Analysis of NAT-Based Internet Connectivity for Multi-Homed On-Demand Ad Hoc Networks

Paal Engelstad, Geir Egeland, Do Van Thanh
University of Oslo (UnIK) / Telenor R&D, 1331 Fornebu, Norway
{Paal.Engelstad, Geir.Egeland, Thanh-van.Do}@telenor.com

Abstract. A prerequisite for a widespread and successful deployment of on-demand ad-hoc networking technology is its ability to provide easy access to the Internet. Existing solutions for Internet access are mainly based on modifying Mobile IPv4 (MIPv4). An easier approach, yet poorly documented in published material, is to implement Network Address Translation (NAT) on Internet Gateway nodes in the ad hoc network. In this paper we describe problems experienced by simulations of common NAT-based solutions under the condition of site multi-homing. Based on our results, we propose a working alternative solution for multi-homed ad hoc networks.

Keywords: Ad Hoc; MANET; NAT; Multihoming; AODV.

1 Introduction

IP-based applications, such as web browsing, e-mail, telnet and ftp, mainly communicate with servers or peers over the Internet. Mobile Ad-hoc Networks (MANETs) [1] have no fixed infrastructure, and services on the Internet might not be available in these networks. A likely scenario is that nodes on an ad-hoc network in some cases also want to connect to nodes on the Internet, using services available there. For a widespread and successful deployment of MANETs, the ability to provide easy access to the Internet is therefore a prerequisite.

A possible solution is to let a node that is participating in a MANET operate as an Internet gateway and provide other nodes on the MANET with Internet access. One approach is to implement a Mobile IPv4 Foreign Agent (MIP-FA) on the gateway [2-3]. MANET nodes that require Internet access, implement a Mobile IPv4 (MIPv4) [4] client, and register the globally routable IPv4 address of the gateway as a care-of-address with their MIPv4 Home Agents (HA).

However, a Mobile IP-based solution has a number of drawbacks and introduces high complexity to implementations. The scheme requires changes to the Mobile IP implementation on both the Mobile Host (MH) side (i.e. on the source node requiring Internet access) and on the Foreign Agent (FA) side (i.e. on the gateway). Since the MH and the FA are no longer on-link, both sides will have to deal with Agent Solicitations and Agent Advertisements in a different way; TTL values and IP destination addresses must be set differently; ARP must be used differently and MAC-addresses are no longer relevant for communication between the MH and the FA. Moreover, independent co-existing implementations of MIPv4 and a MANET routing protocol are not trivially managed, since both implementations will make unsynchronized modifications to the routing table.

Another drawback that limits the applicability of a MIP-based solution for Internet connectivity is that it assumes that the care-of-address of the gateway is globally routable. However, the IPv4 address space is a scarce resource, and many MANET gateways might only be able to acquire a single IPv4 address on the external network to which they are connected [5]. Since NAT-devices can be nested, this solution will work even when the MANET Internet Gateway acquires a private IP address from the external network.

Although NAT solutions for MANETs have emerged in different test-bed implementations (see for example [6]) little has been documented, neither in scientific papers nor in IETF Internet Drafts.

A challenging issue with the use of NAT in general relates to site multi-homing. Since a NAT-device translates both outgoing and incoming packets, all traffic belonging to one communication session (e.g. TCP session) must traverse through the same NAT-device, otherwise the session will break. When the site is multi-homed, it can be difficult to control that all packets from one session are consistently routed through the same NAT-device.

This issue is also highly relevant to MANETs. Since MANETs are without infrastructure, it is difficult to eliminate the eventuality of multi-homing. It is not possible to control the network behavior in such a way that there is only one node on the MANET operating as a MANET Internet gateway. Even if there existed a simple solution to suppress a second node to operate as a gateway, the problem would re-emerge at the moment when two MANETs, each with a NAT-based gateway, merge into one network. Shutting down one of the gateways would mean breaking all on-going communication sessions over that gateway.
In this paper we address the lack of a good mechanism for IPv4 Internet access in on-demand MANETs, i.e. in MANETs that are routed with a reactive routing protocol, such as the Ad hoc On-demand Distance Vector (AODV) [7] routing protocol or the Dynamic Source Routing (DSR) [8] protocol. The paper examines the use of NAT for this purpose and points out problems with common NAT-based solutions and multi-homing as experienced by simulations.

