A Live-Virtual-Constructive (LVC) Framework for Cyber Operations Test, Evaluation and Training

Maneesh Varshney  
Scalable Network Technologies, Inc  
Los Angeles, CA  
mvarshney@scalable-networks.com

Kent Pickett  
MITRE Corporation  
Ft. Leavenworth, KS  
kpickett@mitre.org

Rajive Bagrodia  
Scalable Network Technologies, Inc  
Los Angeles, CA  
rbagrodia@scalable-networks.com

Abstract—Current simulations supporting the Net-Centric Test battlespace do not accurately represent the impact of cyber threats and information operations. When cyber threats are considered, they are typically limited to a small number of isolated physical devices. To further limit consideration, insufficient attention is paid to cyber attacks launched on the basis of passive threats like the eavesdroppers or the coordinated threats. Further, the test technologies are typically limited to incorporation of threats that can be realized physically, which limits both the scale and sophistication of representing such attacks; a Live-Virtual-Constructive (LVC) paradigm for modeling of threats is missing. Lastly, for threats such as jamming, wormhole attacks, large-scale Denial of Service attacks, use of physical threats is expensive, since specialized equipment and manpower is required to realize these threats. The net consequence of these deficiencies is to leave a major gap in the DoD test infrastructure with respect to our ability to realistically test the vulnerabilities and resiliency of Blue Force communication architectures to sophisticated cyber attacks, particularly in networks that include both current force & Future Force communication infrastructure.

In this paper, we present StealthNet, 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. The StealthNet framework provides models for accurate cyber threat simulation at all layers of the networking stack to include passive, active, coordinated and adaptive attacks on networks with hundreds to thousands of wired and wireless components. The LVC technology can stimulate physical Networked-System Under Test (NSUT) with simulated cyber threats that span all the protocol stack layers for real-time testing. Additionally, the framework enables composability with existing Test and Evaluation (T&E) architecture and tools (TENA, SBE environments, etc) to facilitate transition to other T&E programs.

I. INTRODUCTION

With the Army’s in theater adoption of its new smart phone, (Joint Battle Command-Platform JBC-P) and its extensive use of semantic search technology (Distributed Common Ground Station-Army DCGS-A) to support intelligence fusion, new opportunities materialize for realistic cyber attacks against tactical operations. The end-to-end communications technology supporting the identification, targeting and fire engagement chain becomes a mix of both wireless and wired network enclaves which exhibit classic vulnerabilities to cyber attack.

This paper describes a new Test and Evaluation (T&E) capability StealthNet, which will support an “end-to-end” T&E of the network architecture. StealthNet is a Live Virtual Constructive (LVC) environment in which the impacts of a cyber attack can be tested on actual systems; either network devices (routers, firewalls) or Command and Control (C2) systems operating in a tactical military mission thread.

Following this introduction, this paper is divided into four sections. Section II contains a description of different types of cyber attacks that are common against both Radio Frequency (RF) and wired networks. Section III provides an overview of StealthNet, its structure and capability to serve as a real time environment for testing; to test particular hardware in a network under cyber attack and also to test a military network architectures robustness (ability to prevent, detect, and recover) when under cyber attack. Section IV provides a description of a use case for a cyber attack against a Time Sensitive Targeting (TST) mission thread. This section will also discuss the tactical impact of the cyber attack and provide some metrics for the measurement of a networks ability to support fighting through the attack. Section V summarizes the StealthNet project and its expected completion dates and milestones.

II. AN OVERVIEW OF CYBER THREATS AGAINST RF AND WIRED MILITARY NETWORKS

A. Why Ad-hoc Wireless Networks are Especially Vulnerable?

Wireless networks, and especially the ad-hoc and mobile networks, are at greater risk of cyber espionage and attacks compared to their wired network counterparts. Figure 1 illustrates a notional architecture of a wireless ad-hoc network, identifies several components of the architecture and identifies wireless-specific potential security flaws with each component. For the purpose of the present discussion, the understanding of the wireless network architecture as well as the enumeration of the security flaws is not meant to be comprehensive, but rather as a means to gain understanding of the special security-related issues with wireless networks.

Since the wireless signals are broadcasted over a shared channel, it is easy to eavesdrop transmissions. The eavesdroppers do not require physical access to network devices as they
would for a wired network. Furthermore, since the wireless channel capacity is typically orders of magnitude lower than wired networks (e.g. commercial 802.11a WiFi networks offer 54 Mbps capacity, compared to 1 Gbps in typical wired networks), it is easy to deny service. A single or a small group of jammers can effectively disrupt a wireless network, whereas it typically requires tens of thousands of “zombie” computers to successfully execute a Denial-Of-Service (DOS) attack in wired networks.

