Abstract

For about last two decades research and development processes in area of Electronics and Sensors have resulted as significant advancements in electronics and technology, small size, cost effectiveness have resulted sensor nodes as crucial part of real world problem solution applications. The wireless sensor nodes are spread over an area to record the facts of situations like fire, flood and then forward same to meaningful data to the a node, which is generally cluster head node for calculations, resulting an alert to take necessary measures to control the situation. In last few years, WSN have increased significantly in variety of areas and applications, resulted the contemporary demand of high, consistent security mechanism. Also, there is variety of attacks on WSN at their different layers. These tiny, low processing sensor nodes are not strong enough in terms of power, handling attack issues etc. On other hand, applications based on these sensors demand on-time streamed data or information is to be collected and then to send same on a reliable, secure delivery mechanism. Tiny sensors with limited hardware, processing are not able to afford old and in practice security protocols or algorithms to face or sustain the attacks. Many attacks impact WSNs. at their different layers an
affect sensor’s roles like signaling, framing, transmission etc. Many attacks have been identified at each layer of WSN which are intended, pre-planned attacks to obstacle the availability of service, restricting the sensor node’s utilization in solution of a for problem. This paper is mainly focused on WSN structure, threats, attacks and security requirements and security measures against attacks; especially various types of attacks starting from physical layer and data link, network layers, subsequently and particularly variety of attacks at transport layer in details with some effective suggestions as prevention or protection against those attacks.

References


Index Terms

Computer Science Wireless
Keywords

Wireless, Sensor, Security, Processing, Attack, Bandwidth, Vulnerabilities, Networks