Chapter 29

Trust Management in Mobile Ad Hoc Networks for QoS Enhancing

Ryma Abassi
City of Communication Technologies, Tunisia

ABSTRACT

In a collaborative environment such as MANET, nodes reliability evaluation is vital. Trust Management can be used to ensure such healthy collaboration it offers a formal and unified framework for trust specification and interpretation. Establishing trustworthy relationships is generally done by maintaining a reputation for each node computed based on direct observations or neighbors' observations exchanged using recommendations. Unfortunately, for malicious reason, such method may be faked by cheaters: several nodes collude in order to rate each other with the maximum value and decrease other nodes' reputations by giving negative recommendations. The main contribution of this chapter is then, the proposition of a trust based environment for MANET and securing it against collusion attack in order to enhance the network QoS. This is achieved using three steps: (1) the definition of a formal trust based environment (2) the addition of a process handling collusion attack and (3) the extension of the whole proposition by a delegation process allowing nodes functionalities sharing.

INTRODUCTION

MANETs (Mobile Ad hoc NETworks) are wireless mobile nodes dynamically self organizing in arbitrary and temporary network topologies. Their nodes can be internetworked without a pre-existing communication infrastructure. Therefore, such networks are designed to operate in widely varying environments, from military networks to low-power sensor networks and other embedded systems. Dynamic topologies, bandwidth constraints, energy-constrained operations, wireless vulnerabilities, and limited security are among the main MANET characteristics.

Initial MANET routing protocols, such as AODV proposed by Perking and Royer (1999), OLSR Jacquet *et al.* (1998), etc. were not designed to withstand malicious nodes within the network or outside attackers nearby with malicious intent Cordasco and Wetzel (2008) Hence, due to these

DOI: 10.4018/978-1-4666-9624-2.ch029

specific characteristics and to the unreliable medium in MANETs, some security mechanisms must be defined. In the literature, some works have been proposed for securing MANET Arijita *et al*. (2012); Quershi *et al.* (2011); Babu *et al.* (2008); Marmol & Perez (2009); Grafii *et al.* (2007); Cordasco & Wtezel (2008); Sachan & Mohen Khilar (2011); Mathews *et al.* (2011). They can be classified into two categories: those based on cryptography and those based on trust. The cryptography-based systems apply cryptographic methods to the existing protocols to distinguish between legitimate nodes and malicious ones. The main advantage of cryptography based systems is that they allow securing routing information from tampering. However, they suffer from a high computational cost and they can't identify nodes with malicious intention. Trust-based systems take advantage from the intrinsic properties of routing protocols to detect malicious nodes i.e. they behave as an intrusion detection system. This is achieved by using node's reputation to mitigate misbehaving. Reputation is maintained through direct observations as well as reputation messages exchanged with other nodes.

Trust enables collaborating nodes to counter their uncertainty and suspicion by establishing trustworthy relationships. Due to the criticality of used concepts, trust is associated to a unified approach allowing its specification and formalization called Trust Management (TM) Blaze *et al.* (2002). Hence, we define trust relations between a *Trustor* (trust provider) and a *trustee* (trust beneficiary) as a binary decision relationship allowing their collaboration in a given situation with a given security level. This level is proportional to *trustee's* reputation i.e. a perception a party creates through past actions about its intentions and norms. Reputation is obtained through direct observations made by the node itself and/or by indirect observations. These latter correspond to the received appreciations from neighbors who have had interactions in the past and have evaluated and rated each others.

Paradoxically, success of trust based schemes depends on cooperation among the nodes. In fact, the TM process may constitute a security weakness due to its vulnerability to the collusion attack where several malicious nodes may collaborate in order to decrease a benevolent node's reputation.

Moreover, resources availability in MANET is a fundamental and a vital constraint. Availability concerns essentially the network nodes as well as routing and other forwarding actions accessibility. Generally, nodes lifetime is consumed by legitimate traffic. In practice, and in a hostile environment, it also can be shortened or even depleted by deny of service attacks penalizing the routing process.

In this work, we propose a trust environment using reputations in order to detect colluders and consequently enhance the network QoS. The first contribution of this chapter, concerns then the proposition of a model built over three activities constituting the basic steps of any system lifecycle: establishment, update and revocation. In order to establish a trust relation, we propose two schemas. In the first one, a trust request is evaluated and a trust level is affected to the established relation based on reputation computing and maintaining. In the second scheme, recommendations are used in order to ensure trust transitivity and a recommendation level is assigned to the established relation. Update activity concerns the modification of the considered relation i.e. trust level, recommendation level and reputation. Finally, revocation activity concerns the removal of an established trust relation.

The second contribution deals with collusion attack and more precisely with the proposition of a process detecting colluders as well as a process punishing such behavior. Hence, an appropriate attack modeling is proposed. Detection is made by assessing recommendations variance compared with the recommendations average. Punishment discards detected colluders and prevents them from participating in future communications.