Introducing a Cyber Warfare Communications Effect Model to Synthetic Environments

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

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

Jiejun Kong
Scalable Network Technologies
Los Angeles, CA
jkong@scalable-networks.com

ABSTRACT

Network-Centric Warfare (NCW) is characterized by geographically dispersed forces maintaining a high level of situational awareness, allowing increased combat effectiveness. Computer network operations (CNO) are becoming an effective weapon to undermine the capability of net-centric systems. Hence, there exists an urgent need to evaluate and train for *vulnerabilities* and *resilience* of net-centric military systems to computer network attacks from multiple, diverse, and (possibly) coordinated threats on communication networks.

Published research and initial investigations have demonstrated efficacy of countermeasures to security threats. However, such countermeasures to security threats are evaluated *in isolation*, that is, their side-effect on other operational systems have not been considered nor has their impact on other metrics such as force effectiveness been analyzed.

In a synthetic environment, the communication capability is often simulated at a very low fidelity, rarely accurately modeling network constraints. As a result, communications effects are not well considered, often causing actions resulting from near perfect communications to be unrepresentative of reality, contributing to negative analysis and training.

This paper examines and analyzes the impact of using a cyber warfare communication model versus the limitations of simplified communication models in existing synthetic environments.

The authors have created a test bed for the attack/defense of networks that allows integration into a live, virtual and constructive (LVC) environment. Utilizing this framework with commercially available communications and entity simulation software, the authors examine the impact of cyber threat communication modeling on successful analysis and training results.

ABOUT THE AUTHORS

Mr. Lloyd Wihl joined Scalable Network Technologies (SNT) in January 2006, where he is Senior Application Engineer, providing worldwide pre-sales support for potential clients, developing system prototypes and technology interfaces, guiding future product development, providing guidance for customer model development, training customers, and managing customer engineering service contracts.

Mr. Wihl has over 29 years of experience in the Modeling, Simulation and Training industry. His experience prior to SNT 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 holds a Bachelor of Engineering (Mechanical) with distinction, 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 five 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.

Dr. Jiejun Kong is a Senior Engineer at Scalable Network Technologies, Inc. He received his PhD in Computer Science from the University of California at Los Angeles in 2004. He is interested in developing efficient, scalable, and secure network protocols for wireless networks. His research topics include secure and anonymous routing, authentication, access control, distributed data harvesting, and network security modeling in mobile wireless networks, in particular, those with challenging network constraints and high security demands, such as mobile ad hoc networks and underwater sensor networks. He has contributed to the design, implementation, and testing of network protocols within the NSF iMASH, ONR MINUTEMAN/STTR, and NSF WHYNET projects. He is currently working in Scalable Network Technologies, Inc. on network and cyber security.

Introducing a Cyber Warfare Communications Effect Model to Synthetic Environments

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

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

Jiejun Kong
Scalable Network Technologies
Los Angeles, CA
jkong@scalable-networks.com

INTRODUCTION

Information Operations can be an effective weapon to undermine the capability of net-centric systems. Known Computer Network Attack (CNA) methods range from physical threats like jamming to advanced threats like Denial of Service, wormhole attacks, and passive eavesdropping to discover critical nodes, which, when disabled, can cause systemic failures in the communication infrastructure. Hence, there exists an urgent need to evaluate and train for vulnerabilities and resilience of net-centric military systems to computer network attacks from multiple, diverse, and (possibly) coordinated threats on communication networks.

In cyber warfare, the network is the battlefield. Wireless networks, especially mobile networks, are the most critical component of tactical communication infrastructures and the most challenging to defend against cyber attacks. While all networks are vulnerable to attack, mobile wireless networks are the most unprotected because their strengths and benefits—agility, adaptability, node autonomy, and self-organization—also make them harder to defend against malicious packet-level disruption and intrusion.

