A secured dynamic cluster-based wireless sensor network

Abstract

Driven by the technology advances in Micro-Electro-Mechanical Systems which has facilitated the development of smart sensors; we have witnessed in recent years the emergence of WSNs in environment, military, surveillance, natural disaster relief, healthcare, etc. These WSNs carry the promise of drastically improving and expanding the quality of services across a wide variety of settings and for different segments of the population. Therefore, it is very important to develop a WSN with robustness and security in mind. Typically, the sensors are smaller in sizes that have limited processing and computational power resources, and are inexpensive, thus enabling the network to have a large coverage area and longer range. By using hundreds or thousands of them it is possible to build a high quality, fault-tolerant sensor network where failure of one or few nodes does not affect the operation of the network. They are also self-configuring or self-organizing. In this paper, we propose formation of a Secured Cluster-based architecture for a Dynamic Wireless Sensor Network that uses two topology management operations: node-move-in and node-move-out. The proposed security protocol integrates one round Zero Knowledge Proof and AES algorithm to apply for node authentication, where only authenticated nodes will be accepted during node-move-in operation. We also show that it requires O(h+q) rounds for a node to join into a network securely, where h is the height of the dynamic cluster-based wireless sensor network and q is the number of neighbouring nodes of a joining node.