To expose these problems, it was sufficient to limit our analyses to scenarios where a MANET node uses one of the available gateways for external Internet access. Hence, dynamic handovers of gateways could easily be kept beyond the scope of this paper, without a loss of the generality of the presented results. In a realistic scenario, however, a MANET node that is communicating with the Internet might desire to change gateways dynamically to cope with changes in the MANET topology. If the MANET node implements MIPv4 and has been assigned a HA present on the Internet, it might be able change gateway seamlessly. A new gateway means a new destination IP-address for incoming external traffic (i.e. a new translated IP-address for NAT-based gateways or a new care-of-address for MIP-FA based gateways). When the MANET node changes to a new gateway, it must register the new address with the HA. If the new gateway is NAT-based, it might use the NAT-traversal scheme developed for MIPv4 [9].

In Section 2 we present on-demand routing protocols and proposed NAT-based solutions for providing Internet connectivity to on-demand MANETs. In Section 3 we present our simulation results and analyze how a NAT-based solution works in scenarios of multi-homing. Based on our findings, a proposed solution for NAT-based gateways is presented in Section 4.

2 Background

2.1 Reactive (“On-Demand”) Routing Protocols

A number of reactive routing protocols have been proposed. The most widely studied and popular proposals include the AODV and the DSR protocols.

Reactive protocols allow source nodes to discover routes to a destination IP-address on demand. Most proposals, including AODV and DSR, work as follows: When a source router needs a route to a destination for which it does not already have a route, it issues a Route Request (RREQ) packet. The packet is broadcasted by controlled flooding throughout the network, and sets up a return route to the source.

If a router receiving the RREQ is either the destination or has a valid route to the destination, it unicasts a Route Reply (RREP) packet back to the source along the reverse route. The RREP normally sets up a forward route. Thus, the RREQ and RREP messages set up two uni-directional unicast routes in opposite directions between source and destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. (The acronyms RREQ and RREP are borrowed from AODV.)

Different reactive routing protocols have different strategies to deal with route maintenance and route repair. Most protocols let routes that are inactive eventually time out. If a link break occurs while the route is active, the routing protocol normally implements an algorithm to repair the route.

Different protocols have different ways to manage routing state information. With AODV, for example, correct forwarding of packets between source and destination relies on stored state information in routing tables on intermediate nodes in the network. With DSR, on the other hand, the sender of the packet encodes the entire route explicitly into the packet, and the packet is source-routed from source to destination.

The main focus in this paper is set on on-demand networks that use AODV as a routing protocol. However, the analyses, results and proposals presented in this paper are of a general nature and should also be applicable to other reactive routing protocols, such as DSR.

2.2 NAT Solutions for On-Demand MANETs

The Uppsala University’s implementation of AODV [6] includes a NAT-solution. Mobile hosts are unaware of its presence, and there is no explicit NAT discovery. Instead, a Source Node (SN) in search for another node issues a RREQ to establish a route to that node, indifferent on whether the targeted node is present locally on the MANET or externally on the Internet.

Upon reception of RREQs, the Internet gateway responds with an RREP on behalf of any node that it believes is present on the Internet. The destination IP-address in this “Proxy RREP” is set to the IP-address of the node the SN is searching for. The advantage of this approach is that the SN can send packets to external nodes in the same way as it would to nodes that are present on the MANET.

A mechanism is required to ensure that communication will not escape through a gateway when the destined node is present on the MANET. This is normally solved by mandating that the Internet gateway always copy the AODV-specific destination sequence number of the RREQ into the corresponding field of the RREP. The destination sequence number is set to the highest known sequence number of the destination searched for or to zero if the number is unknown (e.g. if the MANET node is external and not present on the MANET). A MANET node present on the network, on the other hand, will always return its non-zero destination sequence number before returning the RREP. Since the highest sequence number gives preference during route discovery, routes to MANET nodes present on the MANET will always have preference over routes established by Proxy RREPs sent by gateways.
2.3 Race Conditions with Proxy RREP for NAT in Multi-homed MANETs

Engelstad et al. [10] reported problems with Proxy RREPs for NATs in a small multi-homed test-bed implementation. They tested site multi-homing in a MANET with two NAT-based gateways present. The analyses presented in the paper are independent on whether the NAT-modules of the gateways do port translation or not. The source node (SN) communicated with an external host (XH), and both gateways (GW1 and GW2) were reachable through the same Intermediate Node (IN). The test configuration is illustrated in Figure 1.

