

Substantial and Flexible Internet Connectivity Solution for Mobile Ad hoc Networks using ‘Tunneling’ Mechanism

Sanjay Kumar

*Department of Information Technology
Rajkiya Engineering College Azamgarh, India*

Abstract

In this paper we will basically study that how the problem of efficient multi hop forwarding of packets can be done in ad hoc networks destined for a gateway providing Internet connectivity. Mobile ad hoc networks have become a major component of the future network development due to their ease of deployment, self-configurability, flexibility and between MANETs and existing IP networks. Indistinct address and routing spaces are hard to integrate. In this paper the AODV reactive routing protocol is extended to support the communication between independence on any existing network infrastructure. So it is able in finding ways to efficiently interconnect them with the Internet. In fact such interconnections are not very easy due to differences in mobility, addressing and routing the MANET and the Internet. We have carried out a systematic simulation based performance evaluation of the different gateway discovery approaches using NS2 under different network scenarios.. On the study of various proposals for MANET-Internet connection we found that many of them are lacking in robustness and in flexibility. For example, many solutions do not consider the presence of multiple gateways, and in such scenarios they either fail, or are less efficient due to the lack of multi-homing capabilities. For an efficient Internet Connectivity in Mobile ad hoc networks, multiple gateways, potentially multi homing and proper hand-over need to be supported. We compare two forwarding strategies; default routes and tunneling to gateways. We find that tunneling is more efficient and flexible in compare to default routes.

Keywords: MANETs, Forwarding Techniques, Default Routes, Half Tunnels, Indirection

I. INTRODUCTION

It is very crucial to interconnect the MANET to the Internet because MANETs are often inconceivable to have flat addressing and flat routing. In this paper, we will discuss that a solution for MANET-Internet connectivity must be robust enough to handle with the challenges in each of the above areas like sensors and MANETs, and should be flexible enough to develop opportunities to improve performance or consistency by doing multi-homing or load-balancing. Here we will discuss mainly three classes of forwarding, among these proposals; ‘host routes’ i.e., one explicit routing entry for each destination, ‘default routes’, that aim to provide route aggregation and ‘tunneling’ that encapsulates packets for the Internet with a gateway's address. Basically we will focus on the two latter strategies, because they are more widely proposed and aim to provide the most benefits. Our giving is the comparison of default routes and tunneling. However, default routes work best in a shared prefix non-transit network e.g., a single hop LAN with one default gateway, which is not the ordinary case for an ad hoc network. As an alternative, we can expect flat addressing in most scenarios, a combination of one or more gateways with network addresses translation (NAT) or Mobile IP connectivity [1]. In straight IP networks addresses are strictly assigned and nodes are placed in a hierarchy according to their address prefixes. The address prefix tells the location of the node and forwarding can be performed by a longest prefix match. With “flat addressing”, where mobile nodes continue to use their home address or pick a randomly chosen one, this does not work very longer. Mobile IP on the other hand allows nodes to keep their home network addresses while visiting a foreign adhoc network and still maintains global connectivity.

The home agent will make sure that packets to the ad hoc nodes are delivered to the foreign agent in the ad hoc network using tunneling. From there, the packets are forwarded to the ad hoc nodes by the earnings of the ad hoc routing protocol. In this paper we look at how “default routes” can be adapted to handle multi-hop forwarding in an ad hoc situation with several gateways running either NAT or Mobile IP. Then we show how forwarding to a gateway can be made more efficient by using “half tunnels”. We propose an approach where several gateways are supported and where the mobile nodes can guide the forwarding path. We will discuss the default route problem and extended default route problem in section 2. Section 3 contains the most important part of the paper called the “half tunnel” mechanism and its benefits over the default routes. In section 4 we will discuss the use of Indirection in MANET-Internet connection and the section 5 is all about the half tunnels and indirection.

