Internet Integrated MANETs using Mobile IP

Shuo Ding, Arek Dadej, Steven Gordon
Institute for Telecommunication Research
University of South Australia
Mawson Lakes Boulevard, SA 5095, Australia
shuoding@ieee.org, {arek.dadej, steven.gordon}@unisa.edu.au

***Abstract*— *Mobile Ad Hoc Networks* are generally considered as stand-alone networks. However, in most practical cases of ad-hoc networking, connectivity to the wider Internet may be possible via some members of the ad-hoc network. If that connectivity is made available to other members of the ad-hoc network, an interesting case of ad-hoc network interconnected with Internet via multiple gateways emerges. Such scenario gives raise to a number of challenges that require solutions involving extensions to Mobile IP and ad-hoc routing procedures, as well as careful planning of the scenarios under which the use of Internet connectivity will be made. The paper discusses the issues of Mobile IP agent registration, routing, and smooth gateway handoff. A network architecture framework for supporting IP mobility and communication across the boundary between ad-hoc network and the wider Internet is proposed and discussed.**

I. Introduction

Ad-hoc networks are usually considered as stand-alone networks, and in most cases no assumptions need to be made about the use of specific network layer protocols, e.g. IP. However, in the majority of practical cases it is reasonable to expect that the use of ad-hoc networking will be as much as possible transparent to the users and applications. This, in practice, means that the IP suite of protocols will be used. Moreover, the most interesting scenario for ad-hoc networking, especially in civilian applications, is that of an ad-hoc network connected to the Internet, or any infrastructure-based networks.

The Internet connectivity can be achieved via user nodes with access subscription to other (infrastructure-based) networks, such as enterprise LANs, wireless LAN hot-spots, or cellular networks. For example, a laptop user may be part of the ad-hoc network via their wireless LAN interface card, but also have Internet connectivity via their 3G phone. User nodes with connectivity to the wider Internet will effectively become gateways (edge routers) between the ad-hoc network domain and the wider Internet. This concept may also be applicable to cases where the coverage of an existing infrastructure network (wireless LAN hot-spot or 3G network) is extended by means of ad-hoc multihop connectivity.

A gateway node providing Internet connectivity to other members of an ad-hoc network is visible to nodes on the Internet via its IP address. To facilitate IP routing to specific nodes on the inside of the ad-hoc network, the gateway has to feature either Network Address Translation (NAT), or Mobile IP Foreign Agent functionality. Of these two, a Mobile IP based solution is better suited to scenarios where an ad-hoc network is treated as temporary means for providing connectivity among wireless/mobile nodes otherwise located within their own "home" networks, e.g. enterprise LANs or ISP domains. We will assume in this paper that the solution for IP routing to ad-hoc network nodes is based on Mobile IP.

Mobile nodes within the ad-hoc network, even though considered by the outside world as connected to the same IP subnet, communicate with each other and with the gateway (Foreign Agent) via multi-hop paths. This renders the typical methods used to exchange Mobile IP signalling (via ICMP messages) useless in the ad-hoc network environment. It also adds extra time needed by the Mobile IP messages to traverse multi-hop paths. New techniques for agent discovery and other Mobile IP procedures have to be found, and extra care is required in the design of Mobile IP procedures to minimise the effects of additional delay.

An even more interesting and challenging case is that of connectivity to the Internet via more than just one gateway. Where the Internet connectivity is provided to ad-hoc network nodes by those nodes that happen to also have 3G or LAN connectivity, such scenario with multiple gateways is very likely. Under such scenario, we expect that ad-hoc network nodes will be able to select the most appropriate gateway (e.g. to minimise hop distance or to satisfy bandwidth requirements of the application). This, and the fact that gateways to the same ad-hoc network may generally be connected to different IP subnetworks, leads to challenges such as Mobile IP handovers between gateways, discovery and selection of gateways, allocation of ad-hoc nodes to gateways, and many others.

Another challenge in the integration of ad-hoc networks with the wider Internet is brought about by the use of on-demand source routing protocols (e.g. DSR). In the case of supporting Internet connectivity via gateway nodes, extensions to the DSR are necessary. Since the scope of DSR is limited to the interior of the ad-hoc network, routing of a packet across the ad-hoc network boundary will require extensions to the source route information in the DSR header.