Initially SN established a route to XH over one of the gateways, i.e. GW1. The SN then established a TCP connection with XH, and periodically sent over short messages on 2 seconds intervals. Using the parameters proposed by the AODV specification, the route between the SN and GW1 would time out after 3 seconds. However, since AODV uses the data traffic to update routes, the route would hardly time out before the TCP connection sent a new packet. Hence, the route remained active, stable and unaltered without experiencing any significant problems.

As the transmission interval of data packets was increased to a period of 4 seconds, however, serious problems occurred. When every new packet was to be sent, the route had already timed out due to the 3 seconds route timeout of the AODV specification [7]. Thus, the SN had to re-discover a new route to the XH over GW1 before transmitting each packet.

Due to dynamics in the system, sometimes the RREP from the other gateway (GW2) would be the first to arrive at the IN during the re-discovery of the route. In these cases, the IN established a route to the XH through GW2.

The cause of this was that the RREPs from both gateways carried the same destination sequence number: Both gateways copied it from the RREQ sent by the SN. Furthermore, both RREPs carried the same hop-count since both gateways were one hop away from IN. Hence, when the RREP from GW1 finally arrived approximately a millisecond later, the IN did not update its route for the XH via GW1. According to the AODV specification, the IN had to discard and not process RREPs for a valid route unless its destination sequence number was higher or its hop-count was lower than those of the RREP that established the route. (Figure 2.)

When the outgoing TCP packets passed out through the NAT-module of GW2, the module naturally translated the source IP address of the TCP packets to a different address than the one used by the NAT-module at GW1. The packets were not recognized when they finally arrived at XH, and the TCP session would therefore break.

When this happens the TCP module of XH will normally respond by a “TCP Reset” message, to which different applications will react differently. When Telnet [11] was tested, for example, the application would shut down the Telnet connection immediately upon reception of the “TCP Reset” message.

In this paper, we will study these race conditions of Proxy RREPs in more detail and for larger networks by means of extensive simulations. Indeed, our simulation results confirm that the problems being reported in smaller test-bed experiments are highly relevant also for larger networks.

3 Simulations

3.1 Simulation Setup

GloMoSim [12], which includes code for AODV, was used as a tool to simulate site multi-homing in an on-
demand MANET. We used the WLAN 802.11 simulation module, and chose the Two-Ray radio channel model. The transmission power was adjusted to arrive at realistic radio ranges of either 50m or 10m, since these are relevant to WLAN scenarios and Personal Area Networking (PAN), respectively.

50 nodes were randomly distributed within a square of variable size. Two nodes were selected as NAT-based gateways. For these nodes, the AODV code was modified to allow them to answer with “Proxy RREP” on behalf of an external host (XH) on the Internet, as described above.

A source node (SN) was selected and communicated with an external host (XH) through either of the gateways, by sending it 1024-byte packets at a Constant Bit Rate (CBR).

3.2 Varying the packet transmission interval

First, we simulated static nodes with 10m radio-range in a 40m X 40m square and static nodes with 50m radio-range in a 200m X 200m square.

If SN periodically sends packets to XH on 500ms intervals (i.e. at a bit rate of 16Kbps) it will rarely experience that the session break due to the Proxy RREP race conditions. Since AODV uses the data traffic to update routes, the route will hardly ever time out before SN sends a new packet. Hence, the route remains active, stable and unaltered, and all traffic will be consistently directed out through the same gateway that SN used for the first packet (Figure 3).

However, as we increased the transmission interval of data packets to a period of more than 3 seconds (i.e. to a bit rate less than 2.67Kbps), the route to XH timed out before each packet was sent. This means that before the transmission of each packet, the route had to be re-discovered. With each such route discovery comes a certain probability that the route will change to another gateway due to the race conditions of Proxy RREPs. In this case the route might be changed to the other NAT-gateway, and the session will then break. Hence, when the transmission interval exceeded the AODV timeout value of active routes, the average number of session breakages per transmitted packet increased dramatically (Figure 3).

Indeed, these simulation results confirm that the Race Conditions for Proxy RREPs in small test-bed implementations, reported in [10], are highly relevant also for larger ad hoc networks.

For higher transmission intervals, the average session breakage per transmitted packet stabilized at around 25%. In such situations only approximately 4 packets on an average can be sent before a session will break. This must be considered a serious networking problem. Figure 4 shows how different network configurations (or "topologies") contribute to this average value for a transmission interval of 4 seconds (which corresponds to a transmission rate of 2Kbps).