II. DEFAULT ROUTE FORWARDING

The gateway forwarding schemes in the MANET plays a vital role for the flexibility of Internet connectivity. A default route is basically a routing table entry pointing to a gateway connected to the Internet. Default route is the entry for using the packets that do not match any other routing table entry. In compare to a host route (which matches only one destination), a default route provides route aggregation. However, there are two main issues with default routes in MANETs: (1). Like host routes, the default routes only maps to a next hop, and hence it suffers from the similar lack of indirection support. (2) The aggregation is in conflict with reactive routing approaches, because they only maintain minimal routing state. Thus, it is not possible to map a destination to the default route because there is no other routing state. Direct forwarding strategies [5] try to always use the shortest route available, and there is no way to identify the indirection points. There are two direct forwarding approaches: host route forwarding and the default route forwarding.

A. Representation of Multi-hop Default Routes

In a single hop LAN environment, the default route entry points to the default gateway that a host uses to forward packets to the Internet. On extending this principle to the multi-hop environment, there are two ways to view this setup. In the Figure 1 we have;

The default routes indicates then next hop to the default gateway.

Table 1: Two different routing table configurations to the same end. The address 66.35.250.151 is a destination on the internet

Table - 1(a)

Default	63.3.5.23	3
---------	-----------	---

Table - 1(b)

Destination	Next Hop	Hop Count
192.168.1.1	63.3.5.23	3
63.3.5.23	63.3.5.23	1
63.23.250.151	Default	-
Default	192.168.1.1	3

Route maps to the gateway address (192.168.1.1) and this gateway entry is used to find out the corresponding next hop. If the gateway can be reached over multiple hops, solution (a) will only indicate the next hop and a node has no state telling which gateway this default route actually leads to. Solution (b) is the solution suggested in the Globalv6 proposal [2]. It is different because the default route maps to the address of the presently selected gateway. We have to maintain the routing table for the next hop to the gateway. Note that (a) may require two routing table accesses and (b) in worst case three. Route look-ups may be necessary at each intermediate node on the path to the gateway and will be costly. One look-up is saved if the nodes in the ad hoc network have a shared prefix or if they run a proactive routing protocol. In the reactive case, nodes have to configure an extra host route entry to avoid subsequent route discoveries. Once the default route concept has been augmented for multi-hop scenarios, like in Figure 1(b), the default route entry is extra because each destination will have its own entry in the route table. These host route entries point straight to the gateway entry, which reduces the required routing table look-ups from three to two.

B. Avoidance of Inconsistent Routes

There are some reasons why approach 1(b) is preferred in a multi-hop environment. There is a precise mapping between a default route and the gateway address. It is very important when a node receives a control message with new information about the default route. Otherwise the node would not be able to tell if the control message will update the default route to point to a new gateway and inconsistencies in the path to the gateway can occur if the message is forwarded. Control messages that conflicts with the currently configured default route can be dropped. Other compensation is that one can configure multiple default routes which are distinguished by their gateway address. At last, if the routing protocol requires destination sequence numbers, it is not compulsory to keep a sequence number for the default route since it is just a mapping to a host entry. In (a), the default route is a "destination" and therefore needs a sequence number of its individual.

C. Modification to Default Route [3]

There are suggestions so that how to extend the default route concept for the use in MANETs. We show these extensions in Fig 1, which shows two alternative routing tables for a node that is located three hops from a gateway with address 192.168.1.1. Routing table 1(a) illustrates the standard usage of a default route, where it simply maps to the next hop (63.3.5.23). Note that there is no explicit entry for the gateway, and hence there is no way for the source node to know which gateway the default route leads to. If multiple gateways are located at several hops away, there is subsequently no way to influence the forwarding in such a way that packets reach a specific gateway. With reactive routing, one extra routing entry must also be installed, once an Internet destination has been discovered, otherwise the discovery is repeated for all the packets for that destination. The implication of this extra Internet destination state is the loss of all aggregation properties, which is the whole point of having a default route to begin with. Another problem is that the state must also be configured on all intermediate nodes on the path to the gateway, in order to avoid cascading route requests. The route reply

