MANET
Internet-Draft
Expires: August 15, 2005

S. Ruffino
P. Stupar
TILAB
T. Clausen
LIX
S. Singh
SAMSUNG AIT

February 11, 2005

Connectivity Scenarios for MANET
draft-ruffino-conn-scenarios-00

Status of this Memo

Copyright Notice

Abstract

This Internet Draft aims at describing a wide spread set of possible connectivity scenarios involving mobile ad-hoc networks, in order to provide reference for standardization effort in this field. The aspects considered for definition and classification of the scenarios are number and characteristics of the gateways that connect MANET nodes to external networks. Analysis will range from a scenario where no connectivity is provided, i.e. an isolated MANET, to more complex scenario where a MANET has multiple mobile Gateways.

Table of Contents

1. Introduction

MANET were initially designed to be employed in highly dynamic and unpredicatable environments, characterized by high mobility of users and terminals. MANETs are essentially autonomous, self-configuring, self-healing networks, whose mobile nodes discover other nodes and supported services in an automatic fashion. MANET routing protocols, as studied in IETF, enable two generic MANET nodes to exchange data traffic through multi-hop connections, if a 1-hop radio link between them is not available. In this way, nodes can freely move within the MANET: routing protocols dynamically react to movement and constantly discover the optimal path according to a predifined metric, e.g. number of hops. If an intermediary node, belonging to a path between a source and a destination, fails, traffic is automatically re-routed through an alternative path.

RFC2501 [1] defines a MANET and also introduces the possibility to connect a MANET to an external network, by means of gateways. These are devices equipped with two or more network interfaces: a MANET interface and an interface typically connected to one or more non-MANET networks. MANET nodes exchange traffic among themselves using multi-hop paths and can reach outside hosts and the Internet by means of the gateways. In this case the MANET acts as a "stub" network, whose nodes route traffic originating and/or terminating within the MANET itself.

Operators, Network and Service providers show increasing interest in this type of network, as a consequence of the wide spread deployment of low-cost radio technologies such as IEEE802.11a/b/g/h and the increasing customer base. Initially, commercial MANETs are expected to be deployed as an extension to the traditional infrastructure networks, to realize the so-called hybrid networks.

An example of this networks are the Mesh Networks, used to extend the coverage area of a public hot-spot or to realize large-scale low-cost wireless coverage in urban areas. A further interesting application and research field is represented by multi-hop cellular networks: MANETs connected to cellular WAN networks. In this case MANETs can be used to realize an extended wireless coverage in areas where "traditional" cellular network is not available.

Many proposals and projects that introduce integration between MANET and 3G+ networks exist: for example, see [2], [3], [4] and [5].

This Internet Draft aims at describing and analyzing connectivity scenarios for MANET, to provide a reference for standardization effort in this field. In fact, the scenarios described herein can be used as a starting point for the design of solutions to technical

problems, such as address autoconfiguration, gateway discovery, Duplicate Address Detection and global prefixes management.

Analysis will range from a scenario where no connectivity is provided, i.e. an isolated MANET, to more complex scenarios where a MANET has multiple mobile Gateways. This document is structured in the following way: in Section 2 a glossary for commonly used terms is given; in Section 3 connectivity scenarios for a MANET are listed. In this section particular attention is paid to the connection of a MANET with other external networks, by means of one or more fixed (Section 3.2.1) or mobile wireless gateways (Section 3.2.2). In Section 4 the roaming of a node from a Infrastractured wireless LAN to an ad-hoc network is considered.

2. Terminology

Node

An IPv4/IPv6 device which is a MANET element: it runs a MANET routing protocol and exchanges data with other nodes within a MANET and with hosts located within external networks. A node has at least one physical interface connecting it to the MANET.

Gateway

A node equipped with at least two interfaces, one of which connects it to an external network, i.e. non-MANET, and can be wired or wireless.

Host

An IPv4/IPv6 terminal/computer, external to the MANET. Host is defined here as only "External" to differentiate it from the nodes of the MANET.

Wireless Interface (or MANET interface)

The physical network interface that connects a node to the MANET.

Radio Interface (or Cellular Interface)

The physical network interface that can connect a gateway to an external Wireless Wide Area Network, owned and administered by an operator.

3. Scenarios

In this section, we describe the typical connectivity scenarios of a MANET. This section is structured as follows: first, the case of an isolated MANET is examined, where no gateways exist. Then, various scenarios of a connected MANET are given, classified by the characteristics and the number of gateways, which can be fixed and/or mobile. In the end, the case of an intermittently connected MANET is analyzed.

