Chapter 10
Trust Management in Ad Hoc Networks

Rafael Timóteo de Sousa Júnior  
University of Brasília, Brazil

Ricardo Staciariini Puttini  
University of Brasília, Brazil

ABSTRACT
Mobile ad hoc networks (MANETs) are wireless networks whose mobile nodes exchange information without the help of a predefined network infrastructure. MANET services, such as auto-configuration and ad hoc routing, must be provided in a distributed and self-organizing manner, by collaboration between network nodes and requiring each participant to both provide its own resources and exploit others’ resources. As the nodes may, continually and at any time, appear, disappear or move around within the network, the structure of a MANET is constructed dynamically and the network topology is subject to frequent and unforeseeable changes. In this situation traditional security solutions are insufficient to exhaustively address all security requirements. The distinctive characteristics of ad hoc networks imply the need for distributed collaboration solutions that are based on some form of trust. In this chapter, the authors survey the modes of utilization of trust as means for providing, with network security mechanisms or as an alternative to them, the necessary services in MANETs.

INTRODUCTION
Mobile Ad Hoc Networks (MANETs), also known as spontaneous networks, are natural places for applying computational trust. Indeed, the distinctive characteristics of ad hoc networks imply the need for distributed collaboration solutions that implicitly are based on some form of trust.
Trust Management in Ad Hoc Networks

with another that is not within its transmission range, it relays its packets via a neighbor node that is closer to the destination node, which in turn relays the packet onward. Therefore, MANETs are multi-hop mobile networks in which the connectivity between nodes is ensured by collaborative routing (Chun, Qin, Yong & Meilin, 2000; Royer & Toh, 1999).

In a MANET, the nodes may, continually and at any time, appear, disappear or move around within the network. As a result, the structure of the MANET is constructed dynamically and the network topology is subject to frequent and unforeseeable changes. This characteristic linked to the mobility of the nodes, allied to the limited bandwidth and unreliability of wireless links, means that the availability of a specific node cannot be ensured. In this way, the services in a MANET cannot be concentrated in centralized entities. Conversely, the services in a MANET must be provided in a distributed and self-organizing manner, by collaboration between network nodes. This collaboration normally makes use of the natural redundancies resulting from the communication model which, to a certain extent, compensates for the lack of certainty regarding the availability of individual nodes.

In MANETs, as presented above, two basic services are necessary to form the networks and ensure the continuity of operations: auto-configuration (Mohsin & Prakash, 2002; Nesargi & Prakash, 2002; Perkins, Malinen, Wakikawa, Royer & Sun, 2001) and ad hoc routing (Clausen & Jacquet, 2003; Johnson, Maltz & Hu, 2004; Ogier, Templin & Lewis, 2004; Perkins & Royer, 2003). While the auto-configuration service is related to the association of the nodes to the network, allowing rapid set-up with little or no user intervention, the routing service is related to the multi-hop nature of MANETs. Thus, configuration and routing protocols must be designed to take into account the constant changes in the network topology due to the mobility of the nodes.

Given these specificities of ad hoc networks, their relation to trust aspects can be discussed and the possible roles of trust technologies in this context can be identified as means for providing, with other mechanisms or as an alternative to them, the necessary services in MANETs.

The objective of this chapter is to present the modes of utilization of trust in ad hoc networks. We begin by describing the distinctive characteristics of ad hoc networks, discussing how the concept of trust can be useful to deal with the issues related to these characteristics and presenting the possible roles of trust technologies in this context.

We then present an overview of the underlying technologies and protocols for ad hoc networks so as to establish the basis for describing vulnerabilities of these networks. This leads to the description of attacks exploiting these vulnerabilities and to the discussion on the utilization of trust to mitigate these attacks. This issue is approached both from the point of view of autonomic trust reasoning by each node and the collaboration among nodes regarding trust aspects, based on the specification of an ad hoc trust management architecture. This approach allows the description of formal methods and languages to express the concept of trust, the presentation of trust models, including evidence management and trust calculation, and the collaboration for managing and exchanging information about reputation.

The chapter is concluded with other applications of trust in ad hoc networks, such as the utilization of trust for choosing alternative routes, and visualization of trust as a human oriented metric of the behavior and performance of ad hoc networks.

TRUST ASPECTS WITHIN AD HOC NETWORK OPERATIONS

In this section we examine some of the ad hoc operations and explain in which aspects trust technologies can be applied to perform these operations.