Abstract

wireless networks of low-power sensing devices are poised to become a ubiquitous part of
the computing landscape. In sensor network security, an important challenge is the design of
protocols to bootstrap the establishment of a secure communications infrastructure from a
collection of sensor nodes, which may have been pre-initialized with some secret information
but have had no prior direct contact with each other. Sensor nodes should be resilient to
attacks. Since sensor nodes are resource constrained and run on battery, energy consumption
should be low to make it operate for many days. In this paper we propose an energy efficient
secure framework that proves the authentication, Integrity, and also provides secure
communication among sensor nodes by using public key algorithms.

Reference
Energy Saving Secure framework for Sensor Network using Elliptic Curve Cryptography


Index Terms

Computer Science Wireless Networks
**Key words**

<table>
<thead>
<tr>
<th>Security</th>
<th>Public Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptography</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>Sensor Network</td>
<td></td>
</tr>
<tr>
<td>attack</td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td></td>
</tr>
</tbody>
</table>