DETECTING WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS USING HOP COUNT ANALYSIS

Lan Yao, Zhibin Zhao and Ge Yu
School of Information Science and Engineering
Northeastern University, Shenyang
Liaoning, China
Emails: {yaolan, zhaozhibin, yuge}@mail.neu.edu.cn

Submitted: Nov. 05, 2012 ***Accepted: Jan. 20, 2013*** ***Published: Feb. 20, 2013***

Abstract- The wormhole attack is a severe threat to wireless sensor networks. Most existing countermeasures for detecting and locating wormhole links either require extra hardware or are too complex for the inherently capability-constrained sensor nodes. Actually, wormhole links can enormously change the original sensor network topology. In this paper, we introduce the HCA4DW mechanism for detecting and locating wormholes in wireless sensor networks. It is based on the basic idea that the change of topology can be detected through neighborhood validation. We discover the maximum necessary hop count between the sensors in the same neighbor set for neighborhood validation. We describe the detail procedure of HCA4DW in this paper and test the performance of the HCA4DW mechanism rigorously through simulative experiments.

Index terms*:* wireless sensor networks, wormhole attack, hop count, neighborhood validation.