Common Gateway Architecture for Mobile Ad-hoc Networks

Marcin Michalak
Telscom AG
Sandrainstr. 17, 3007 Bern, Switzerland
marcin@telscom.ch

Torsten Braun
Institute of Computer Science and Applied Mathematics
University of Bern
Neubrueckstrasse 10, 3012 Bern, Switzerland
braun@iam.unibe.ch

Abstract

Ad-hoc networks are by definition created on demand, without any infrastructure. On the other hand, they are often considered as an extension of the range of Internet access points, providing multihop wireless access to them. This paper tries to examine the situation where there exist several Internet access points in a single ad-hoc network. We present a Common Gateway Architecture which allows to use multiple access points and send traffic using the closest one.

1. Introduction

Seamless and ubiquitous Internet access is becoming more and more important nowadays. A lot of companies start to offer wireless access, building infrastructure with 802.11b technology. However, Wireless LAN access points (APs) have limited coverage (up to several hundred meters in open space). For this reason multi-hop ad-hoc routing protocols are considered to provide ways to extend the range of access points. Nodes which are not directly covered by the APs can connect through the other nodes. They can discover the route to the gateway using ad-hoc routing protocols like AODV [11]. This idea has been presented in [9].

Currently, if multiple gateways exist in the area of one ad-hoc network, they are independent of each other and manage different address spaces. This requires extensions to the ad-hoc nodes, since they need to decide which gateway to choose. Handovers are performed on top of their routing protocol. Our approach, called Common Gateway Architecture (CGA), provides a micromobility solution for the ad-hoc network. We show how to install several Internet access points in one ad-hoc network, which simplifies handovers and can be used without any changes to the routing protocol.

The rest of the paper is organized as follows: Section 2 describes the micromobility concept and Cellular IP. Section 3 presents Internet connectivity solutions for ad-hoc networks. In Section 4 we describe the proposed solution. Section 5 describes the solution and tests in a simple scenario, while Section 6 presents more advanced scenarios and simulation experiment results. The paper finishes with conclusions and ideas for future work.

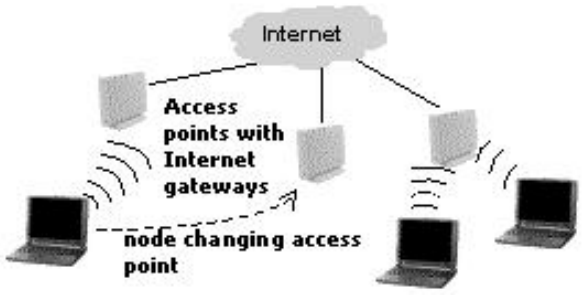
2. Micro-mobility and Cellular IP

In the current architectures which provide single-hop wireless Internet access there exist several micromobility solutions [5]. Micromobility is a way to manage the movement of a mobile node between different points of attachment (see Figure 1).

If the change is very frequent standard Mobile IP [10] does not work, since its mechanisms bring too much overhead. Micromobility mechanisms try to minimize signalling, handover time and avoid communication with distant servers. There are several solutions in the area of micromobility: Cellular IP [6], Hawaii[12] and Hierarchical Mobile IP[13]. They all work in a scenario where a mobile node is moving and changing its point of attachment to the network. The communication with point of attachment (e.g. access point) is always direct, i.e. single-hop. A good comparison of micromobility solutions is given in [5].

From the above methods, Cellular IP [6] seems to have most in common with ad-hoc routing protocols, especially AODV.