This paper presents an architecture framework suitable for integration of ad-hoc networks with the Internet via multiple gateways. We discuss gateway discovery and handoff schemes suitable for the Mobile IP based routing of IP packets across the multiple gateways. As part of the the presented architecture, we propose new mechanisms designed with performance improvements in mind, such as: a new route discovery scheme; modifications to the routing protocol DSR facilitating routing across a gateway; and new handoff triggering and buffering scheme useful in smoothing handoffs between gateways.

The rest of this paper is organised as follows: Section II presents the essential network architecture framework. Section III discusses the issues of Mobile IP agent (gateway) discovery. Section IV discusses the issues in routing interoperability in the context of DSR routing across a gateway. Section V illustrates the scheme for multiple gateway handoff. Conclusions and future work are provided in Section VI.

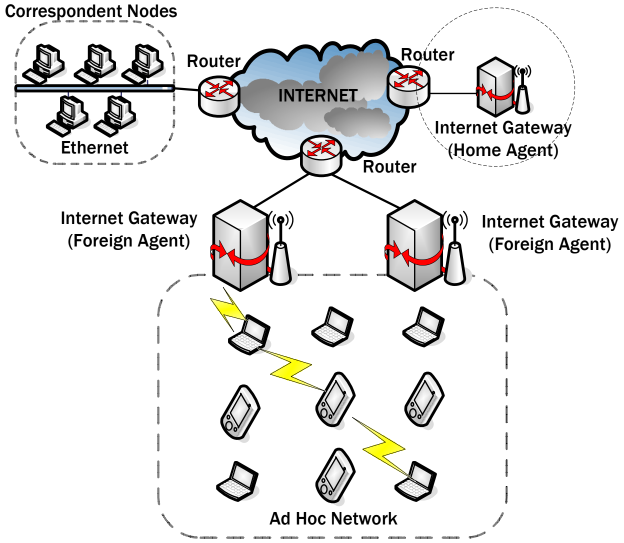
Correspondent Nodes
Router
Router
INTERNET
Internet Gateway (Home Agent)
Ethernet
Router
Internet Gateway (Foreign Agent)
Internet Gateway (Foreign Agent)
Ad Hoc Network

Fig. 1. Network architecture

II. Architecture framework

An example of an ad-hoc network integrated with the Internet is shown in Fig. 1. We assume the network under consideration comprises the following elements:

- The ad-hoc network consisting of mobile nodes with wireless interfaces and routing capabilities to perform multi-hop communications.
- Correspondent nodes, which are nodes connected to the Internet, and hence assume connectivity is possible with all other nodes, including ad-hoc network nodes.
- Gateways between the Internet and an ad-hoc network. The gateways are user nodes of the ad-hoc network (via, for example, their wireless LAN interface) that feature access to the Internet via additional interfaces (e.g. a 3G or LAN). These are effectively IP (edge) routers. The gateways may be either a Mobile IP Home Agent or Foreign Agent (or both).

The challenge with integrating the ad-hoc network with the Internet is to ensure the ad-hoc network nodes and correspondent nodes can communicate seamlessly. For this, we need to utilise Mobile IP, combined with enhancements to cope with the additional complexities introduced by the ad-hoc network.

According to the Mobile IP principles, when a node roams to a new foreign domain, it can receive a care-of address from the Foreign Agent, and all packets addressed to this node's home address will be tunneled to the care-of address. In the case of an ad-hoc network integrated with the Internet, the ad-hoc network becomes the foreign domain for the roaming node, and the gateway node becomes its serving Foreign Agent. The home IP address of the roaming node will therefore have to be the IP address identifying the node globally, and it also has to be retained as the roaming node's identifier within the ad-hoc network domain.

The ad-hoc network is visible from the Internet side via the IP address of the gateway. This gateway also happens to be a Foreign Agent for the nodes currently in the ad-hoc network. However, the ad-hoc network nodes will have their home addresses featuring a network prefix different from that of the gateway, and therefore will have to register with the gateway as their Foreign Agent. The registration procedure is discussed further in Section III. This becomes a more complicated and challenging task when there are multiple gateways and the ad-hoc nodes need to be able to select and change gateways.