Whether relying on an impromptu network of smart phones or emerging technologies like the Joint Tactical Radio System, the benefits of mobile ad-hoc network architecture make it hard to distinguish between malicious packet loss and loss from environmental effects such as RF interference and rugged terrain. “Network wise” attackers can capitalize on the numerous network algorithms and protocols, such as ad-hoc routing, which assume that all nodes are cooperating with the same goal in mind.

Even passive eavesdropping can be used to reveal the location of other network nodes and the traffic pattern can be used to deduce other strategic information. If a wireless device is physically captured or hijacked, it risks revealing location information and packet contents while the rest of the network remains unaware.

Most modeling and simulation systems assume perfect communications between entities in the virtual world. Exercises have made clear the negative effects that result from such simplified modeling. Not only are real world communications rarely perfect, but disruption of communication networks due to network attack are rarely if ever taken into consideration. This effect is particularly relevant for live virtual constructive (LVC) training environments.

The authors have integrated a cyber warfare communications model with a commercial-off-the-shelf (COTS) Computer Generated Forces (CGF) system. The resulting system much more accurately models the effects of cyber warfare in the synthetic battlefield.

Network-Centric Warfare

Network-Centric Warfare (NCW) is a military doctrine that seeks to translate an information advantage, enabled in part by information technology, into a competitive warfighting advantage through the robust networking of well informed geographically dispersed forces (DoD, 2005). This networking, combined with changes in technology, organization, processes, and people allows new forms of organizational behavior. The doctrine contains the following four tenets in its formulation:

- A robustly networked force improves information sharing;
- Information sharing enhances the quality of information and shared situational awareness;

- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command; and
- These, in turn, dramatically increase mission effectiveness.

As is obvious, NCW requires a robust communications backbone. Training soldiers in the use of NCW requires not only accurate modeling of communications, but also modeling of cyber warfare, in order to avoid negative training.

Modeling and Simulation

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.

Computer Generated Forces are used to populate the synthetic combat space with entities – friendly, enemy and neutral. These systems model many factors at play in combat, such as entity movement, effectiveness of weapons systems, terrain, and overarching combat strategy.

Communications Modeling

Historically, most simulations have assumed that communications are perfect – that any entity (whether virtual or constructive) can instantly and reliably communicate with any other entity, and that networks have infinite bandwidth and virtually no latency. In reality, perfect communication is rarely if ever achieved in battle, being impacted by terrain (natural and urban), radio interference, routing, bandwidth available, and network traffic. A simulation is much more realistic when it is linked to a communications effects server (CES), which uses a discrete event simulation engine to accurately determine, in real-time, the success or failure, and timing, of every packet delivery. Incorporating network attacks and defenses into the CES brings additional realism to the simulation of Network-Centric Warfare.

Cyber Offense/Defense

Unraveling the complexities of cyber operations requires a comprehensive understanding of information generation, distribution and consumption, as well as the recurring patterns that affect this information flow. Such patterns include information protection, information corruption, threat detection and response. Cyber Operations Analysis is a study of these patterns and their impact on the information itself.

A brief note on terminology used in this paper: '*blue force'* refers to those entities (human operators, communication assets, battlefield applications) that are the owners and primary users of the network infrastructure, whereas '*red force*' are those entities that attempt to disrupt the proper operation of the blue force's network.

The Arms Race Nature of Cyber Technology

There is a constant arms race struggle between the red and blue force cyber technology development. Red forces strive to defeat the protection strategies of blue forces' networks and disrupt their operations, whereas the blue forces defend both proactively and reactively by developing even further sophisticated intrusion prevention, detection and response systems. The technology, from both sides, therefore advances in generations, where a later generation has better attacks or defenses compared to previous ones, and it is highly unlikely that this technology escalation will ever arrive at a stalemate. Hence, there exists an urgent and ongoing need to evaluate and train for vulnerabilities and resilience of net-centric military systems to computer network attacks from multiple, diverse, and (possibly) coordinated threats on communication networks.