Figure 1. Micromobility principle



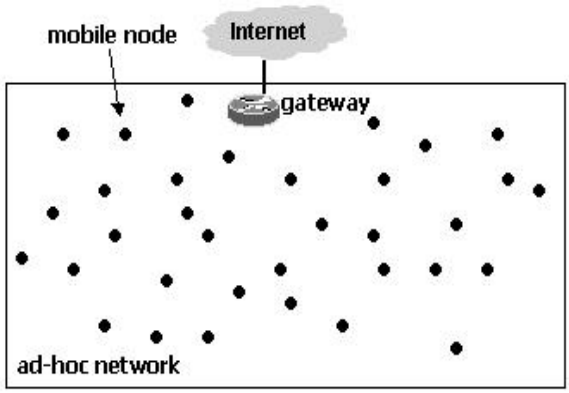
Cellular IP supports fast handoff and paging techniques. To minimize control messaging, it uses data packets to refresh host locations. It supports two types of handoffs: hard and semisoft. In hard handoff, packets sent during the handoff time are simply lost. In semisoft handoff packets are sent via both APs during handoff, which makes the change of either of them arriving higher. Cellular IP uses mobile-originated data packets to maintain the reverse path. When packets need to be sent to the host to which there is no route, a mobile node is paged using limited broadcast. Here we can see many similarities to ad-hoc routing protocols, especially AODV. AODV uses data packets to refresh host location and maintain the reverse path (if needed). Limited broadcast is also used to locate the node. Paging techniques are also built into the ad-hoc routing protocols.

As we can see, ad-hoc routing protocols provide enough mechanisms to support micromobility, since they can already manage movement of nodes. In ad-hoc networks, we can see the neighbouring nodes as 'points of attachment', through which we can access more distant nodes. Our solution builds on this conclusion. Instead of using any micromobility mechanisms to support handover between multiple points of Internet access, we can use ad-hoc routing protocols directly.

3. Internet connectivity for ad-hoc networks

Initially, nodes belonging an ad-hoc network can only communicate among themselves, using multi-hop wireless transmission. In this case, each node has a unique address which is 'meaningless' outside the ad-hoc network, since there is no external connectivity. However, there are some solutions which extend this architecture providing Internet access for ad-hoc nodes. This means that one (or more) of the nodes has at least two network interfaces, one making it part of the ad-hoc network, and another connecting to the Internet (see Figure 2). This node becomes a gateway and provides Internet access for the wireless-only nodes. The gateway is managing a certain address space, and each ad-

Figure 2. Ad-hoc network with Internet access



hoc node needs to acquire the address which it will use to communicate through the gateway. This is required to enforce that data packets from the Internet to the ad-hoc node travel via the gateway.

There are two general approaches for providing Internet connectivity: with and without tunelling. In both approaches, a mobile node needs to know the gateway address and have a route to it. Mobile nodes also need to know their network prefix and compare it with the destination address. When using the tunnel, if the destination lies outside the mobile network, mobile nodes encapsulate the packets directed to the Internet and put the gateway address as a destination. When such a packet is received by the gateway, it decapsulates its contents and forwards the packet to the desired destination. Because of this encapsulation, we can say that the packets are tunnelled between the mobile node and the gateway.

In another approach, if the destination lies outside the mobile network, mobile nodes send the packet with the 'real' destination address and direct the packet to the next hop for the gateway. Each of the nodes needs to keep a default route, as in standard Internet connectivity. The next hop for such route is the next hop to the gateway. The tunneled solution is transparent to the intermediate nodes, since it doesn't require gateway support in them. However, if each node can distinguish external address from internal ones the tunneled approach is not required. Basic extensions have been presented in AODV+ [9], Globalv4 [3] and Globalv6 [15]. Globalv6 [15] is the one that is currently developed in IETF MANET group. It provides a solution for global connectivity by adding the following extensions:

- how to obtain a routable address
- how to communicate through the gateway

Two methods for Internet gateway discovery are pro-

posed: proactive and reactive. In the first one, the gateway sends its advertisements periodically announcing its address, global prefix and scope. The reactive way means that a node must initiate gateway discovery by itself and the gateway responds to it on demand. In this case, the address is also assigned on demand. Globalv6 is defined for AODV6 and OLSR, but can also work with other protocols.

