A Virtual Cyber Range for Cyber Warfare Analysis and Training

Lloyd Wihl
SCALABLE Network Technologies
Los Angeles, CA
lwihl@scalable-networks.com

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

ABSTRACT

There is a need to accurately model the effects of cyber weapons for analysis, system testing and hardening, and training. Current simulations of the Net-Centric Battlespace do not adequately recreate the impact of cyber warfare due to a lack of realistic cyber threat and defense representations.

Hardware-based cyber ranges are limited in scale, costly, and time-consuming to configure. Moreover, they have no capability to simulate the inherent vulnerabilities endemic to wireless tactical networks. They also do not effectively model the overall effect of a cyber attack on a mission and are therefore unsuitable for mission analysis or training.

In this paper, we present a new approach, the Virtual Cyber Range, a portable modeling and simulation 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 communications via key performance indicators. The range 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 range enables interoperability with Live-Virtual- Constructive (LVC) simulations providing assessment of human-in-the-loop performance, and can stimulate physical networked systems with simulated cyber threats for real-time testing.

Utilizing this framework, the authors present findings for a targeting mission regarding the adequacy of defenses against cyber attacks that attempt data exfiltration and disruption of situational awareness.

ABOUT THE AUTHORS

Mr. Lloyd Wihl is Director of Technical Sales at SCALABLE Network Technologies, providing worldwide pre-sales support for potential clients, developing system prototypes and technology interfaces, guiding future product development especially in the area of cyber warfare, providing guidance for customer model development, training customers, and managing customer engineering service contracts.

Mr. Wihl has over 30 years of experience in the Modeling, Simulation and Training industry. His experience prior to SCALABLE includes 24 years at CAE, where he developed system architectures for military simulation and training, and led multi-million dollar projects in the areas of synthetic military environments, network-centric systems, distributed mission training, air traffic management, space systems, visual systems, and flight simulation. Mr. Wihl graduated with distinction in Engineering from McGill University.

Dr. Maneesh Varshney is a Senior Member of Technical Staff and EXata Product Research and Development team leader at SCALABLE Network Technologies, Inc. He received his PhD and M.S. in Computer Science from the University of California at Los Angeles in 2008 and 2004 respectively, and Bachelor of Technology in Computer Science and Engineering from Indian Institute of Technology, Kanpur, India . His research interests are in the area of wireless network modeling and emulation, the topics in which he has over seven years of experience and has published about a dozen scientific papers in various international conferences. He is currently researching on the real time simulations of large scale and complex wireless networks that can interface with physical and live networks. The subject of this research has been submitted for two patents and transitioned into a commercial product.

A Virtual Cyber Range for Cyber Warfare Analysis and Training

Lloyd Wihl
SCALABLE Network Technologies
Los Angeles, CA
lwihl@scalable-networks.com

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

INTRODUCTION

Most military applications and systems are network-centric, and they must protect vast amounts of sensitive data as it is stored on devices or transferred over a network. These systems depend on accurate data arriving in a timely manner. In cyber warfare, the network becomes the battlefield. All future conflicts are going to involve attempts to disrupt information technology systems, which are necessary for communication and also for the operation of highly sophisticated weapons systems, most of which are computer driven.

Most serious security breaches are due to multiple failings in people, processes, and technology. The technology encompasses an escalating arms race of cyber attacks and defenses. However, regardless of how well data is encrypted and hidden, software is restructured and tested, and equipment is hardened and shielded, humans and the processes they follow remain the weakest link and the greatest risk to cyber security.

So how can we protect our net-centric systems? Awareness is the first line of defense. For a long time, the emphasis has been on prevention, and not enough on detection and response. There is an urgent need for warfighters to understand cyber attacks and defenses, and train for cyber warfare in a high fidelity representation of their operational environment. This is a challenging problem because the training network must be isolated yet highly representative of operational networks, since small changes in configuration and interconnection may produce drastically different results.

The current solution has been to build a physical cyber range. However, hardware-based cyber ranges are limited in scale, costly, and time-consuming to configure. Moreover, they have no capability to simulate the inherent vulnerabilities endemic to wireless tactical networks. They also do not effectively model the overall effect of a cyber attack on a mission and are therefore unsuitable for mission training.

In this paper, we present a new approach, the Virtual Cyber Range, a portable modeling and simulation framework that provides a real-time, hardware-in-the-loop capability for simulation of cyber threats to the entire net-centric infrastructure. The framework enables interoperability with Live-Virtual- Constructive (LVC) simulations, providing training and assessment of human-in-the-loop performance.

