The Joint Network Emulator (JNE) Program
The StealthNet Project

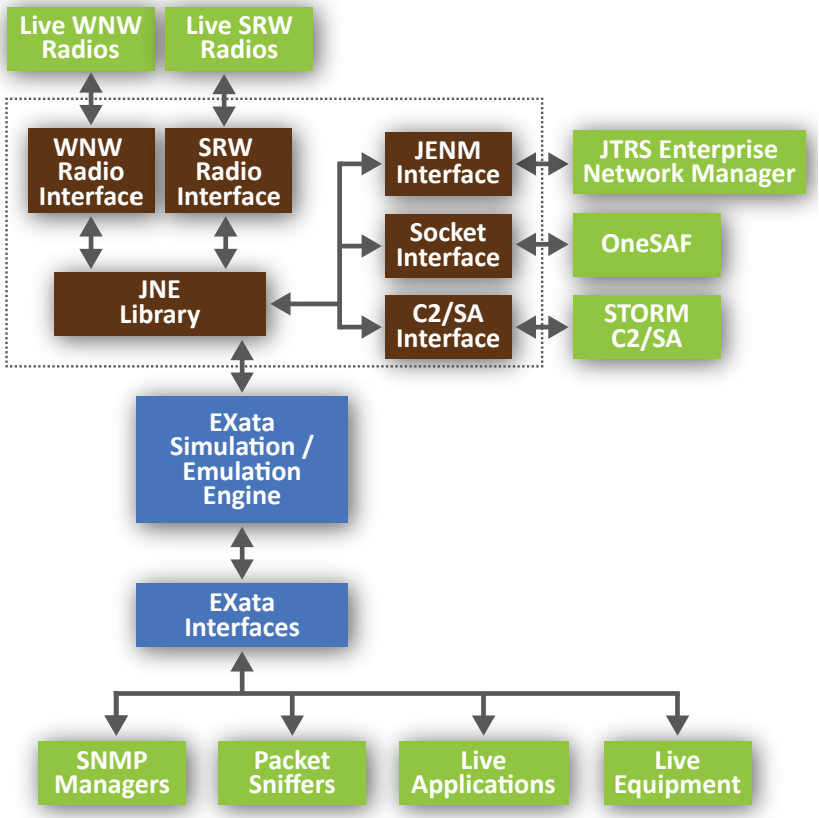
OVERVIEW

WHAT IS JNE ?

The Joint Network Emulator (JNE) program is sponsored by the Joint Tactical Network Center (JTNC) (previously the JPEO JTRS) to **provide a scalable Live-Virtual-Constructive (LVC) simulation-emulation environment to facilitate analysis, test and evaluation, mission planning, mission rehearsals and training** for networks of both new JTRS and current radio equipment that can scale to thousands of nodes.

JNE is a GOTS "library" of functionality that runs on the EXata® COTS simulation/emulation platform from SCALABLE. It runs in a Linux environment.

JNE was successfully field-deployed in support of the US Army Network Integration Evaluation (NIE) 12.2 exercise, and is being used to plan scenarios for upcoming NIE events.



WHAT IS STEALTHNET ?

The StealthNet research project is funded by the Test Resource Management Center Test and Evaluation / Science & Technology Program through the US Army PEO STRI. StealthNet is a Live-Virtual-Constructive (LVC) framework that **provides a real-time, hardware-in-the-loop capability for simulation of cyber threats** to the entire net-centric infrastructure. It also provides the ability to evaluate the effectiveness of the threats in disrupting Blue Force communications via key performance indicators, i.e. bandwidth, reliability, delay and quality of service metrics.

ARE JNE AND STEALTHNET RELATED ?

- JNE v4 is available as a no-cost GOTS product upon approval from the JTNC.
- StealthNet is a research experiment that has produced some innovative technology. It is currently at Technology Readiness Level 6 (TRL 6).
- A Delivery Order under the JNE program has been funded to integrate the StealthNet technology into the JNE platform to enable operational network models to be subjected to various cyber attacks and evaluated for behavior and resiliency.

CAN JNE / STEALTHNET BE FEDERATED ?

