Enhancing Wargaming Fidelity with Network Digital Twins

Ha Duong, Jeff Hoyle, Jeff Weaver, Ung-Hee Lee, Rajive Bagrodia
SCALABLE Network Technologies
Culver City, CA
{hduong, jhoyle, jweaver,ulee,rbagrodia}@scalable-networks.com

ABSTRACT

Human decision-making fundamentally relies upon communications and networks to contain, extract, and disseminate time-sensitive, mission-relevant information to win decisively against opposing forces, particularly when engaged in asymmetrical combat. Future conflicts will involve attempts to disrupt information systems that are critical for communication and for assured operation of highly sophisticated weapons systems. Disruption is already a capability of potential adversary forces and will spread to secondary threats allied to them. This creates an urgent need for wargames to incorporate real-world cyber, communications and networking effects to support development of effective operating concepts, capabilities and plans. The complexity of a multi-domain, combined cyber and kinetic battlefield requires incorporation of high fidelity, physics based Network Digital Twins into future wargaming environments to adequately account for potential impacts resulting from degraded network operations and/or cyber vulnerabilities on overall mission outcomes.

A Network Digital Twin refers to a computer simulation model of the communication network together with its operating environment and the application traffic carried by it. It can be used to enhance overall wargaming fidelity in a low-cost and zero-risk environment, improving the knowledge and insights gained from wargame execution. In order to do so effectively, the Network Digital Twin must have sufficient fidelity to accurately reflect the network dynamics due to the interplay between the communication protocol and topology, application traffic, the physical environment, and cyber attacks, thus appropriately discriminate among cyber attacks that are a mere annoyance from those that have the potential to disrupt the mission timeline.

This paper will present a case study on the use of an innovative and unique prototype to incorporate high fidelity cyber, communications and networking simulation into a wargaming environment. This prototype establishes an interface between the Advanced Framework for Simulation, Integration, and Modeling (AFSIM) and a proposed Network Digital Twin of high fidelity, physics-based cyber, communications, and networking modeling and simulation software to incorporate real-world connectivity and cyber vulnerability effects. Distributed Interactive Service (DIS), an IEEE standard interface, is leveraged to provide a reliable and standards-compliant interface between AFSIM and the proposed Network Digital Twin. The resulting prototype capability enhances wargaming capability by enabling physics-based cyber, communications and networking simulation driven by authoritative device configurations, network topology, and environmental and terrain data sources to better assess overall mission outcomes that incorporate realistic cyber and connectivity effects.

ABOUT THE AUTHORS

Dr. Ha Duong is Principal Engineer at Scalable Network Technologies where he has worked on modeling JTRS waveform for the Communication Effects Server (CES) project in the context of the Future Combat System (FCS) and Brigade Team Modernization (BCTM) programs. Over the past several years, Dr. Duong has focused on modeling vulnerabilities and cyber attacks in the StealthNet project at SCALABLE, and leveraging those models into the JTRS Network Emulator (JNE) product and the Cyber Test Analysis and Simulation Environment (CyberTASE) project. Dr. Duong has also led the Human-centric Training and Assessment System for Cyber Situational Awareness project. His current research interests include LVC-based cyber-attack representation, modeling and simulation techniques to represent complex operations in simulation environments, and analysis of cyber effects on DoD tactical networks.

Dr. Jeffrey Weaver is Vice-President of Engineering at SCALABLE. He obtained his Ph.D. degree in Electrical Engineering as an NSERC-PGS Scholar from Western University in Ontario, Canada. Dr. Weaver has held key

technical and executive engineering roles during his career and has over twenty years of product development experience in hardware and software systems. His research interests include digital communication and propagation modeling using switched stochastic differential equations, signal processing and hybrid analytical-numerical modeling techniques. Dr. Weaver has seven patents in the areas of IP routing, VLAN, QoS, and high-performance hardware design.

Captain Jeff Hoyle (US Navy, Retired) leads Scalable Network Technologies communications and networking developments for the Department of Defense and Intelligence communities. Prior to joining Scalable, he served as Director of Advanced Maritime Programs for Northrop Grumman Aerospace Systems, a leading provider of military autonomous systems, and Director of Technology and Navy Programs for AtHoc, Inc., a leading provider of crisis communications capabilities to multiple Federal agencies. While on active duty, Captain Hoyle supervised all aspects of US Navy operations on five submarines and one aircraft carrier, including command of USS MAINE (SSBN 741) and ten deployments to forward operating regions on missions vital to national security. As a Defense Acquisition Program Manager, he led development of submarine exterior communications systems and joint tactical networking capabilities for the Army, Navy, Air Force and Marine Corps.

Dr. Ung-Hee Lee is the Chief Engineer at SCALABLE. He has 20 years of experience in computer networks and military waveforms. His research interests include multi-channel routing/MAC protocols, MANET routing protocols, and computer network simulation and emulation. He has spent over a decade with SCALABLE, and serves as the chief software engineer for a wide variety of projects in the realm of wireless military communications. Currently, Dr. Lee is leading a project supporting PM-WINT in U.S. Army for the low-tier communication emulation environment with various waveforms. Dr. Lee has led the technical design for a number of SCALABLE projects, including many of the model libraries in the Joint Network Emulator (JNE). Dr. Lee holds B.S. and M.S. degrees in Computer Science from Inha University, Korea and a Ph. D. (Computer Engineering) from Virginia Tech.