Routing is an essential function in scenarios where the ad-hoc network is treated as an extension to the wider Internet. We assume a reactive routing protocol and the ability of the gateways to decide if the packets received on the Internet or ad-hoc side interfaces need to be forwarded across the boundary between the two networks or not. The detailed operation of routing schemes proposed as part of our architecture is described in Section IV.

If there are multiple gateways connecting the ad-hoc network to the Internet, the mobile nodes need to be able to select the gateway that can provide the most appropriate service. The paths between mobile nodes and the gateway may be multi-hop routes, thus the link status detection used in standard Mobile IP [1] to handle triggers for Mobile IP procedures is not applicable within the ad-hoc network architecture. In addition, mobility of a node will usually necessitate multi-hop route reconstruction between mobile nodes and gateway. In Section V, we propose new handoff triggers that can be used in this multi-hop scenario with multiple gateways.

III. Mobile IP Gateway Discovery

Whenever a Mobile IP node roams to a new access network, it must discover a Mobile IP Agent and register with it. The method used to discover the agent (gateway) is heavily dependent on the networking and communications scenario. The specific methods that can be used to propagate Mobile IP control messages throughout ad-hoc networks will determine the network performance, especially the registration and handover delays. In this section, we discuss two groups of methods for gateway discovery (Sections III-A to III-C). Once the gateway is discovered, the actual registration requests and replies follow the normal Mobile IP procedure, except that the control packets are propagated via multi-hop routes.

A. Agent Advertisements

The gateway between the ad-hoc network and Internet is configured as a Mobile IP Agent. On the wireless interface, it has to advertise its existence by broadcasting the Agent Advertisement, an *ICMP Router Discovery Protocol* (IRDP) packet. The ICMP packet is generated in order to broadcast the address of a router. The Agent Advertisement has an IP header with local broadcast as a destination address, and an ICMP header. The Registration Request and Registration Reply packets in standard Mobile IP [1] are application layer packets using UDP as the transport protocol. The standard Agent Advertisement message is a direct (local) broadcast packet which will not be propagated further than one hop away. Hence in the ad-hoc network where the majority of mobile nodes are located multiple hops away from the gateway, the approach to propagating the ICMP and registration packets multiple hops away from the source is the key for mobile nodes to receive the appropriate agent discovery information.

B. Proactive vs Reactive Agent Discovery

Mobile IP agent discovery methods are discussed in [3][4][5]. The two main methods are *proactive* and *reactive* gateway discovery.

- **Proactive Discovery**: The Foreign Agent periodically broadcasts the Agent Advertisement that can be rebroadcast by ad-hoc nodes to flood the entire ad-hoc network.

All mobile nodes can register with the Foreign Agent once they have received the rebroadcasting message, and periodically refresh the registration information.

- **Reactive Discovery**: The Foreign Agent does not broadcast advertisements periodically, but instead mobile nodes broadcast solicitation messages in search of an agent. The Foreign Agent unicasts its advertisement to the mobile node via the multi-hop route once it receives the solicitation. In this method, mobile nodes may elect to seek a Foreign Agent and register only when they have data to transmit across the gateway to the wired network.

There are two opposite views concerning the gateway discovery schemes in ad-hoc networks. The first one maintains that flooding gateway advertisements will enable MANET nodes to select a closer gateway. This will reduce the average distance between gateways and MANET nodes, which in turn will reduce the number of packet transmissions required to transfer user data between gateways and MANET nodes. Depending on user activity, this reduction can be larger than the overhead of flooding control packets. Other flow-on benefits from minimising the average distance between MANET nodes and gateways are the decrease in average user data delay, and less frequent loss of contact between MANET nodes and their gateways [3]. The other view deduced from [4] maintains that periodical advertisements will cause the majority of advertisements received by MANET nodes being redundant. Nodes that do not require Internet connectivity will receive and transmit unnecessary control messages. The bandwidth and energy will be wasted. Flooding of any packets (including control messages) can easily lead to severe degradation in throughput performance of the network, hence periodical advertisements for the purpose of agent discovery should be abandoned.

A number of researchers have proposed agent discovery mechanisms based on the proactive and reactive approaches (e.g. [2-6]). A brief qualitative summary of the results in [3] and [5] using AODV are presented in Table I.

