Extending the Coverage of a 4G Telecom Network using Hybrid Ad-hoc Networks: a Case Study

Tânia Calçada, and Manuel Ricardo
Fac. Eng. Univ. Porto, INESC Porto, Portugal

Abstract—Ad-hoc networks that are connected with the infrastructure Internet are named hybrid ad-hoc networks. In 4G communications scenarios, hybrid ad-hoc networks seem to be valuable since they may increase the coverage of wireless networks with minor costs. Using them, terminals out of range of an access point or a base station, or not having adequate network interfaces, may reach the operator's infrastructure via other terminals. This paper presents a hybrid ad-hoc network solution and a testbed implementation.

I. Introduction

Ad-hoc networks can be used to enable infrastructureless and spontaneous communications between nodes. In an ad-hoc network each terminal behaves as a router, forwarding traffic (IP packets, in this case) to other terminals. In hybrid ad-hoc networks [1] the ad-hoc nodes can also communicate with an infrastructure network either directly or via other nodes, in a multi-hop topology.

The operator of a 4th Generation communications network will deploy IP access networks which offer connectivity to wired and wireless nodes. These nodes are miniaturized computers supporting multiple network interfaces (e.g. GPRS, UMTS, 802.11, Ethernet and DVB), and having communications capabilities analogous to a computer interconnected to the Internet. By using the hybrid network concept, the 4G networks can extend their coverage to shadow areas where it would be expensive or unfeasible to have radio coverage provided by base stations.

This paper presents a solution for deploying an hybrid ad-hoc network based in IPv6. A real prototype is described, that uses a reactive ad-hoc routing protocol and a proactive gateway discovery protocol. Combined, they optimize the interconnection from the operator's perspective.

The Section II of this paper describes the goals, requirements, and assumptions of this work. Section III presents the state-of-the-art in ad-hoc gateway discovery protocols. Section IV proposes a solution. Section V gives the details about the prototype implementation. Section VI addresses the issues open in the solution and required to be solved. The Section VII concludes this paper.

The work described in this paper is based on results of IST FP6 Integrated Project DAIDALOS (http://www.ist-daidalos.org/). DAIDALOS receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. This paper may contain forward-looking statements relating to advanced information and communication technologies. Neither the DAIDALOS project consortium nor the European Community does accept any responsibility or liability for any use made of the information provided in this paper.

We acknowledge the financial support of FCT (Fundação para a Ciência e Tecnologia) / POSI (Portuguese Science and Technology Foundation).

The authors are with the INESC Porto – Instituto de Engenharia de Sistemas e Computadores do Porto, 4200-465 Porto, Portugal (e-mail: tcalcada@inescporto.pt, mricardo@inescporto.pt).

II. Goals, Requirements and Assumptions

The main goal of this work is to provide mobile terminals located in shadow areas, or having inadequate radio interfaces, with access to an operator infrastructured network, assuming that IPv6 is used. More than providing efficient communications within ad-hoc networks, this work aims at providing an efficient interconnection between an ad-hoc mobile node and the operator infrastructure.

The main requirements are (1) low signalling overhead, (2) resilience, and (3) support of operator driven policies. Ad-hoc networks demand routing protocols and interworking mechanisms having low signalling overheads, for good efficiency. Multiple gateways to the infrastructured network shall be supported, in order to eliminate single points of failure, balance traffic, and provide multipath connections. The infrastructured network shall have full control of communications, in order to enable security, QoS, and

