Abstract

Wireless sensor networks have become a growing area of research and development due to the tremendous number of applications that can greatly benefit from such systems and has lead to the development of tiny, cheap, disposable and self contained battery powered computers, known as sensor nodes or “motes”, which can accept input from an attached sensor, process this input data and transmit the results wirelessly to the transit network. Despite making such sensor networks possible, the very wireless nature of the sensors presents a number of security threats when deployed for certain applications like military, surveillances etc. The problem of security is due to the wireless nature of the sensor networks and constrained nature of resources on the wireless sensor nodes, which means that security architectures used for traditional wireless networks are not viable. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. In this paper we discuss some security threats and challenges faced by WSNs.
Wireless Sensor Networks: An Overview on its Security Threats

Reference


Index Terms

Computer Science Wireless Networks
### Key words

<table>
<thead>
<tr>
<th>Security</th>
<th>Wireless</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Networks (WSN) threats</td>
<td>Denial of Service (DoS)</td>
</tr>
</tbody>
</table>