If only one gateway exists in the ad-hoc network, it is a bottleneck for Internet access. We can increase the number of gateways, but then (in current approaches) each gateway manages its own address space is unaware of the other gateways [8, 9]. This creates some drawbacks:

- nodes need to decide which gateway to choose by themselves (outside normal routing decisions)
- multiple prefixes exist in one ad-hoc network. It is no longer possible to determine whether node is local or external by checking the gateway prefix
- if a node needs to change the gateway, it needs to change the address and perform IP handover, possibly with Mobile IP. This requires exchanging several messages and takes time.

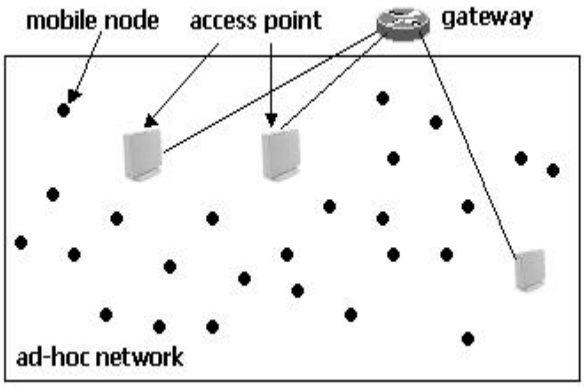
In order to overcome those problems, we need a micromobility solution. Our approach provides a simple and effective way of managing micromobility in ad-hoc networks using non-modified ad-hoc routing protocol.

4. Solution description

In the previous section we concluded that there is a need for multiple Internet gateways in ad-hoc networks. However, having several gateways using current solutions has some drawbacks. This is why we propose the idea of Common Gateway Architecture (CGA) for MANETs. Using standard ad-hoc routing protocols it provides a simple way of managing micromobility in ad-hoc networks. The architecture is as follows: several access points (APs) are connected to one common Internet gateway. The APs are part of the ad-hoc network and provide Internet access to the mobile nodes. The gateway is physically not part of the MANET, but is connected (e.g. via wired links or ip tunnels) to each of the APs. It runs the MANET routing protocol on the links to APs and thus becomes a logical member of the MANET. Although physically there may be several points of Internet access (all APs), mobile nodes see only one gateway. This feature is the most important part of our approach. By making the gateway, connected through APs, a logical part of the MANET we can:

- use a single address space
- use ad-hoc routing protocols to manage micromobility

Figure 3. Common Gateway Architecture concept



Those features eliminate the drawbacks mentioned in section 3. The basic idea of CGA is presented in Fig. 3.

In order to explain this solution, let us take AODV [11] as a MANET routing protocol and assume that all APs have a wired connection to the gateway. In our solution, there are 3 types of nodes:

- Mobile nodes

  These are standard ad-hoc nodes, running AODV with any of the extensions letting them discover and use the Internet gateway.

- Access points

  An access point has two interfaces: one wireless connecting to the ad-hoc network and another one connecting to the gateway. Access points are full routers, they are able to forward packets between interfaces. They run AODV on the ad-hoc interface and on the gateway interface. To avoid creation of the mobile-node to mobile-node through the gateway only the route requests to the gateway are forwarded on the gateway interface. This way the gateway receives only the requests directed to itself and learns the route back to the mobile host.

- Gateway

  There is only one gateway node for the different APs. It has connections to all the access point nodes and an interface connecting to the Internet. It is also managing the IP address space. The gateway is running AODV with one of the Internet connectivity extensions (e.g. [9, 3, 15]) on the links to all access points. It has full router capabilities, it is forwarding packets between any of the access point links and Internet interface.

If a gateway receives a route request, it replies to it on the link where it came from, building a route to the source of the request. This is standard AODV operation. AODV assures that the closest access point is chosen, since it uses hop counts as metric for the route selection. When a gateway needs to find a route to the mobile node, it sends ('broadcasts') the request to all APs, which repeat it further on their wireless links (or answer immediately if they know the route already).