Dr. Rajive Bagrodia is the founder of Scalable Network Technologies, Inc. and an Emeritus Professor of Computer Science at UCLA. He obtained his Ph.D. degree in Computer Science from the University of Texas at Austin. Dr. Bagrodia has published over 150 research papers in refereed journals and international conferences on high performance computing and communication. At SCALABLE, Dr. Bagrodia initiated the design and development of the Communication Effects Server (CES) for the Future Combat System Program. The contribution of the CES in advancing the modeling and simulation of DOD communication systems was recognized by an Army M&S Award in the Acquisition category.

Enhancing Wargaming Fidelity with Network Digital Twins

Ha Duong, Jeff Hoyle, Jeff Weaver, Ung-Hee Lee, Rajive Bagrodia
SCALABLE Network Technologies
Culver City, CA
{hduong, jhoyle, jweaver, ulee, rbagrodia}@scalable-networks.com

INTRODUCTION

In wargames, the ability to extract and disseminate time-sensitive, mission-relevant information is critical to win decisively against opposing forces. This, in turn, depends on the underlying communion network and the kinetic and cyber threats that it is exposed to, which can seriously degrade the network's ability to provide reliable communications. But many wargaming platforms assume perfect communications and do not account for the threats and consequent degradation that the network is subjected to. Future conflicts will involve attempts to disrupt information technology systems that are critical for communication and for assured operation of highly sophisticated weapons systems. This creates an urgent need for wargames to incorporate real-world cyber, communications and networking effects to support development of effective operating concepts, capabilities and plans. The complexity of a multi-domain, combined cyber and kinetic battlefield requires incorporation of high fidelity, physics based Network Digital Twins into future wargaming environments to adequately account for potential impacts resulting from degraded network operations and/or cyber vulnerabilities on overall mission outcomes.

In this paper, we present a technical prototype and case study where a Network Digital Twin is used to incorporate high fidelity cyber, communications and networking simulation into a wargaming environment. In the next section, we describe what we mean by a Network Digital Twin and how it can be used. We then describe a method for creating Network Digital Twins followed by a description of the digital twin interfaces for wargaming. Lastly, we illustrate the use of digital twins in war games by means of use case.

NETWORK DIGITAL TWINS

One approach to incorporating realistic cyber and communication effects in wargames uses a Network Digital Twin. A Network Digital Twin refers to a digital replica of the physical communication network along with its operating environment and the traffic that it carries. In essence, a Network Digital Twin is a computer program that takes real-world data about a physical object or system as input and produces as outputs predications or simulations of how that physical object or system will be affected by those inputs. The digital twin can be used to study the behavior of its physical counterpart under a diverse set of operating conditions, including cyber attacks, in a low-cost and zero-risk environment. In order to do so effectively, the Network Digital Twin must have sufficient fidelity so as to accurately reflect the network dynamics that can cause networks to behave unpredictably. Thus the Network Digital Twin must reflect all the components which contribute to the network dynamics, including communication protocols, device configurations, network topology, application traffic, physical environment, and any cyber threats. Moreover, the Network Digital Twin should run faster than real-time so that it can be used for efficient 'what if' analyses such as monitoring the behavior of the system under different network configuration settings, varying traffic distributions, and diverse cyber threats using stochastically generated traffic profiles. For wargaming exercises, live hardware and software applications can be seamlessly interfaced with, or integrated into, a Network Digital Twin that executes in real-time. These real-time Network Digital Twins can then be used to provide a realistic platform for war games which represents all aspects of the mission and the underlying communication network, so that kinetic, communication, and cyber effects can be effectively incorporated in the war games. Digital twins can also integrate things like artificial intelligence (AI) and machine learning (ML) to bring data, algorithms, and context together, making it possible to test new ideas and uncover problems before they occur.

In particular, a Network Digital Twin can be a very cost effective tool to test cyber resilience of wargaming systems. Performing cyber test on live wargaming systems can be a difficult and challenging task, but many of the common challenges with cyber testing can be resolved effectively by applying a Network Digital Twin, such as:

- Large-scale wargaming system: It is difficult to test live large–scale wargaming systems due to time and resource constrains. A Network Digital Twin can replicate the whole or a segment of the wargaming system, making large scale tests more feasible.
- Cyber threats: Network Digital Twins can increase the scope of cyber resilience test as many cyber attacks, especially active attacks such as vulnerability exploitation, virus/worm propagation, or DDoS (Distributed Denial of Service), can be performed on models without the risk of compromising the system.
- Extending a test: Post-test analysis and After Action Review (AAR) often identify additional test cases that might lead to a more comprehensive understanding of the system operation and potential mitigation of threats, for example, "what would be the result of turning off the compromised router and activating the backup router to provide an alternative path for mission data flow". Such tests can be easily and quickly set up in a Network Digital Twin.
- Effective test planning: A Network Digital Twin can run multiple configurations and profiles to prioritize test cases and to make effective and justifiable selections.

CREATING ACCURATE NETWORK DIGITAL TWINS

The Network Digital Twin must have sufficient fidelity to capture the network dynamics and thus appropriately discriminate among cyber attacks that are a mere annoyance from those that have the potential to disrupt the mission timeline.