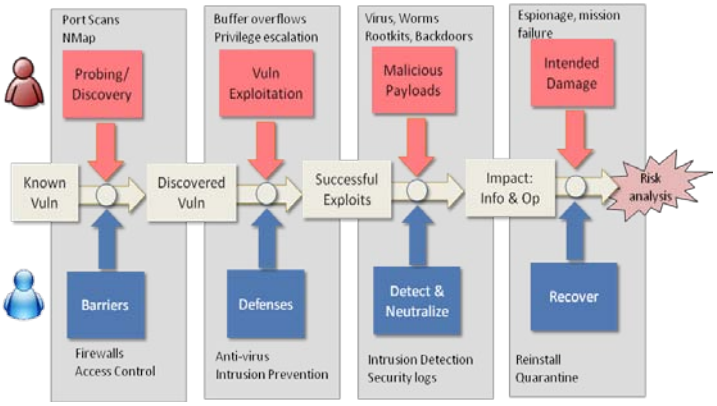

Figure 1: Cyber operations between red/blue forces

Figure 1 illustrates a typical concept of operation for cyber activities by red and blue forces. The temporal sequence of activities is shown from left to right.

The first round of contest between the blue and red forces is the discovery of the network and host assets,

as well as vulnerabilities exposed to an intruder. The red force attempts to discover the state of the blue network by tools and techniques such as port scanners, network mapping etc. The blue force, on the other hand, attempts to hide this information by installing firewalls, access control mechanisms and so on.

The second round of contest between blue and red forces is in the vulnerability exploitation. Blue forces block potential attacks by upgrading and patching system and application software against known attacks, installing intrusion detection and prevention systems, anti-virus systems and so on. The intruders, meanwhile, launch attacks that attempt to circumvent these protection mechanisms. Thus, the sophistication in prevention strategies coerces the red forces to develop stronger attacks, and similarly the sophistication in attacks compels the blue forces to develop stronger prevention schemes.

The third level of contention occurs when some attacks have been successfully injected in the network. In this case, the red forces work toward the survivability of the attack, that is, the initial attack seed should evolve into a full-scale attack that can compromise the informational or operational capabilities of the blue forces. The blue force's counterpart strategy is to detect and neutralize the attacks in their early stages. The struggle, therefore, is in developing attacks that go undetected and, at that the same time, developing detection algorithms to discover any malicious activity.

The final tug-of-war happens after the attack has been successfully launched. The red force has been able to disrupt the informational or operational capability of the blue forces. At this point, the blue force responds to these attacks by defensive or offensive measures. The defensive strategy is to isolate and quarantine the attack to diminish its impact. Offensive strategies could be to neutralize the attack at its source by counter cyber attack, administrative means, or kinetic attack. In either approach, the blue force has the objective of terminating the attack, whereas the red force has the antagonistic objective of keeping the blue force network disrupted for as long as possible.

Note that the above discussion applies equally well when the blue force is in fact launching the cyber attacks. The point is that the actions by either force, as an attacker or defender, are dependent on the actions of the other force. This sequence of attacker and defender actions makes the simulation and training of Computer Network Operations ideally suited to a role playing interactive environment.

Taxonomy of Attack Vectors

Cyber attacks come in many flavors, each targeting different kind of vulnerability within the network or computer system, and at different layers of the protocol stack. *Attack Vector* is the term used in cyber parlance to refer to the paths or means by which an intruder can gain access to a computer or network server in order to deliver a payload or malicious outcome. 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 toward a unified classification methodology, or taxonomy, of such attacks. However, most of the existing taxonomy schemes focus exclusively on the software vulnerability exploits, largely ignoring those attacks that specifically target overall network centric operations. Table 1 presents our