TABLE I
REACTIVE VERSUS PROACTIVE METHODS COMPARISON.

	Proactive	Reactive
Mobile IP overhead	High	Low
On-demand routing overhead	Low	High
Total overhead	Low	High
Throughput	High	Low
Average delay	Low	High
Packet delivery ratio	High	Low
Energy consumption	High	Low

A conclusion can be reached that in the majority of cases proactive gateway discovery will lead to lower delays and better throughput performance. With the increasing size of the ad-hoc network, the performance of proactive agent discovery generally decreases. However, this does not mean that the reactive agent discovery schemes will always be better for larger networks. From Sun's work [5], we can see that the reactive registration method not only leads to long latencies, but also fails to address the resource consumption problem. In proactive schemes, only one flooding of an Agent Advertisement message could satisfy registration requirements of all MANET nodes. In the reactive method, a node still needs to broadcast an Agent Solicitation message to flood the entire MANET, but only one Agent Advertisement message can be sent back to the source node via a known multi-hop route. Agent Solicitation messages sent by many nodes can cause serious throughput degradation.

C. Advertisement Propagation Options

We propose two options for propagating the Agent Advertisement messages: the first option involves simple rebroadcasting of the whole packet; the second involves encapsulating the Agent Advertisement packet in the extension field of `RREQ` (Route Request) packet. When the first option is used, the Agent Advertisement packet will not be processed as part of normal ad-hoc routing procedures, so the receiver will not be able to obtain the ad-hoc route information from the packet, and subsequently an extra route discovery will have to be activated to find a valid route to the gateway. With the second option, the receiver will be able to obtain the ad-hoc route to the agent together with the Agent Advertisement message when it receives the broadcast of the `RREQ` packet. The first option is suitable for a low mobility environment. The second option will work well in the high mobility environment because the *agent discovery time* is reduced. An optimised rebroadcasting scheme is used to avoid rebroadcasting of duplicate packets. Before rebroadcasting, each node uses the *Sequence Number Table* to check if the advertisement has been received and rebroadcast before.

IV. ROUTING INTEROPERABILITY

On-demand routing protocols, e.g. DSR or AODV, use unique node identifiers, e.g. IP addresses, MAC addresses, or ID numbers. Few researchers have considered the interoperability of ad-hoc routing protocols with other routing protocols in cases such as the architecture for ad-hoc networks integrated with the Internet considered in this paper. It is usually assumed that for stand-alone ad-hoc networks successful implementation of route discovery and maintenance mechanisms is independent from the presence or absence of IP at the network layer. This assumption is no longer appropriate when we consider ad-hoc routing within the realms of IP-based networking, especially when communications across the boundary between ad-hoc network and the Internet are required. Therefore, the interoperability between (or interfacing of) IP routing and ad-hoc routing is well worth attention.

We propose a new solution for interfacing of on-demand ad-hoc routing protocols (specifically, DSR) to IP routing and Mobile IP. In the next subsection, we provide a detailed description of the proposed solution.

A. Interfacing to IP

Here, we present a protocol structure at the network layer level suitable for on-demand routing protocols. The interface between IP routing and on-demand routing is based on IP forwarding principles. It is assumed that the on-demand routing is a child process of IP forwarding, activated to obtain next hop address for IP routing, in cases where IP routing fails to locate the next hop towards the destination in the routing table.

Fig. 2 shows the flowchart of processing packets at the network layer level of our network model. The on-demand routing configured on the gateway's wireless interface is responsible for transfer of packets between wired and wireless interfaces, and processing of packets transmitted from/to the correspondent nodes on Internet. All on-demand routing