For example, the position, intensity, and type of a jammer or denial of service attack that is used by an adversary will determine if the communications that are critical to the wargaming mission are disrupted by that attack. The interference needed to disrupt streaming video, may be very different from that needed to disrupt Position Location Information (PLI). In order to answer such a question, the digital twin must accurately represent the communication network with sufficient fidelity.

A proposed Network Digital Twin to help answer the example question consists of the following elements: network topology, device configuration, host profile, traffic profile, and vulnerabilities. Each element can be represented by one or more system artifacts as shown in Table 1.

Table 1: System Artifacts of a Network Digital Twin

Element of Network Digital Twin	System Artifacts
Network Topology	Visio diagram files, Network monitoring & management tools (e.g., HP Network Automation)
Device Configuration	Cisco configuration files
Host Profile	Reports from scanners such as NMAP, SolarWinds, Nexpose, Nessus
Traffic Profile	PCAP files, NetFlow records
Vulnerabilities	Vulnerability database (https://nvd.nist.gov)

Some system artifacts are more widely applicable, whereas others may be associated with proprietary devices. For a wireless environment, additional system artifacts such as path loss values for radio frequency (RF) signal propagation and nodes' mobility patterns may also be used.

Figure 1 shows the process of importing artifacts in our proposed prototype for this example. The first step is to import the network topology to lay down the initial infrastructure for the wargaming scenario. The imported network topology may not adequately reflect the infrastructure for the wargaming scenario and may require some refinement. If topology refinement is needed, it is done manually. In subsequent steps, device configuration, host profile, and traffic profile artifacts are imported to create the initial device configuration, host profile, and traffic profile,

respectively, for the wargaming scenario. These are manually refined, if needed, to accurately reflect the characteristics of the wargaming scenario.

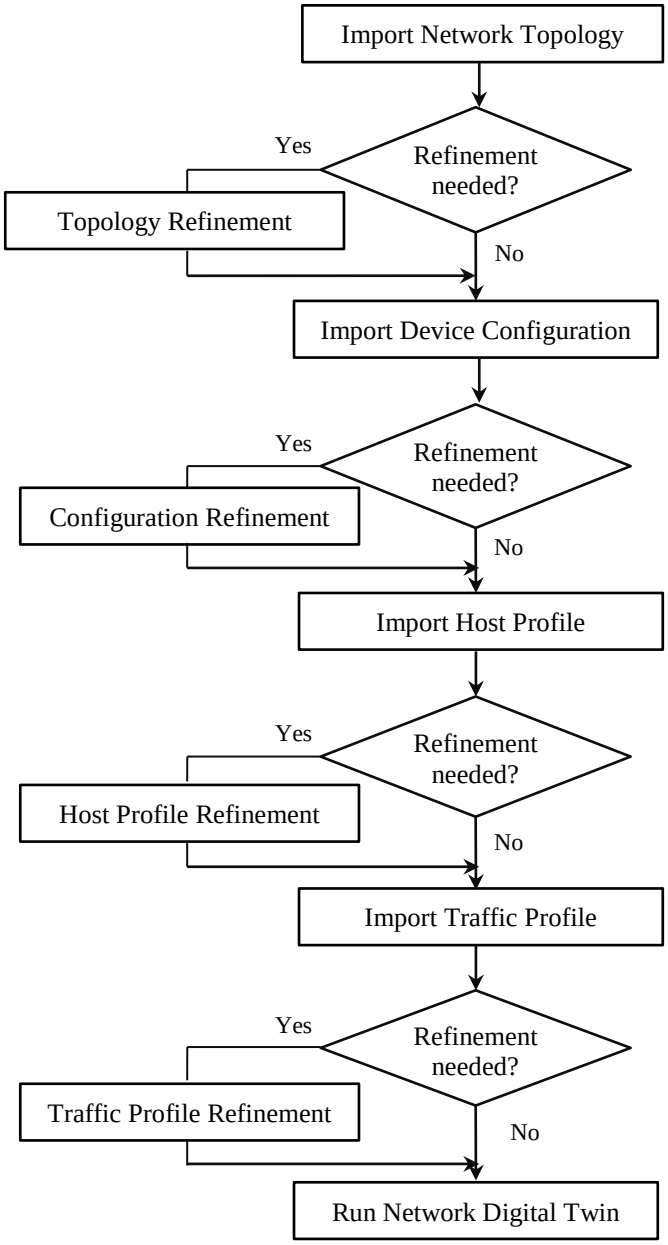

Figure 1: Importing System Artifacts

Our proposed Network Digital Twin also employs a vulnerability model which uses the following attributes defined by the National Vulnerability Database (https://nvd.nist.gov/)

- Attack vector:
  - Access vector: Local, Adjacent Network, Network
  - Access complexity: High, Medium, Low
  - Authentication: Non Authentication, Singe Instance, Multiple Instances
- Impact vector:
  - One or more impact types: Confidentiality, Integrality, Availability (often called the CIA impact)

  - Each impact type has impact level rated as No Impact, Partial, Complete
- System Services which need to be present (i.e., application software or OS) for the vulnerability to be applicable
- Action to be taken when the vulnerability is exploited

The list of vulnerabilities obtained from the NVD database can be imported into the Network Digital Twin, and then specific vulnerabilities can be configured using a host profile. An example in the sub-section "Building Network Digital Twin" will illustrate this attribute.