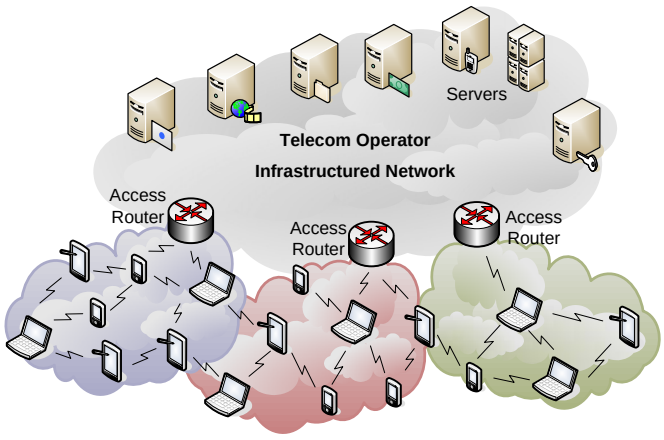

Fig. 1. Ad-hoc as an extension of the operator's infrastructure network. Three hybrid ad-hoc networks provide access to mobile nodes.

charging policies.

The scenario envisaged is the extension of the operator's network coverage to nodes only reachable via the ad-hoc network, and it is shown in Fig. 1. Traffic flows are expected mainly between ad-hoc and infrastructure connected nodes. A few tens of nodes are expected in a single ad-hoc network.

The ad-hoc point of attachment to the infrastructured network is the gateway. The gateway forwards packets between ad-hoc and infrastructure nodes, and can be a mobile node or a fixed access router. Many functions are expected to be deployed in the gateway, such as QoS mapping, node authentication, charging, and security. In an operator driven scenario, the gateway shall preferably be a fixed access router, which is owned, managed, and trusted by the network operator.

III. Ad-Hoc Gateway Discovery Protocols

A gateway discovery protocol provides the node with Internet connectivity, that is, it enables the node to discover the address of the gateway, defines the mechanism to forward a packet towards the gateway, and may also auto-configure a globally routable address.

A gateway discovery protocol may be proactive or reactive. In the proactive mode, the gateway spreads periodically information through the ad-hoc network; this is useful if a node communicates frequently with the infrastructured network. In the reactive mode, a node requests the gateway information and the network prefix when it needs to communicate with the infrastructured network; this is useful when ad-hoc nodes communicate between them and, occasionally, access the Internet. The operation mode of the gateway discovery protocol may be selected considering the traffic scenarios, just like a routing protocol; however, these choices shall be independent.

A study of some gateway discovery protocols exists in the literature [2]. However we will focus on gateway discovery protocols currently available at IETF as internet drafts [3-6]. Two of them deserve special attention: GwInfo [3], and Global6 [4]. These methods are described in next sub-sections and are compared in Table 1. The methods presented in [5, 6] are excluded since they are dedicated to AODV [7]. Although AODV was the routing protocol selected for our test-bed, we require that the gateway discovery protocol works with other routing protocols.

TABLE I
Evaluation of Gateway Discovery Protocols

	GwInfo	Global6
Operation Mode	· Proactive	· Proactive, with proactive routing · Reactive, with reactive routing
Routing Protocol Compatibility	· Any · Tests made with OLSR	· Any · Tests and examples with AODV
Signaling	· GwInfo messages	· Extended AODV routing protocol messages · Extended NDP messages
Multiple Gateway support	· Possible, but a node uses one GW at time · Mentioned multihoming · 3 selection algorithms specified	· Possible with restrictions · Selection algorithms not specified
Packet Forwarding towards the Gateway	· Prefix continuity · Next hop forwarding · Default route on proactive routing	· Default route via the gateway · Routing extension header

A. GwInfo

Similarly to IPv6, the GwInfo [3] protocol forces the gateway to announce periodically a network prefix. The method supports multiple gateways, which announce different global network prefixes. An ad-hoc node may listen announces from multiple gateways. In order to select one of them, some algorithms are proposed based on metrics such as distance to the gateway, or stability (keep the network prefix as long as possible). The method is independent of the underlying routing protocol, and it can be used with proactive and reactive routing protocols.

Each gateway broadcasts periodically an advertisement message whose destination is a link local multicast address, reaching 1 hop distant nodes. This message carries the gateway address, the network prefix length, and the distance to the gateway. When a node receives this message, it may decide to use the prefix announced. In this case, the node configures a global address, using the network prefix information received and its 64-bit interface ID; then, the node updates its hop count, and multicasts the message again to its one hop neighbours.