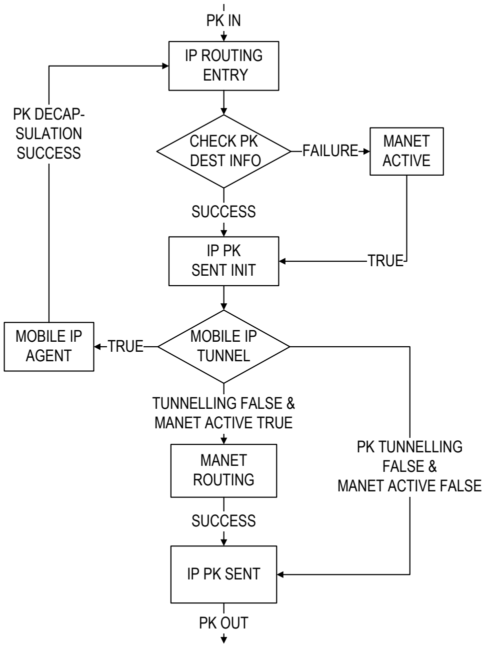

Fig. 2. Flowchart of processing packet on network layer

control messages sent to the correspondent node will be intercepted and processed by the gateway node. The gateway node determines if the requested routes are external, by checking for all route requests initiated by the ad-hoc nodes if the target address is located within the ad-hoc network or on the Internet. In Fig. 2, if there is a packet received from higher layer or received from MAC layer, it enters the IP routing, and subsequently the *packet destination information checking* function will compute the destination information to decide where to send this packet, to higher layer, broadcast, or external network interface. If the information cannot be obtained via the IP routing function, the MANET routing function is activated to set the required destination information for ad-hoc routing (`MANET_ROUTING`). Otherwise, if the node is not a part of active MANET, the packet is initialised for sending (`IP_PK_SENT_INIT`) as if the ad-hoc routing function does not exist. Before the packet is ready to send according to the obtained destination information, the *Mobile IP packet tunnelling* function checks whether this packet is used to tunnel another IP packet; if so, the packet is sent to the *Mobile IP Agent* for decapsulation, and the decapsulated packet is subjected to the routing procedure again. If the packet is not an IP-in-IP packet, and MANET routing has been activated, this packet will be sent to `MANET_ROUTING` to obtain the multi-hop routing information.

Fig. 3 illustrates the flowchart of *packet destination information checking* function in Fig. 2. If the check returns `FAILURE`, the MANET routing will be activated to handle the packet. If the destination is a broadcast address or the packet is a MANET packet, then the function returns the value `SUCCESS`. If the packet is from a lower layer and the processing node is not a gateway node, then the packet is destroyed but the function still returns `SUCCESS`.

B. Route Discovery

In a stand-alone MANET, the route discovery is based upon a query-reply cycle, with flooding of queries towards a target of an unknown address. In the ad-hoc network interconnected with Internet, if the target node is located outside the ad-hoc network, the source node will not receive a reply from the target directly, but via other MANET nodes acting as proxies for the target.

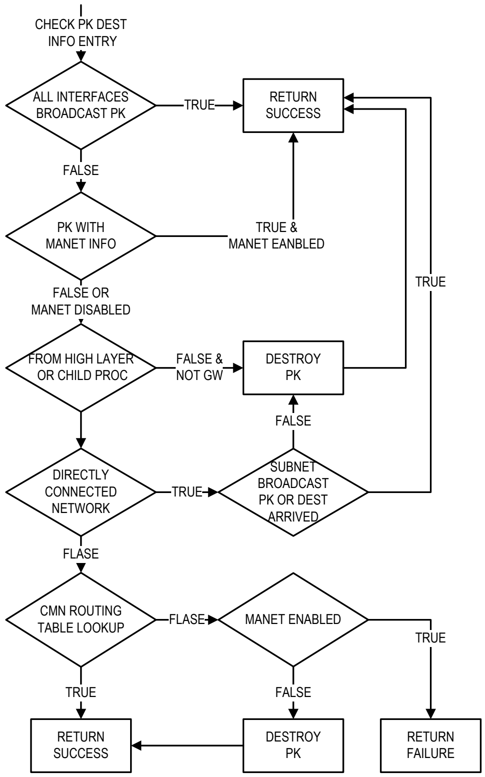

Fig. 3. Flowchart of IP routing to obtain destination information

Sun [5] presented a route discovery scheme for the gateway to detect the location of the target of `RREQ`. The Foreign Agent doesn't store any information on external routes, but determines from its AODV route table if the target is a registered node within the ad-hoc network. A main drawback of this scheme is that the Foreign Agent assumes that the target address is on the Internet when it is not a registered node within the MANET. Obviously, the assumption is that the Internet nodes are not registered with the Foreign Agent. Such procedure means that for all target nodes on the Internet, the Foreign Agent has to send back `FA-RREP`s to the initiator, and the initiator has to wait until a predetermined number of `RREQ` attempts have been made before it can transmit packets via the Foreign Agent. This may cause undue delay when the attempt is made to communicate with correspondent nodes on the Internet. It also causes unnecessary `FA-RREP` messages from FA when the target is a registered node within MANET and the initiator could receive the `RREP` directly from it within the MANET.