INTERFACES OF A NETWOK DIGITAL TWIN

For the Network Digital Twin prototype, we propose a set of interfaces that enable providing communication and cyber effects to external systems such as OneSAF or Advanced Framework for Simulation, Integration, and Modeling (AFSIM).

Communication and Cyber Effects

When interfacing with the AFSIM, the Network Digital Twin simulates nodes (platforms) in AFSIM as communication devices with appropriate network topology and links. Traffic from AFSIM will be sent to Network Digital Twin through an external interface such as Distributed Interaction Simulation (DIS), and will travel from the source node to the destination node. During transit from the source to the destination, traffic is subject to communication effects, such as routing and transmission delays, effects of link capacity and queue sizes, etc. If communication between two nodes along the path takes place over a wireless link, the operation model will take in to account the characteristics of RF transmission, antenna properties, path-loss due to attenuation, fading and shadowing, interference from other transmissions and the impact of terrain and weather on the transmitted signal. Packets reaching the destination node will be injected back into AFSIM via the DIS interface. Depending on network conditions, the packets may be delivered after a delay or may be dropped because of, for example, queue overflow or no routes to the destination. If the Network Digital Twin is composed of high fidelity models of network components, the traffic through the Network Digital Twin will undergo the same communication effects as traffic in the real network.

Beside communication effects, a Network Digital Twin can model cyber attacks which cause cyber effects on the network traffic. For instance, a specific attack vector, such as a compromised router, can be used to launch a worm attack to install bots across the simulated network. In turn, these bots can be used to trigger a Denial of Service attack on the emulated network which could result in degraded communications.

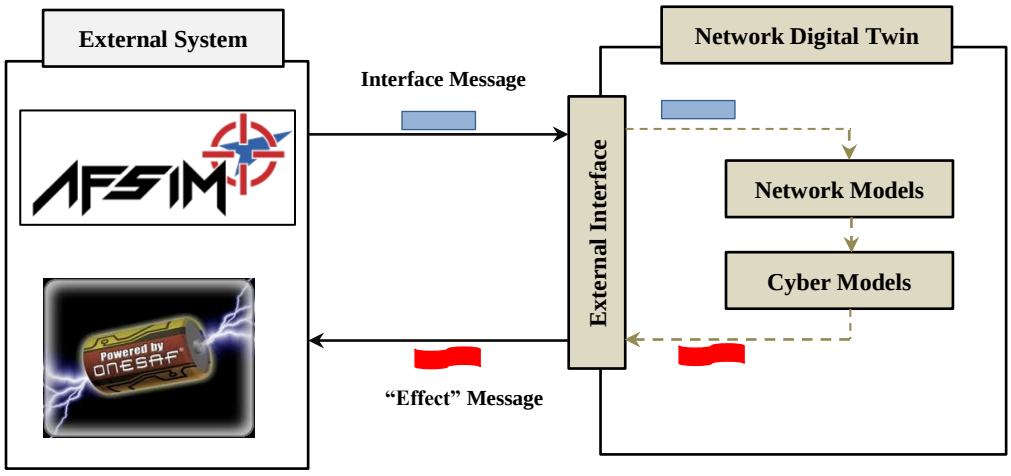

Figure 2: Network Digital Twin's Interfaces

Update Platforms' Positions
As platforms from AFSIM move according to the mission plan, the updates in platforms' positions can be made available to Network Digital Twin via an *Update* message sent through the DIS interface. The Network Digital Twin processes the Update message and updates the position of the platform's equivalent in the digital twin, which, in turn, can affect the propagation path, path-loss, etc.

Update Platforms' Status
A platform in AFSIM may become disabled due to, for example, damage from enemy's strike, and thus not be able to communicate with its peers. This "disabled" status can be communicated to Network Digital Twin via the DIS interface so the corresponding node within the Network Digital Twin will be turned off. This means communication to, from, or via this platform is no longer possible, thus impacting the mission execution.

USE CASE SCENARIO: OPERATIONAL LEVEL FIRES DURING AMPHIBIOUS LANDING

Description
The Naval Expeditionary Strike Group (ESG) has deployed a Marine Air Ground Task Force (MAGTF) ashore as part of a forced entry into a hostile country. Marines ashore come under heavy enemy fire and require fires support from the ESG. The AFSIM-DIS-Network Digital Twin prototype models the necessary communications network to request and implement fire support from multiple air and sea-based platforms, as well as enemy activity to defeat the necessary communications such as physical layer jamming and cyber attacks to disrupt communications and/or inject false information into communications transmissions such as incorrect Blue Force locations or Red Force target positions.

For this scenario, we evaluated an opposing force cyber tactic and employed various counter cyber tactics. We evaluated the effectiveness of the counter measures by computing the message delays and the change in the content of the message.

Scenario Assumptions
Blue Force entities include a Marines platoon ashore, a Naval ESG, and a Fire Support Unit from a carrier. Each entity has its own internal network, and uses satellite links to communicate with each other.

- The Marines platoon uses a TDL (Tactical Data Link) such as ANW2 to communicate among themselves
- The Naval ESG runs an enterprise-like network
- The Fire Support Unit also employs an enterprise-like network and a TDL network

The logical network laydown is as shown in Figure 3.

