Integration of Mobile IP with MANET

Priyanka Sharma

Assistant Professor, Computer Application, Dr.C.V.Raman University
Raipur(C.G.) India

Abstract — In this paper we propose the method of combine the Mobile IP and MANET. Mobile IP (MIP) is often mentioned when it comes to routing support for mobile hosts. This is technology to support nomadic host roaming, where a roaming host may be connected through various means to the Internet other than its well known fixed-address domain space. A Mobile Ad-hoc Network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. We use to MANET Routing Protocols Destination-Sequenced Distance-Vector Routing (DSDV), Ad-Hoc On-Demand Distance Vector Routing (AODV) for MIPMANET. In this paper we have studied the integration mechanism of Mobile IP with MANET for better performance and benefit of MANET.

Keywords — MANET, Mobile IP, Routing Protocols

1. INTRODUCTION

Mobile IP (MIP) is often mentioned when it comes to routing support for mobile hosts. This is technology to support nomadic host roaming, where a roaming host may be connected through various means to the Internet other than its well known fixed-address domain space. The host may be directly physically connected to the fixed network on a foreign subnet, or be connected via a wireless link, dial-up line, etc. A Mobile Ad-Hoc Network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. Ad-hoc is Latin and means “for this purpose”. Information exchange in a network of mobile and wireless nodes without any infrastructural support. Such networks are often called ad hoc networks to emphasize that they do not depend on infrastructural support. A Mobile Ad-Hoc Network is a Mobile, multi-hop wireless network which is capable of autonomous operation. Destination-Sequenced Distance-Vector Routing (DSDV), Ad-Hoc On-Demand Distance Vector Routing (AODV) [1]

2. Back Ground Details

MIPMANET is designed to provide nodes in ad hoc networks with access to the Internet and the mobility services of Mobile IP. The solution uses Mobile IP foreign agents as access points to the Internet in order to keep track of in which ad hoc network. The ad hoc routing protocol is used to deliver packets between the foreign agent and the visiting node. A layered approach with tunneling is used for the outward data flow to separate the Mobile IP functionally from the ad hoc routing protocol. All this makes it possible for MIPMANET to provide Internet access with the ability for nodes to select and perform seamless switching between multiple access points.[2]

3. In short, MIPMANET works as follows:

1. Nodes in an ad hoc network that want Internet access use their home address for all communication and register with a foreign agent.
2. To send a packet to a host on the Internet: Tunnel the packet to the foreign agent with whom you are registered.
3. To receive packet from hosts on the Internet: the packets are routed to the foreign agent by ordinary Mobile IP mechanisms. The foreign agent will then deliver the packets to die node in the ad hoc network.
4. Nodes that do not require Internet access will see the ad hoc network as a stand-alone network, i.e., they will not need any knowledge about routes to destination outside of the ad hoc network.[2]
5. The layering of mobile IP and ad hoc routing functionality is illustrated in figure. By the use of tunneling; the ad hoc network becomes transparent to mobile IP

Figure- I conceptual view of MIPMANET
1.2. Foreign Agent & Tunneling

Using Mobile IP foreign agents as Internet access points is advantageous in many ways. A mobile IP foreign agent can provide Internet access to an entire ad hoc network using a single IP address as care-of address in addition to die home addresses of each mobile data is to be reachable from the Internet. A node with arbitrary home address can attach to any ad hoc network and have Internet access as long as there is a foreign agent that is willing to serve in that network. When with a foreign agent, the node is routed by its home address. Mobile IP also provides seamless Transparent Roaming between different networks, including different Ad-hoc Network [3] [4].

If an Ad hoc Network does not have a network ID it is not possible to decide whether a destination is located within the ad hoc network or not by simply looking at the destinations network ID. Instead, MIPMANET lets the route discovery mechanism of the ad hoc routing protocol search for the destination within the Ad hoc network before it can be decided whether the destination is within the Ad hoc Network or not.

By using tunneling, MIPMANET can incorporate the default Route concept into on-demand ad hoc routing protocols like AODV and DSR without incurring any major modification. Packets addressed to destinations that are not found within the ad hoc network can simply be Tunnelled to the foreign agent (assuming that the registered with a foreign agent).[5]

1.3 Adapting Mobile IP

On issue when using Mobile IP foreign agents is that according to Mobile IP visiting nodes must have link-layer connectivity with their foreign agent. Since such link-layer connectivity cannot be expected in ad hoc network, ad hoc routing has to be used between the foreign agent and me visiting node. Instead of using link-layer addresses as identifiers, network-layer identifiers, i.e., IP addresses have to be used. In this paper it is assumed that a mobile node must wants Internet access has been assigned a home address that is valid on me Internet. This home address can then be used on the ad hoc network as well.[2]

5. Movement Detection

Since there can be multiple hops between foreign agents and the visiting nodes, it is not as straightforward to choose between foreign agents in an ad hoc network as an ordinary Mobile IP enable networks. Unfortunately none of the movement detection methods provided by Mobile IP is situation. For example, Lazy Cell Switching (LCS) says that a node should stick to the same foreign agent as long as possible. However, because of the multihop nature of ad hoc networks, this decision might be very bad in many situations. The problem with Eager Cell Switching (ECS) is that it assumes movement along a straight line. Because of this it does not allow a visiting node within range of two different foreign agents to switch back and forth between them. The ability to do so might in fact be desirable, since the ranges of the foreign agents are extended by the multihop communication [2].

MIPMANET uses hop count as the metric to decide whether a visiting node should change foreign agent or not. The expectation is that the number of hops to the Internet access point is closely related to both delay and the fraction of packets received. The MIPMANET Cell Switching (MMCS) algorithm is as follows:

A registered visiting node should registered with another foreign agent if is at least two hops closer to this foreign agent than the foreign agent that it is currently registered through, for two consecutive agent advertisement.