Modeling and Simulation of Cyber Attacks

Computer-based simulations have long been used to train troops and develop new warfighting techniques. Networked modeling and simulation systems realistically represent combat, from sensors and weapons systems to the tactical behavior of individual entities and military units. They also incorporate detailed models of the natural environment and the effect of these environmental factors on simulated activities and behaviors. The modeling and simulation of cyber attacks requires some special features, which are dependent on the nature of the attacks. A brief discussion of these follows.

Passive attacks do not actively influence the network. The intention is to glean information about the state of operational networks. The information could be data itself or other kinds of non-data information such as location and strength of troops, direction of movement, or identification of commanders. Prevailing strategies for passive attacks include wireless eavesdropping, packet sniffing and comprehensive network traffic analysis. To replicate these attacks in a simulation, the latter must model information as packet data in the same way it is transmitted over the real network, and also include other attributes such as location, mobility, and operator roles. To model eavesdropping, the simulation must also include models of wireless authentication, trust management, and key management.

Denial of Service (DoS) involves overwhelming networking or computation resources to render them incapable of servicing genuine operations. This is one of the most popular kinds of attack vector and includes attacks such as ICMP Smurf, TCP SYN flood etc. To model these attacks, the simulation must represent the protocol stack with high fidelity as well as packet level interactions (e.g. TCP sequence numbers, ICMP packet buffer allocation etc).

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. The influence of these attacks on network-centric system performance can be investigated by integrating the cyber warfare and network models with real hosts and their real software loads, so that the malicious agents propagate in a controlled testbed environment. The attack model must interoperate with real configurable Intrusion Prevention Systems and Intrusion Detection Systems.

Topology misconfiguration applies to mobile ad-hoc networks (MANETs), which have a self-organizing nature to route traffic. A malicious agent could subvert the routing topology construction and maintenance protocol to force traffic to be routed along a preferred path. A well-known attack is Wormhole (Hu, Perrig, & Johnson, 2003), where two or more collaborating nodes can influence the entire network topology such that all traffic is directed towards them. Simulating such attacks requires modeling the routing protocols and topology construction algorithms with high accuracy.

Code exploits utilize software vulnerabilities to execute malicious code. The victim software may be the operating system, applications, databases, web browsers and so on. Modeling these attacks requires that the simulation framework must be able to interface with physical hardware and software. Such a technique is known is emulation, where the simulation models interact (by exchanging data and control information) with physical host machines.

Human error refers to that broad class of attacks where an operator makes an error, for example visiting a malicious web page, or clicking a harmful email link. Furthermore, there could be intentional actions by compromised personnel. Modeling this attack behavior requires a human-in-the-loop interface, where operators can actively participate in a training exercise to influence the state of the network.

Finally, wireless specific attacks target the specific characteristics of wireless communications, such as broadcast nature, hidden terminal effects, frequency hopping etc. For these attacks, the simulation must model the wireless specific details of communication, including detailed physical layer effects, jamming susceptibility, and mobile ad hoc network routing.

In summary of the above discussion, any cyber warfare simulation model must provide following features:

- Data communication at packet level and network security (for eavesdropping)
- Model information such as location, movement, roles (eavesdropping)
- Protocol stack operations (DoS), including routing (routing misconfiguration) and wireless (wireless specific)
- Emulation with real hardware and software (malicious agents and code exploits)
- Human-in-the-loop (human errors)
- Wireless detailed physical layer models and routing models

The Importance of Wireless

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. With the profusion of smart phones and tablets, and the US Army’s movement toward Bring Your Own Device (BYOD), it is imperative to provide training for the vulnerabilities inherent in wireless networks. Wireless networks are among the most vulnerable areas to cyber warfare, and modeling and simulation of this aspect of attack and defense is particularly challenging.

Since wireless signals are broadcast over a shared channel, it is easy to eavesdrop transmissions. 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.

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 too 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. 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 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.

Impact of Attack

Privacy of data refers to corporate or military espionage through network infiltration or exfiltration. As noted earlier, the information could be data, or other elements such as position, movement, number of troops etc. The blue force can protect information against privacy invasion by cryptographic algorithms or anonymizing the information.

Integrity of data refers to loss of fidelity of information due to data corruption or seeded false information from intruders, with an objective to undermine the quality of information and hence the situational awareness. The blue force responds by protecting the data through authentication.