that sets up the Internet destination state must therefore be augmented to carry also the address of the Internet destination. If the route is changed, or optimized, any new nodes that become part of the route must also install all the forwarding state for Internet destinations on that default route. We refer to this problem of managing Internet destination state as the state replication problem. The Globalv6 scheme [3] advocates the extended default route approach shown in Fig 1(b). Under this scheme, the default route maps to the gateway address which in turn maps to the corresponding next hop. The improvement here is that the default route points to the gateway instead of the next hop, and therefore several default routes can be installed even if they share the same next hop. However, by definition this route is no longer a default route, since now several can exist simultaneously. Still, Globalv6 insists on the default route terminology. Further, extra host state is necessary to indicate which default route is used for a particular destination. This state must be consistent at each hop to the gateway and, unless consistency is rigidly enforced, the approach may suffer from state replication problems. The tunnel ends at the gateway, which decapsulates the packets before they are sent further. Fig. 2 shows tunneling between a source node and a gateway in a MANET. There are other potential optimizations that can be achieved with tunneling – usually with the trade-off of more tight integration with the routing protocol. For example, intermediate nodes could be made gateway aware by marking gateways with an extra flag in the routing tables. The benefit of this is that intermediate nodes do not have to perform gateway discovery themselves when they also want to communicate with the Internet. If nodes furthermore have configured a common IP prefix, they can directly determine whether packets should be tunneled to the Internet on already available gateway routes. After the modifications to the default route concept there is, as we see it, only one advantage remaining over host routes; namely the explicit listing of an Internet route in the routing table. While the host route approach needs a new route request for each Internet destination (like for any other MANET destination), the default route approach can reuse an existing default route in order to avoid having to do unnecessary route discoveries when locality can be determined directly. On the other hand, the host route approach would be able to discover different gateways for each Internet destination, while the default route approach would be bound to the default gateway.

III. PROPOSED WORK

For providing an increased amount of indirection, we suggest to use 'half tunnels'. This creates a one hop illusion between MANET node and the gateway. This half tunnel set up will provide a lightweight indirection point through the gateway on the path to the internet destination. In this section we will discuss tunneling proposed by Jonsson Etalin [1] as an alternative approach to default routes.

A. Half Tunnel Solution

The default routes has his own attractive benefits but the main advantage of a tunneling solution over the default routes is that the source node of a flow is always in full control and alone carries all the state necessary to forward a packet to a gateway. A half tunnel is in fact a transparent two-step for-warding mechanism for ad hoc network outbound packets. It can be viewed as a translation function for inter context forwarding or loose source routing with one indirection point. Fig 2 depicts an overview of the mechanism behind our half tunnel forwarding. . A half tunnel takes care of the forwarding of packets to an Internet gateway; it does not pact with how a mobile node is attached to the Internet. The half tunnel mechanism provide a smooth way of the transition of the packets to the gateway in the MANET-Internet connection and it has many advantages over the default route scheme for the packet transition in various areas like sensors and MANET to the connection with the Internet. Generally the name half tunnel refers to the fact that tunneling actually is only needed in the forward direction. But a disadvantage of tunneling is the overhead of encapsulation, which could be large for small data packets. But leaving this disadvantage overall it is a very strong mechanism for the packet transition to the gateway. The benefits of half tunnels are inherent from the indirection. By using half tunnel the one-hop illusion is created between a mobile source node and the internet gateway. Fig 2 provides a detailed view of the mechanism behind this process. In the first step, when a packet is found to be for an Internet host, it is routed through a half tunnel to the gateway by encapsulation. An encapsulated packet is sent to the gateway using the gateway's explicit IP address and the IP forwarding mechanism as configured by the ad hoc routing protocol. At the gateway, the packet will exit the tunnel and is decapsulated. In the second step, the initial packet is routed towards the final destination in the global Internet, after possibly having been subject to some address translation. Note that a packet like this is not using a default route, but use standard host route entries. Comparison can be made between the half tunnels and the way how in a LAN setting the IP stack and its ARP table translate a global IP address into the link layer address of the next hop. In the LAN case, a packet is forwarded to the gateway's MAC address without changing the destination address. In our case we map a global IP address to the ad hoc network address of the gateway and "override" a packet's destination by tunneling over numerous hops. In the invalidate direction no tunnel is needed, since packets entering the ad hoc network from the fixed Internet will be translated to a local address by the address translation or will already have a valid "return address" if the gateway is the source node's Mobile IP home agent.