![Security Issues with Ad-hoc Wireless Networks](Image)

Fig. 1. Security Issues with Ad-hoc Wireless Networks

The wireless network device itself is typically resource constrained. For example the battery life and CPU power are typically lower than computers on wired networks. This implies that advanced security mechanisms from wired networks cannot be easily migrated to wireless networks. The wired security protocols typically exchange many request-response messages, have high overheads, and have strict timeouts, which makes it difficult to be supported by wireless networks.

When individual devices form an ad-hoc network, additional security issues arise. It is easy to gather intelligence, through eavesdropping as discussed earlier, and attackers can use Signals Intelligence (SIGINT) approaches to learn RF signatures of radios, location, movement and activity of troops even if the data is encrypted. It is also easy to disrupt since the ad-hoc networks are ‘self-organizing’, which means that attacks such as wormhole attacks and rushing attacks can introduce false information in the network to disrupt the formation of routing topology. Furthermore, these attacks do not require physical access to routers. And finally, these networks are typically deployed and dismantled over short time periods, which gives insufficient time for cyber defense planning, especially since security experts are often not on site.

### B. Taxonomy of Attack Vectors

Cyber attacks come in many flavors, each targeting different kinds of vulnerability within the network or computer system, and at different layers of the protocol stack. Attack vectors enable intruders to exploit system vulnerabilities, including the human element. Protecting the network assets against intruders requires an understanding of these attack vectors, which is why significant effort has been devoted towards a unified classification methodology, or taxonomy, of such attacks. However, most of the existing taxonomy schemes [3] focus exclusively on the software vulnerability exploits, which in our judgment largely ignore those attacks that specifically target network-centric operations. Table 1 presents our classification of the attack vectors into seven distinct modes of attacks. These vectors include, among others, attacks that target the network protocols, e.g. the routing protocols, as well as attacks that target wireless networks. For each attack vector, we have outlined a few prominent attacks that exist today; it is not our intention to provide a comprehensive list in this paper.

**Passive attacks**, as the name suggests, do not actively influence the network. The intention is to glean information about the state of operational networks. Note that the information could be data itself (files, streaming video), or other kinds of non-data information such as location and strength of troops, direction of movement and identification of commanders. Prevailing strategies for passive attacks include wireless eavesdropping, packet sniffing and comprehensive network traffic analysis.

**Denial of Service** involves overwhelming the networking or computation resources of a network or host computers to render them incapable of servicing genuine operations. This is one of the most popular kinds of attack vector and includes attacks such as Internet Control Message Protocol (ICMP) Smurf, and TCP SYN flood.

**Malicious agents** are software programs, such as viruses and worms, which leech themselves to a host computer to infect their resources and utilize the host computer’s resources to propagate themselves further. Other examples include malware, trojans, backdoors and rootkits.

**Topology misconfiguration** applies to mobile ad-hoc networks (MANETs), which has a self-organizing nature to route traffic. A malicious agent could potentially subvert the correct routing topology construction and maintenance protocol to force the traffic to be routed along a preferred path. A well-known attack is Wormhole [4], where two or more collaborating nodes can influence the entire network topology such that all traffic is directed towards them.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive Attacks</td>
<td>Gleaning Information</td>
<td>Eavesdropping, Sniffing, Network traffic analysis</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Overwhelming the computation or network resources to make a service unavailable</td>
<td>ICMP flood, Smurf ping flood, TCP SYN flood, Teardrop attack, Reflection attack, Blind DOS, Distributed DOS</td>
</tr>
<tr>
<td>Malicious Agents</td>
<td>A malicious undetected program executing on victims computer</td>
<td>Virus, Worms, Malwares, Trojans, Rootkits, Backdoor</td>
</tr>
<tr>
<td>Topology Misconfiguration</td>
<td>Subverting the traffic flow paths</td>
<td>Wormhole attack, Rushing attack, Blackhole attack, Grayhole attack</td>
</tr>
<tr>
<td>Code Exploits</td>
<td>Exploiting software bugs to execute malicious code</td>
<td>Buffer overflows, OS / Services / Applications / Database exploits</td>
</tr>
<tr>
<td>Human Error</td>
<td>Intentional or accidental operator actions</td>
<td>Phishing, Incorrect data entry, compromised personnel</td>
</tr>
<tr>
<td>Wireless Specific</td>
<td>Targeting the specific attributes of wireless communication</td>
<td>Jamming, RF signature identification, Signals Intelligence (SIGINT)</td>
</tr>
</tbody>
</table>
Code exploits utilize the documented or undocumented vulnerabilities of software to execute malicious code on the victim machine. The victim software may be the operating system, applications, databases or web browsers.

