Getting Rid of Cheats and Liars in Mobile ad-hoc Networks *

Sonja Buchegger
IBM Zurich Research Laboratory
Saeumerstrasse 4, CH-8803 Rueschlikon
sob@zurich.ibm.com, http://www.zurich.ibm.com/~sob

Abstract:

Getting Rid of Cheats and Liars in Mobile ad-hoc Networks

In mobile ad-hoc networks nodes need to cooperate to communicate, but there are many reasons for non-cooperation. Saving power or preventing other nodes from obstructing a service are merely selfish reasons for non-cooperation, whereas nodes may also actively and maliciously deny service or divert traffic for all sorts of attacks. However, without an infrastructure to rely on, nodes depend on each other's cooperation. In game-theoretic terms, this is a dilemma. The dominating strategy for individual nodes is not to cooperate, as cooperation consumes resources and it might result in a disadvantage. But if every node follows that strategy, the outcome is undesirable for everyone as it results in a non functional or entirely absent network. Thus non-cooperation poses a threat on the availability of a mobile ad-hoc network.

Our approach is to find the selfish and/or malicious nodes that cheat and to isolate them, so that misbehavior will not pay off but result in isolation and thus cannot continue. We developed a protocol called CONFIDANT, short for 'Cooperation Of Nodes, Fairness In Dynamic Ad- hoc NeTworks', which detects malicious nodes by means of observation or reports about several types of attacks, thus allowing nodes to route around cheating nodes and to isolate them. CONFIDANT components are extensions to a routing protocol such as Dynamic Source Routing (DSR).

Nodes have a monitor for observations, reputation records for first-hand and trusted second-hand observations about routing and forwarding behavior of other nodes, trust records to control trust given to received warnings, and a path manager to adapt their behavior according to reputation and to take action against malicious nodes. The term reputation is used to evaluate routing and forwarding behavior according to the network protocol, whereas the term trust is used to evaluate participation in the CONFIDANT meta-protocol itself.

The first version of CONFIDANT raises some robustness issues, nodes can potentially be deceived by wrong observations or more effectively by wrong accusations spread by lying nodes. In order to avoid such slander and to evaluate trust dynamically we use a Bayesian approach. This enables the nodes to make informed decisions on how to classify events such as observations or reports, how to classify and represent the reputation of a node in terms of routing and forwarding cooperation, which reports to believe, and with whom to exchange their reputation-related beliefs.

*Presented at 1st Workshop on Security in Ad-hoc Networks. , Bochum, Germany, December 2002