Integration of Heterogeneous Ad hoc Networks with the Internet[1]

Nico Bayer, Dmitry Sivchenko, Bangnan Xu
T-Systems, SSC ENPS (Technologiezentrum)
64295 Darmstadt, Germany
Nico.Bayer@t-systems.com

Sven Hischke
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
D-53113 Bonn, Germany

Veselin Rakocevic
School of Engineering and Mathematical Sciences
City University, London EC1V 0HB, UK

Joachim Habermann
University of Applied Sciences Friedberg
61169 Friedberg, Germany

Abstract

This paper describes a testbed realized at T-Systems in Darmstadt (Germany) that handles the integration of ad hoc networks with the Internet. The testbed contains a Mobile Gateway that connects an IPv6 based ad hoc network over a cellular network (e. g. GPRS or UMTS) with the Internet. The testbed is also able to handle multiple gateways within the same ad hoc domain. This paper describes several mobility scenarios developed within the testbed, namely inter ad hoc domain mobility, intra ad hoc domain mobility and mobility of the whole ad hoc network. The paper also discusses main issues in the development of the testbed - gateway discovery, seamless mobility and the transmission of IPv6 packets over IPv4 infrastructures.

1. Introduction

In future communication systems mobile ad hoc networks (MANETs) will play an important role. Ad hoc networking does not require any infrastructure. In ad hoc networks it is possible to establish spontaneous communication between network-enabled electronic devices (e. g. mobile phones, PDAs, Laptops). In areas where only local communication around the sender is required ad hoc networking has major advantages compared to ”conventional” wireless systems, such as GSM (Global System for Mobile Communications) and UMTS (Universal Mobile Telecommunications System). For example, MANETs are ideal for establishing an instant tactical communication network needed by emerging military applications such as situational awareness systems for manoeuvring. Sensor networks are another application that is currently in a global research focus. Other MANET applications are: wireless networks for disaster recovery operations, wireless home and office area networks. One drawback of MANETs is that communication is limited to the ad hoc domain. Many applications, however, need a connection to an external network, like the Internet or a cellular network. For instance members of a conference which have configured an ad hoc network to exchange information among each other may also need a connection to the Internet to download their Emails. Another application could be that the base station of a sensor network collects all sensor information and transmits this information over a cellular network to a server in the Internet. For such scenarios interworking between the protocols and standards in the ad hoc network and the external network is needed. This paper tackles this fundamental problem and addresses the interworking between ad hoc networks and external networks. It describes a testbed that was realized at T-Systems in Darmstadt, Germany. A ”Mobile Gateway” was developed that connects an IPv6 based ad hoc network over a cellular network with the 6Bone (IPv6 based Internet). The paper also discusses the main issues to realize the interconnection between ad hoc and cellular networks. A Gateway Discovery mechanism is needed that provides ad hoc nodes the possibility to find and set up a route to the Mobile Gateway in order to be able to send packets to the Internet. Another challenge is that IPv6 is supported in the ad hoc network and IPv4 in the cellular network. To solve this a tunnel is used to send IPv6 packets over an IPv4 infrastructure. The testbed can also handle multiple Mobile Gateways within the same ad hoc domain. Ad hoc nodes will always use the nearest gateway. Furthermore the breakdown of one gateway can be handled by switching to another one. Using a Mobile Gateway gives the ad hoc network the possibility to be mobile within the coverage area

[1]This work is partly supported by the German Ministry of Education and Research under IPonAir Project

of the cellular network. Mobility will be handled at layer 2 of the cellular access network. But if a single ad hoc node is mobile and wants to roam between different ad hoc/access networks this needs to be handled at layer 3. The paper also describes a mechanism based on MobileIPv6 that provides seamless roaming. Figure 1 gives an overview about the described scenario.

