Abstract

Mobile ad hoc network (MANET) is highly challenging network environment due to its own properties like open medium, dynamic topology, distributed cooperation, and capability constraint. MANET is self-directed and infrastructure less network. As network is wireless, routing plays an important part in the security of the whole system. Secure transmission of data in between nodes is an imperative concern. Any attacker get remote node by using transceiver and without being caught. The objective of this paper is to propose new secure unobservable routing protocol with trust management mechanism, where attacker gets blocked while making spoofing or eavesdropping attacks. Only unobservable message could be gathered by attacker. An USOR protocol is implemented on ns2 with its performance is evaluated by comparing with AODV and AMODV. The proposed protocol will also protect privacy information among network and will detect and block compromised nodes through trust-aware routing framework.

References

An Unobservable On-demand Routing Protocol with Trust Management Mechanism

An Unobservable On-demand Routing Protocol with Trust Management Mechanism

TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 11, NOVEMBER 2011.

  - Huei-Wen Ferng, Rachmarini, D., &quot;A secure routing protocol for wireless sensor networks with consideration of energy efficiency/Network Operations and Management Symposium (NOMS),&quot; 2012 IEEE.
  - Anfeng Liu, Zhongming Zheng, Chao Zhang, Zhigang Chen, and Xuemin (Sherman) Shen, &quot;Secure and Energy-Efficient Disjoint Multipath Routing for WSNs,&quot; IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 7, SEPTEMBER 2012.

Index Terms

Computer Science
Networks

Keywords

Eavesdropping attack  secure unobservable routing protocol  Trust mechanism  trust-aware routing framework