). Before any communication between a mobile node in an ad hoc network and the Internet can take place, the Internet Gateway needs to be found. Internet Gateway assigns a global prefix for the ad hoc network, which makes it possible for mobile nodes in ad hoc network to communicate with Internet. Internet Gateway is also referred as Internet Router or Access Router, and is responsible for routing packets between the ad hoc network and the Internet. AODV is used as routing protocol to find an Internet Gateway. As discussed earlier, AODV is a reactive routing protocol that only discovers routes when they are required. Once discovered, the routes are then maintained as long as required by the source node.

One of the earliest technique for providing Internet connectivity for ad hoc networks is described by Lei and Perkins in [19]. In this proactive approach, a method for integrating the ad hoc routing protocol with Mobile IP routing protocol (called Mobile IP Daemon, MIPD) is presented. This integration results in a combined route table. Routing within the ad hoc network is provided by *routed*, a modified version of RIP(Routing Information Protocol), which is implemented on each mobile node within the ad hoc network. This integration enables foreign agents to participate in the ad hoc network routing. Because of proactive nature of the approach, for mobile nodes not in the transmission range of foreign agent, *routed* forwards agent advertisements to MIPD. Each mobile node uses the foreign agent as its default router [17].

Another initial approach of integrating the DSR routing protocol with Internet routing protocols and Mobile IP is presented by Broch, Maltz and Johnson in [20]. In this approach, an addressing technique for ad hoc networks is presented. Mobile nodes in an ad hoc network are assigned home addresses from a single network. The nodes within range of the foreign agent act as gateways

between the ad hoc network and the wired network, the Internet. As a reactive approach, foreign agent discovery is only done when required. DSR is utilized for routing within the ad hoc network, while traditional routing protocols for wired networks are used on the Internet side. In this approach, foreign agents are responsible for connecting the ad hoc network with the wired networks [17].

Another proactive solution, MIPMANET, is presented by Jonsson, Alriksson, Larsson, Johansson and Gerald in [21]. Mobile nodes in an ad hoc network that want connection to Internet register with the foreign agents and use their home address throughout the communications. The packets destined for the Internet are *tunneled* to the foreign agents, which in turn forwards the packets to the destination in the Internet. The AODV routing protocol is used to find routes between mobile nodes and the foreign agents. A new algorithm, called MIPMANET Cell Switching (MMCS), is used to determine when mobile nodes in the ad hoc network should register with a new foreign agent. In this solution, it is assumed that a mobile node that wants Internet access has been assigned a home address that is valid on the Internet [17].

5 Summary

Most of the existing research limits a mobile ad hoc network to a stand-alone isolated network. Such networks are not suitable for applications that require access to services from other networks, specifically Internet. This paper first discusses ad hoc routing protocols that take proactive and reactive approaches to provide mobility within ad hoc networks, and Mobile IP that enables a mobile node to move between networks while maintaining the network connectivity. It then discusses the integration of ad hoc routing protocols and Mobile IP to achieve the connectivity of ad hoc networks with external networks, specifically the Internet. The paper also discusses some proposed architectures for this integration.

References

1. Schiller, J.: Mobile Communication 2nd Edition. Addison Wesley (2003)
2. MANET: Mobile Ad hoc Networks. <http://www.ietf.org/html.charters/manet-charter.html> (2002)
3. Perkins, C.E., Myles, A.: Mobile IP. Proceedings of International Telecommunications Symposium (1994) 415–419
4. Solomon, J.D.: Mobile IP, The Internet Unplugged. Prentice Hall (1998)
5. Kurose, J.F., Ross, K.W.: Computer networking: a top-down approach featuring the Internet 3rd edition. Addison Wesley (2003)
6. Perkins, C.E.: Ad Hoc Networking. Addison Wesley (2001)
7. Tseng, Y.C., Shen, C.C., Chen, W.T.: Mobile IP and Ad Hoc Networks: An Integration and Implementation Experience. In: IEEE Computer, 36(5). (2003) 48–55
8. Perkins, C., Bhagwat, P.: Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In: ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications. (1994) 234–244

9. Royer, E., Toh, C.: A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks. In: *Mobile Wireless Networks*. IEEE Personal Communications. (1999)
10. Broch, J., Maltz, D.A., Johnson, D.B., Hu, Y.C., Jetcheva, J.: A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In: *Proceedings of the fourth annual ACM/IEEE international conference on Mobile computing and networking*. (1998) 85–97
11. Park, V.D., Corson, M.S.: A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks. In: *INFOCOM (3)*. (1997) 1405–1413
12. Johnson, D., Maltz, D., Broch, J.: DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks. In Perkins, C.E., ed.: *Ad Hoc Networking*, Addison-Wesley (2001) 139–172
13. Perkins, C.: Ad Hoc On Demand Distance Vector (AODV) Routing. In: *IETF, Internet Draft, draft-ietf-manet-aodv-00.txt*. (1997)
14. Perkins, C.E.: *Mobile IP: Design Principles and Practice*. Prentice Hall (2001)
15. Xi, J., Bettstetter, C.: Wireless Multi-Hop Internet Access: Gateway Discovery, Routing, and Addressing. In: *Proc. Intern. Conf. on Third Generation Wireless and Beyond (3Gwireless)*, San Francisco, USA (2002)
16. Ratanchandani, P., Kravets, R.: A Hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks. In: *Proceedings of IEEE WCNC*. (2003)
17. Sun, Y., Belding-Royer, E., C. Perkins, e.a.: Internet Connectivity for Ad Hoc Mobile Networks. In: *International Journal of Wireless Information Networks, special issue on Mobile Ad hoc Networks*. (2002)
18. Wakikawa, R., Malinen, J., Perkins, C., Nilsson, A., A.Tuominen, e.a.: Global Connectivity for IPv6 Mobile Ad Hoc Networks. In: *IETF Internet Draft, draft-wakikawa-manetglobalv6-02.txt*, November 2002. (2002)
19. Lei, H., Perkins, C.: Ad Hoc Networking with Mobile IP. In: *Proceedings of 2nd European Personal Mobile Communication Conference*. (1997)
20. Johnson, D., Maltz, D., Broch, J.: Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks. In: *In Proceedings of the Workshop on Mobile Computing held in conjunction with the International Symposium on Parallel Architectures, Algorithms, and Networks*, Perth, Australia. (1999)
21. Jonsson, U., Alriksson, F., Larsson, T., Johansson, P., Gerald Q. Maguire Jr., e.a.: MIPMANET - mobile IP for mobile ad hoc networks. In: *2000 First Annual Workshop on Mobile and Ad hoc Networking and Computing, MobiHoc*. (2000) 75–85