Design of a Novel Trust Model and its Application in Trust based Routing to Defend against Dishonest Recommenders

Abstract

Trust management frameworks play a very important role in securing the mobile ad hoc networks against various insider attacks that could occur during data forwarding. The success of a trust management framework greatly depends upon the proper design of each of its major components including the direct trust computation component as well as the indirect trust computation component. Specifically, the indirect trust computation component should be robust to handle the dishonest recommendations. The current paper shows the application of a trust model involving a robust indirect trust computation component called as RecommFilter which has been proposed in our earlier work. It can overcome the various attacks caused by dishonest recommenders. The application involves the integration of the trust model with a routing protocol based upon a reliability measure called as Path Allegiance metric (PAM) which is a cumulative value obtained through the trust values of the on-path nodes upon each other. Experimental results show that the proposed scheme along with PAM routing protocol is robust to different dishonest recommendation attacks and accurate in the detection of dishonest recommenders.


Index Terms

Computer Science

Information Sciences

Keywords

Dempster Shafer Theory

Dishonest Recommenders

Slandering attack
Self-promoting attack

Collusion attack

Recommendation Filtering

Jousselmes distance

Path Allegiance Metric.