DETECTING SYBIL ATTACKS IN WIRELESS SENSOR NETWORKS USING SEQUENTIAL ANALYSIS

P. Raghu Vamsi and Krishna Kant
Department of Computer Science and Engineering,
Jaypee Institute of Information Technology, Noida, India.
E-mails: prvonline@yahoo.co.in, k.kant@jiit.ac.in

Submitted: Dec. 3, 2015 ***Accepted: Mar. 31, 2016*** ***Published: June 1, 2016***

Abstract: Wireless Sensor Networks (WSNs) suffer from many security attacks when deployed either in remote or hostile environments. Among possible attacks, the Sybil attack is one of the severe attacks in which malicious nodes report false identities and location information such that the remaining nodes believe that many nodes exist in their vicinity. The current study proposes a method for detecting Sybil attack using sequential analysis. This method works in two stages. First, it collects the evidences by observing neighboring node activities. Further, the collected evidences are consolidated to provide input to the second stage. In the second stage, collected evidences are validated using the sequential probability ratio test to decide whether the neighbor node is Sybil or benign. The proposed method has been evaluated using the network simulator ns-2. Simulation results show that the proposed method is robust in detecting Sybil attacks with very low false positive and false negative rates.

Index terms: Sensor networks, Sybil attacks, malicious activities, sequential analysis, received signal strength, false identity, false location information.