MMCS is similar to ECS. The difference is that MMCS allows visiting nodes to switch back and forth between foreign agents in a somewhat controlled manner, MMCS prevent high frequent oscillation and decreases the probability of a visiting node registering wimp a foreign agent mat is only temporarily better. MMCS will also help to spread the visiting nodes registrations among the available foreign agents. Figure 27 illustrates MMCS in action.[2]
According to Mobile IP a visiting node should always have a valid agent advertisement from the foreign agent through which it is currently registered; otherwise it should consider me contact with the foreign agent to be lost. As the lifetime of an agent advertisement is three times the beacon period, a node should be allowed to miss three consecutive agent advertisements.

If the visiting node considers the contact to be lost, but has received agent advertisements (that have not expired) from other foreign agents then the node will register with the closest known foreign agent. Otherwise it will send an agent solicitation. MIPMANET uses the hop count to each foreign agent as the metric to determine which foreign agent a visiting node should be registered with. The hop count can be acquired by for example letting all foreign agents use a well-known predetermined value in the time-to-live field of the IP header. [28]

An agent advertisement beacon period of 5 seconds results in an agent advertisement lifetime of 15 seconds. In the worst case a node would wait 15 seconds before it would consider the contact with its foreign agent to be lost. To make the node detect the loss of contact faster, feedback from the underlying protocols is used. If a node wants to send a packet to the Internet it first has to tunnel it to the foreign agent. If the routing protocol cannot find a route it will send a destination unreachable message to Mobile IP. Mobile IP can then act as if it has lost contact with the foreign agent and start looking for a new foreign agent. In this way, the time it takes for a node to decide that it has lost contact with its foreign agent is reduced down to the time it takes for the underlying protocol to decide that the foreign agent is unreachable. [2]

6. Registration & Datagram Delivery

The registration procedure is almost the same as in ordinary Mobile IP with the exception that the registration request now may have to traverse multiple hops before reaching the foreign agent (and vice versa for the registration reply). What has to be modified is the way the foreign agent handles its visitor list and since reverse tunneling is used, the setup of the tunnel between the visiting node and the foreign agent.

In Mobile IP the foreign agent stores the link-layer address from which the registration request is received in its visitor list. If a visiting node uses multihop communication to reach the foreign agent, that link-layer address belongs to the first intermediate node (seen from the foreign agent). Thus, packets that are destined for a visiting node should instead be forwarded using information provided by the ad hoc routing protocol. If the link-layer address is used and the route to the visiting node changes, the entry in the visitor list has to be modified. If the routing table is used instead, the visitor list can remain unchanged as long as some route exists.

When a node registers with a foreign agent, Mobile IP sets up a default route to that foreign agent. In MIPMANET, the route discovery mechanism of the ad hoc routing protocol is used for all destinations. If the destination is not found within the ad hoc network, a host route is set up that tunnel packet to the foreign agent according to the default route. Packets destined to a correspondent node on the fixed Internet can then be tunneled to the foreign agent from where they can be delivered to the correspondent node by ordinary IP routing.

When Mobile IP (in the visiting node) determines that it has lost contact with the foreign agent it was registered with, Mobile IP has to remove the default entry in the routing table as well as all host routes that use the tunnel, as the tunnel no longer should route exist. [2]

MIPMANET uses reverse tunneling as defined in RFC 2344. This means that packets from a registered visiting node should be tunneled all the way to the home agent. However, for MIPMANET to work properly, the only requirement is that packets that are destined to the fixed Internet are tunneled from the JW visiting node to the foreign agent. When the foreign agent receives a tunneled packet it could send die encapsulated packet to the correspondent node directly. Our reason for choosing reverse tunneling is that many Mobile IP implementation already include this mechanism.
7. The MIPMANET Interworking Unit

To be able to use the original code in the foreign agents all new functionality has been put in a separate interworking unit, the MIPMANET Interworking Unit (MIWU), that is inserted between me foreign agent and me ad hoc network. The MIWU can be put either in the foreign agent itself or in a host on the same link as the foreign agent, as shown in Fig. From a foreign agent’s point of view the MIWU will look like a visiting node mat is registering different IP addresses, but with the same link-layer address. The MIWU transforms Mobile IP’s link-layer communication into network layer communication etc. manet can be routed on the ad hoc network (and vice versa). All Ad-hoc Routing functionality can be put in the MIWU. [2]

CONCLUSIONS

IN THIS PAPER WE HAVE STUDIED THE INTEGRATION MECHANISM OF MOBILE IP WITH MANET FOR BETTER PERFORMANCE AND BENEFIT OF MANET. EXTENSIVE EXPERIMENT HAS BEEN DONE HAVING DSDV PROTOCOL FOR THE INTEGRATION OF MOBILE IP IN WHICH ONE NODE OF MANET IS USE AS GATEWAY TO PROVIDE FACILITY FOR COMMUNICATION WITH INTERNET. IN THIS SITUATION CONNECTED NODE CAN COMMUNICATE WITH OTHER MANET NODES TOO. IN THIS TYPE OF NETWORK STRUCTURE NODES CAN DISCOVER MULTI-HOP PATHS TO FOREIGN AGENTS, THEREBY MANET GAINING INTERNET CONNECTIVITY. DSDV & AODV MAY BE UTILIZED FOR THE DISCOVERY AND MAINTENANCE OF ROUTES WITHIN THE AD HOC NETWORK.

REFERENCES
3. Rfc 3775.html