It is assumed that the Red Force has RF scanning capability to scan the TDL network, and is therefore able to set up an attack vector into the Marine Platoon's network. In addition to RF scanning capability, the Red Force is able to iterate through the steps of the Cyber Kill Chain model (*Hutchins E., Cloppert M. and Amin R. [2011]*) such as reconnaissance, weaponization, delivery, exploitation, and installation on ESG network, and ready to launch cyber attack during mission execution.

As AFSIM runs the mission execution, it continuously provides communication requests and platform updates to the Network Digital Twin for modeling effects. Alternatively, a mission timeline tool (*Ha Duong, Brian Salisbury, Rajive Bagrodia, and Scot Dietz [2018]*) can also be used to model mission activities in a chain manner. An example of a possible mission timeline is shown in Figure 4.

A criterion of successful mission completion is that the Marine Platoon lands safely at the planned location in the hostile country within the time threshold.

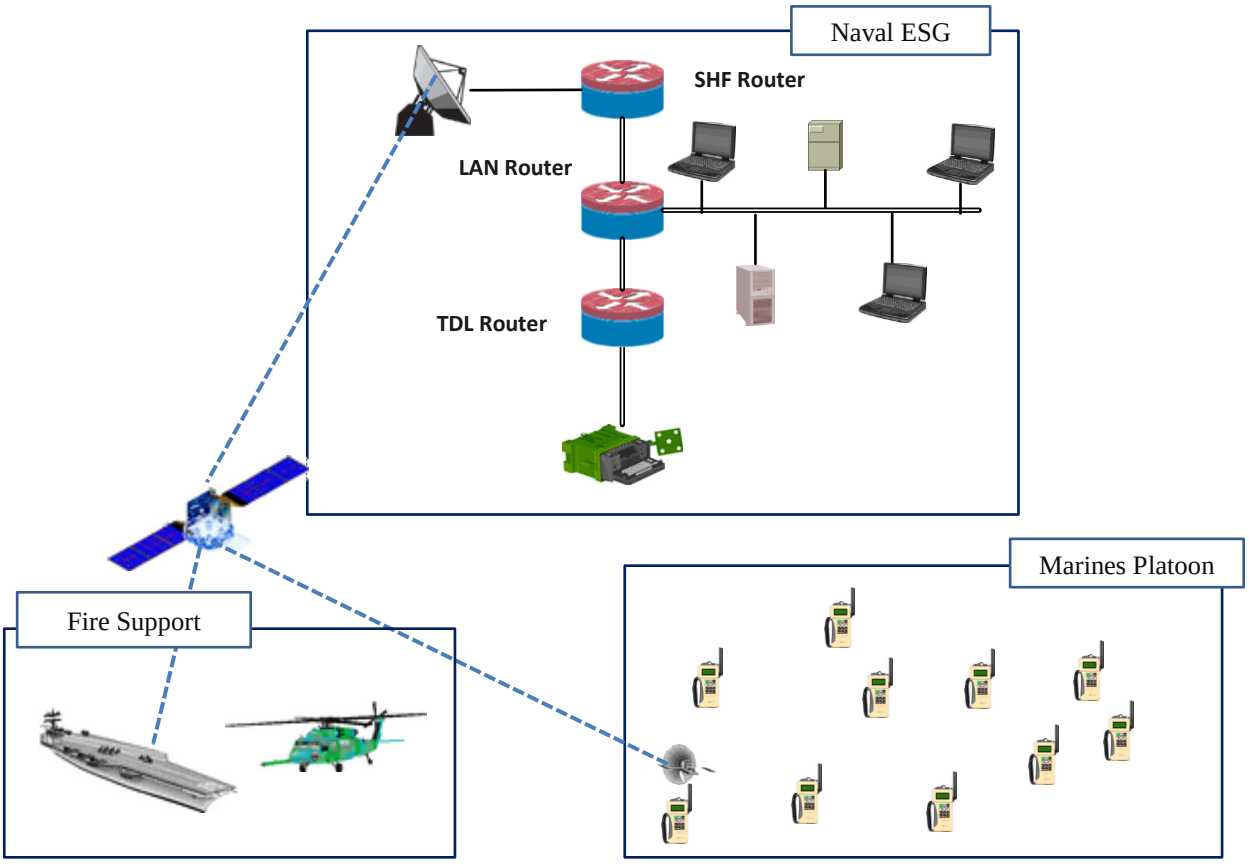

Figure 3: Network Laydown for Operational Level Fires Scenario During Amphibious Landing

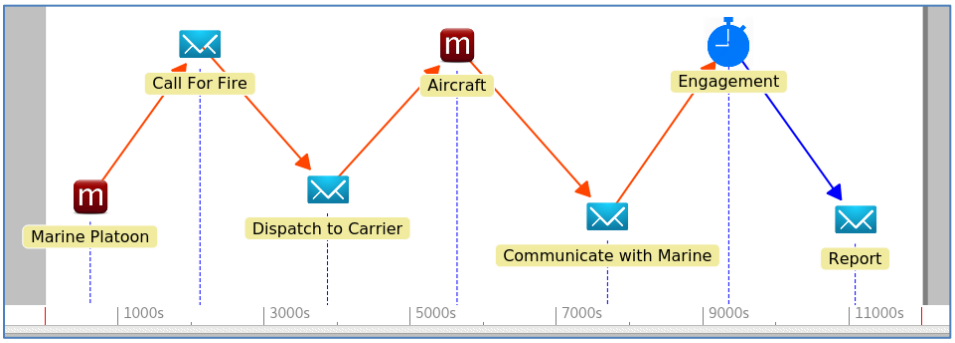

Figure 4: Mission Timeline

Building Network Digital Twin

To build the scenario, we will leverage existing system artifacts as much as possible. In most cases, system artifacts of network topology and traffic profile are likely available and make up of most of the Network Digital Twin.

