

In cyber warfare, the network is the battlefield. While all networks are vulnerable to attack, mobile wireless networks are the most unprotected because their strengths — agility, adaptability, node autonomy and self-organization — also make them harder to defend against radio frequency (RF) distortion and malicious packet-level disruption and intrusion.

Up to now, wireless has been the most neglected network security domain in terms of spending, in both military and enterprise spaces. Yet wireless networks, especially mobile networks, are the most critical component of tactical communication infrastructure and the most challenging to defend against cyberattacks.

Testing for Cyber Readiness

It is not yet known if future on-the-move communication networks can be made secure enough. Given what's at stake to meet cyber defense and cyberattack objectives, it's critical that network designs, applications and users are stressed in an ultra-high fidelity and complex virtual space environment that accurately mimics the environment they will need to survive in.

EXata/cyber creates Software Virtual Networks (SVNs) that make it possible to represent the communication infrastructure at such high levels of fidelity that applications running on it — such as a mix of third-party streaming video, voice over IP, e-mail, chat, video Web conferencing, video teleconferencing — can be deployed unmodified on top of large emulated networks of both legacy and future communication devices.

Beyond cyber security, all networks face common challenges like bandwidth limitations, bottlenecks,

security attacks, session management, scalability, traffic congestion, and quality of service trade-offs. Mobile networks face even more challenging issues including terrain, weather, and environmental conditions, spectrum management, mobility effects and limited battery power. EXata/cyber is here to address all these challenges.

What Sets EXata/cyber Apart?

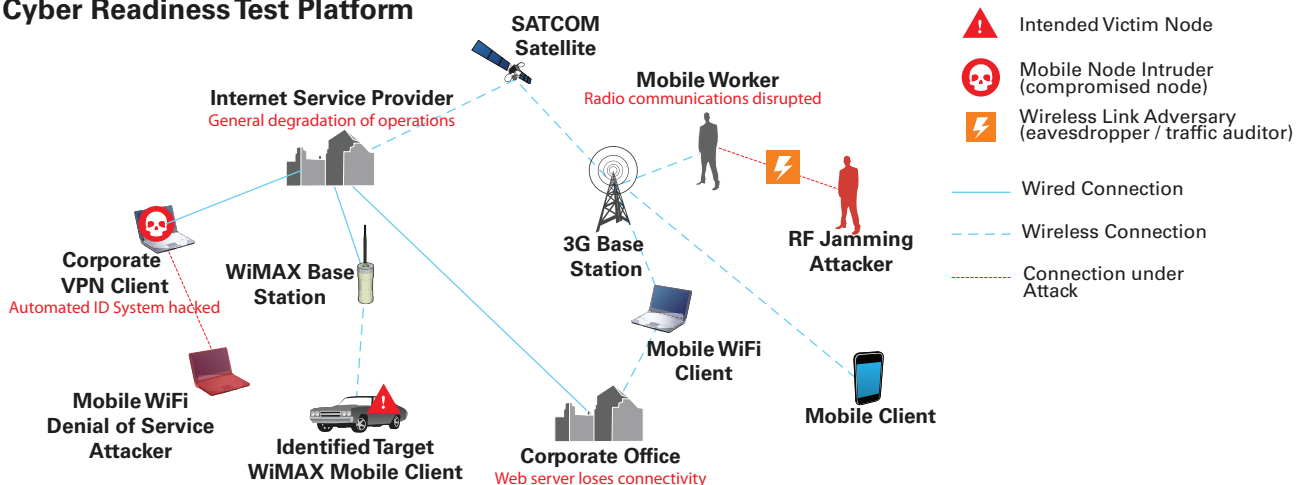
EXata/cyber is new evaluation technology for new wireless technologies. EXata/cyber is a network emulation ... a representation so accurate that a user or component connected to the virtual network can not discern whether it's connected to the digital representation or the real thing.

EXata/cyber is a realistic software virtual network. It enables you to digitally represent your entire network - devices, software, transmitters, antennas, terrain effects, atmospheric effects, and human interaction effects. You can now represent every variable that will affect the performance of your real network in EXata/cyber.

EXata/cyber empowers you to move from months to minutes. With emulation, network and equipment tests that traditionally required months to perform all the calculations can now be performed in minutes, with real-network behavior.

EXata/cyber brings ultra-fidelity at 50 or 1,000 nodes. Competitors' simulation programs, written with legacy sequential processing code, can only simulate a maximum of about 200 devices, and fidelity drops as you approach that number. With EXata/cyber, you get the same accurate representation of your network whether you're testing 50 nodes or thousands.

Cyber Readiness Test Platform



Components of EXata/cyber

Included with EXata/cyber* are protocol models for cyber scenarios, such as 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), and Adversary (Wormhole Attacker and Eavesdropper).

EXata/cyber's main components include:

GUI

EXata features an easy drag-and-drop GUI to build network topologies and advanced editors to allow fine-grained design of devices and networks. In visualization mode, 2D and 3D controls allow you to monitor emulation progress and control per-layer & per-event animation. Also included are powerful analysis and debugging tools

Emulation Kernel

The emulation core of EXata ensures that your network's digital replica (the emulated or virtual network) runs in real-time and treats packets as real packets, not abstract ones. EXata/cyber has high-fidelity models that can interoperate with real networks. EXata is designed to take full advantage of processing power on multi-core, multi-processor, cloud and cluster systems. EXata's multithreaded kernel speeds up networking, requiring very little user intervention to achieve optimal performance.

Universal Protocol Adapter (UPA)

The EXata Universal Protocol Adapter (UPA) enables users to run multiple real applications on a single computer and assign each to run on a different emulated node in EXata.

Connection Manager

Applications need no modification or customization to use the Connection Manager and run their network traffic over the EXata network. Connection Manager supports a large variety of applications such as Internet browsers, tactical communications, situational awareness information, VoIP, streaming video, etc. For testing of network for cyber warfare readiness, EXata/cyber can also interface with Semi-Automated Forces (SAF) or Computer Generated Forces (CGF) via HLA or DIS.

Packet Sniffer and SNMP Agent

EXata/cyber supports a packet sniffer interface to enable capture and analysis of network traffic using standard packet sniffer/analysis tools like Wireshark or Microsoft Network Monitor**. Additionally, EXata/cyber can be managed using standard SNMP network managers like HP OpenView, IBM Tivoli or SolarWinds Orion**.

* Note: All product features and functions are subject to change without notice.

** The third party applications are listed as examples and do not imply explicit support of all their features. Microsoft Network Monitor is a trademark of Microsoft. HP OpenView is a trademark of HP. IBM Tivoli is a trademark of IBM. SolarWinds and Orion are registered trademarks of SolarWinds Inc.