- The EXata simulation platform that drives JNE has an optional Standard Interfaces library that includes support for the High Level Architecture (HLA) and Distributed Interactive Simulation (DIS) protocols, enabling comprehensive federation.
- JNE includes a socket-based integration interface to the OneSAF semi-automated forces application. Both JNE and StealthNet can be integrated with other tools via sockets.

WHAT IS THE EXATA CYBER ENVIRONMENT ?

SCALABLE has commercialized portions of the StealthNet technology into a COTS Cyber Library of simulated cyber attack, defense and vulnerability models that works with the EXata platform. The EXata Cyber Environment is a bundle of this Library and the EXata platform. It is **used as an analysis and training tool for understanding the impact of various cyber attacks** such as jamming and denial-of-service floods on varied communications environments.

DEVELOPMENT / DEPLOYMENT ROADMAPS

JNE

- The JTRS Reference Implementation Laboratory (JRIL) responsibilities are being spread across various service-specific organizations (e.g. the WNW RIL will be managed by SSC-LANT in Charleston, SC and the SRW RIL will be managed by CERDEC at the Aberdeen Proving Grounds). JNE is being deployed at all of the RILs in support of waveform verification and new radio equipment certification and acquisition.
- There are a series of new Delivery Orders with a wide range of program enhancements being defined and negotiated, including additional waveform development, user interface enhancements, and network management system integration.

STEALTHNET

- The StealthNet research is being migrated to a product development path under the JNE program. This will add a library of cyber effects to the network testing, deployment and training functionality.

EXATA CYBER ENVIRONMENT

- The EXata Cyber Environment is being expanded in two dirtections:
  - The **EXata Cyber Training System**: a red force | blue force training platform that provides guided free-form hands-on interactive scenarios in a simulated communications environment to teach IT personnel the skills for cyber defense
  - The **EXata Cyber Assessment System**: a product that can import the network topology and element details of an existing communications environment and perform a suite of automated and user-guided vunerability and resiliency assessments
- EXata and the Cyber Library have been successfully used as part of the Limited Objective Experiments by USSTRATCOM

Joint Network Emulator

Software Virtual Networks (SVNs) use advanced simulation technology to create digital replicas of communication networks and the propagation environments in which they operate. SVNs are software-driven environments that use state-of-the-art modeling and simulation technology to accurately represent all of the elements and communications dynamics of highly mobile, multi-tiered heterogeneous networks together with the applications that run on these networks.

The key technology innovation that powers an SVN is the ability to leverage commodity multi-core and parallel computers for real-time and faster-than-real-time execution of high-fidelity network models, also called network emulations. In a context where an SVN is integrated with live applications, hardware, or humans, a “hybrid virtual network” (HVN) is created where the model executes in precise real-time. This enables ‘communication effects’ of large, tactical networks to be directly injected into end-to-end application performance. These realistic network effects to be reproduced in the laboratory or at a forward location, in the context of actual netops tools and warfighter applications.

SVN / HVN technology has been used to develop JNE to provide very precise emulations of legacy and emerging tactical networks, that include the communications protocols (transport applications) used among the various communications equipment, to the degree that they are indistinguishable by network management systems and other applications development tools from their physical manifestations.

Key capabilities provided by JNE include:

- JNE can scale from a small company tactical network up to thousands of nodes engaged in the Lower Tactical Network Environment
- JNE can overlay systems mobility, terrain effects and weather effects on a communications model
- JNE can interface with live physical hardware (e.g., radios running the Wideband Network Waveform (WNW)) and fully integrate live battlefield application software (e.g., FBCB-2, JVMF messages, IBEX,) even for brigade-sized networks
- JNE has been interfaced with network managers that include the JTRS Enterprise Network Manager (JENM), and JNE scenarios can be initialized using identical Radio Mission Data Set (RMDS) files used to configure live networks of WNW and SRW radios
- JNE is being interfaced with instrumentation and data collection tools used on live networks (e.g. OASIS, Ethereal, and Wireshark)
- Communications scenarios in JNE can be recorded and replayed
- JNE can run on notebook PCs for portability or in-theatre use, and on multi-processor servers for scalability to brigade and larger networks
- JNE can be used in purely constructive or virtual contexts for training, rehearsals or laboratory-based risk reduction events