In this use case, we import the Naval EGS network topology in the form of a Visio file using the Topology Converter utility. As the Visio file describes the network via shapes and connections between them in XML format, the Topology Converter utility will process XML elements and build the equivalent Network Digital Twin.

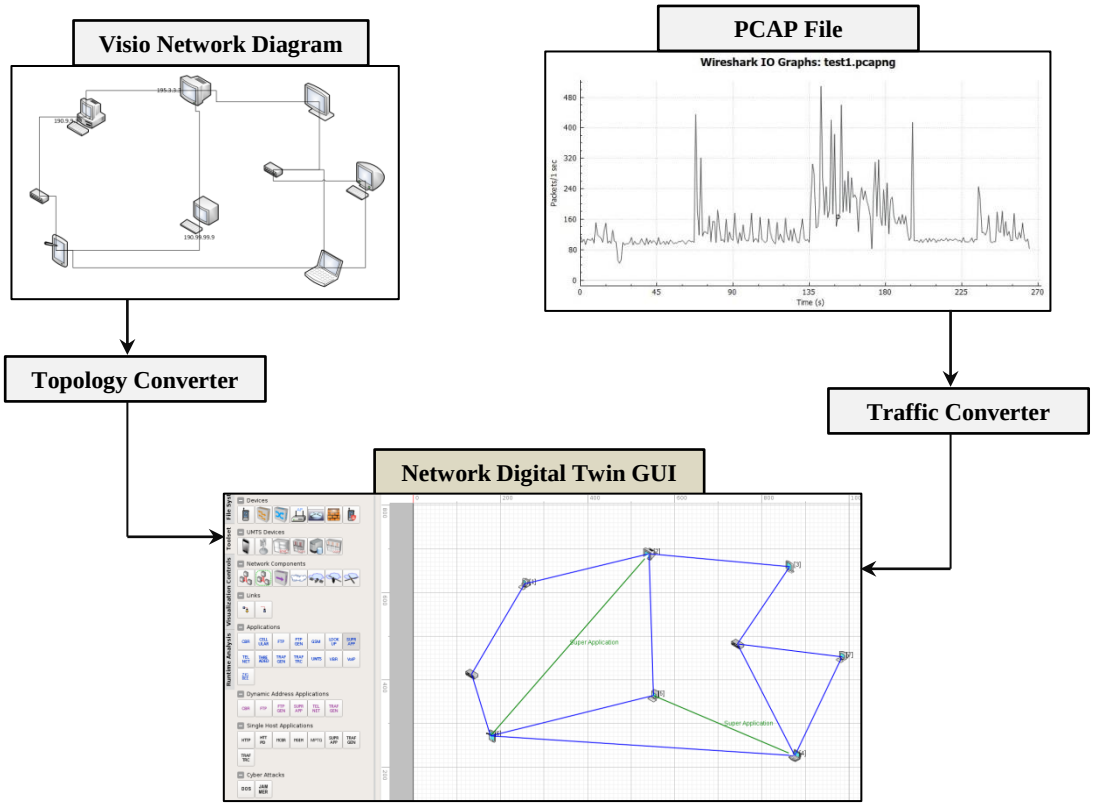

Figure 5: Applying Network Digital Twin

Another system artifact is a PCAP (Packet CAPture) file, a file in the libpcap format used in TcpDump/WinDump, Snort, and many other networking tools. In our Network Digital Twin, the PCAP file can be used in the following ways:

- PCAP playback in the scenario
- Aggregating flows in PCAP file(s) to generate various traffic profiles

When playing back the PCAP file, we can use the exact playback or flow playback. In an exact playback, IP packets are injected into the scenario in the same timeline in which the packets were recorded. Each packet is injected at the node specified by the source address from the IP header, travels along the network, and stops at the network layer of the destination node specified by the destination address from the IP header.

In a flow playback, the Traffic Converter utility examines each flow from the PCAP file to decide how each packet is injected into the scenario. For example, we can assume that a subsequent packet was sent as the result of receiving the previous packet (this is called packet chain), as shown in Figure 6.