The node that delivered the prefix information is named upstream neighbour. Even in the presence of multiple network prefixes, the prefix selection policy and the propagation method lead to the concept of "prefix continuity". The prefix continuity property ensures that all nodes on the path to the gateway have the same network prefix and, together, they form a tree towards the gateway.

When used with proactive routing protocols (e.g. OLSR [8]), each node creates a default route which uses its upstream neighbour as the next hop; the prefix continuity property avoids the use of an IPv6 routing header, if the link to the upstream neighbour is bi-directional. When used with reactive routing protocols (e.g. AODV [7]), the periodic announcement message is not used to add a default route, since a default route is said to be incompatible with the reactive routing paradigm; in alternative, the route to the gateway can be obtained using the route lookup method of the routing protocol. GwInfo has been tested with OLSR.

B. Global6

The Global6 [4] protocol provides two solutions, proactive and reactive, which shall be combined with proactive and reactive routing protocols, respectively. The proactive solution disseminates periodically gateway advertisements to all nodes in the ad-hoc network; the reactive solution uses solicitation

and advertisement messages, which are exchanged between a node and the gateway. The Neighbour Discovery Protocol or the routing protocol messages are extended in order to support the solicitation and advertisement information.

After accepting an advertisement from a gateway, the node configures a routable IP address using the network prefix announced and its 64-bit interface ID; then, the node creates a default route using the gateway as the next hop, and a host route to the gateway using the routing protocol. The packets for the infrastructure network are, thus, forwarded to the gateway and may carry out a routing header containing the gateway address and the address of the infrastructure destination node. If allowed by the routing protocol, hop-by-hop forwarding can also be used but, in this case, there is no guarantee that the correct gateway is used. If Mobile IPv6 is used, the node can use the address acquired as its care-of-address. Global6 is said to be independent of the routing protocol, but the implementations known are integrated only with AODV.

IV. PROPOSED SOLUTION

In order to carry out our experience we used an ad-hoc routing protocol, a gateway discovery protocol, and an interface between them.

Several routing protocols have been proposed for mobile ad-hoc networks during the last years. AODV [7] was the routing protocol selected for our experience, since it fits well in the scenario envisioned: small ad-hoc networks, some node mobility, and most of the flows destined to infrastructure nodes. AODV has reduced control traffic when compared with pro-active protocols, but increases the latency when new routes are required. This increase is mostly caused by the discovery and update of the routes which are created and maintained when needed.

The gateway discovery protocol selected was the GwInfo protocol. Prefix continuity is a relevant characteristic of this solution since it enables the creation of topologically coherent networks. From the operator management perspective, an organized network is preferable; that is, users take advantage of the ad-hoc facilities, but the operator still has an organized network. Another benefit of prefix continuity is that it enables hop-by-hop default routing, and does not demand an additional routing header mentioning the gateway. The proactive nature of the GwInfo protocol, even when combined with reactive routing protocols, is also an advantage from the operator's perspective. Using it, the operator announces itself and its gateway, and may force the node to authenticate, even before this node needs to communicate. As consequences, the operator becomes aware of the node's location, and the other ad-hoc nodes may start using the recently authenticated node to forward their packets. The GwInfo method can interact with any routing protocol, which is an advantage when comparing with the other methods. Although Global6 also supports every routing protocol, its operation mode follows the proactive or reactive nature of the routing protocol.