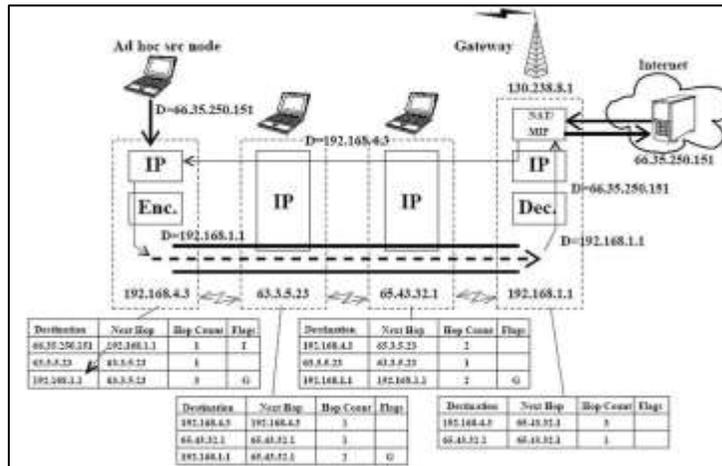


Fig. 1: Half tunnel forwarding showing the routing table state at each node and how encapsulation (Enc.) and decapsulation (Dec.) changes the destination address of packets for Internet destinations (I flag). Because of the encapsulation, intermediate nodes only have to maintain the gateway route (G flag). The gateway acts as a NAT or mobile IP home foreign agent.

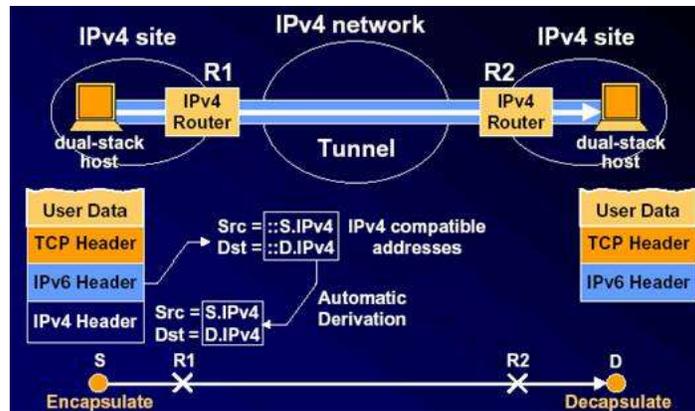


Fig. 2: Half Tunneling

If the gateway is foreign agent; it will be the end point of a Mobile IP reverse tunnel and will thus decapsulate the incoming packet to a nearby routable one where the destination is the source node's home address.

B. Benefits of Half Tunnels

Half tunnels have following attractive properties:

1) Free From Cascading Route Requests

Cascading effects are not a problem because only the source node and the gateway need to know about the destination in the fixed internet. Inside the ad hoc network all packets are explicitly addressed for a gateway and corresponding host entries will exist in all intermediate nodes.

2) Route Aggregation

Tunneling achieves route aggregation at intermediate nodes because it only requires individual host entries pointing to the few gateways instead of an entry for every potential global IP address.

3) Stability and Reduced Overhead

Once a source node has configured a tunnel to a gateway, that tunnel will not be diverted to another gateway unless connectivity with the gateway is completely lost. In that case the source node will be notified and can take proper actions. For example to re-register at a new gateway in case the source node is using Mobile IP.

4) Multiple Gateways

Intermediate nodes can preserve routes to multiple gateways so that end nodes may tunnel Internet traffic bound for different gateways over a general intermediate hop, which is not the case for default route forwarding. End nodes could even keep up flows through different gateways at the same time by configuring multiple tunnel entry points (see Figure 3). In this case extra tunnel can be used as backup routes if the connectivity to one gateway is lost. This will avoid route request flooding for all its current Internet destinations. Additionally, tunnels to multiple gateways are helpful when a node wants to do a handover between gateways or wants load balancing.

