Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS)

ABSTRACT

Wireless sensor networks (WSNs) are an emerging technology used in many applications in both the civilian and military domains. Typically, these networks are deployed in remote and hostile environments. They are vulnerable to various kinds of security attacks, of which sybil attacks are some of the most harmful. Thus, it is necessary to solve the problems related to sensor node constraints and the need for high WSN security. This paper proposes an energy trust system (ETS) for WSNs to effectively detect sybil attacks. It employs multi-level detection based on identity and position verification. Then, a trust algorithm is applied based on the energy of each sensor node. Data aggregation is also utilized to reduce communication overhead and save energy. We analyze the performance of the proposed system in terms of security and resource consumption using theoretical and simulation-based approaches. The simulation results show that the proposed ETS is effective and robust in detecting sybil attacks in terms of the true and false positive rates. By virtue of the application of multi-level detection, the proposed system achieves more than 70% detection at the first level, which significantly increases to 100% detection at the second level. Furthermore, this system reduces communication overhead, memory overhead, and energy consumption by eliminating the exchange of feedback and recommendation messages among sensor nodes.

Keyword: Energy; Trust; Detection; Sybil attack; Wireless sensor network