

Abstract

Study of the effects of pairwise key pre-distribution scheme on the performance of a Topology Control Protocol

Collecting information from open and possibly hostile environments makes the wireless Sensor Network (WSN) vulnerable to different types of security threats. To provide secure communications for the WSNs, all messages have to be encrypted with a secret key. Message encryption using the public key cryptosystems in WSN is not applicable due to sensor's constrained resources. A random key pre-distribution scheme and its enhanced versions to deal with pairwise key establishment are of popular approaches that have higher resilience for nodes compromising. On the other hand, the topology control protocols are special forms of WSNs that add some constraints for controlling the construction of wireless networks. This paper aims to identify whether it is applicable to apply a key pre-distribution technique on a topology control protocol and evaluates its performance.