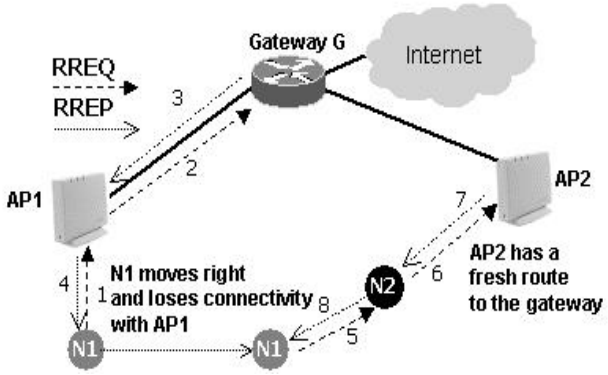
This architecture is completely transparent to the mobile nodes. New APs may be added easily. The only requirement is to connect them to the gateway and apply filtering. Since there is only one gateway, its address may be preconfigured in the mobile nodes. Even if the gateway is initially not known, its discovery may be performed only once, saving time and limiting overhead traffic. Because the nodes communicate with the gateway and not APs, when the route is lost (e.g. due to mobility), a new 'optimal' route to the gateway shall be established by the means of the routing protocol. Handovers (if needed) shall be performed without extra overhead.

In order to avoid Internet gateway extensions in the mobile nodes, application level proxies may be installed on the gateway and thus provide indirect access to Internet services. One example is a web proxy. When installed in the gateway it allows all mobile nodes to use web-based services without any Internet extensions to the ad-hoc routing protocol. This way mobile nodes may also benefit from cached content in the proxy.

Another approach is presented in [14]. The authors propose a solution which combines the Cellular IPv6 infrastructure with AODV. Access points (called base stations there) are running AODV and are answering to the route requests either on behalf of themselves (so-called proxy-disabled mode) or on behalf of the gateway (proxy-enabled mode). Cellular IP signalling is added on top of the ad-hoc routing protocol. The difference to the CGA approach is that the gateway is not running AODV, thus being logically outside the ad-hoc network. Mobile nodes, gateway and base stations must implement the Cellular IP protocol. When a mobile node wants to send through the gateway, it sends a request to a special 'all-base stations' multicast address. This architecture has following consequences:

- All sessions need to be initiated by the mobile nodes.
- It does not work with other gateway discovery solutions (since it provides its own).
- It is not transparent to mobile nodes.
- Mobile nodes need to send route update to the gateway every time they change the base station
- More signalling (ad-hoc routing + Cellular IP) is required.

Figure 4. Simple scenario setup



5. Simple scenario test

In order to test the solution, several simulations have been performed using the modified ns-2 [16] simulator. AODV code in the simulator has been modified in such a way that it implements the CGA concept as described in Section 4. To check if this solution works, a simple scenario has been simulated. A mobile node is moving from one AP towards another. This scenario is presented in Figure 4. Access points are connected to the gateway via wired Ethernet links, each having bandwidth of 10 Mbps and delay 10 ms.

Node N1 sends constant bit rate traffic of 64kbps (16 packets of 512 bytes per second). Simulation time is 100s. In the 50th second N1 starts to move towards N2 with a speed of 20m/s and stops when it is 50 meters away from N2. At this point, it is not in the range of AP2, so the route to it goes through N2. The opposite direction has also been simulated, i.e. the gateway sending traffic to N1. Simulation results are presented in Table 1.

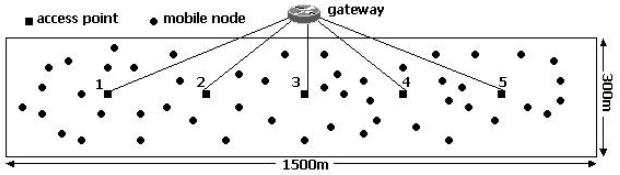
Table 1. Simple scenario simulation results

Parameter	Result mobile	Result static
Average delay	18.62 ms	16.24 ms
Delivery rate	99%	100%

For comparison, results of the static setup (no movement) are also presented.

