

Network Security Library for **QualNet**® & **EXata**®

The Network Security Library is an important addition to SNT's already rich collection of network models. Networks that include wireless mobile nodes are particularly vulnerable to attack because these nodes have a higher degree of autonomy and more dynamic network states, and don't require physical access to be eavesdropped upon, attacked or otherwise compromised.

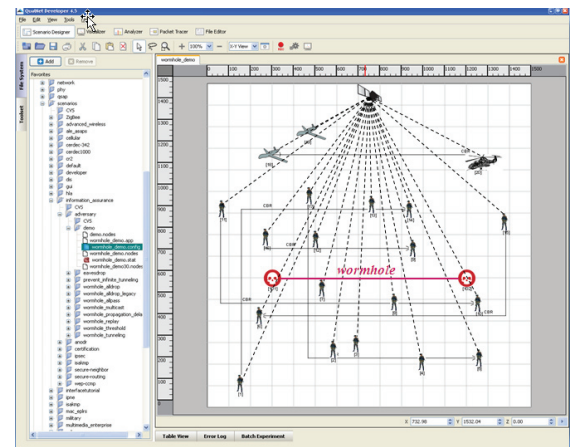
Components of the Network Security Library

The Network Security Library is a toolkit with models that encrypt, authenticate, route securely, mimic adversaries, and manage keys and certificates. It builds on the IPSec model included with QualNet and EXata, and consists of the following models:

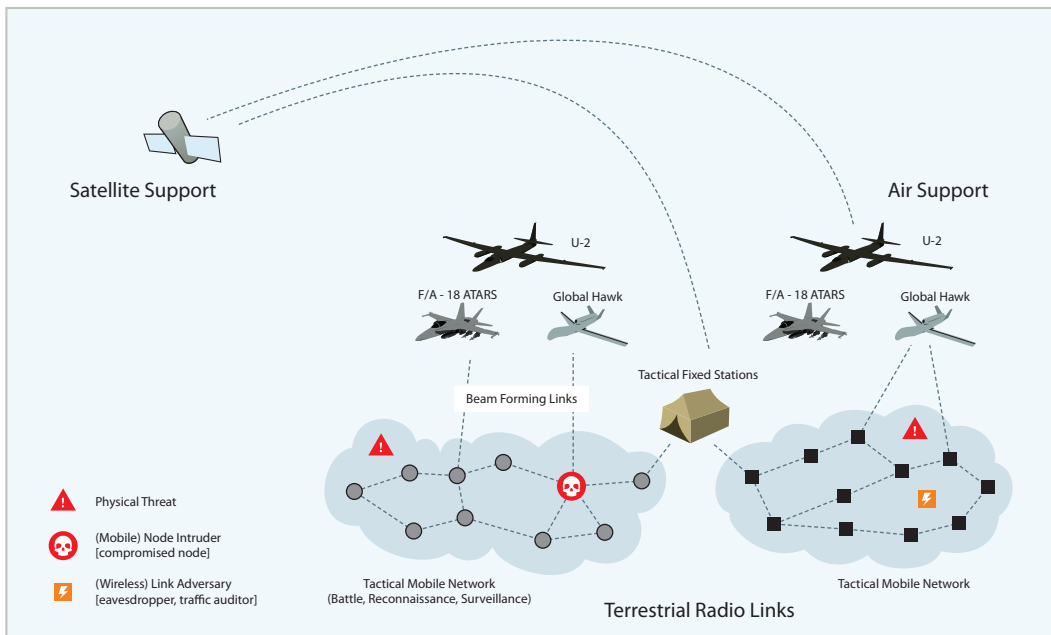
- ANODR (Anonymous On-Demand Routing)
- Secure Neighbor
- WTLS Certificate
- WEP (Wired Equivalent Privacy) Encryption
- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
- ISAKMP (Internet Security Association and Key Management Protocol)
- Adversary
 - Wormhole Attacker
 - Eavesdropper

To illustrate why mobile networks need network security, let's look at a mobile ad-hoc network. Properly functioning mobile nodes will generate incorrect or quickly outdated network information that must be interpreted by sophisticated network protocols. Out-of-date network information from a legitimate node may look similar to information generated by a compromised or attacking node.

Once in, the attacking node can send messages to the network to route all traffic through itself or add undesired traffic, thus compromising the security and performance of the network. Communication protocols and systems must be designed to avoid and defend against such network attacks.



Network Security Library includes adversary models such as Wormhole Attacker (shown above) and Eavesdropper.



Sample combat network showing ways in which nodes can be compromised. QualNet and EXata model both attackers and defensive responses by the network.