Abstract

In the last few years management of trust and reputation models over distributed systems has been proposed as a novel and accurate way of dealing with some security deficiencies which are inherent to distributed environments. Many models and theories have been designed in order to effective and accurately manage trust and reputation in those environments. Nevertheless, very few of them take into consideration all the possible security threats that can compromise the system. In this paper, an analysis of the effect of the security threats on the selection percentage of trustworthy servers (the accuracy) and average path length suggested by the Linguistic Fuzzy Trust Model over static Wireless Sensor Network are presented. It is observed that the accuracy of the model with collusion decreases as compared to the accuracy of the model without collusion while the results about the average path length suggested by the model are better and the change in it by varying the number of trustworthy servers is very low, so the average path length of the model with collusion is better than of it without collusion. Also it must be mentioned that the evaluation environment used in this paper is Trust and Reputation Model Simulator for Wireless Sensor Network.

References
Security Threats of Collusion-based Linguistic Fuzzy Trust Model for WSN Symposium. DOI: 10.1109/ICC.5199545, Dresden, Germany.

Index Terms

Computer Science

Wireless

Keywords

Collusion  Fuzzy  Security Threats  Sensor Networks