StealthNet

StealthNet is a Live-Virtual-Constructive (LVC) framework for test and evaluation of operational network defenses against cyber attacks. It has the following objectives:

- Accurately assess the readiness of systems in the Net-Centric Battlespace for Information Operations (IO)
- Provide an LVC framework for simulation and stimulation of operational net-centric systems under cyber attack
- Recreate the impact of IO within the simulation of the Net-Centric Battlespace by providing realistic cyber threat representations that include passive, active, and coordinated threats
- Assess ability to measure impact of cyber threat vectors (denial-of-service, virus, wormhole) on tactical network architectures and net-centric systems under test in the accomplishment of the mission

The StealthNet framework includes the simulated network architecture (tactical radios, network hardware and software), and interfaces from the simulated network to other LVC elements that include real network hardware (routers, firewalls, etc), live intrusion detection or intrusion prevention systems (e.g. Snort), real C2 systems under test (e.g. situation awareness (SA) applications) and other virtual and constructive elements. Within this LVC architecture cyber threat models are also included that are capable of launching various attacks against the network architecture, as well as simulated physical attacks to exploit vulnerabilities (e.g. Metasploit, Nmap).

The benefit of the HVN approach is that real equipment can be connected to the virtual network, and real application traffic such as sensor feeds, voice communications, or video can be streamed through it. Thus the effects of the network state and its ability to route traffic to the intended destination along with delay and losses can not only be analyzed, but also be seen and heard in real-time. Third party network analysis, management and diagnostic tools, such as packet sniffers, SNMP managers may be used to concurrently study the purely simulated network and the physical network. By integrating real applications with the emulated cyber warfare communications effects models, it becomes possible to evaluate the impact of cyber attacks on operational systems and mission threads.

The second key component of the StealthNet framework is the Cyber Library of attack, defense and vulnerability models that can operate in LVC modes, and thus is able to simulate and stimulate the LVC networked system under test. This library contains models for accurate cyber threat simulation at all layers of the networking stack to include passive, active, coordinated and adaptive attacks. StealthNet leverages Parallel Discrete Event Simulation (PDES) concepts to model large-scale coordinated cyber threats on networks with hundreds to thousands of wired and wireless components. The high-fidelity implementation of the cyber models ensure that the physical network-system under test can be stimulated with simulated cyber threats that span all protocol stack layers for real-time testing.

Example cyber attack and defense models available in StealthNet:

Denial Of Service: DOS attacks overwhelm the resources (primarily memory or processing cycles) of a victim computer or network element so that it cannot service requests from other clients. The clients, therefore, are denied service from the victim computer or network. This is accomplished by sending a large volume of traffic.

The DOS model in StealthNet supports three kinds of attacks:

- Basic attack, where the attacker(s) send large volumes of UDP traffic to the victim host or network. The UDP traffic consumes the network buffer memory as well as CPU resources.
- TCP SYN attack, where the attacker(s) send TCP SYN packets to the victim computer. Each TCP SYN packet opens a new TCP connection at the victim computer, thus consuming the transport layer buffer memory.
- IP Fragmentation attack, where the attacker(s) send partially fragmented IP packets to the victim computer. The victim computer buffers these fragmented packets and waits for remaining segments, thus consuming the network layer buffer memory.

Radio Jamming, or simply jamming, is transmission of radio signals at sufficiently high energy to cause disruption of communication for nearby radios. The signals transmitted by jammers interfere with other legitimate signals in the vicinity of the jammer, causing the signal to noise ratio of the latter signals to drop significantly, and resulting in corruption of those signals. Currently three strategies of frequency selection for jamming are supported:

- Wideband jamming: jam all transmissions in a given range of frequencies.
- Sweep Jamming: The jammer divides the frequency range in contiguous chunks of frequency bands. The jammer jams each chunk at a time for a specified duration before moving to next chunk.
- Custom jamming: model arbitrary frequency selection and hopping pattern for jamming.

Channel Scanning is an act of gathering information by intercepting and analyzing the signals. No attempt is made to decode the signal; only the characteristics of signals, such as frequency range, power of transmission, and RF signatures are determined. The Channel Scanning model provides a basic framework and API upon which advanced intelligence gathering algorithms may be developed.