It demonstrates that for the major part of the simulated static network configurations, one gateway is closer to the SN than the other gateway. The packets will then be almost consistently routed over the closest gateway, since AODV gives priority to the RREPs with the lowest hop count. With such network configurations, the probability of a session breakage is close to zero.

However, there is also a considerable share of network configurations (shown on the right hand side of Figure 3) where the gateway is an equal number of hops away from SN. It is these network configurations that contribute to the 25% average session breakage per packet reported in Figure 3.

3.3 Varying the terrain size

Since the network configuration has a major impact on the probability of a session breakage (Figure 4), we would expect that it would also be influenced by the terrain size.

With a small enough terrain size, every node will be one hop away from every other node, and both gateways will be
one hop away from the SN. Such a network configuration belongs to the set of configurations represented on the right hand side of Figure 4. As the terrain size increases, the probability that the two gateways are the same number of hops away from SN decreases, and more configurations belong to the set of configurations represented on the left side of Figure 4. Indeed, Figure 5 confirms the assumption that the probability of a session breakage per packet due to Proxy RREP race conditions decreases as the terrain size increases.

![Figure 5](image)

**Fig. 5.** The probability of session breakages per transmitted data packet due to race conditions of Proxy RREPs decreases as the terrain size increases. (95% confidence intervals)

An interesting property seen in Figure 5 is that the probability of a session breakage is about 50% in the case where every node sees every other node. This happens when the sides of the square is of 5m in the case of 10m radio range, or 25m in the 50m radio-range. A 50% probability means that the Proxy RREP has an equal chance to arrive from either of the two gateways. Thus, every time a new packet is to be sent, there is a 50% chance that the Proxy RREP from the ‘wrong’ gateway will arrive first. Then the packet will be routed to a different gateway than the one that was traversed by the previous packet.

The reason for the equal probability of receiving either of the Proxy RREPs first, can be accredited to the ‘ideal’ model of GloMoSim. The link delay is set to a constant value in the simulator, and every node has equal capabilities, such as processing power. There is nothing to distinguish the delay of the two different Proxy RREPs.

Each data packet to be transmitted will trigger a route re-discovery, with an approximate 50% chance of a session breakage for configurations where the gateways are the same number of hops away. For such configurations, this will also lead to a probability of a session breakage per transmitted data packet of approximately 50%. This explains why the network configurations on the right hand side of Figure 3 are distributed around a probability of about 50%.

In a real network, however, different factors would often favor one of the two gateways, even when they are an equal number of hops away from the SN. There will be differences in link delays, node capabilities, operating systems, and so forth. Engelstad et al. [10], for example, reported an 86% chance in favor of one of the gateways in such a scenario. Although this number is less damaging than the 50% value derived by simulations, the remaining 14% of the Proxy RREPs made considerable trouble in the test-bed. The SN was only able to send approximately 8 packets before the session broke.

### 3.4 Varying mobility and network dynamics

The simulation results presented until now have considered only static networks with no node mobility. Route discoveries were mostly initiated due to route timeout with the transmission interval exceeding the AODV timeout of active routes.

![Figure 6](image)

**Fig. 6.** The probability of session breakages per transmitted data packet increases as the level of mobility increases (95% conf. int.). A 1 second packet transmission interval is used.

To illustrate the effects of mobility, we simulated 50 nodes with a radio range of 10m in a square of 80m X 80m, and 50 nodes with radio range of 50m in a square of 400m X 400m. The SN sent a packet every one second (i.e. with a transmission rate of 8kbps). Nodes were allowed to move according to the Random Waypoint model with zero rest-time. The level of mobility was varied by changing the maximum velocity of the nodes (Figure 6). The zero-mobility result in Figure 6 corresponds to the result with a 1000 ms packet transmission interval depicted in Figure 3.

Although the packet transmission interval was safely below the timeout of active routes in this simulation, mobility leads to link breakages when neighboring nodes move out of each other's radio range. Link breakages will invalidate existing routes and force routes to be re-discovered. Each re-discovery of a route to an external host may trigger a possible race condition. Hence, as mobility increases, the probability of a session breakage increases (Figure 6).

Figure 6 shows that the effects of mobility can be dramatic: For example, in a PAN scenario of nodes with 10m radio range, mobility at only 1m/sec leads to an
approximately 17% probability of a session breakage per transmitted data packet. Hence, a session may only last for approximately 6 data packets before it breaks.