5) Efficient Forwarding

In terms of routing table lookups, half tunnels are more efficient than the default route counterpart. A source node needs to Look-ups in the routing table (first, to find the host route entry that maps the destination to the tunnel entry point and thereafter the tunnel entry point itself, i.e., the gateway route).on intermediate nodes, only one look-up is needed, which is an obvious advantage over the default route approach that most likely needs three table accesses, both at the source node and at intermediate nodes.

6) Implementation Simplicity

Half tunnels needs only minor changes to the routing protocol. The tunnel state needs to be maintained at the source node only and intermediate nodes can forward tunneled packets without extra sense or state. As opposite to lose source routing, tunnels do not require extra ordinary processing when forwarding a packet.

7) Security

Half tunnels are not as security insightful as default routes; only the source node adds redirection state on the source node itself. Default routes on the other hand can be redirected at any intermediate hop and all Internet traffic abstracted by a nasty node. It is true that any node can pretend to be a gateway, hence could divert tunnels to itself. However, this is a common problem of ad hoc routing and any authentication solution for trusting the gate way would be applicable to the half tunnel setting too.

IV. ROLE OF INDIRECTION

For a smooth Internet connectivity, forwarding strategies must support indirection. Indirection allows the routing of Internet traffic to a specific gateway that may not be the "closest" one. Under the mobility conditions, such indirect routing is required to maintain flows to old gateways while the flows are bound to state in them. The lack of indirection [4] in many existing proposals for Internet connectivity leads us to believe that the problem of interfacing MANETs with the Internet has not been properly analyzed, although there may be point solutions that work for specific environments. Our goal is to make clear the requirements of MANET Internet connectivity, such as indirection, in order to reduce misconceptions about how to design it, and to reduce the risk of point solutions that only apply to very specific scenarios and protocols. An example significance of without indirection in the design is, what we call, the state replication problem. State replication is mainly a problem in reactive hop-by-hop protocols, such as AODV, and manifests itself when a route to an Internet gateway is changed by an intermediate node due to route optimizations or repairs, without all nodes along the route being notified. Any new nodes that become a part of the updated route must not only have the routing state required to reach the gateway, but also some state for the Internet destination in order to, avoid subsequent route discoveries when forwarding data packets destined for the Internet. While indirection is important, it is not the only component needed for robust and flexible Internet connectivity. There are many subtle design problems related to gateway discovery and integration between the routing protocol and macro mobility schemes, such as Mobile IP and NAT based networks. Thus gateway indirection plays a very important role in Internet-MANET connectivity and provides a smooth way to connection.

V. EVALUATION

On the basis of our simulation we have compare the two gateway forwarding scheme default route forwarding and the half tunneling. We have compared these two techniques for throughput, control traffic per data and for packet delivery ratio. On comparison we found that half tunnel solution shows better result in compare to the default route forwarding, due to the cascading effect, multiple changing and gateway problem and state replication problem which is found in default route forwarding.

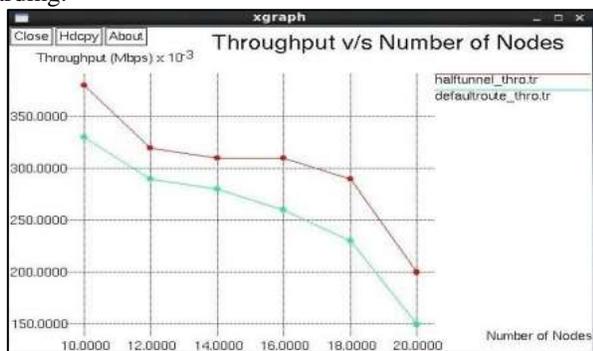


Fig. 3: Through put with respect to no. of nodes

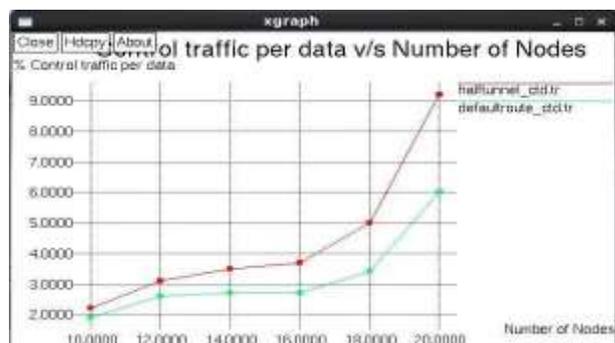


Fig. 4: Control traffic data with respect to no. of nodes.

