Chapter 10
Survey on Autoconfiguration Schemes in IPV6 Based Manets

Reshmi TR
VIT University - Chennai, India

ABSTRACT

The MANETs are spontaneously formed infrastructure-less networks with self-configuring nodes. The network is characterized with a dynamic nature as the member nodes are highly mobile resulting in network merging and partitioning. Each node in MANETs acts as routers to assist in communication. To start with self-configurations, the autoconfiguration schemes are used in these networks to assign unique addresses to the nodes and allow them to communicate with other nodes. Due to the dynamic nature of MANETs and the intervention of new technologies in next generation networks, the existing autoconfiguration schemes face many issues. The research focuses to resolve the pertaining issues in autoconfiguration schemes are discussed in this book chapter.

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are a category of wireless net-works that operate without any fixed infrastructure. MANET allows nodes to communicate directly (point-to-point) without the need for a bridging device like Access Point (AP). The nodes in these networks act as routers too, and redirect packets to the destination nodes. Therefore, each node in the network acts as router in order to provide connectivity to other nodes. Each node maintains host routes to the rest of nodes within the network, in addition to network routes to destinations outside the MANETs. MANETs do not require any infrastructure or a centralized administration connecting mobile devices quickly and spontaneously. These networks support network merging and partitioning and hence allow devices to maintain dynamic connections to the network. MANET applications are diverse, ranging from video conferencing, emergency rescue communication networks, defense tactical communications, and so on. There are a few issues and challenges that affect the design, deployment and performance of MANETs. The major issues and challenges in MANETs are listed below.

DOI: 10.4018/978-1-5225-6023-4.ch010

- The frequent change in the network topology due to the mobility of the nodes in network.
- The infrastructure-less nature of the network and the mobility of the intermediate nodes between the source and destination acting as routers of the nodes often makes the routing of the packets challenging.
- The self-configuration of a unique identifier or address for each of the nodes is challenging in the network.
- Bandwidth and resource constraints - The wireless bandwidth and the resource constraints in the network also causes challenges in communication.
- The infrastructure to check the security and privacy lacks in the network. The complex security algorithms cannot be applicable in the resource constrained networks.

The autoconfiguration can be defined as a task of automatically assigning conflict-free unique IP address to every node in the MANET without any manual intervention. The major requirement of autoconfiguration is ensuring uniqueness of addresses and ensuring there is no ambiguity when nodes try to communicate with each other. But distributing and maintaining conflict-free addresses in the dynamic environment is challenging in many ways. The autoconfiguration is challenged when a MANET cloud split into different subnets or when two MANET clouds merge into the same subnet. Likewise, the wireless nature such as limited bandwidth, power, limited resources and high error rate makes the autoconfiguration even more challenging. Besides handling all these challenges, autoconfiguration could perform well only if they ensure scalability, robustness and effectiveness. So to ensure best performance the autoconfiguration schemes must satisfy the characteristic requirements listed below:

1. **Unique Address Assignment:** Each of the nodes in the network must be assigned to a unique identifier for its identification and communication. There must not be any conflict or ambiguity during communication.
2. **Recovering and Allocating Addresses During Network Merging and Partitioning:** A node maintains the same IP address reserved for it in the net-work until it is available in the network. When there is network partitioning (i.e., a node leaves the network), the IP address must be released by the node. These addresses must be managed and reused by the protocol. Whenever a network merges with an existing network, the addresses of these nodes must be reconfigured to avoid inappropriate routing.
3. **Availability of Addresses:** The addressing protocol must be scalable to support any number of nodes. The protocol must provide an address without waiting for reclamation of address. The nodes must be able to configure its address from a server which requires multi-hop communication to reach it.
4. **Authentication of Rival for an IP Address Request:** The protocol must be able to manage the address request from two nodes simultaneously. The protocol must authenticate the identifiers provided for both the nodes.
5. **Synchronization of Address Information:** The nodes in network stores address information that needs to be synchronized to avoid address conflicts.