In wireless ad-hoc networks there will also be a certain amount of non-deterministic dynamics apart from node mobility, due to factors such as radio fading, packet collisions and so forth. These are factors that are not easily caught by the simulation model. However, just as for node mobility, these factors lead to link breakages, which will increase the probability of Proxy RREP race conditions.

4 An alternative to Proxy RREPs

In a network configuration where every node happens to see every other node, the race conditions of Proxy RREPs can easily be avoided. Since a SN receives all Proxy RREPs that gateways send, it can select which gateway to use from the source IP address of the Proxy RREP.

However, in a general multi-hop scenario that AODV is designed for, this is not possible. Even if intermediate nodes passed all the Proxy RREPs through to the SN, the intermediate nodes would only be able to establish one outgoing route to the destination address in the Proxy RREP. Hence, the SN would not be able to select a gateway, since the routing algorithm of the intermediate nodes has already made the decision.

One solution that eliminates the route race conditions in a general multi-hop scenario is to prohibit the use of Proxy RREPs. Instead, all NAT-based gateways must answer to RREQs for external hosts, with RREPs that establish an outgoing route to the IP-address of the gateway [10]. Hence, the SNs discover gateways explicitly.

For the detection of gateways, a SN could for example set a “Gateway”-bit in the RREQ when it believes that the targeted IP-address might be present on the Internet (e.g. if it has not succeeded in finding a route to it locally on the MANET). Upon reception of a RREQ with this bit set, a gateway will return a RREP that establishes a route to its own IP-address.

The packets that a SN wants to send to an external host are tunneled to the IP address of the gateway (Figure 7). The gateway decapsulates each tunneled packet, and the inner (encapsulated) packet is translated in the NAT module before it is forwarded onto the Internet. The first packet that the SN sends to an external host establishes NAT state in the selected gateway as the inner packet is passed through the NAT-module.

The external host will normally send a response to the IP-address found in the IP source address field of the first packet, which is the IP-address that has been translated by the NAT-module. Return traffic will therefore end up by the external interface of the NAT gateway. The gateway will translate the destination IP address and tunnel the resulting packet to the MANET node, as explained in detail in [10].

The tunneling functionality can easily be integrated into the routing modules of MANET nodes that might require global Internet access. The fact that the tunneling solution is SN-aware (unlike a traditional NAT-solution) does not introduce any problem since it does not affect protocols and applications above the IP networking layer.

An obvious disadvantage of tunneling, however, is that every packet tunneled in and out of the MANET will carry an overhead of 20 bytes if IP-in-IP encapsulation is being used [13]. However, to avoid non-deterministic network behavior due to race conditions, this is a small price to pay. Proxy RREPs can cause serious networking problems, as we have demonstrated in this paper.

5 Summary

By using Proxy RREPs, NAT-based gateways respond to RREPs on behalf of external nodes, and all data traffic destined for an external node will be received by the gateway. The NAT-module of the gateway translates the packet before it is forwarded onto the Internet.

By extensive simulations, however, we have shown that this solution experiences serious problems when the MANET is multi-homed. With a NAT-based gateway, all outgoing packets belonging to the same communication session must pass through the same gateway – otherwise the session will break.

Our simulations of static multi-hop network scenarios showed that communication sessions with an external host would break when the packet transmission interval exceeds the active route timeout of 3 seconds. This lead to a probability of race conditions between Proxy RREPs of different gateways that is unacceptably high. Traffic will be directed over different gateways in a non-deterministic way, and communication sessions will easily break.

By introducing dynamics into the network, such as node mobility, the situation gets worse. Already at relatively low levels of mobility, there is a high probability of a session
breakage - even when the packet transmission interval is safely below the active route timeout.

In summary, our simulations showed that the Proxy RREP solution is not appropriate for routing between the source node and gateways used for communicating with external hosts on the Internet. The most obvious solution is to prohibit the use of Proxy RREPs. Instead source nodes must tunnel packets to the IP-address of a selected gateway. This means that the source node must explicitly discover available gateways and their different capabilities, and select one according to its capabilities.

Further analyses of the proposed solution should be addressed by future work. Control message overhead due to gateway discovery and packet overhead due to tunneling are elements that should be evaluated. Furthermore, MANET nodes might use the NAT-traversal scheme developed for MIPv4 to be able to do a controlled and seamless change gateways. How this scheme should work when the mobile node resides on a MANET is an issue that needs to be examined in detail.

References

[6] Uppsala University's implementation (version 6) of AODV. http://user.it.uu.se/~henrik/aodv/