Human error refers to that broad class of attacks where operators make an error, for example visiting a malicious web page or clicking a harmful email link. Furthermore, there could be intentional actions by compromised personnel.

Finally, the wireless specific attacks target the specific characteristics of wireless communications, such as broadcast nature, hidden terminal effects and frequency hopping.

III. THE STEALTHNET TEST AND EVALUATION LVC FRAMEWORK

StealthNet is a Live-Virtual-Constructive (LVC) (Figure 2) 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 high level operational view of the StealthNet framework is illustrated in Figure 3. It 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 core of StealthNet is Software Virtual Network (SVN) technology [5] that makes it possible to represent the communication infrastructure at high levels of fidelity. In this SVN simulation/stimulation environment, actual applications and actual network traffic, such as a mix of sensor data, streaming video, voice communications, chat, collaboration, video web conferencing can be deployed unmodified through the virtual networks. SVNs utilize network emulation technology to provide a high fidelity, computationally efficient, and scalable environment for cyber operations.

The benefit of the SVN 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. This is a significant improvement to communications modeling in a live or virtual environment. 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 Attack and Defense library 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.

Next we describe selected cyber attack and defense models that will be 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:

1. **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.
2. **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.
3. **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:

1. **Wideband jamming:** jam all transmissions in a given range of frequencies.
2. **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.
3. **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. The model itself reports the following information for each signal it detects: channel frequency, received signal power, direction of arrival (azimuth and elevation angles), and time and duration of transmission.

**Firewalls** are software or hardware components in a computer host or system that are used to implement network access and security policies. All traffic must pass through firewalls, which determine, based on access or security policies, the traffic that is allowed to pass through the network, or dropped at the firewalls.

The firewall model in StealthNet is a *packet-based stateless software* firewall. The firewall model is a software process that inspects each packet to determine if the said packet should be allowed or denied access. The firewall model is stateless. It does not retain state once a packet has been processed by the firewall.

The firewall model is loosely based on the *iptables* packet filter software found in Linux/Unix based systems [6]. Specifically, it models the Filter table of iptables, which is used for firewall actions (other tables, such as NAT and MANGLE are used for packet filtering and modification actions that are unrelated with firewalls).

**IV. CYBER ATTACKS AGAINST A TIME SENSITIVE TARGETING MISSION**

**A. Time Sensitive Target Use Case**

The following describes an operational use case for highlighting the impact of a cyber attack on an Army Time Sensitive Targeting mission. Figures 4 and 5 provide a pictorial of the mission thread. A high value enemy target is quickly moving through a Battalion’s Area of Operations Center (AOC) when it comes under surveillance by an Unmanned Aerial Vehicle (UAV). The UAV streams video to a Battalion intelligence section (G2) where the target is immediately recognized as a convoy potentially carrying a highly placed leader in a terrorist organization.

As the UAV streams video to the intelligence section, the Distributed Common Ground SystemArmy (DCGS-A) database is interrogated to verify the most recent sightings of the suspected terrorist leader. The UAV is immediately sent to track the enemy target and its video is uploaded to the DCGS-A database for presentation to the Battalion and Brigade Commanders (Figure 4, Step 1). In an effort to minimize collateral damage, the Battalion commander radios a reconnaissance team (Figure 4, Step 2) posted along the road requesting an “eyes on” target validation. Using the Army’s smart phone, the Joint Battle Command-Platform (JBC-P), the reconnaissance team texts confirmation of the target also sending a ground based image of the terrorists van and current coordinates (Figure 4, Step 3).

Figure 5 contains a description of the strike process. Having confirmed the target and given its current location (which continues to be updated through UAV tracks), the Battalion commander radios an attached Brigade Non Line of Sight
Artillery Battery calling for an immediate engagement of the target (Figure 5, Step 4). The Battalion G2 has also uploaded all target data (to include current location and believed vehicle type) to the FTP server at Brigade Headquarters. Using his JBC-P device, the NLOS Battery commander immediately queries the Brigade server for current target track and target type. (Figure 5, Step 5). In addition the NLOS commander downloads the locations of all friendly personnel in the area. Upon being assured that there are no friendly troops and that collateral damage will be minimal, the NLOS commander engages the target using current tracks from the Brigade server (Figure 5, Step 6).