The GwInfo protocol running on an operator access router (the gateway) sends periodically the advertisement message through the ad-hoc network; when receiving this information, a node may configure a default route. AODV is a reactive routing protocol, so it does not maintain an extensive routing table to all the nodes in the ad-hoc network, and it should not have a default route. In order to AODV interoperate with the GwInfo protocol, it must suffer some modifications. A possibility would be not to use the default route and to forward internet packets directly to the gateway relying on a path accumulation paradigm [9] on the route discovery. Another solution is to change the forwarding table lookup process. When a node has a packet to send or forward, it first checks if the destination address is outside the ad-hoc network. If the destination address has the same network prefix of the source node, then AODV finds a route as it usually does. Otherwise, the node forwards the packet through the default route, which uses the node's upstream neighbour as next hop. The solution is not optimal for routing between ad-hoc nodes associated to different gateways and using different network prefixes, since the packets must visit the two gateways; however, this is not a big problem since the communications towards the gateway are expected to be the most frequent. This method is simple, and it has low overheads when compared with the first possibility.

V. IMPLEMENTATION AND VALIDATION

A prototype was implemented in order to validate the solution advocated in last section. This prototype, shown in Fig. 2, consists of a gateway (GW), 3 ad-hoc nodes (MN1, MN2, and MN3), and a computer in the infrastructure network (Server). The nodes are laptops and the gateway is a desktop, all running Mandrake 10.0 Linux, and equipped with wireless LAN cards (Cisco Aironet 350 series) configured in ad-hoc mode. The nodes and the gateway run AODV, based on the UU-AODV [10]; changes were made to this implementation, in order to support IPv6 addressing and to run on kernel version 2.6. The nodes and the gateway also run the GwInfo protocol implementation [11]. In order to let the GwInfo and the AODV modules interoperate, the modification in the forwarding table lookup process described above was implemented in the AODV code. The information about the selected network prefix is passed from the GwInfo module to the AODV module using UNIX sockets.

The tests using these equipments were made indoors, all computers in the same room, with all the WLAN cards configured with the same ESSID. For that reason, the powers transmitted enabled every computer to reach all the others. In order to overcome this situation, and simulate an ad-hoc environment, MAC filtering was implemented using the ip6tables tool of the Linux distribution.

The initial configuration of the network is presented on the top of Fig. 2, and the messages exchanged by the GwInfo

