Abstract

Secure routing in wireless ad hoc network has been an active area of research and in recent years, a number of secure routing protocols have been introduced. These solutions may be classified as proactive, reactive, and hybrid based on the routing information update mechanism deployed. Studies reveal that the reactive (on-demand) ones often outperform the others due to their ability to adjust the amount of network overhead created to track the mobility in the network. However, the existing secure on-demand routing protocols have also some limitations. In this paper, the weakness of existing popular secure reactive routing protocols is analyzed on the ground of topology exposure. Then a new topology-hiding secure on-demand routing protocol, called TSOR is proposed based on timestamp approach and asymmetric cryptography. Security analysis of TSOR shows that it efficiently defeats all possible threats imposed by external or internal adversaries. Simulation results demonstrate that our protocol has a better capability of finding reliable and shortest routes in the presence of malicious nodes at the cost of low routing overhead.
References


**Index Terms**

Computer Science

Wireless

**Keywords**