Availability of data refers to disruption in services by isolating the information generators from consumers. This is achieved by bringing down communication hardware such as routers, satellites etc, or infrastructures such as power grids, telecom networks etc. The Blue force responds by establishing backup or secondary channels through which the service can continue.

In training for cyber warfare, privacy, integrity and availability are the measures of performance. Moreover, the key challenge for a training system is not simply to develop metrics for these factors that are measurable and demonstrable; it is also to evaluate how these come to play in the larger context of mission effectiveness. For this reason, we chose to develop a cyber trainer that can be integrated into live virtual constructive environments, so the effects of compromised data privacy, integrity or availability would affect operational systems, humans in the loop, or constructive entities, resulting in changes in battlefield outcome. To achieve this, the cyber trainer would need to integrate with High Level Architecture (HLA) based simulations and also be able to bring real battlefield application traffic and communications into the modeled communications network.

Current Cyber Training Approaches

Cyber Ranges

In order to safely train for cyber operations, it is necessary to isolate the training system from the operational system, while maintaining a high fidelity representation of the latter. The current approach is to build a cyber range, which duplicates a subset of hardware from the operational system and connects it on a wired network. The DoD Cyber (IA) Range is an example of this approach, providing an operational representation of today's Global Information Grid (GIG) Information Assurance (IA) architecture within a Network Operations (NetOps) construct. The IA Range is an infrastructural platform designed to integrate distributed and heterogeneous IA architectural systems and solutions with the DoD Computer Network Defense (CND) operational hierarchy.

Current hardware-based cyber ranges, though realistic, are limited in scale, costly, and time-consuming to configure. Due to their cost, there are only a small number of them, which limits the number of players who can be trained on any executing scenario, and also limits the total number who can be trained annually. Importantly, wired ranges have little or no capability to model wireless tactical networks with their inherent vulnerabilities not found in wired networks. While they can train defenders of the network itself, they do not effectively model the overall impact of a cyber attack on a mission. Thus they do not train all users of the net-centric system, from commander to front line warfighter, on what to expect during cyber warfare and how to react.

Pure Simulation

Another current approach to cyber training is to create scenarios in which the cyber attack is simulated. That is, the attack itself is abstracted, but the effect of it is assumed to have occurred, for example a successful attack against the Domain Name System (DNS). An example of this approach is DHS's biennial Cyber Storm series of exercises. These exercises are effective for establishing strategy and policy and refining procedures in the event of a successful large scale attack. However, the abstract nature of the simulated attacks limits the ability to provide precise training in early recognition and containment of the attacks. The training is directed more toward reaction than prevention.

The Virtual Cyber Range

We are developing a new modeling and simulation framework known as the Virtual Cyber Range. Using software, it emulates how complex networks will behave under battlefield conditions and respond to cyber warfare. It is tightly integrated with physical hardware, live applications, human operators, network monitoring tools, and constructive battlefield simulations, enabling accurate training for the effects of cyber defense and offense on entire mission outcome.

The core of the Virtual Cyber Range is Software Virtual Network (SVN) technology that makes it possible to represent the networking infrastructure at sufficiently high levels of fidelity that applications running on it—such as a mix of sensor data, streaming video, voice communications, web browsing, collaboration, video web conferencing,— can be deployed unmodified on top of large emulated networks of both legacy and future communication devices.

SVNs utilize network emulation technology to provide a high quality, efficient, scalable training environment for cyber operations. Emulation refers to the ability of substituting a real system with a counterpart that is easier to manage while providing the same functionality as the component it replaces. The holistic system is comprised of two parts: the physical component, which is of interest to the designers and evaluators (e.g. machines running Intrusion Detection Software), and an emulated component that "completes" the system (e.g. the wireless channel and waveforms for an operational scenario). For the emulation to be meaningful and useful, it is imperative that no live component in the system can discern differences between a physical component and the corresponding emulated component.

A benefit of the SVN approach is that real equipment can be connected to it, and real application traffic such as sensor feeds, voice communications, or video can be streamed through the emulated network. Thus the effects of the network state and its ability to route traffic to the intended destination along with disruption due to cyber attack can not only be analyzed, but be seen and heard in real-time. Real software loads with their vulnerabilities can also be connected and subjected to attack. Third party network analysis, management and diagnostic tools, such as packet sniffers, SNMP managers etc, 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 model, it becomes possible to train for the side effects of cyber attacks on operational systems.

