Abstract

Due to infrastructure-less networks and multi-hop communication features of Mobile ad hoc network (MANET), every node in MANET has to cooperate with each other. Therefore, node security becomes one of the important research areas of MANET. The resources that provided to MANET nodes such as battery power, memory, and bandwidth are limited. As a result, developing a resource-aware node authentication protocol becomes challenge for researchers. The proposed protocol provides One Time Node Authentication (OTNA) for every node joining MANET. To achieve this, the OTNA protocol provides one additional field \textit{status} in the routing table of the legitimate nodes, and the Malicious Node Table (MNT). The \textit{status} field shows authentication status of the nodes present in MANET. The MNT is used to keep record of the malicious nodes detected during node authentication. To perform node authentication, OTNA uses the basics of Challenge-Response Protocol (CRP) and one-way hash function with three message exchanges. In the OTNA protocol, only two nodes are involved in authentication process, which allows other available nodes for packet forwarding process. To the best of our knowledge, OTNA protocol facilitates optimal secure packet delivery. The correctness of the OTNA protocol is proved with the help of GNY logic.
References


**Index Terms**

Computer Science  
Security

**Keywords**

MANET  Node Authentication  Challenge-Response protocol  GNY Logic.