Wireless sensor networks are ideal candidates for a wide range of applications such as critical infrastructure protection. It is necessary to guarantee the trustworthiness and resilience of sensor networks as well as the sensing applications, especially when the failure of these applications may result in catastrophic events with impacts affecting safety, security, the economy and society at large. Wireless sensor networks introduce several unique challenges. First, sensor nodes are typically resource constrained. Second, sensor nodes are expected to be deployed in physical environments, with no guarantee of physical security. As a result, sensor nodes may be compromised and used against the desired applications.

This project focuses on practical broadcast authentication, trustworthy and resilient clock synchronization, and lightweight and collaborative intrusion detection in wireless sensor networks. To handle the unique challenges, this project seeks effective integration of cryptographic techniques, application semantics, and other knowledge or constraints.

This project benefits the nation and society by developing new mechanisms to protect wireless sensor networks used for mission-critical applications, providing tools for industry and other research groups, and training the next-generation engineers and scientists.

### Approach and Impact

<table>
<thead>
<tr>
<th>New approaches</th>
<th>Research Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DoS-resilient broadcast authentication</td>
<td>• Peer-reviewed publications</td>
</tr>
<tr>
<td>• Mitigation (weak authentication, pre-authentication)</td>
<td>• MobiHoc '05, MobiQuitous '05, TDSC '05, SecureComm '06, CCS '06, ACSAC '06, MobiHoc '07, MobiQuitous '07, TOSN '08, TISSEC '08, WiSec '08, IPSN-SPOT '08</td>
</tr>
<tr>
<td>• Containment</td>
<td>• TinySeRSync: clock sync for dense sensor net</td>
</tr>
<tr>
<td>• Secure and resilient clock synchronization</td>
<td>• TinyECC: ECC for sensor platforms; 1300+ downloads</td>
</tr>
<tr>
<td>• Application independent compromised node detection</td>
<td></td>
</tr>
</tbody>
</table>

### TinySeRSync: Secure and resilient time synchronization in wireless sensor networks

1. Hardware-assisted pair-wise time synchronization
   - Used in [Liu et al. '05], [Generiwal et al. '05]
   - Our contributions
     - Prediction-based MAC layer timestamp
     - Hardware-assisted, authenticated MAC layer timestamp

2. Secure and resilient global time synchronization

TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks
- Common ECC ops: ECDSA, ECDH, ECIES
- Configurable: with compile time switches
- Portable: all major sensor platforms running TinyOS
- Optimized: optimizations; optimized for common platforms

URL: [http://discovery.csc.ncsu.edu/software/TinyECC/](http://discovery.csc.ncsu.edu/software/TinyECC/)