Danger theory based node replication attacks detection in mobile wireless sensor network

ABSTRACT

Mobile wireless sensor networks (MWSNs) are commonly deployed in a harsh climate, notably unattended without any tamper-resistant tools; thereby an attacker can easily capture the sensor nodes in a very limited time. Once captured, the attacker can duplicate the sensor and subsequently deploys numerous clone nodes into the network in minimum time duration. This new breed of attack is called node replication attack, and while several solutions have been proposed to address such a security threat, they are mainly centralized and somewhat limited to static WSN. In this paper, we propose a hybrid (centralized and distributed) node replication attack detection method for MWSN, which operates based on Danger Theory in human immune system. As depicted in Danger Theory, the proposed method consists of two main security approaches, namely attack detection and security control. These approaches perform a multi-level detection, which is not only responsible to identify but also to verify the existence of clone nodes in the network. Performance evaluation demonstrates the efficiency (in terms of true and false positives) of the proposed detection method in detecting clone nodes in MWSN environment.

Keyword: Danger theory; Danger zone; Mobile wireless sensor network; Node replication attack