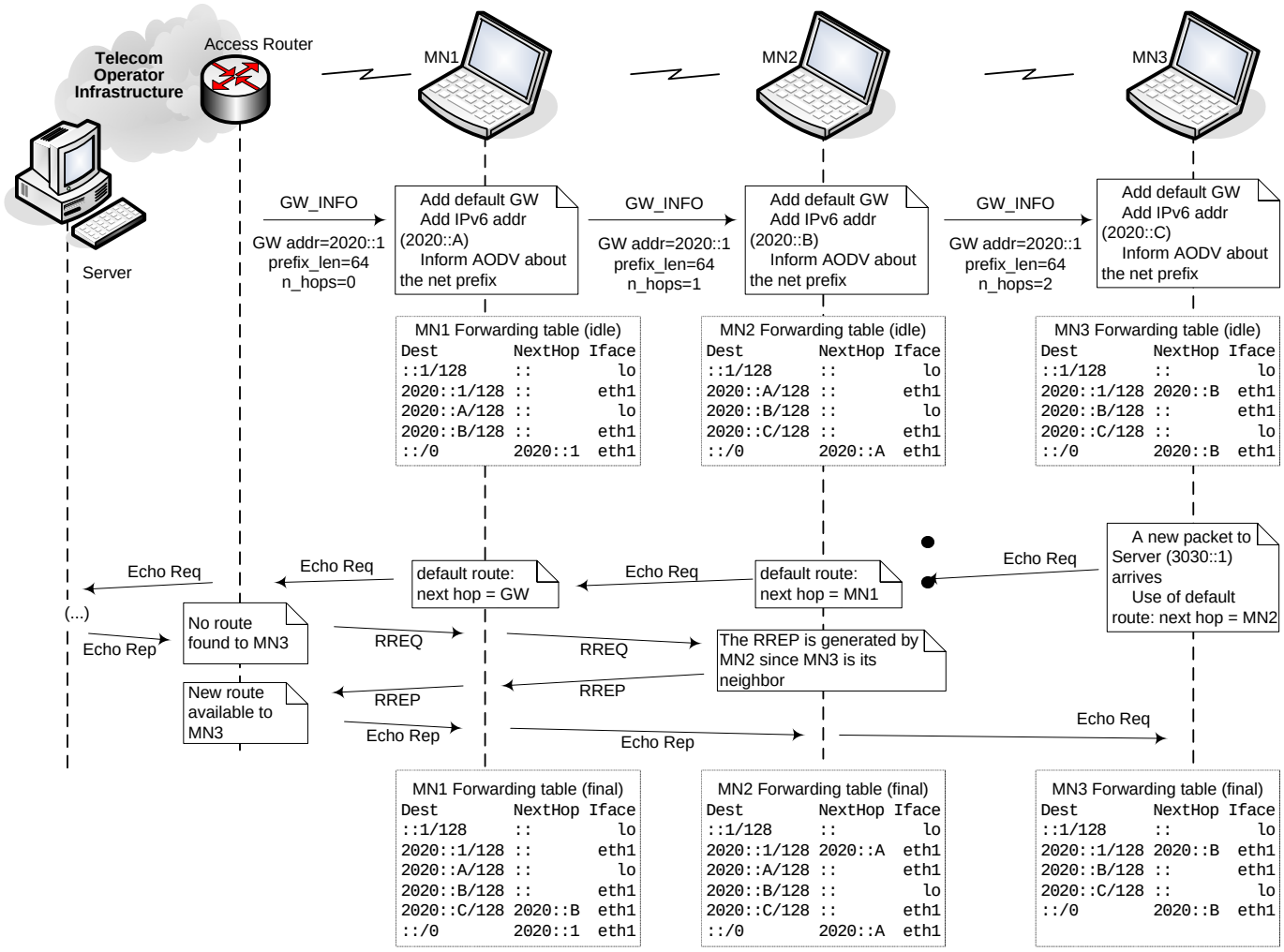

Fig. 2. Prototype of the Ad-hoc Integration Scenario and messages exchanged. The tested scenario is shown on top. Initial messages and actions, and the resulting forwarding tables of the mobile nodes are shown in the middle of the figure. On the bottom we present the forwarding tables when data packets are sent between an ad-hoc node and a server located in the infrastructure network.

modules are shown just below. The GW_INFO message is propagated hop-by-hop, and each node receiving the message (1) configures a global address (MN1-2020::A, MN2-2020::B, and MN3-2020::C), (2) configures a default route using the network information received, and (3) informs the AODV module about the ad-hoc network prefix. The AODV HELLO messages are exchanged between neighbours who are used to create host routes to adjacent neighbours in each node forwarding table; in order to simplify the figure, the HELLO messages are not represented. After these steps, the forwarding tables of the nodes have the information shown in the centre of Fig. 2. Entries to link local and multicast addresses are hidden, since they are irrelevant for this discussion; the route for 2020::/64 is also hidden since it is never used.

The AODV implementation intercepts every outbound packet and compares its destination network prefix with the one delivered by the GwInfo module. If its destination address belongs to the ad-hoc network, in this case 2020::/64, the packet is retained until a host route is found; the other packets are released immediately, i.e. queued in the Linux IPQueue, and follow the default route.

In order to show the network behaviour and the interoperation between GwInfo and AODV, a simple experience is described; having all the nodes configured as shown in Fig. 2, MN3 will ping the Server in the infrastructure network. To ping, consists in sending a set of ICMP Echo Request packets and receiving ICMP Echo reply packets. The bottom of Fig. 2 describes this communication. The source of the first packet is MN3; since the network prefix of the destination address is different from 2020::/64, the default route is used to forward the packet in each ad-hoc node in the path towards the gateway. When the ICMP Echo Reply message, sent by Server to MN3, arrives to the gateway and there is no host route to it, the conventional AODV route lookup is started: RREQ messages are propagated hop-by-hop and the MN2, which already has a route to MN3, sends a RREP back to the gateway. In this process, MN1 also learns the route to MN3. Then, the ICMP Echo Reply message is sent hop-by-hop to MN3.

