The M-Core is a modular, extensible and lightweight security layer that gathers relevant data for the development of defense mechanisms. Similar to Metasploit, which significantly reduces the time to manufacture an exploit, the M-Core is being developed to reduce the design and development time for new detection and defense mechanisms for WSNs. The M-Core allows for the monitoring of both internal and external threats simultaneously facilitating the execution of new or existing detection and defense techniques against different attacks in parallel.

Marco Valero*, Sang Shin Jung, A. Selcuk Uluagac, Yingshu Li*, and Raheem Beyah

**MAINT IDEA**

**THE MONITORING CORE (M-CORE)**

**M-Core: To Support Distributed Security Systems**
- Wireless Sensor Networks (WSNs) are deployed for monitoring in different domains (e.g., health care, military, critical infrastructure) and should be resilient to attacks.
- The problem with the traditional approach to defending sensor networks is that the solution for the Jamming attack does not defend against other attacks (e.g., Sybil and Selective Forwarding).
- M-Core addresses the challenges with the traditional approach to securing sensor networks and presents a comprehensive framework that can defend against all known and forthcoming attacks.
- M-Core has a built-in modular and flexible software architecture that provides an easy means to add, remove, and replace sub-modules. It is a lightweight monitoring and control layer invisible to upper layers.

**M-CORE ARCHITECTURE**

The M-Core services module advertises all the services provided by the sub-modules to the M-Core module, and the M-Core module allows the security modules to access those services.

To implement a defense mechanism against Sybil Attacks, our sybil module uses the rssivalue interface (service) provided by the RSSI sub-module of the M-Core.

**M-CORE SERVICES**

<table>
<thead>
<tr>
<th>Component</th>
<th>Interface</th>
<th>Command/Event</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel</td>
<td>channelSet</td>
<td></td>
<td>Sets the number of consecutive successfully sent packets</td>
</tr>
<tr>
<td>packetCount</td>
<td>packetCount</td>
<td></td>
<td>Sets the number of received packets per second</td>
</tr>
<tr>
<td>RSSI</td>
<td>rssPacket</td>
<td></td>
<td>Updates the RSSI value by each node</td>
</tr>
<tr>
<td>Varing</td>
<td>varying</td>
<td></td>
<td>Updates the variance value aggregated in the M-Core</td>
</tr>
<tr>
<td>neighborV</td>
<td>neighborValue</td>
<td></td>
<td>Updates the average received value aggregated in the M-Core</td>
</tr>
<tr>
<td>packetInfo</td>
<td>packetInfo</td>
<td></td>
<td>Updates the packet information table</td>
</tr>
</tbody>
</table>

**TESTING M-CORE**

**DEFENSE MECHANISMS USING M-CORE**

Using M-Core and MCL, we implemented detection and defense mechanisms against Jamming, Selective Forwarding, Sybil, and Internal attacks representing different layers of the communication stack simultaneously on sensors.

**REFERENCES**