Within this SVN, cyber warfare 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).

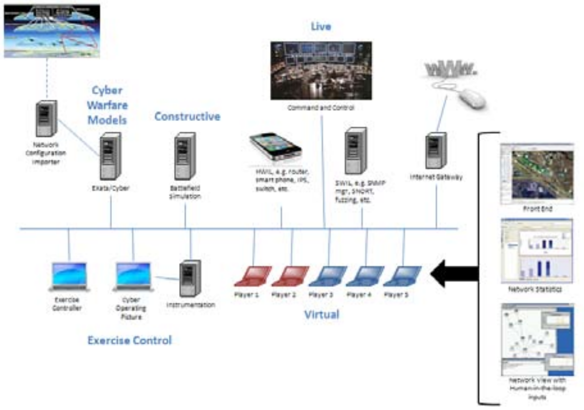

Fig. 1. A Virtual Cyber Range for Training

Figure 1 illustrates an architecture for a Virtual Cyber Range for training. It integrates live, virtual, and constructive elements with the cyber warfare SVN, which in this case is the commercial product EXata/Cyber. EXata/Cyber emulates the battlefield network (tactical radios, enterprise networks, satellites, routers, and other network components) and contains cyber warfare models that are used to attack or defend the network as well as the connected equipment and applications. Real devices (e.g. routers, firewalls, smart phones), live intrusion detection or intrusion prevention systems (e.g. Snort), and live C2 systems (e.g. situation awareness applications) connect and exchange data (e.g. streaming sensor data, VoIP, Unmanned Aircraft Systems control) over the emulated network. The privacy, integrity, or availability of these data can be compromised by cyber warfare, with resulting effects observed on the live equipment. An Internet gateway permits live traffic to be brought into the exercise from external sources, if desired.

Role players participate in the scenario at blue/red stations, with red players using real exploitation and penetration tools to attack the virtual network and the connected live components. The blue role players monitor and defend network, and can launch cyber counterattacks. An exercise controller controls the scenario, assigning privileges and monitoring overall network and equipment status with a Cyber Operating Picture. The exercise controller is also provided with instrumentation that gathers detailed statistics during scenario execution for after action review.

Constructive battlefield simulations are integrated into the Virtual Cyber Range, modeling the behavior of additional friendly and opposing entities. The constructive entities communicate with one another over the software virtual network, with the success of these communications being subject to degradations in the network due to cyber attack. Compromised communications affect the entities' situational awareness and behavior, and therefore overall mission outcome. We have integrated OneSAF, VT MÄK's VR-Forces, and Presagis' STAGE. For the integration, we took advantage of an Interface Control Document (ICD) that works via the HLA signal and data interactions to facilitate communications modeling between HLA federates (Dickens, Wihl, Holcomb, & Aplin, 2009).

We have demonstrated the real-time performance and scalability of the Virtual Cyber Range, and its integration with real equipment, virtual players and constructive simulations. Some networks have been modeled along with some threats and defenses including eavesdropping, jamming (basic and silent), firewalls, virus and worm propagation, denial of service, vulnerability exploitation, operating system resource depletion, SIGINT, routing attacks, port and network scanning, intrusion detection, user behavior, and decision tree-based attacks. The library of cyber threats is modular and extensible and can support diverse threats for all levels of classification.

Example Usage: Time Sensitive Target Training

The following describes an operational use case for the Virtual Cyber Range, highlighting training for the impact of a cyber attack on an Army Time Sensitive Targeting (TST) mission. Figures 2 and 3 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 System Army (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 2, Step 1). In an effort to minimize collateral damage, the Battalion commander radios a reconnaissance team (Figure 2, 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 2, Step 3).

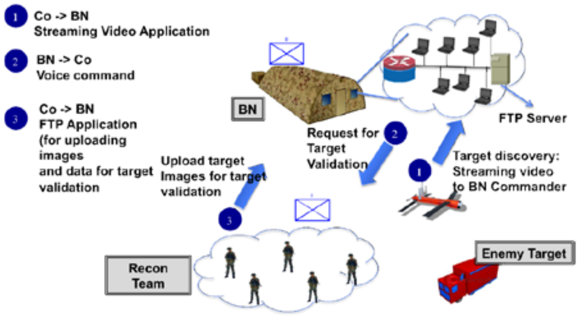

Fig. 2. Discovery, Tracking and Validation of a High Value, Time SensitiveTarget

Figure 3 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 (NLOS) Artillery Battery

