Abstract

This paper proposes a strategy based on processor utilization value provided by each sensor node of the network for detecting their malicious activities by comparing the node's present processor utilization value with the old estimated value. If the difference between the two values is higher or less than the expected value then that particular node become suspicious. A knowledge based system can take decision to expel the malicious node from the network topology.

References

- Song JianHua, Ma ChuanXiang: A reputation-based Scheme against Malicious Packet Dropping for Mobile Ad Hoc Network.
- http://spie.org/x8693.xml?ArticleID=x8693, Internet 28 Feb 2011
Detection of Malicious Sensor Node in Ad Hoc Sensor Networks based on Processor Utilization


S. Meguerdichian, F. Koushanfar, G. Qu and M. Potkonjak, "Exposure In Wireless Ad-Hoc Sensor Networks," Computer Science Department, University of California, Los Angeles, Electrical Engineering and Computer Science Department, University of California, Berkeley, Electrical and Computer Engineering Department, University of Maryland, March 2002.


Index Terms

Computer Science

Wireless

Keywords

Malicious node  Node profile  Threshold value  Regression analysis  Technical efficiency