Abstract

Designing and architecture of Trust model in WSN is now a days research challenge. Trust is important in wireless networks because collaboration and cooperation among nodes and critical towards achieving the system’s goals, such as routing reliability. IP-spoofing attacks remain one of the most damaging attacks in which a router replaces the original source IP-address by a new one. This paper present a novel approach using Entropy inference model that evaluates the trustworthiness of an access router and distributed router with regards to forwarding packets. The trust values for the Group router is computed by a judge router that samples all traffic being forwarded by the access router. The trust values for the access router and distributed router are computed by distributed router and ingress/egress router respectively. The simulation results to detects malicious access routers and malicious distributed routers.

- Wang Yonghong, Singh Munindar P. , &quot;Formal Trust Model for Multiagent Systems," National Science Foundation under grant ITR-0081742, IJCAI-07 1551-1556.
- Peng Shih-Hao, Chang Kai-Di, Chen Jiann-Liang, Lin I-Long, and Chao Han-Chieh, &quot;A Probabilistic Packet Marking scheme with LT Code for IP Traceback,&quot;
Entropy Trust based Approach against IP Spoofing Attacks in Network

Index Terms

Computer Science
Wireless

Keywords

Trust   IP-spoofing   Group Routing System   Access Router   Distributed Router
Entropy Inference