3.1 Isolated MANET

An isolated MANET is a network that is autonomously set-up among wireless mobile nodes localized in the same geographical area. Nodes activate Layer 2 radio links, by which they can exchange traffic with their neighbors, and run an ad-hoc routing protocol, which enables multi-hop data forwarding through intermediate nodes. Routing protocol constantly discovers routes between nodes, in a proactive ([13], [15]) or reactive fashion ([14], [16]): this enables each node to route traffic to all other nodes within the MANET also during movements.

In this type of MANET there is no connection to an external network: all traffic is generated by MANET nodes and addressed to MANET nodes.

Typical applications of this scenario are temporary networks, that must be set-up in areas where neither wireless coverage nor infrastructure exist. Examples can be emergency networks used for disaster recovery, battlefield applications, electronic surveillance. Other examples can be found in occasional work meetings, where networks are set-up to enable file sharing among co-workers.

3.2 MANET connected to an external network

In this scenario a MANET is connected to an external network by means of one or more gateways (Figure 1). A generic MANET node can exchange data traffic with every other node through multi-hop paths and communicate with hosts located in the external network, routing its uplink traffic towards a gateway. Such gateway, in turn, will receive return traffic from the host and will route it to the source node.

```
                                     H1
                                      |
                               +---------------+
                               |   Internet    |**
                               +---------------+  *
                                 *           *     *
                                 *           *      *
                             GW1**           *       GW3
                               |         +--GW2-------+
                               |         |   |
                            ---N1--------+   |
                           /      \          |
                         N4        \        N2
                                    N3-----/
```

Figure 1: MANET interconnected to an external network

Gateways play a critical role here. If the number of nodes in the MANET increases, gateways can become bottlenecks, as they route an increasing and possibly huge amount of traffic. This also depends on the available bandwidth on the uplink interface. Moreover, gateways can be equipped with a number of additional features. For example, they could participate to the external routing protocol, in order to announce internal routes to external routers and hosts, possibly performing some kind of aggregation. They can act as enforcement points for security purposes: they can control access to external networks and, following a common practice, they can enforce Ingress Filtering on MANET generated traffic. Finally they can also provide services like DNS to MANET nodes.

This scenario can be expanded, depending on the characteristics of the network interface connecting gateways to the external network: it can be either wired or wireless, which can, in turn, be of a different type with respect to the MANET interface. In the first case Gateways are fixed, while in the second case they can also be mobile, as the other MANET nodes.

Moreover, a MANET can have only one gateway (fixed or mobile) or can have multiple gateways (fixed or mobile). Other than guaranteeing a high degree of reliability and fault tolerance to the entire MANET, the presence of multiple gateways enables load balancing among the gateways themselves. This can be very useful especially when the external network is a low-throughput cellular WAN, such as GPRS/EDGE, in order not to overload a single gateway with traffic potentially generated by many nodes at the same time. Single traffic flows of multiple nodes or many flows of a single node can be routed through

different gateways, consequently implying an improvement of the overall performances of the MANET.

Gateways can also be equipped with additional resources in order to grant better fault tolerance to the entire MANET: additional energy resources, more processing power, more volatile and non-volatile memory. This is especially true in case of fixed gateways, that can be directly powered and directly operated.

The following sections detail usage scenarios for fixed and mobile gateways.

3.2.1 Fixed Gateways

In this scenario, gateways are deployed in predefined positions planned by the network operator. Each gateway is connected to the external network by means of a wired or wireless interface.

Mesh networks and networks used for environmental surveillance can be categorized under this scenario.

- Mesh Networks: these are probably the most widespread ad-hoc networks. In a Mesh Network, user terminals (nodes) exchange traffic between them directly through a layer-2 radio link and using other nodes or fixed wireless devices as intermediate relays. A Mesh Network is typically connected to an external infrastructure network by means of fixed wired Access Points, which act as gateways and typically connect the Mesh to an external infrastructure network.
  Mesh Networks can be further classified depending on the kind of devices which form the mesh itself. In fact, in some deployments, the mesh is realized only among the wireless Access Points, which are devices endowed with two wireless interfaces: the first interface forms the mesh with other peer access points, participating to a routing protocol, the second interface provides local connectivity to nodes, which cannot set-up a network themselves, as they don't run any routing protocol. In another case the mesh is realized among all the nodes, which have to run a routing protocol.
  Applications of this networks are Internet public access (browsing, email etc.) by mobile users from outdoor areas, wireless coverage of corporate building to give employees access to shared data and commonly used services (email, Intranet browswing). These solutions can bring to savings on cabling and maintenance costs.