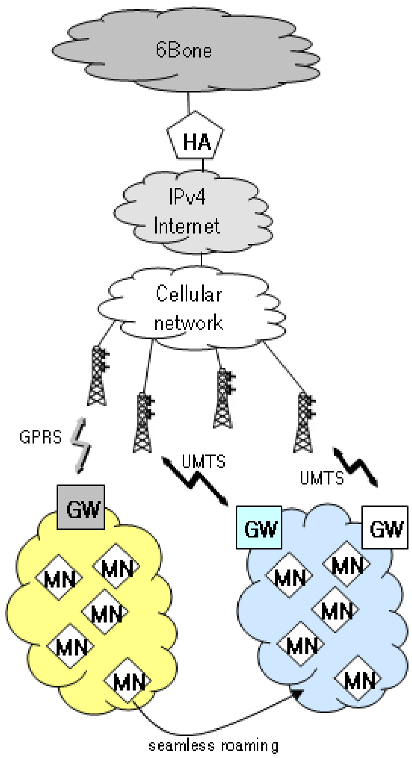

Figure 1. Scenario

A lot of research work has been done on autonomous ad hoc networks in the last years while the integration of heterogeneous networks has not been analysed much. Only a few papers handle this issue, e. g. [1], [2], [3], [4]. But they all do not handle a Mobile Gateway that connects ad hoc networks over a cellular network with the Internet. The rest of this paper is organized as follows: Section 2 gives an overview of the testbed and describes the functionality of the Mobile Gateway. Furthermore it handles the gateway discovery mechanisms, address autoconfiguration in ad hoc networks and the problem how to send IPv6 packets over IPv4 based infrastructures. In section 3 a mechanism is described that provides seamless mobility between heterogeneous networks. A conclusion of the paper is presented in section 4.

2. Testbed and Mobile Gateway

Figure 1 shows two groups of ad hoc nodes that form two independent ad hoc networks. Communication within the ad hoc networks is established through multihop paths. To realize multihop communication an ad hoc routing protocol is needed. The Ad hoc on demand Distance Vector protocol (AODV) [5], [6] is used within the testbed. As already mentioned one gap of ad hoc networks is that ad hoc nodes cannot communicate with external nodes in the Internet. To provide Internet access for ad hoc nodes an interface between the ad hoc network and the access network is needed. In our testbed we use a Mobile Gateway that establishes a connection over a cellular network. In [4] a similar scenario is described that uses a Wireless Gateway to connect an ad hoc network with a WLAN based access network, e. g. a hotspot or a company network. In order to be able to route packets between the different domains the Mobile Gateway needs the protocols and standards of both networks. The protocol stack of the Mobile Gateway is depicted in Figure 2. On the ad hoc side it uses physical and data link layers of the IEEE 802.11 standard. This standard has an optional ad hoc mode that enables decentralized direct operation. On the cellular network side the Mobile Gateway uses standard GPRS/UMTS (GPRS: General Packet Radio Service) physical and data link layer protocols. To realize two different

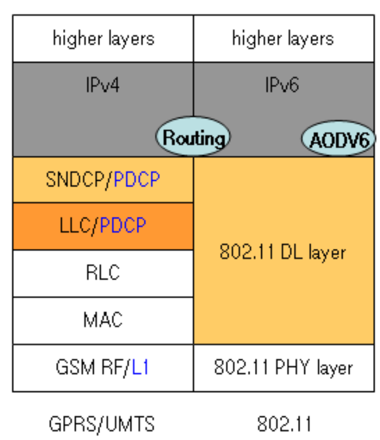

Figure 2. Protocol stack on Mobile Gateway

protocol stacks on the Mobile Gateway it needs two different network interfaces. On ad hoc side it uses a WLAN card configured for the ad hoc mode and on cellular side it uses a combined GRPS/UMTS card. The primary selection of this card is UMTS. If the UMTS signal strength is poor and reaches a specified threshold the card connects seamless to GPRS (if available). The main issue to realize in the interworking is the gateway discovery mechanism that provides ad hoc nodes with a route to the Mobile Gateway even if the ad hoc nodes are multiple hops away. Furthermore the nodes need a global routable IP address so that packets from the Internet can be routed to the correct location. And finally the issue that an IPv6 based ad hoc network is connected to the 6Bone over an IPv4 based cellular network. This means that IPv6 packets need to be sent over an IPv4 network. To solve this, an IPv6 in IPv4 tunnel is used.

