Distributed address auto configuration protocol for Manet networks

Sonia Mettali Gammar · Elabidi Amine · Farouk Kamoun

Published online: 5 November 2009
© Springer Science+Business Media, LLC 2009

Abstract Mobile ad hoc networks are wireless networks characterized by: limited bandwidth, shared transmission channel and the lack of central processing unit of administration and configuration. Most research related to Manet assures that host IP address is configured as the node joins the network. However, it is impossible to ensure that because there is no infrastructure. Therefore, an auto configuration scheme is needed to perform network management and to attribute connection parameters. Hence, we present a new distributed IP address configuration approach for Manet networks. Our solution provides a unique address allocation for each node in the network. The address assignment is assured under different network conditions including node failures, network partitioning and merging.

Keywords Autoconfiguration · Ad hoc network · Address recovery

1 Introduction

Mobile ad hoc networks are infrastructure-free, highly dynamic wireless networks. Significant research works in this area have been carried out to improve quality of services and to handle network limitations, including such as limited power, mobility and transmission range. Any solution for these problems assumes that the network was already “IP configured” without any conflict. However, this assumption can not be fulfilled in all cases because of variable Manet topology. Hence, dynamic address configuration is a required feature for mobile network management. A popular mechanism is the Dynamic Host Configuration Protocol (DHCP) [1], used to configure a wired network. It requires the existence of a centralized server to provide dynamic address allocation. It can not be used in Manet since the network does not have any centralized administration. Even if this server exists, with highly dynamic topology, it may not be permanently reachable.

Due to the node mobility in Manet, configured networks can split into different partition or merge. These events can lead to address conflicts. Then merged networks have to deal with eventual conflict problem. Partitioned networks can later be separated to form independent networks. An auto configuration solution has to manage this kind of problems without disturbing network communications.

In this paper, we present a distributed address auto configuration protocol to provide configuration of mobile nodes. Our approach ensures that each node of the Manet acquires a unique IP address. It handles problems arisen due to Manet limitations, node departure and network partitioning and merging.

The rest of the paper is organized as follows: related research efforts are introduced in Sect. 2. Section 3 describes the solution. Section 4 defines metrics for performance evaluation and presents simulation results. Finally, Sect. 5 concludes the paper.
2 Related works

Most solutions proposed to ensure Manet auto configuration can be categorized in three classes: Stateless auto configuration schemes, Stateful and hybrid solutions.

In the first class, no status information about assigned addresses is maintained. Each node, self-assigns an address. These solutions define different ways to choose a new address. It can be random or a function based on the node physical address. Then the address uniqueness is ensured by a distributed feature: Duplication Address Detection (DAD). An initial work is presented in [3]. It is a simple mechanism based on the Duplication Address Detection (DAD). Each new node chooses randomly an address then it sends a request to this address. If no reply is received, the selected address may be used for permanent communication. In the other case, the node must choose another address. This approach is easy to implement. However it applies only if message delays between all pairs of nodes are bounded. Another problem persists if we have a concurrent request for the same address and this conflict can not be detected. To overcome DAD drawbacks, a new variant is presented: Weak DAD [4]. Vaidya proposed to use a unique key with DAD mechanisms. With the selected address the node uses this key for all its communications. This mechanism prevents a packet from being routed to a wrong destination even if duplicate addresses exist. Another solution called PDAD (Passive Duplicate Address Detection) [2] tries to detect conflict without any additional control information. This approach relies on the routing information. Every node analyzes the received routing packets to detect eventual conflict. This scheme is well adapted with link state routing protocols.

In stateful auto configuration approaches, the nodes already configured are charged to provide a valid address for each new client. They keep a trace of all the allocated addresses in an “allocation table”. A mechanism for Manet auto configuration called ManetConf is presented in [6]. In this work, each configured node maintains a list of used addresses. When a new node requests configuration parameters, one of its neighbors replies by giving valid IP address. The assignment process is similar to the mechanism of [5]. The configuring node asks for the permission of the whole network to use a new address for the requestor. This approach prevents concurrent assignment by maintaining an additional allocation table for pending configuration requests. Another stateful solution in [8] makes a compromise between overhead and data consistency by using a “Quorum vote” mechanism where only a partial decision is sufficient to have a valid IP address. In [11] the used solution minimizes the overhead by attributing to every new configured node a part of the addressing pool. But it needs a complicated mechanism to solve starvation when no available pool can be given. The same approach is also used in [10]. A clustering approach is adopted in [9] to distribute addresses. Any Decision will be taken locally in the cluster head.

In hybrid category, distributed attribution where each node configures its address, can be combined with a stateful mechanism. PACMAN [7] (Passive Autoconfiguration for Mobile Ad hoc Networks) is based on PDAD [2]. No protocol overhead is generated, since it uses information from ongoing traffic. The allocation table is passively deduced from the routing information without any global synchronization. When the node receives a routing packet, it performs a combination of procedures based on routing information to detect any address conflict. Like PDAD, PACMAN gives interesting results with link state protocols. With this solution a huge processing time is needed to perform the conflict detection process.

The solutions mentioned above have made significant contributions to the Manet auto configuration research area. However, all of these approaches handle only a subset of the treated topic. Stateful approaches are completely reliable on the synchronized allocation table maintained. Then, the presence of packet loss may lead to an inconsistent state, address conflicts and many unnecessary address changes. Stateless approaches are specially based on the DAD mechanism to detect address conflicts. They use the flooding technique, so they consume a considerable part of bandwidth. Also, they don’t specify any mechanism to handle network merger or partitioning.

Consequently, an auto configuration solution for ad hoc networks must present a simple, fast and effective approach for the various problems. It must handle the ad hoc properties such as: mobility, power limitation, radio range and packet loss. It must minimize the exchange traffic control and not to disturb the communications. It had also to protect the network against false routing caused by the address conflicts.

3 Solution description

The goal of the proposed solution is to assign a unique IP address to each new node and to handle network merge and partitioning.

3.1 Network model

We consider a Manet with no connection to a wired network. Every new node that wishes to join the Manet needs to have a unique IP address during its connection. The address assignment is the responsibility of configured nodes. For this allocation, we will use a private IP address block such: 10.0.0.0–10.255.255.255, 169.254.0.0–169.254.255.255, 172.16.0.0–172.16.255.255, 192.168.0.0–192.168.255.255 for private IP version 4 networks [13]