121. SECURE DATA AGGREGATION TECHNIQUE FOR WIRELESS SENSOR NETWORKS IN THE PRESENCE OF SECURITY THREATS

Kokilavani.V
M.E-Scholar-Mother Teresa College of Engineering and Technology

Network security involves the authorization of access to data in a network, which is controlled the network administrator. Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. Collision attack means the group of nodes to access the illegal data. The data collected from individual nodes is aggregated at a base station or host computer. Due to limited computational power and power resources, aggregation of information from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging. Data aggregation process can enhance the robustness and accuracy of information which is obtained by entire network. In a wormhole attack, the attacker receives packets at one point in the network, forwards them throughout a wired or wireless connection with less latency than the system links, and relaysthem to another point in the network. A distribute Warmhole detection algorithm for wireless sensor networks, which detect wormholes based on the distortions they create in a network.

Key words: Data aggregation technique, Collusion attack, Wireless sensor networks, Iterative filtering algorithm.

ISBN 978-81-904760-6-5