VI. Future Work

Many issues related to this topic need to be further investigated, which include: 1) a multiple gateway solution, capable of integrating the GwInfo protocol and multi-homing; 2) handover between gateways, keeping context information such as charging, authentication, and QoS; 3) improve the routing between ad-hoc networks holding different prefixes; 4) support the node automatic "handover" between infrastructure and ad-hoc modes; 5) secure the GwInfo protocol; 6) support multiple L2 technologies; 7) port the solution for PDAs and mobile phones.

VII. Conclusions

In this paper we proposed a solution for integrating ad-hoc with IPv6 infrastructure networks. For that purpose, we carefully characterized the state of the art in gateway discovery protocols. Based on previously identified requirements, we proposed a solution which consists in integrating GwInfo with AODV, and in introducing modifications on the forwarding table look up mechanism: for a host route not in the forwarding table, AODV is used only when the packet destination address belongs to the ad-hoc network prefix; otherwise, a route via the node´s upstream neighbour is used. In order to demonstrate the value of this solution, we implemented a prototype network and carried out meaningful experiments.

Acknowledgment

We thank Eng. Filipe Abrantes for his valuable help on the implementation work, and Dr. Norbert Vicari for porting the AODV implementation to IPv6.

References

[1] S. Ruffino, P. Stupar, T. Clausen, and S. Singh, "Connectivity Scenarios for MANET," IETF, Internet-Draft draft-ruffino-manet-autoconf-scenarios-00.txt, February 2005.

[2] M. Ghassemian, P. Hofmann, C. Prehofer, V. Friderikos, and H. Aghvami, "Performance Analysis of Internet Gateway Discovery Protocols in Ad Hoc Networks," presented at WCNC 2004, 2004.

[3] C. Jelger, T. Noel, and A. Frey, "Gateway and address autoconfiguration for IPv6 adhoc networks," IETF, Internet-Draft, February 2005.

[4] R. Wakikawa, J. T. Malinen, C. E. Perkins, A. Nilsson, and A. J. Tuominen, "Global connectivity for IPv6 Mobile Ad Hoc Networks," IETF, Internet-Draft, October 2003.

[5] H.-W. Cha, J.-S. Park, and H.-J. Kim, "Support of Internet Connectivity for AODV," IETF, Internet-Draft, February 2004.

[6] H.-W. Cha, J.-S. Park, and H.-J. Kim, "Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks," IETF, Internet-Draft, October 2003.

[7] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF, RFC 3561, July 2003.

[8] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," IETF, RFC 3626, October 2003.

[9] C. E. Perkins, E. M. Belding-Royer, and I. D. Chakeres, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF, Internet-Draft draft-perkins-manet-aodvbis, July 2004.

[10] E. Nordstrom and H. Lundgren, "AODV-UU," v0.8, Uppsala University, available online at http://www.docs.uu.se/~henrikl/aodv/.

[11] A. Frey, "GWINFO," Université Louis Pasteur - LSIIT, available online at http://clarinet.u-strasbg.fr/~frey/.

Tânia Calçada (tcalcada@inescporto.pt) received a licenciatura degree in electrical and computer engineering, from Porto University, Portugal in 1999. She is a PhD student at the Faculty of Engineering at Porto University, Portugal. She works as a researcher in INESC Porto and is currently participating in the European DAIDALOS project. Her research interest is Mobile Ad-hoc Networks.

Manuel Ricardo (mricardo@inescporto.pt) received a licenciatura degree in 1988, a M.S. in 1992, and a Ph.D. in 2000, all in electrical and computer engineering, from Porto University, Portugal. He is an assistant professor in the Faculty of Engineering, Porto University, where he gives courses in mobile communications, and computer networks. He also leads the Communication Networks and Services Area at INESC Porto.