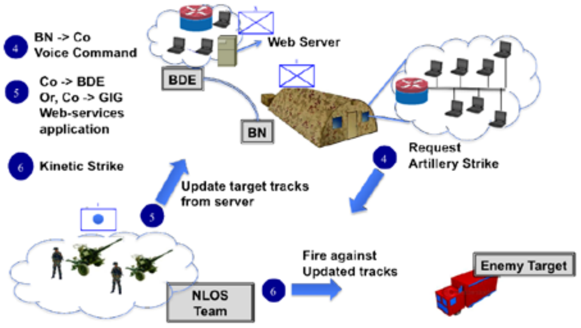

Fig. 3. Tracking and Strike Against a High Value Target

calling for an immediate engagement of the target (Figure 3, 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 3, 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 3, Step 6).

Possible Cyber Attacks Against this TST Mission

The end-to-end description of the TST mission thread represents many of the opportunities for cyber attack available to the threat.

In this scenario, 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 4 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.

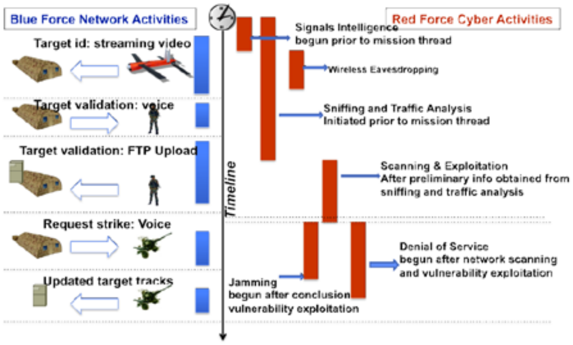
Blue Force Network Activities
Red Force Cyber Activities
Target id: streaming video
Target validation: voice
Target validation: FTP Upload
Request strike: Voice
Updated target tracks
Timeline
Signals Intelligence
begun prior to mission thread
Wireless Eavesdropping
Sniffing and Traffic Analysis
Initiated prior to mission thread
Scanning & Exploitation
After preliminary info obtained from sniffing and traffic analysis
Denial of Service
begun after network scanning and vulnerability exploitation
Jamming
begun after conclusion vulnerability exploitation

Fig. 4. Cyber Threats and Time for Attack Windows in TST Mission

Figure 4 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.

Training With the Virtual Cyber Range

The Virtual Cyber Range was used to assess the impact of two attacks against the TST mission thread. A Silent Jammer (SJ) is a difficult-to-detect attack 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 the TST scenario, recall that the discovery/tracking video from the UAV was RF based.

Making use of the Virtual Cyber Range architecture, we integrated the wireless network model, the silent jammer attack model, and the real sensor feed. In that way, the cyber attack interacts with the live or virtual net-centric application being operated by trainees.

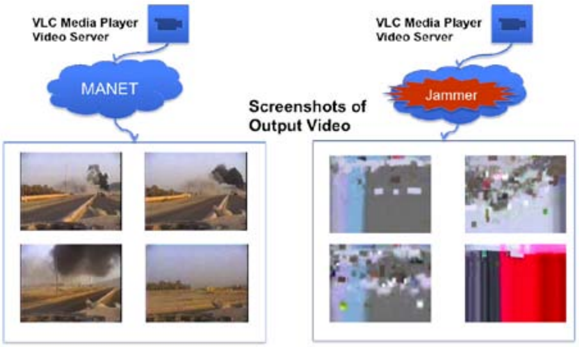

Fig. 5. Impact of Silent Jammers on Video Streams

Figure 5 represents the impact of an SJ on the "video packet rate" for the UAV.

The four images in each set are screenshots from the sensor display at the Battalion intelligence section. Each screenshot was recorded 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 packet loss; 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 scenario execution. This implies that an untrained operator looking at the sensor display cannot conclude that the network link is not operational, and would most likely attribute the poor video quality to poor wireless channel conditions. The untrained operator would not suspect that switching to an alternative, non-jammed data rate could restore the video. The operator could be trained to visually recognize differences between poor reception and silent jamming, and learn when to use SIGINT to look for a silent jammer's location so that it could be destroyed.