2.1. Gateway Discovery

The gateway discovery mechanism provides ad hoc nodes with a route to the gateway. The ad hoc nodes can use this route to send/receive packets addressed to/from external networks. The gateway discovery can be realized proactively or reactively. The reactive gateway discovery only provides the gateway information if the ad hoc node requests the gateway to get access to external networks. In this case the ad hoc node sends a GWSOL (gateway solicitation) message via broadcast into the ad hoc network. Intermediate nodes will rebroadcast this message. If the wireless gateway receives the GWSOL, it replies via unicast with a GWADV (gateway advertisement) message that contains the gateway information so that the requesting node can set up a route to the gateway. In the proactive gateway discovery method the gateway periodically sends HELLO messages that contain a special option called PROAGW option. This option has all information about the gateway that is needed to set up a route to it. All ad hoc nodes that have received the PROAGW option can add the option to their own hello messages. A detailed description of both mechanisms and the implementation based on the AODV protocol can be found in [4] and [7]. This paper focuses on the reactive mechanism and handles only new approaches needed to handle multiple gateways. If an ad hoc node wants to send packets to the Internet it must start the reactive gateway discovery mechanism to find a route to the gateway. If multiple Mobile Gateways are available it will receive multiple answers. The ad hoc node has to decide which gateway it should use. In our testbed the hop count is used as metric to decide which gateway should be used. Further enhancements of the testbed should also consider other parameters to select the best gateway. For instance the nearest gateway must not be the best one. Congestion, overload, available bandwidth, delay, etc. could lead to a scenario where a far gateway would be the better choice. If the ad hoc node has chosen one gateway, all packets send over this Mobile Gateway to the Internet need a source address with the same prefix as the gateway. Therefore the ad hoc node has to start address autoconfiguration (section 2.2) to obtain an address from this gateway. Whether it has configured a new address or it already has an address with the prefix of the selected gateway this address must be used as source address for all packets send to the Internet. In case the ad hoc node has configured a new address and MobileIPv6 is used it needs to do a binding update with the Home Agent. After the ad hoc node has selected one gateway and has an address with the prefix of this gateway it can start communication with external networks. If the mobility within the ad hoc networks leads to a break of the route between Mobile Gateway and ad hoc node the normal AODV behaviour will start a new gateway discovery mechanism. The result could be that the ad hoc node needs to select a new Mobile Gateway and again start the address autoconfiguration and binding update if needed. A future enhancement of the Mobile Gateway should also trigger a new gateway discovery if the gateway is still available but has lost the connection to the cellular network and is not able to forward packets any longer.

2.2. Address autoconfiguration

Ad hoc nodes need an address autoconfiguration mechanism in order to configure a global routable and topological correct address. This address is needed otherwise packets coming from the Internet can never be routed to the ad hoc node. Current autoconfiguration mechanisms used in the Internet are not applicable in the multihop networks. To solve this we already proposed two mechanisms in [8]. The first mechanism is based on the stateless address autoconfiguration for IPv6 that was defined for single hop applications. To overcome the single hop limitation and to enable stateless address autoconfiguration in multihop scenarios the mechanism has been enhanced in such a way that intermediate nodes that have received a Router Advertisement (RA) from the gateway are also able to send RA to ad hoc nodes that are multiple hops away. The second mechanism is based on the stateful address autoconfiguration and uses DHCPv6. In normal cases the DHCPv6 protocol does not work in multihop scenarios. This is solved by using temporary addresses on the ad hoc nodes and multihop compatible multicast addresses on the DHCPv6 server. Details of both mechanisms can be found in [8]. Several other solutions [9], [10], [11] for address autoconfiguration in multihop networks exist. However, their limitation is that they do not provide the autoconfiguration for a global routable address in ad hoc networks. Furthermore they are limited to stateless solutions. Therefore, existing mechanisms can only be used either for configuring a global routable address without multihop support or for configuring a local IP address with multihop support.