B. Possible Cyber Attacks Against this TST Mission

This use case provides an end-to-end description of a TST mission thread. While it is notional (not requiring the full fire coordination between air and ground assets often seen in Joint TST operations), it does represent many of the opportunities for cyber attack available to the threat.

In this Use Case, target discovery, validation and tracking were conducted with systems linked by RF external networks to the Brigade and Battalion data and intelligence fusion centers. The ability of these centers to provide current target validation and tracking information and updating the NLOS firing battery again by RF networks provides ample opportunity for Red to launch multiple cyber attacks against key data structures supporting this mission thread. Figure 6 provides a list of possible threats at each step of this mission thread. These threats violate the Confidentiality, Integrity and the Availability (CIA) of the data needed to track and engage the target.

Figure 6 also provides a set of time windows for both Blue and Red forces. Blue time windows represent Blues network activities at key moments in the engagement mission. Red time windows represent cyber activities that Red may take to both determine the architecture and identify key nodes within the Blues network during their information-gathering mode. Further Red timelines represent their windows to temper, and ultimately deny, key tracking and target identification data to Blue forces.

C. Case Studies of Cyber Attacks: Silent Jammers and Distributed Denial of Service and Their Impact on the TST Mission Thread

The StealthNet architecture was used to assess the impact of two attacks against the TST mission thread. A Silent Jammer (SJ) is a system targeted at specifically active RF frequencies. SJ technology searches for active RF bands and then provides low-level energy bursts aimed specifically at interrupting the packet rate on that band. The jammer does not “block” the band, just causes multiple high data rate packets to be dropped. Those coming under SJ attack are often unable to distinguish between the attack and just a “bad link”. Within TST Use Case, recall that the discovery/tracking video from the UAV was RF based. Figure 7 represents the impact of an SJ on the “video packet rate” for the UAV.

The four images in each set are screenshots from the video application at the destination. Each shot occurs 30 seconds after the previous image. The first set of four images shows a fluid streaming video, whereas in the case of the silent jammer there is significant video distortion; enough to make this video useless for target tracking. Note also that the screenshot images are different; in fact, the video was ‘progressing’ all along the execution run, which implies that an operator by looking at the video application cannot conclude that the network link is unavailable or not operational, and would most likely attribute the poor video quality to poor wireless channel conditions.

The second case evaluated using the StealthNet Architecture was a DDOS attack on the Blue Brigade Web Server. Recall from Figure 5 Step 5 that the tracks were fused and passed
StealthNet is a three year project begun in 2010 and has just completed its first milestone. The system is currently able to represent the impact of jamming and DDOS on RF and wired networks. Goals for the second year include maturing the simulation/emulation representation of computer hosts (with their OS and browser application vulnerabilities and human behavior vulnerabilities) to represent the propagation and possible isolation of an attack in a complex wired/wireless environment.

StealthNet is being constructed as an LVC environment that can interface with existing LVC military network simulation and emulation tools like the Communication Effects Server (CES) [1], the Army’s Brigade level model OneSAF, and the Operational Test Commands test environment Battle Command Network Integration and Simulation (BCNIS) [2] as well as commercial network simulators. It currently provides interfaces to tactical network hardware to include routers, gateways and computer hardware serving as C2 devices on the wired tactical network. Ultimately (following Phase 3 development) it is targeted to interface with live-fielded tactical radios. In its LVC mode, StealthNet is being designed to scale to 1,000 simulated network nodes delivering message traffic in real time through the LVC environment to live tactical systems in a network under cyber attack. This size was chosen so that StealthNet could be used to provide a T&E capability for typical network architectures supporting Army Brigades. StealthNet will not only support the T&E of specific C2, radio and network hardware in a cyber attack but it will also provide an environment to determine the robustness of different network architectures to sustain a tactical mission while under cyber attack. Both simulated and live attack tools can be used in the StealthNet environment.

ACKNOWLEDGMENT

The authors would like to thank Mr. Gil Torres, Ms Abigail Maul (Cyber Test Technology, Science & Technology Test Resource Management Center), Mr. Jim Buscemi, Ms Kathy Smith and Mr. Kenneth Thomas (GBL Corporation) and Ms Laura Feinerman (MITRE Corp) for providing valuable insights and comments on versions of this paper.

REFERENCES