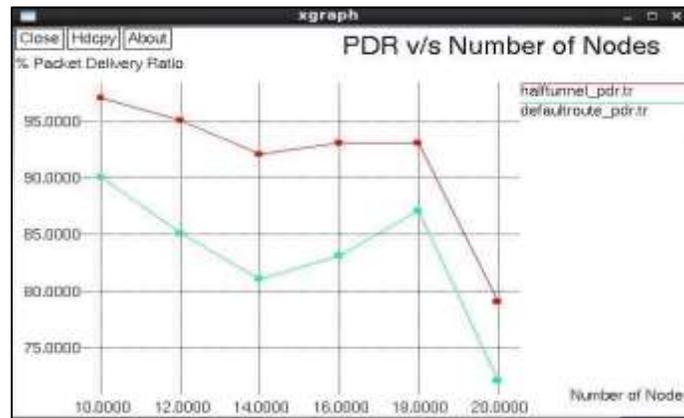


Fig. 5: Packet delivery ratio with respect to no. of nodes

VI. CONCLUSION

A robust forwarding strategy is necessary to build Internet connectivity solutions for MANETs so we have compared the efficiency of default routes and tunneling. Our conclusion is that 'tunneling' packets to a gateway in ad hoc networks with fat addressing and reactive routing is more efficient and flexible in compare to default routes. On the basis of our study for the solutions to Internet connectivity, we found an important idea that many of them do not support indirection and are hence not robust enough, not even in less difficult scenarios. Furthermore, many of the solutions are only proposals that have not been implemented and evaluated, neither in simulation nor in reality. In contrast, our suggested scheme is very interesting, and is a complete Internet connectivity solution for AODV routing. We expect that other routing protocols can also be supported with little effort, reactive ones as well as proactive ones. In our comparison of forwarding strategies for Internet connectivity designs in a multiple gateway scenario – one design using default routes and one using tunneling for indirection. Normally default route scheme's lack of indirection can have serious impact on the performance due to incorrect routing while the indirection approach does not suffer from the default route's inherent problems, and is also more flexible in terms of multi-homing capabilities. We have suggested the 'half tunnels' as a way to improve efficiency in forwarding of packets to an Internet gateway in ad hoc networks. We argue that half tunnels are simple to implement. Half tunnels also have elements of self-configuration, since tunnels are configured automatically by the route reply. Half tunnels can be implemented proactively or reactively. Our conclusion is that tunneling schemes, or other approaches that allow indirection, are essential for building robust and flexible Internet connectivity for Mobile ad hoc networks. The main advantage of a tunneling solution is that the source node of a flow is always in full control and alone carries all the state necessary to forward a packet to a gateway. No state is replicated at intermediate nodes, except the state for the route to the gateway. This makes 'tunneling' very transparent to existing routing protocols and route aggregation is achieved at intermediate nodes. Thus we can say that a robust forwarding strategy is necessary to construct smooth Internet connectivity solutions for MANETs.

REFERENCES

- [1] U. Jonsson, F. Alriksson, T. Larsson, P. Johansson, and G. Q. Maguire Jr. MIPMANET - Mobile IP for Mobile Ad hoc Networks. In 1st ACM international symposium on Mobile ad hoc networking and computing (Mobihoc'00), 2000.
- [2] R.Wakikawa, J.Malinen, C.Perkins ,A.Nilsson ,and A.Tuominen .Global connectivity for IPv6 mobile ad hoc networks ,October 2003 .IETF Internet Draft ,draft-wakikawa-manet global v6-03.txt.
- [3] R.Wakikawa, J.Malinen ,C.Perkins ,A.Nilsson ,A.Tuominen ,Global connectivity for IPv6 mobile ad hoc networks, March 2006,IETF Internet Draft ,draft-wakikawa-manet-globalv6-05.txt.
- [4] Erik Nordstrom et.al "Robust and flexible Internet connectivity for mobile ad hoc networks", ©2010 Elsevier B.V.All right reserve