The second case evaluated using the Virtual Cyber Range was a DDOS attack on the Blue Brigade Web Server. Recall from Figure 3 Step 5 that the tracks were fused and passed to the NLOS Commander through the Brigade web server. Figure 6 shows a notional architecture of 5 attackers launching an attack against the Brigade firewall/web server. The attacks use the TCP SYN denial of attack model where each attacker continuously sends the SYN packets to force the web server to open new TCP connections and thus allocate memory for each new connection. After a number of these new connections, the web server will have consumed all available memory resource, crash and shutdown.

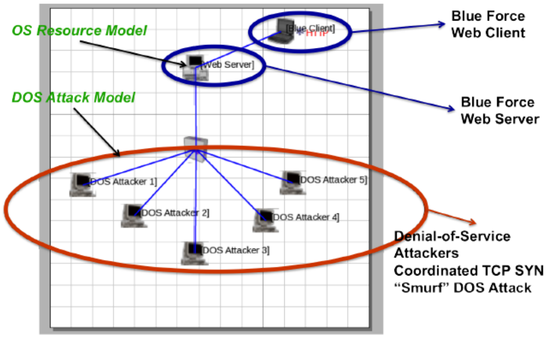

Fig. 6. Architecture of a DDOS Attack Against the Brigade Fire Wall in TST Scenario

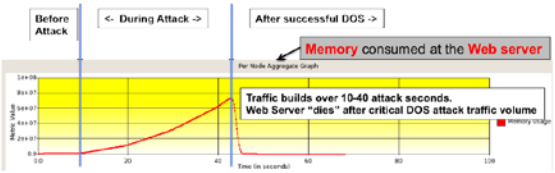

Fig. 7. Impact of 5 cyber attackers launching attack against Brigade firewall.

In Figure 7 we see the impact of this attack over a 40 second period as the server is overcome with message traffic. The curve shows the amount of memory used by the web server over time. The time-axis is divided in three phases: Before Attack, During Attack, and After Successful DOS. Before the attack, the memory usage at the web server was minimal since only a few clients were connected. During the attack phase, the memory usage increases steadily until it reaches the critical limit, at which point the node shuts down. With the configurations of attack traffic rate and the memory capacity, the interval between commencement of attack to its successful culmination is 40 seconds.

The importance of these 40 seconds is critical to the Blue mission as it impacts the download and tracking of the target by the NLOS commander. In short, the engagement must take less than 40 seconds or the trainee must recognize the attack and invoke a recovery procedure (use of an alternate server) in less than 40 seconds for the mission to be successful.

This sample scenario with cyber attacks illustrates a few key points. Mission success can be very dependent on operators quickly recognizing and taking action in response to cyber attack. Training for recognition and rapid, correct response, and understanding the consequences of late or incorrect action is essential. Training (or analysis) of how this time sensitivity affects a mission can be greatly improved over traditional hardware ranges, using a Virtual Cyber Range that integrates cyber attacks, live, virtual and constructive components and a Software Virtual Network.

CONCLUSION

Using modeling and simulation, the authors have created a Virtual Cyber Range for training for the attack/defense of network centric systems. The integration into a LVC environment provides an improved assessment of the impact of cyber warfare on operational systems and force effectiveness.

The key technical benefits the Virtual Cyber Range holds over a traditional hardware cyber range include scalability to thousands of nodes, the ability to accurately train for defense of both wired (GIG) and wireless (tactical) environment, and the ability to integrate with existing trainers to evaluate overall mission effects.

Other benefits include significantly lower cost than hardware ranges, reduced setup time, repeatability and transportability. A valid training baseline could be replicated or scaled down and installed at any military base, allowing significantly higher numbers of trainees to pass through the system. Scale and flexibility are achieved by having most of the system simulated, with specific equipment added as needed wherever it is located.

REFERENCES

Dickens A., Wihl L., Holcomb B., & Aplin R. (2009), "*Interfacing a Communications Effect Model to Provide Accurate Modeling of Communications in Computer Generated Forces,"* Interservice/Industry Training, Simulation & Education Conference *(*I/ITSEC) 2009 Conference Proceedings.

Yih-Chun Hu, Adrian Perrig, David B. Johnson, "*Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks*", in Proceedings of the 22nd IEEE INFOCOM, 2003.

Powell R., Holmes T., Pie C., *"The Information Assurance Range,"* International Test and Evaluation Association (ITEA) Journal 2010; 31: 473-477.

Wihl L., Varshney M., & Kong J. (2010), "*Introducing a Cyber Warfare Communications Effect Model to Synthetic Environments,"* Interservice/Industry Training, Simulation & Education Conference *(*I/ITSEC) 2010 Conference Proceedings.