We propose the following route discovery scheme. The gateway will be able to respond promptly if it can maintain more routing information in its IP routing table. Since the gateway is a Foreign Agent, it should have information about all ad-hoc nodes registered with it. On the other hand, the gateway may gather external routing information in a way typical of an edge router. The gateway can use the information about the exterior and about the registered ad-hoc nodes to form responses to route request queries. There are a number of possible scenarios for route discovery. Two examples are as follows:

1) Host Initiated Scenario: If the ad-hoc network nodes are configured with IP addresses characteristic of this specific ad-hoc network (this scenario is unlikely in the case of hosts configured with their own home IP addresses), they will feature the same subnet address. The initiating host will then be able to recognise from the network prefix that the target is not within the ad-hoc network. Now the initiator only needs to know a route to the gateway and send the packet directly to the gateway.

2) Affirmative Reply Scenario: If the MANET nodes have IP addresses (e.g. home addresses) with a range of network prefixes, the initiator will not know whether the target is within the ad-hoc network or not. It will broadcast a `RREQ` to enquire about a route to the target. The `RREQ` packet floods the ad-hoc network and eventually will also be received by the gateway. The gateway looks up its IP routing table and enquires other Foreign Agents to find a matching network prefix for the target address. If the target address is confirmed to be outside the MANET, the gateway will create a proxy `RREP` containing the route from the target to the initiator and send it back to the initiator of the `RREQ`. The initiator can use the proxy `RREP` to update the route to the target. If the initiator of the `RREQ` does not receive any `RREP` within the *request expiry time*, it will conclude that the target is an unknown address on the Internet and send packets to the gateway.

C. Ad Hoc Routing Extension

Problems may arise when external routes are incorporated into stand-alone ad-hoc routes. This is especially so if source routes are used. For example, in the standard DSR routing protocol [10], every node maintains a *Route Cache* with all complete routes to known destinations. Every data packet exchanged between hosts on the ad-hoc network will have a DSR header with a *source route option* listing all intermediate addresses of nodes along the path to the destination. Nodes from outside the ad-hoc network are excluded from DSR route discovery procedures, hence packets to and from external nodes cannot normally be routed by means of DSR. Therefore, it is essential to develop extensions to ad-hoc routing to facilitate routing of packets across a gateway.

In [9], Broch described a technique that allows a single ad-hoc network to span across a range of heterogeneous link layers. Some assumptions are also presented in [9] for integrating MANET with heterogeneous interfaces, e.g. other Mobile IP networks. In [10], a method for including external route flag in DSR is mentioned, where two external flags indicating an arbitrary path external to the DSR domain, are reserved for future use. However, the details of using the external flags have not been discussed in [10]. In our work, the DSR internet extension is operating in the following way:

1) When an IP packet arrives at the gateway from the Internet, the gateway inserts the DSR header, including source route, and marks the DSR packet as First Hop External. The packet indicates the source is the Internet correspondent node, and source route contains the gateway node as the first intermediate node, followed by the rest of the route to the destination ad-hoc network node.
2) The route maintenance and route cache update are sensitive to the external route. Upon receiving the DSR packet, an intermediate ad-hoc node sends an acknowledgment to the preceding ad-hoc node. The intermediate node also updates the route to the correspondent node in its route cache and marks it as Last Hop External.

Further details on the DSR modifications, including maintenance, salvage, route update and route error, will be presented in the future.

V. Multiple gateways handoff

The topic of multiple gateways between an ad-hoc network and the Internet and the handoffs of mobile nodes between gateways has not received significant attention in the known research literature. In our architecture, the relevant issues are considered to be of high importance.

