Abstract

Mobile ad-hoc network is suffering with various attacks due to the infrastructure-less network. Hence, MANET needs very specific security methods to detect false entrance of the misbehavior nodes. The networks work well if the nodes are trusty and act rightly cooperatively. In this paper, we are identifying and detecting packet dropping nodes using Support vector machine. Support vector machine is used reactively to classify nodes in two different classes either normal or malicious nodes. SVM takes as input the neighbor trust value, calculated with data packets and control packets. Our technique is implemented with AODV (Ad-hoc on demand vector routing) protocol. Our experimental results evaluated using packet delivery ratio (PDR), End-To-End delay, Average throughput, Normalized Routing Overhead, Average Energy Consumption.

References

- Abderrahmane Baadache and Ali Belmehdi, "Fighting against packet dropping..."
Detecting Packet Dropping Misbehaving Nodes using Support Vector Machine (SVM) in MANET


Detecting Packet Dropping Misbehaving Nodes using Support Vector Machine (SVM) in MANET


Index Terms

Computer Science

Software Engineering

Keywords
Mobile ad hoc network  machine learning techniques  packet dropping attacks  support vector machine (SVM)