**Abstract**

A wireless sensor network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. In the wireless sensor networks, data aggregation scheme is used to reduce the large amount of transmissions. In the wireless sensor network, security is an important concern. So, in order to overcome this problem a new concealed data aggregation scheme is used. It has three contributions: First, it is designed for a multi-application environment. The base station extracts application-specific data from aggregated cipher texts. Next, it mitigates the impact of compromising attacks in single application environments. Finally, it degrades the damage from unauthorized aggregations. In this method, the aggregator is selected based on the transmission range. But the drawback is less security and less efficient. So, in this paper, an innovative technique called Trust Computation Model for Secure Data Aggregation (TCMSDA) in wireless sensor networks is introduced. A new trust management scheme is essential to differentiate illegal and normal nodes and filter out the malicious nodes in the network. In the trust computation model, each node identifies trustworthiness of sensor nodes. This model suggests a defensible approach against insider attacks incipiently beyond standard authentication mechanisms and conventional key management schemes. Experimental results show that when compared to the existing system, the proposed system achieves more efficiency and high security.