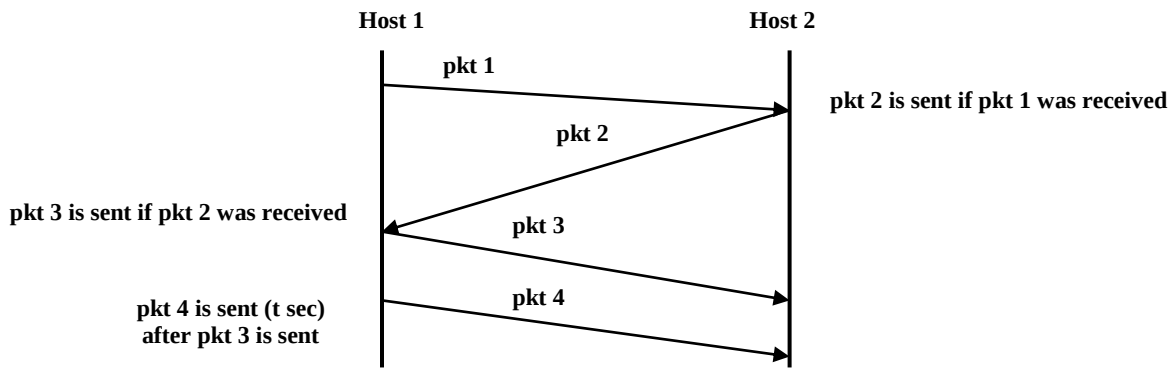

Figure 6: PCAP Flow Playback

Finally, we can aggregate flows into a PCAP file and scale them in various ways to generate different traffic profiles. This feature is useful when the recorded PCAP file only represents a small fraction of the entire network traffic but can still be used to produce larger, meaningful traffic profiles.

We can also configure a "host profile" from the list of vulnerabilities imported from the NVD database. For each vulnerability, a set of system services (i.e., software) has been identified as the condition for vulnerability's presence. In other words, if a host is configured to run those sets of system services, it inherits the vulnerability as described in the NVD database.

As shown in Figure 7, a list of vulnerabilities (CVE-2016-xxxx) is imported into the Network Digital Twin and we can select the system service "Microsoft Windows 7" in the host configuration.

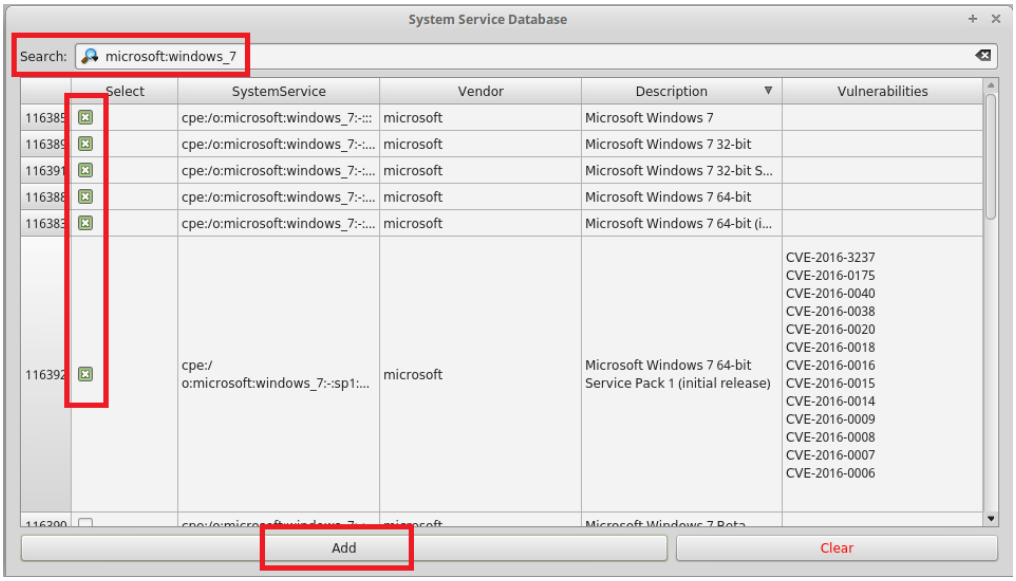

Figure 7: Configuration of Host Profile

Running Wargaming with Network Digital Twin

Once the Network Digital Twin scenario is built, we can set up the test-bed that comprises the AFSIM, the Network Digital Twin and the DIS interface between them. The scenario can be run in scripted or interactive modes.
In the scripted mode, all actions of the Blue and Red Forces are pre-configured. This mode is useful for "what-if" analysis that requires a large number of runs to accommodate various scenario conditions and behaviors.

In interactive mode, actions are performed by players during the run through a Human-In-The-Loop (HITL) interface. This mode can be used for training. In this mode, certain actions, for example, cyber attacks by the Red Force, can be scripted to create specific and repeatable scenario behavior for the training.

