Energy trust system for detecting sybil attack in clustered wireless sensor networks

ABSTRACT

Wireless Sensor Network (WSN) is an emerging technology that offers great promise for various applications. The sensing capabilities combined with relatively small processing power and wireless communication makes it one of the main technologies to be exploited in the future. Despite its attractive features, WSN is vulnerable to various security attacks. The constraints of WSN such as limited energy and memory make the security problem even more critical. One of the security issues of WSN is it is susceptible to sybil attack. In this attack, the adversary forges multiple entities to disrupt the entire network. This paper addresses the problem by developing a lightweight trust system using energy as a metric parameter for a hierarchical WSN. The performance evaluation of this system shows efficiency and scalability for detecting sybil attacks in terms of true and false positive detection in a heterogeneous WSN. Furthermore, this system reduces the communication overhead in the network by cancelling feedback and recommendations among sensor nodes (SNs).

Keyword: Wireless sensor network; Sybil attack; Energy trust system; Detection