2.3. IPv6 in IPv4 Tunnel

As described before the testbed connects an IPv6 based ad hoc network over a cellular network with the 6Bone network. The cellular network only provides IPv4 connectivity so a solution to send IPv6 packets over an IPv4 infrastructure is needed. To solve this, a server located in the 6Bone (e. g. a Home Agent (HA)) is needed. A tunnel between Mobile Gateway and Home Agent is used to encapsulate IPv6 packets in IPv4 packets. As an example, Figure 3

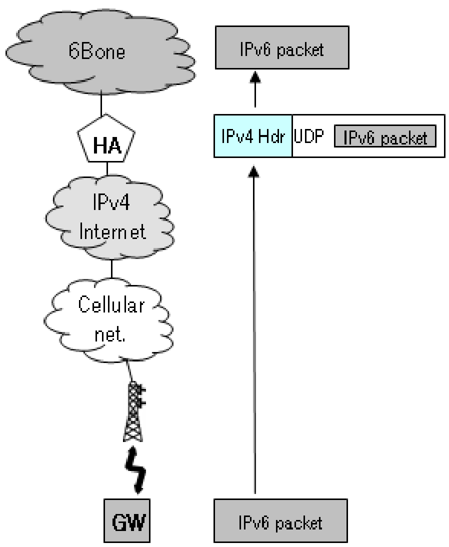

Figure 3. IPv6 in IPv4 tunnel

shows the packet handling for the uplink. IPv6 packets from the ad hoc network arrive at the Mobile Gateway. The gateway encapsulates the IPv6 packets into the UDP payload of an IPv4 packet. This packet is now ready to be submitted over the cellular IPv4 network. As destination address the address of the Home Agent is used. After the packet arrives at the gateway, the IPv4 and UDP header will be stripped off and the original IPv6 packet can be routed in the 6Bone network. In the downlink this mechanism works in a similar way. The HA encapsulates the IPv6 packets and sends them over the IPv4 infrastructure. The Mobile Gateway will decapsulate the packet and send it into the ad hoc network. The Crypto IP Encapsulation (CIPE) [12] tunnel software is used in the testbed to set up the IPv6 in IPv4 tunnel. This software is able to tunnel IP packets in UDP packets. It can also encrypt these packets to provide a high level of security. Furthermore it can handle the dynamic IP address allocation in cellular networks. The problem is that the Mobile Gateway will get a different IP address at each login to the cellular network. So a static tunnel configuration can not be used. CIPE can handle the dynamic IP address at the gateway and provide a more dynamic configuration.

3. Seamless Mobility

In the previous sections this paper described how mobility within ad hoc environments can be achieved. Ad hoc routing protocols provide mobility within the ad hoc network. Enhancements of these protocols are also able to provide mobility between different gateways within one ad hoc domain. Using a Mobile Gateway gives the whole ad hoc network the possibility to be mobile without having to lose the Internet connection. This section analyses the case of