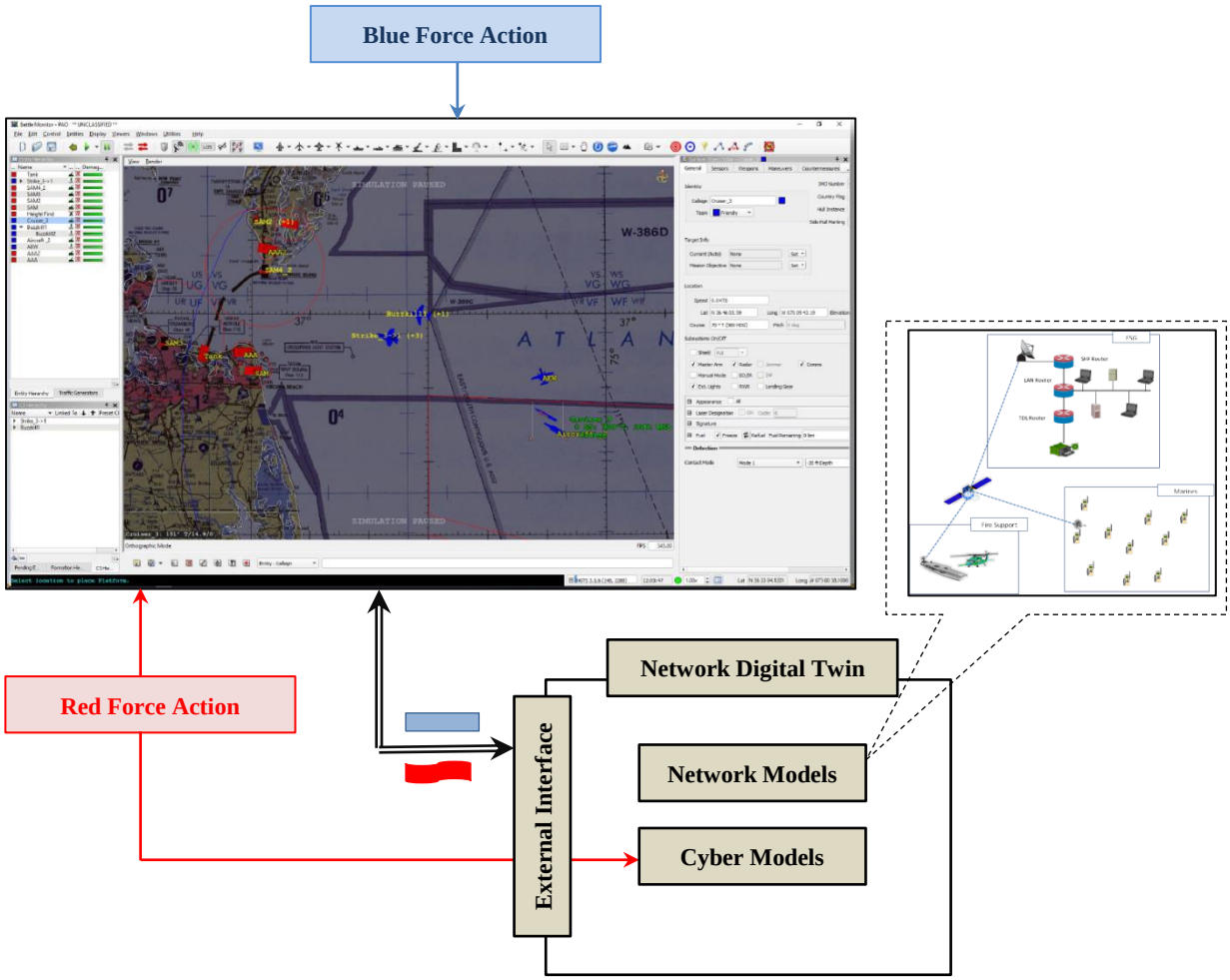

Figure 8: Running Wargaming with Network Digital Twin

Performance Analysis

The analysis will include network performance similar to LVC-TE based training systems (*Luis E. Velazquez, Lloyd Wihl, Ha Duong, Jeff Weaver, and Jeff Hoyle [2018]*). The assessment on network performance is conducted in various scenarios without and with cyber attacks.

In addition, mission completion is also assessed using the stated criteria, i.e., the Marine Platoon lands safely at the planned location in the hostile country within the time threshold. The analysis will break the mission timeline into multiple segments (or mission milestones) and track status of each milestone during mission execution. For example, in a scenario under cyber attack, a mission segment "Call For Fire" is delayed, resulting in an impact on subsequent segments. We can re-run the scenario with the Blue Force's counter-measures to assess whether the mission can be completed with the counter-measures in place.

SUMMARY

In this paper we presented the concept of a Network Digital Twin that can be used to enhance wargaming fidelity. With the capability to import system artifacts, the Network Digital Twin can be quickly set up and used with

external gaming systems to provide communication and cyber effects. Currently the proposed Network Digital Twin supports various system artifacts such as network topology, traffic profile, host profile, device configuration and vulnerabilities. A use case employing the AFSIM and DIS interface with Network Digital Twin was presented to illustrate the application of the Network Digital Twin in a tactical wargaming scenario.

Network Digital Twins can be used in much wider environment such network deployment, maintenance, and upgrade, as well as testing. For example, the Network Digital Twin can help developers of network instrumentation tools to set up various systems to test the tool, and when deployed, train IT personnel to use the tool. "What-If" analysis can be performed on a Network Digital Twin where an operational network can be transferred into models; extensive analysis can be performed to help make network changes or evaluate system patches.

REFERENCES

Hutchins E., Cloppert M. and Amin R. (2011) *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lockheed Martin White Paper, from https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Luis E. Velazquez, Lloyd Wihl, Ha Duong, Jeff Weaver, and Jeff Hoyle (2018), *Effective Deployment of LVC-TE on Wide Area Networks*, I/ITSEC 2018.

Ha Duong, Brian Salisbury, Rajive Bagrodia, and Scot Dietz (2018), *Assessing Cyber Resilience of Military Systems Using LVC Models*, I/ITSEC 2018.