- Surveillance networks: several wireless nodes endowed with sensors of various kinds are spread over high enviromental risk areas

(e.g. fires in wooden areas). They communicate through multi-hop connections and run a routing protocol. When an emergency situation arises, data collected by sensors are transmitted from the collecting nodes upwards one or more gateways (which can have both a wired or wireless interface) and conveyed to a manned monitoring station.
Topologies of this kind of network are typically static, as the nodes are installed in fixed positions within the monitored areas. Moreover, these networks are characterized by multiple constant low-throughput data flows going from the sensors to the gateways.

3.2.2 Mobile Gateways scenario

In this scenario, the gateway's radio interface, connecting the MANET to the external network, can be a cellular WAN interface (GSM, GPRS, EDGE, UMTS), a broadband wireless MAN (WMAN) interface (e.g. 802.16x, 802.20) or a WLAN interface (802.11a/b/g/h/j). In each of these cases, gateways can forward uplink traffic outside the MANET only if located within the transmission/reception range of one or more Base Stations or Access points. Gateways not only can move freely within the coverage area, but they can also move outside this area. In such case, the gateway can't forward uplink traffic destined to external hosts anymore, nor downlink traffic destined to internal nodes.

In this outlined scenario, the MANET can be seen as a coverage extension of the radio infrastructured network to which the gateways are connected. The primary benefit of such extension is that local communication between two nodes is performed without using any cellular radio resource, e.g. radio channels. Another benefit is the possibility to grant network access also to those terminals that are not equipped with a cellular radio interface (e.g. access sharing). The implication of this business model on security, accounting and rewarding aspects are out of the scope of this draft, neverthless must be carefully investigated.

A more advanced scenario can be realized when most of the nodes are also equipped with two heterogeneous interfaces. In this case gateways can be "occasional": they can be nodes that, after setting up the connection towards the external network, whenever located within its coverage area, can start forwarding other nodes' outbound packets. In this kind of scenario, gateways can be "special" nodes endowed with additional features, but they can also be ordinary MANET nodes, such as mobile phones and PDAs. In this last case, gateways are characterized by low computational power and limited energy resources. Although the MANET can again exploit benefits given by multiple gateways, additional issues arise: in fact, gateways are not under operators control anymore. It's possible that the owner of the

gateway establishes abruplty to turn his terminal off or to tear down the connection towards the cellular network, in order to save battery life. Thus, the number and the position of gateways are higly dynamic and this can cause frequent re-routing of uplink data flows.

o Automotive scenario: a MANET is set up by a group of vehicles. One or more of these may become a mobile gateway after connecting to the Wireless LAN of a petrol station or setting up an UMTS connection and, therefore, may be used by the other vehicles of the MANET to exchange traffic with the external hosts.

3.3 MANET intermittently connected to external networks

Gateways in a MANET, especially if mobile and equipped with a radio interface, may not be permanently connected to the external network. MANETs of this kind have the characteristics of both MANET described in Section 3.1 (while not connected) and of the ones described in Section 3.2 (while connected).

Most of the nodes belonging to a MANET of this kind shall exploit the connection temporally set up to an external network to communicate with hosts they can't reach while the MANET is isolated. As a consequence, such MANETs may experience a burst of exchanged traffic while connected to the external network. The amount and the distribution of such traffic depends on how long the MANET can be connected to an external network.

o Train network: a MANET built in a train, which is connected while stopped at the station and disconnected otherwise. In particular, if the MANET is set up by some passengers, it may happen that while the train is stopped at the station, some of the nodes may become gateways. For example, the station area may be covered by a wireless technology and some nodes equipped with a non-MANET interface of the same technology may therefore set up a connection to the external network. In this case, most of the users may use the gateways to connect to their mail server, download and eventually send their e-mails: the MANET they belong to may therefore experience a burst of traffic exchanged with the external network.

4. Roaming from a MANET to an Infrastructure Network

A mobile node, connected e.g. to a IEEE 802.11 network (infrastructure mode), can roam to a nearby IEEE 802.11 (ad-hoc mode) MANET. This situation can be very commonly experienced by a mobile node, during its movement, even not voluntarily. It is worth noting that such roaming doesn't involve only layer-2 operations. It is indeed likely that the procedures used within IEEE 802.11 network, e.g. for address configuration or duplicate address detection, are different from those used in a MANET. This is mainly due to the fact that a MANET is characterized by multi-hop paths while in a WLAN all hosts are connected to the same link.