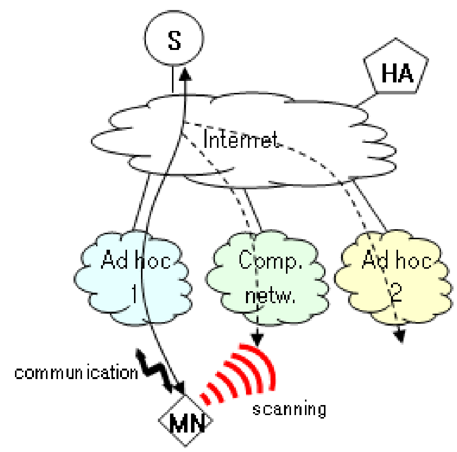

Figure 4. seamless roaming scenario

a single ad hoc node moving between different ad hoc or access networks. A seamless mobility scenario is depicted in Figure 4. A mobile ad hoc node (MN) wants to roam between two ad hoc networks and one access network (e. g. company network). At the beginning the ad hoc node is connected to ad hoc network 1 and has an active data connection to a server S in the Internet. MN is moving away from ad hoc network 1 towards the company network. The company network is configured for the infrastructure mode so the normal WLAN mobility cannot provide a handover between ad hoc network 1 and the company network. We have ascertained two problems for a mobile ad hoc node that wants to roam between different ad hoc or access networks. The first problem is that the automatic scanning mechanism of WLAN cards is not able to switch between infrastructure mode and ad hoc mode. If the interface is configured for infrastructure mode the card will never scan for ad hoc networks. Another problem appears when the scanning is triggered from the userspace. In this case the scanning process might last up to 2 seconds [13]. During this period the wireless card is not able to communicate and packets arriving within this time will be lost. To overcome these gaps and to provide seamless mobility between heterogeneous networks, we have equipped the mobile ad hoc node in the testbed with two WLAN interfaces. One interface can be used for data communication, in parallel the second one can scan for other networks, thus the data connections are not disrupted. The MobileIPv6 implementation was modified for these purposes. Our idea is depicted in

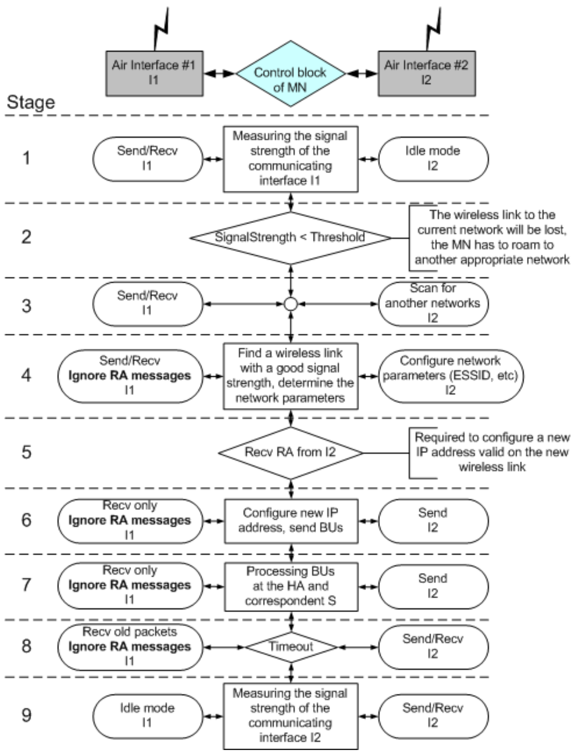

Figure 5. seamless roaming procedures

Figure 5 and works as follows. During the whole data session with the server S, the MN measures the signal strength of the communicating wireless interface (1). If this signal becomes less than a certain value, it is expected that the MN is able to lose the wireless link to its neighbours within the ad hoc group 1 (2). Then the second interface is set into the scanning mode, thus other appropriate networks may be found for a possible roaming purpose (3). If a network with a better signal strength is determined, this network is selected as target network and the corresponding network parameters (e.g. ESSID, operation mode, frequency, etc.) are identified and the second interface is configured accordingly (4). In the next step the MN needs to obtain a topological correct address for the second interface and needs to register it with the Home Agent using MobileIPv6. A stateless address autoconfiguration as described in the previous section is used for this. A new address for the second interface is configured as soon as the first Router Advertisement (RA) message from the new network is received (5, 6). These signalling messages are also used by MobileIPv6 for movement detection. The movement detection mechanisms would not work properly now because both interfaces will receive RAs, from the ad hoc network 1 and from the target network (company network). MobileIPv6 may use two handover modes: either Eager Cell Switching (ECS) or Lazy Cell Switching (LCS). Using ECS the MobileIPv6 accepts any new RA, thus it switches to the new network immediately. This mode cannot be applied in our situation, as MobileIPv6 will always switch to another network after an RA was received on one of the interfaces. Thus a ping-pong effect appears, while the MN is in overlapping area of two networks. Using LCS the MN switches to a new network as soon as it receives a new RA while it has not received a certain number of RAs from the current network. The MN will only reestablish IP connectivity through the new network after losing the connection to the current network, thereby data packets will also be lost. Thus, no seamless mobility may be achieved applying this handover mode, too. For this issue we have modified the MobileIPv6 implementation as follows. The enhanced MobileIPv6 implementation prioritizes the interfaces. Thus, after configuration the previous scanning interface for communication with a new network, this interface gets a higher priority. Only the RA messages received on this interface are accepted; the RA messages received on the other interface will be ignored (4). Thus MobileIP will only receive RA messages on the interface with the higher priority and start a binding update with the HA and S (6). After the Binding Updates was successful (7), all data packets will be delivered to the MN over the company network (8, 9). Older packets S send before the Binding Updates can still be received by the MN because the first interface will remain for a certain time in the communication modus (8). After this time the first card is set to idle and can be used for scanning if needed (9). Using two independent interfaces provides seamless mobility. The handling of these two interfaces is done by the modified MobileIPv6 implementation. In normal cases MobileIPv6 only supports one interface on the mobile node. In our case we needed to enhance our implementation to work with two independent interfaces.

