International Journal of Engineering Sciences Paradigms and Researches Vol. 05, Issue 01, June 2013
ISSN (Online): 2319-6564
www.ijesonline.com

Abstract Details

Title: Sybil Attack Detection and Recovery Using Immune Collaborative Model in WSN

Author: Sachin Minocha, Deepak Goyal, Sangeeta Malik

Abstract: WSNs are composed of a large number of sensor nodes, which communicate in a radio channel. The main aim of the network consists of a sensing a certain physical variable, gathering data and forwarding them to the base station where the information is processed for further purposes. When any node create multiple copies of itself to create confusion in the WSN network or illegally claims multiple identities or claims fake ID'S and also can cause collapse in the network then that kind of situation can be referred as Sybil attack. This system can attack both internally and externally in which external attacks can be restricted by authentication but not internal attacks. The biological immune system is a robust, complex, adaptive system that defends the body from foreign pathogens. It is able to categorize all cells (or molecules) within the body as self-cells or non-self cells. It does this with the help of a distributed task force that has the intelligence to take action from a local and also a global perspective using its network of chemical messengers for communication. The proposed algorithm applies the Sybil attack detection and recovery using the proposed immune collaborative model. The proposed model consists of Immune Body that can combine to form Immune collaborative Body. It also defines the structure of IB as well as ICB. And the search and the exit criteria for any IB to join and exit any ICB. The immune algorithm applied to the model is the clonal selection algorithm. The proposed algorithm detects and prevents the Sybil attack in the WSN.

Keywords: Immune Collaborative Model, WSN, Security Challenges, Sybil Attack.