

# Abstract

Computer networks security is a topic that has been extensively researched. This research is fully justified due to the dimensions of the problem faced. Different kinds of networks and a large quantity of network protocols and applications conform a vast research field, where it is possible for a researcher to set his (or her) interests over a set of threats, vulnerabilities, or types of attacks, so devising mechanisms to prevent the attack, mitigate its effects, or repair the final damages, based upon the specific characteristics of each particular scenario.

The Computer Networks Research Group from the Technical University of Valencia (Universidad Politécnic de Valencia) has been researching on computer networks security risks, specially those affecting wireless networks. In previous doctoral works, detection and exclusion methods for dealing with malicious nodes in Mobile Ad hoc Networks (MANETs) had been proposed, from the point of view of every individual network node, using a technique called Intrusion Detection Systems (IDS) based on Watchdog methods. In this scope, we pretend to optimize network throughput removing misbehaved nodes from the network communication processes, a task performed specifically by Watchdog systems.

A way to improve the whole network performance is to use mechanisms for cooperatively sharing information between well-behaved nodes to speed up misbehaved node detection and increase accuracy. Obviously, these mechanisms will have a cost in terms of network transmission overhead and also a small computing time overhead needed. The key issue here is to adequately balance the costs and the benefits related to these cooperation techniques to ensure that the overall network performance is increased if compared with a non-collaborative one.

In this doctoral thesis, we have designed a mechanism to allow individual watchdogs to share reputation information about their neighbour nodes to characterize them as soon as possible. We call this method Collaborative Bayesian Watchdog, which is based on a non-collaborative bayesian version

---

of a watchdog. We have evaluated our approach through simulation methods, and also by proposing an analytical model to reduce the time and effort needed to evaluate this kind of solutions in different scenarios.

These evaluations showed that the use of the adequate collaboration mechanisms between well-behaved nodes could improve the performance of the watchdog techniques at an affordable cost in terms of computational and message overhead.