4. Conclusions

This paper describes a testbed that connects ad hoc networks with the Internet. A Mobile Gateway has been developed that uses a cellular network for the connection. It handles the challenges that had to be solved to realize this interconnection and describes a way how to connect two IPv6 networks over an IPv4 infrastructure. Different levels of mobility are described. Mobility within the ad hoc domain and between different Mobile Gateways of this ad hoc domain is handled using an enhanced AODV routing protocol. Mobility of the whole ad hoc network is handled by the mobility mechanisms of the cellular network and finally the seamless mobility of single ad hoc nodes is realized using two interfaces and a modified MobileIPv6 implementation.

References

[1] Jin Xi and Christian Bettstetter. Wireless multihop internet access: Gateway discovery, routing, addressing. *Technical University Munich, Institute of Communication Networks*.

[2] Alex Ali Hamidian. A study of internet connectivity for mobile ad hoc networks in ns2. *Department of Communication Systems, Lund Institute of Technology, Lund University*.

[3] R. Wakikawa, J. T. Malinen, C. E. Perkins, A. Nilson, and A. J. Tuominen. Global connectivity for ipv6 mobile ad hoc networks. *Internet Draft, November 2001, Work in progress*.

[4] Nico Bayer, Bangnan Xu, and Sven Hischke. An architecture for connecting ad hoc networks with the ipv6 backbone (6bone) using a wireless gateway. *In Proc. European Wireless Conference 2004*.

[5] C. E. Perkins, E. M. Royer, and S. Das. Ad hoc on demand distance vector (aodv) routing. *Internet Draft, March 2001, Work in progress*.

[6] C. E. Perkins, E. M. Royer, and S. Das. Ad hoc on demand distance vector (aodv) routing for ip version 6. *Internet Draft, November 2000, Work in progress*.

[7] Matthias Rosenschon, Tilmann Maenz, Joachim Habermann, and Veselin Rakocevic. Simulation results on a gateway discovery algorithm for ad-hoc networks using hello packets. *In Proc. International Workshop on Wireless Ad-hoc Networks 2005*.

[8] Nico Bayer, Bangnan Xu, and Sven Hischke. Address autoconfiguration in wireless ad hoc networks with connection to the ipv6 backbone (6bone). *In Proc. Wireless Personal Multimedia Communications Conference 2005*.

[9] C. E. Perkins, J. T. Malinen, R. Wakikawa, E. M. Belding-Royer, and Y. Sun. Ip address autoconfiguration for ad hoc networks. *Internet Draft, November 2001, Work in progress*.

[10] J. P. Jeong, J. Park, H. Kim, and D. Kim. Ad hoc ip address autoconfiguration. *Internet Draft, February 2004, Work in progress*.

[11] K. Weniger and M. Zitterbart. Ipv6 stateless address autoconfiguration for hierarchical mobile ad hoc networks. *Internet Draft, February 2002, Work in progress*.

[12] http://sites.inka.de/sites/bigred/devel/cipe.html.

[13] IEEE. Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. *IEEE Standard 802.11, 1999*.