If the ad-hoc nodes are allowed to select and change the gateway to the Internet, the handoff between gateways becomes an important issue. Mobile IP was originally designed without any assumptions about the underlying link layer, and as a consequence, the link layer handoff is usually assumed to occur prior to Mobile IP handoff. However, because of the multi-hop nature of ad-hoc network paths, the handoff between gateways cannot use the knowledge of link connectivity status to trigger handoff events. Some problems arising from the multi-hop nature of ad-hoc network are as follows.

- Before a mobile node can receive an advertisement from a new agent, it must establish connectivity with the new agent. Direct link connectivity is generally not available in ad-hoc networks and has to be replaced by a multi-hop path. The path re-establishment process (replacing link level handoff) may be a lengthy process, during which the node is unable to send or receive packets. The handoff latency and packet loss are therefore serious problems of the Mobile IP agent handoff in our scenario.
- Nodes that have no direct link connectivity with the Foreign Agent cannot detect the existence of a new agent directly and utilise link layer triggers.
- If smooth handoff procedure (optimised Mobile IP) is not used, a mobile node may lose both agents until the Registration Reply from the new FA is received, and the packets traversing the multi-hop path during the blackout time will be lost. On the other hand, buffering of packets during handoff may lead to packet disordering and duplication.
- If an ad-hoc node has no valid route to a new FA, even though it has obtained the new FA's information, it will have to establish a new route at the expense of extra delay (more handoff latency) before it can actually register with the Agent.

Here, we present briefly our proposed solution. Throughout the future course of our research, we intend to develop a comprehensive scheme that considers various conditions in making the gateway selection and handoff decision. *Layer 3 proactive trigger*, *unpredictable route error*, and *predictable link status trigger* will be used to implement the desired strategies for gateway selections and handoff between gateways. In this paper, we don't address the specific criteria for gateway selection, but only provide the framework for handoff triggering mechanisms.

A. Multi-hop Handoff Trigger

If the nodes intend to register with a Foreign Agent via multi-hop paths, it is important to define the moment when the gateway handoff procedure should be triggered. We propose three essential triggers for FA handoffs in an ad-hoc network. In brief, they are *selective*, *passive* and *predictive* triggers.

- **Layer 3 Proactive Trigger**: For this trigger, we assume that the node has registered with a Foreign Agent already, and there is a valid active route between the mobile node and the FA. The new FA advertises its presence by broadcasting Agent Advertisement packets. When a mobile node receives the advertisement within a *hearing time*, possibly from several Foreign Agents, the FA at the shortest hop distance and highest priority is selected. If the preferred FA has higher priority than the current registered FA, the node may be triggered to execute a handoff while the current registration is still valid.
- **Unpredictable Route Error Trigger**: This trigger is caused by a Layer 3 Route Error due to an unpredictable wireless link break. If DSR routing is used, a node may attempt to salvage the data transmissions before sending back a RERR message to the source node [10]. If a new route can be found the packet may be salvaged by replacing the original source route with the new route. Otherwise, the source node upon receiving a RERR message will attempt to discover a new route to the destination. If the source node receives a RERR message indicating a broken route to the Foreign Agent, the source will interpret it as a trigger to execute a gateway handoff. However, in this case, the node has lost connectivity with the FA already, and packet loss is inevitable. This trigger can be seen as *post link failure trigger*.
- **Predictive Link Break Trigger**: The reliability of a link (or route) is estimated and the loss of connectivity is predicted before the link goes down, so the mobile node can execute a gateway handoff in advance. From the source to the destination, each node monitors the link status with its previous hop node. The mobile node measures the signal power and then estimates the link break time. The trigger can be considered as a predictive trigger issued before the links of a route are broken.

In our proposed solution, the three triggers may be used together. Firstly, *layer 3 proactive trigger* and *post link failure trigger* are employed. Then, *predictive* method allows the mobile node to send solicitations for a new FA before connectivity with the current FA is lost, which ensures smooth handoffs in most cases. We propose an improvement to the *predictable link break trigger*, two *prediction levels*, applicable to a high mobility environment. When the intermediate node receives the *predictive link break trigger* from the link layer, it will send back to the source node a notification, and then a handoff will be triggered. The first prediction level will indicate that the broken link can be repaired by ad-hoc route reconstruction; the second level will indicate that the link cannot be repaired and a new route must be established to a new FA. The handoff must start between the first and second levels of the trigger.