The steps for the mobile scenario can be described as follows. In the beginning, mobile node N1 wants to send packets to the gateway (G). It broadcasts the route request (1), which is received by access point 1 (AP1). AP1 forwards the request to the G(2), which replies to N1 through AP1 (3 and 4). After a while, N1 starts to move towards N2 and at a certain point moves out of the AP1 range. AODV invalidates the route entry it had and broadcasts the request

Figure 5. Advanced scenario setup



for a new route to the gateway (5), which is heard by N2. N2 does not know the route to G, so it broadcasts the request further (6). This request is heard by AP2, which has a fresh enough route to G and returns it to N1 via N2 (7 and 8).

Simulation results show that the concept works and handover between the access points is performed. Average delay in the mobile scenario is only slightly higher (1.5%) compared to the static setup. Only 1% of the packets are lost during handover time. This occurs due to short connectivity loss when N1 moves out of the AP1 range. Low loss and delay difference prove that handover is performed smoothly and the transmission continues.

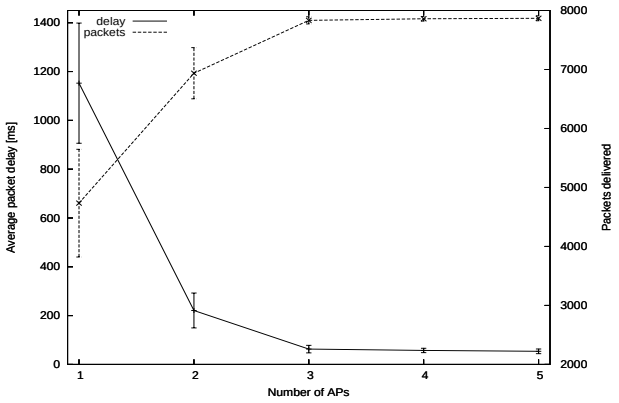
6. Simulations for Performance Evaluation

After checking the operation in simple conditions, we performed more complex simulations with ns-2. 50 mobile nodes have been placed on the area of 1500x300m. All nodes are moving using random waypoint model[4], with speeds ranging from 1 to 20m/s and no pause time. 20 nodes want to send data to the gateway, each sending 4 packets of 512 bytes per second (16 kbps CBR traffic). The opposite direction is also investigated (gateway sending traffic to the mobile nodes), and the average result is taken. The simulation setup is described in Figure 5 and Table 2.

Table 2. Simulation parameters

Parameter	Value
Simulator	ns-2.27
Area	1500x300m
Wireless MAC	802.11
Channel bandwidth	1Mbps
Number of nodes	50
Number of access points	1-5
Number of transmissions	20
Packet size	512 bytes
Packet rate	4 packets/sec
Mobility model	Random Waypoint
Node speed	1-20 m/s
Pause time	0s
Simulation time	100s

Figure 6. Simulation results



The simulations have been performed for 1-5 access points, for 6 randomly generated scenarios. Each of the access points is connected to the gateway using wired links with 10 Mbps and 10 ms delay. 5 gateways are horizontally spaced by 250 m, as presented in Figure 5. Scenarios with less APs have been realized by removing some APs from the 5-APs scenario. For 4 APs, number 4 is removed. For 3 APs, number 2 and 4 are removed. For 2 APs, number 1 and 3 are left, and for one AP number 3 is left. This assures that results do not depend on the position of the AP.

Fig. 6 shows the simulation results: the average packet transmission delay (between mobile node and gateway) and total number of packets received per session, along with confidence intervals of 95%. The total number of packets sent is 8000 (4 pkts/s * 100s * 20 sessions). We can see that the confidence is low for 1 and 2 APs, since there congestion is very high and conditions are very variable.

By adding more access points, we increase the probability of route establishment (new node is added), and reduce congestion. It should be mentioned that the results are strongly affected by the ns-2 wireless model. This model presumes transmission ranges of mobile nodes equal to 250 m and interference ranges of 550 m. This means that 2 nodes (this applies also to access points) which are closer to each other than 550 m are not able to transmit at the same time.

The presented results show that the CGA concept works also in the advanced scenario and allows to introduce several access points while having one gateway.