There can be also situation where the destination MANET uses a different radio technology for multi-hop links. This scenario, not addressed in this document, brings added difficulties, because radio interface should be dynamically switched to use a different Layer 1 and 2 technology.

5. Security Considerations

This document raises no security issue.

6. IANA Considerations

This document has no actions for IANA.

7. References

[1] Corson, S. and J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations", RFC 2501, January 1999.

[2] Siebert, M., "On Ad Hoc Networks in the 4G Integration Process", Med-Hoc 2004 , June 2004.

[3] "Ambient Networks", http://www.ambient-networks.org .

[4] "Daidalos", http://www.ist-daidalos.org .

[5] "World Wireless Research Forum", http://www.wireless-world-research.org .

[6] Wakikawa, R., Malinen, J., Perkins, C., Nilsson, A. and A. Tuominen, "Global connectivity for IPv6 Mobile Ad Hoc Networks", I-D draft-wakikawa-manet-globalv6-03.txt, October 2003.

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

[8] Jeong, J., Park, J., Kim, H. and D. Kim, "Ad Hoc IP Address Autoconfiguration", I-D draft-jeong-adhoc-ip-addr-autoconf-02.txt, February 2004.

[9] Perkins, C., Malinen, J., Wakikawa, R. and E. Belding-Royer, "IP Address Autoconfiguration for Ad Hoc Networks", I-D draft-perkins-manet-autoconf-01.txt, November 2001.

[10] Singh, S., Kim, JH., Choi, YG., Kang, KL. and YS. Roh, "Mobile multi-gateway support for IPv6 mobile ad hoc networks", I-D draft-singh-manet-mmg-00.txt, June 2004.

[11] Paakkonen, P., Rantonen, M. and J. Latvakoski, "IPv6 addressing in a heterogeneous MANET-network", I-D draft-paakkonen-addressing-htr-manet-00.txt, December 2003.

[12] Jelger, C., Noel, T. and A. Frey, "Gateway and address autoconfiguration for IPv6 adhoc networks", I-D draft-jelger-manet-gateway-autoconf-v6-02.txt, April 2004.

[13] Clausen, T. and P. Jacquet, "Optimized link state routing protocol", RFC 3626, October 2003.

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

[15] Ogier, R., Templin, F. and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", RFC 3684, February 2004.

[16] Johnson, D., Maltz, D. and Y. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", I-D draft-ietf-manet-dsr-10.txt, July 2004.

[17] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[18] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[19] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[20] Aboba, B., "Dynamic Configuration of Link-Local IPv4 Addresses", Internet-Draft draft-ietf-zeroconf-ipv4-linklocal-17, July 2004.

[21] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[22] Sun, Y. and E. Belding-Royer, "A study of dynamic addressing techniques in mobile ad hod networks", I-D Wireless communication and mobile computing, May 2004.

[23] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[24] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[25] Engelstad, P., T°nnesen, A., Hafslund, A. and G. Egeland, "Internet Connectivity for Multi-Homed Proactive Ad Hoc Networks", First IEEE International Conference on Sensor and Ad hoc Communications and Networks , October 2004.

Authors' Addresses

Simone Ruffino
Telecom Italia LAB
Via G.Reiss Romoli 274
Torino 10148
Italy

Phone: +39 011 228 7566
Email: simone.ruffino@telecomitalia.it

Patrick Stupar
Telecom Italia LAB
Via G.Reiss Romoli 274
Torino 10148
Italy

Phone: +39 011 228 5727
Email: patrick.stupar@telecomitalia.it

Thomas Heide Clausen
Laboratoire d'informatique
Ecole Polytechnique
Palaiseau Cedex 91128
France

Phone: +33 1 6933 2867
Email: thomas.clausen@polytechnique.fr

Shubhranshu Singh
SAMSUNG Advanced Institute of Technology - i-Networking Laboratory
San 14-1, Nongseo-ri, Giheung-eup
Yongin-si, Gyeonggi-do 449-712
Korea

Phone: +82 31 280 9569
Email: shubhranshu@samsung.com

Appendix A. Acknowledgments

The authors would like to thank Ivano Guardini for his valuable comments.

Intellectual Property Statement

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.