B. Smooth Handoff

Another possible problem in gateway handoff is duplication or disordering of packets resulting from buffering scheme. When the mobile node switches to another agent, the previous agent can buffer packets destined to the mobile node, and then send these packets to the new agent after the handoff is finished. If the buffered packets are not sent to the new agent before the new agent starts forwarding new incoming packets to the mobile node, the mobile node may receive disordered or duplicate packets. If TCP is used, it may falsely trigger a TCP sender's loss recovery and congestion control. A spurious retransmit will occur [11], as well as unnecessary reduction of the TCP congestion window and slow start threshold. In the optimised smooth handoff scheme [7][8], when a node sends Registration Request to new FA, a previous FA notification is attached. However, before the previous FA receives the Binding Update from the new Agent, the packets in transit are still lost, because the previous FA has lost connectivity with the mobile node. To combat this problem we propose to buffer packets at the new FA. When the new FA receives the Registration Request from the mobile node, it sends a *Handoff Request* to the previous FA, then the previous FA will send a *Handoff Ack* and all packets destined to mobile node, to the new FA. During the handoff procedure, the new FA buffers all packets in the correct order until a Registration Reply from Home Agent is sent to the mobile node. The previous FA has the responsibility for redirecting packets from the previous CoA to the new CoA of the mobile node after it has received a Binding Update from the mobile node. By this method the packet losses and disordering are reduced.

VI. Conclusion

Integrating ad-hoc networks with infrastructure-based Internet is a challenging task. In this paper, we analysed the Mobile IP agent registration, routing interoperability, and smooth gateway handoff issues arising when an ad-hoc network is connected to the Internet via multiple gateways. We proposed an architecture framework for supporting IP mobility and communications across the boundary between ad-hoc network and the Internet. Future work will include detailing extensions to DSR at the Internet gateway, and analysing the performance of the options. The use of other on-demand routing protocols, e.g. AODV, will also be explored.

References

[1] C. Perkins, Editor, "IP Mobility Support", RFC 2002, *Internet Engineering Task Force*, Oct., 1996.

[2] Y.-C. Tseng, C.-C. Shen, and W.-T. Chen, "Integrating Mobile IP with Ad Hoc Networks", *IEEE Computer*, Vol. 36, No. 5, May 2003, pp. 48-55.

[3] U. Jonsson et al.,"MIPMANET: Mobile IP for mobile ad-hoc networks," *in Proc. MobiHoc*, (Boston, USA), 2000.

[4] R. Wakikawa, et al., "Global Connectivity for IPv6 Mobile Ad Hoc Networks" (draft-wakikawa-manet-globalv6-03.txt), *Internet Draft, Internet Engineering Task Force,* Oct. 2003.

[5] Y. Sun, E. M. Belding-Royer, and C. E. Perkins. "Internet Connectivity for Ad hoc Mobile Networks." *Intl. J. Wireless Information Networks*, 9(2), April 2002.

[6] P. Ratanchandani and R. Kravets, "A Hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks", *Proc. Wireless Communications and Networking 2003*, Vol. 3, March 2003, pp.16-20.

[7] C. Perkins and D. Johnson, "Route Optimization in Mobile IP", *IETF Internet Draft,* March 2003.

[8] C. Perkins and K-Y. Wang, "Optimized smooth handoffs in Mobile IP", *Proc. IEEE Symp. Computers and Communications*, Egypt, July 1999.

[9] J. Broch, D. A. Maltz, and D. B. Johnson, "Supporting Hierarchy and Heterogeous Interfaces in Multi-Hop Wireless Ad Hoc Networks," in Proc. *Wrkshp. on Mobile Computing, in conj. Intern. Symp. on Parallel Architectures, Algorithms, and Networks*, (Perth, Australia), June 1999.

[10] David B. Johnson, David A. Maltz, and Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt, *IETF Internet draft,Internet Engineering Task Force,* April 2003.

[11] D. Badache et al., "Performance enhancement of smooth handoff in mobile IP by reducing packets disorder", *Computers and Communication, 2003. (ISCC 2003). Proceedings. Eighth IEEE International Symposium on,* 30 June-3 July 2003, pp.149-154 vol.1.