7. Conclusions and future work

The Common Gateway Architecture provides a simple way to install and use several Internet access points in ad-hoc network. Those access points run in the same address space and are connected to one common Internet gateway.

By running the ad-hoc routing protocol on the gateway, we allow the mobile nodes to use the closest access point by the means of standard ad-hoc routing protocol operation. The strength of the solution lies in its simplicity as well as transparency to the gateway discovery and address assignment procedures. Its performance depends on the routing protocol mechanisms.

Performed simulations show that the common gateway architecture works. It has following features:

- It provides micro-mobility.
- No IP address change is required.
- It allows several access points in one addressing domain.
- Sessions may be initiated both from gateway as from the mobile nodes.
- Handover is handled by the routing protocol.
- It is transparent for the mobile nodes.
- It is transparent for gateway discovery and addressing assignment mechanisms.
- New APs may be easily added.
- The gateway address can be fixed, since there is only one.
- No Internet access extensions are required when accessing only the gateway (e.g. as central server/proxy).

This architecture can also be extended to provide a wired transit for the traffic between two mobile nodes, which could be investigated in future work. It could also be interesting to check how protocols other than AODV perform in this setup. Another area of application could be sensor networks. Sensor nodes could benefit from the existence of several access points, since shorter routes to the gateway should decrease energy consumption needed for communication with the gateway.

References

[1] C. Ahlund, A. Zaslavsky, *Software Solutions to Internet Connectivity in Mobile Ad Hoc Networks*, 4th International Conference on Product Focused Software Process Improvement, PROFES 2002. Springer-Verlag, December 2002

[2] G. Andreadis, *Providing Internet Access to Mobile Ad-hoc Networks*, London Communications Symposium 2002, September 2002

[3] E. Belding-Royer, Y. Sun, C. Perkins, *Global Connectivity for IPv4 Mobile Ad hoc Networks*, IETF Internet Draft, November 2001

[4] C. Bettstetter, H. Hartenstein, X. Perez-Costa, *Stochastic properties of the random waypoint mobility model*, Wireless Networks, September 2004

[5] A. Campbell, J. Gomez, S. Kim, C. Wan, Z. Turanyi, A. Valko, *Comparison of IP Micromobility Protocols*, IEEE Wireless Communications, February 2002

[6] A. Campbell, J. Gomez, C-Y. Wan, S. Kim, Z. Turanyi, A. Valko, *Cellular IP*, IETF Draft, January 2000

[7] H. Cha, J. Park, H. Kim, *Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks*, IETF Draft, October 2003

[8] M. Ghassemian, P. Hofmann, H. Aghvami, C. Prehofer, *Analyses of Addressing and QoS Approaches for Ad Hoc Connectivity with the Internet*, IEEE PIMRC 2003, Beijing, China, September 2003

[9] A. Hamidian, *A Study of Internet Connectivity for Mobile Ad Hoc Networks in NS 2*, Masters thesis, Departement of Communication Systems, Lund Institute of Technology, Lund University, Sweden, January 2003.

[10] C. Perkins et al., *IP Mobility Support for IPv4*, IETF RFC 3344, August 2002

[11] C. Perkins and E. Belding-Royer, S. Das, *Ad hoc On-Demand Distance Vector routing*, IETF RFC 3561, July 2003.

[12] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, L. Salgarelli, *IP micro-mobility support using HAWAII*, IETF Draft, July 2000

[13] H. Soliman, C. Castelluccia, K. El-Malki, L. Bellier, *Hierarchical Mobile IPv6 mobility management (HMIPv6)*, IETF Draft, June 2003

[14] V. Typpo, T. Sukuvaara, M. Jurvansuu, P. Mahonen, *Extending IP Micro-mobility to AODV based ad hoc networks*, WWIC 2002, June 2002

[15] R. Wakikawa, J. Malinen, C. Perkins, A. Nilsson, A. Tuominen, *Global Connectivity for IPv6 Mobile Ad Hoc Networks*, IETF Draft, October 2003

[16] http://www.isi.edu/nsnam/ns2/ - NS-2 Simulator