Available online at www.sciencedirect.com
SCIENCE DIRECT®
Ad Hoc Networks 3 (2005) 656–667
Ad Hoc Networks
www.elsevier.com/locate/adhoc

Secure hosts auto-configuration in mobile ad hoc networks

Ana Cavalli *, Jean-Marie Orset

Institut National des Télécommunications, 9, rue Charles Fourier, F-91011 Evry Cedex, France

Available online 15 September 2004

Abstract

All existing routing protocols of Mobile Ad Hoc networks (MANET) assume that IP addresses of hosts are already configured before they join the network. In traditional schemes, this task is delegated to the dynamic host configuration protocol (DHCP [R. Droms, Dynamic host configuration protocol, RFC 2131, March 1997]), which allots an IP address to each requesting node. However, this process can not be applied in the context of MANET because of the lack of infrastructure and the great mobility that characterize them. A manual management of the addresses can be considered as long as the number of nodes remains reasonable. On the other hand, it is not possible any more since the network reaches a certain size. Some works proposed solutions to allow an automatic configuration of the nodes, i.e. without human intervention. Unfortunately these processes, often inspired of the traditional wired networks, are not always well adapted to MANET and appear relatively greedy concerning for example the delay, the address space or the bandwidth. Moreover, they apply only to ideal networks in which all nodes can trust each other. In this manner, they do absolutely not consider the security aspects and are thus not adapted to a real use in potentially hostile environment. In this paper, we propose a node auto-configuration scheme which uses the buddy system technique to allocate the addresses, as well as an algorithm allowing to authenticate the participants inside the network.

Keywords: Ad hoc networks; Auto-configuration; Security; Authentication; Address-attribution

1. Introduction

An ad hoc network is a group of mobile and wireless computers which communicate between them without the assistance of any infrastructure. Information is transmitted directly by the means of radio interface, or is relayed by other nodes till their destination. In this manner, each participant can at any moment act as a router to ensure a communication between other distant nodes. Hence, those networks are based on the cooperation between nodes. Moreover, they are characterized by a very dynamic topology and a totally open media. Several protocols were created to adapt specifically to these environments while presenting

* Corresponding author. Tel.: +33 1 6076 4427; fax: +33 1 6076 4711.
E-mail addresses: ana.cavalli@int-evry.fr (A. Cavalli), jean-marie.orset@int-evry.fr (J.-M. Orset).

1570-8705/$ - see front matter
doi:10.1016/j.adhoc.2004.08.011

pretty good performances (DSR [2], AODV [3], OLSR [4], etc).

Nonetheless, they all suffer from two significant drawbacks. First of all, they all suppose that IP addresses that will be used to identify the nodes in the network are configured in advance. In traditional networks, this task is carried out by hand when the number of nodes is reasonable, and by DHCP when the network becomes vaster. However, the use of this protocol requires the installation of a fixed and centralized DHCP [1] server, what can not always be feasible in MANET. Indeed, the strong mobility of the nodes can lead to partitions in the network and this approach would go against the independence of nodes with respect to any infrastructure. The second drawback is that these protocols were created according to an ideal model in which each node can trust any other one. Consequently, they appear very vulnerable face to participants who divert the normal operation of the protocol with malicious aims.

Many solutions were recently proposed to override these weaknesses and also to secure the routing process within MANET (ARIADNE [5], SEAD [6], ARAN [7]). However, they rely almost all on the routing layer. This is the reason why none of them allows actually to protect the configuration of nodes at the moment of their entry in the network, i.e. before proper routing is possible. On the other hand, several protocols were proposed to configure automatically IP addresses of nodes in ad hoc networks. But the problem in this case, is that none of them considers the security attacks which could disrupt the normal operation of the process. Nonetheless, since a lot of them rely on spoofing (impersonation), the address attribution is a very judicious moment to launch an attack and it also constitutes a very vulnerable step. The security also has to be considered as of the attribution of the addresses.

Accordingly, the protocol we propose in this paper is conceived to meet two goals. The first one is to offer an efficient auto-configuration mechanism compatible with the MANET context, i.e. which would use the different resources (bandwidth, delay, traffic) with parsimony. The second goal of our approach is to protect as much as possible the mechanism against impersonation or denial of service attacks. The scheme is thus divided in two steps. The first one is the authentication phase during which a node requesting for an address will have to be identified by several already configured nodes in the network, so that its messages can be authenticated. During this same step, the requester identifies the network to ensure that it is not in presence of colluded malicious nodes. The second phase is the address attribution one, thanks to which the node receives an IP address to join the network. Since the authentication has to be done by already configured nodes (i.e. the network itself), the best solution is to entrust the address allocation monitoring to the network. That is why we chose to rely on a stateful approach through the use of the buddy system mechanism [8]. The address allocation tables are disjonctive and distributed among all nodes in the network. Indeed, by entrusting to the network disjonctive pools of addresses, we prevent nodes to choose arbitrarily duplicate addresses or to usurp identities. The state of global address space remains consistent and the need for costful update is all the more reduced. Then, by distributing the capability to allot an address, we allow every node to configure an incoming other one and we also increase the reactivity and the robustness of the protocol.

The original contributions of the paper are as follows:

- We secure the address attribution process by mutually authenticating nodes before they join the network, what has not been attempted before. Since nodes are inter-certified, the scheme can tolerate the presence of several attackers in the network.
- The protocol is also protected against the exhaustion of address space by the use of a threshold authorizations scheme.
- We use chaining references to reduce significantly the probability that addresses conflicts occur and to increase the speed of attribution process. In addition, contrary to other proposals, there is no loss of whole addresses blocks after a node departure and the global address space also remains coherent.