Attack Vector	Definition	Examples
Passive attacks	Gleaning information	Eavesdropping, sniffing, network traffic analysis
Denial of Service	Making service unavailable by overwhelming the computation or network resources	ICMP flood, Smurf ping flood, TCP SYN flood, Teardrop attack, Reflection attack, Blind DoS, Distributed DoS
Malicious Agents	A malicious undetected program executing on victim's computer	Virus, Worms, Malware, Trojans, Rootkits, Backdoor
Topology mis-configuration	Subverting the traffic flow paths	Wormhole attack, Rushing attack, Blackhole attack, Grayhole attack
Code Exploits	Exploiting software bugs to execute malicious code	Buffer overflows, OS / Services / Applications / Database exploits
Web Exploits	Exploiting the client-server interactions of Web protocols	Cross-site scripting, HTTP header injection
Human Error	Intentional or accidental operator actions	Phishing, Incorrect data entry, compromised personnel
Wireless Specific	Targeting the specific attributes of wireless communications	Jamming, RF signature identification

Table 1: Taxonomy of Attack Vectors

attempt to classify the attack vectors into eight 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. By no means is this a complete or comprehensive list. Our intention here is to introduce the reader to these different kinds of attacks.

Modeling and Simulation of Cyber Attacks

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 etc), 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 synthetic environment, the latter must model information not only as packet data, but also as other attributes such as location, mobility, and operator roles. Authentication, trust management, and key management models must be included in the communications simulation.

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 role of these attacks on network performance can be investigated by connecting the network model to real hosts and real operating systems, so that the malicious agents propagate in a controlled testbed environment. The network 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 testbed 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 communications effect 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

Impact of Attack

The previous section outlined the various mechanisms through which the red force can launch attacks in the blue force's network. The impact of attack can be broadly classified as attacking the privacy, integrity or availability of data, or any combination thereof.

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 a cyber operation analysis, these three factors - privacy, integrity and availability - are the measures of performance. Moreover, the key challenge for a test bed 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 test bed that could be integrated into live virtual constructive environments, so that 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 test bed 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.

Solution: Software Virtual Networks (SVNs)

Software Virtual Networks (SVNs) make it possible to represent the communication infrastructure at sufficiently high levels of fidelity that applications running on it—such as a mix of sensor data, streaming video, voice communications, chat, 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 higher 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 or the corresponding emulated component.

The 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 delay and losses can not only be analyzed, but be seen and heard in real-time. 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. 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 model, it becomes possible to evaluate the side effects of cyber attacks on operational systems.

Integration Into Battlefield Simulation

Working together, Scalable Network Technologies (SNT) and VT MÄK (MÄK) integrated COTS software, notably SNT's EXata communications effects server, which is a COTS implementation of an SVN with MÄK's VR-Forces CGF. SNT developed cyber warfare models including jammer, eavesdropper, distributed denial of service, and network attack and implemented them within EXata. For the integration, both tools 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).

CGF Implementation

When one VR-Forces entity needs to send a radio message to another, the radio model passes the message to the communications model, which then processes the message based on the radio's parameters and the parameters of the communications model. The communications model then delivers the message to any entities that are capable of receiving the message. The receiving entities then process the message they received, possibly taking new action as a result of contents of the message.

When an external communications effects server is in use, the VR-Forces radio model works the same as in the baseline system. However, when a radio message is ready to be sent, the new VR-Forces communications model sends a request to the EXata server and holds the signal message until the server adjudicates the signal, and responds. When the VR-Forces communications model receives the response from EXata it delivers the message to the entities that are able to receive the signal – or not, as appropriate.

Communications Effects Server Implementation

Using components from the ICD definition, EXata monitors the HLA federation, listening for VR-Forces to send HLA interactions to EXata requesting processing of communications effects. EXata responds by sending HLA interactions to VR-Forces to report on results of communications. While monitoring the state of the virtual world as represented in HLA, EXata tracks the following information:

- Entity objects, including location, orientation, speed, and damage state
- Radio objects, on/off state
- ApplicationSpecificRadioSignal (ASRS) interactions
- EXata-specific messages indicated via UserProtocolID parameter

Using this information, EXata determines:

- Changes in the mobility patterns of EXata nodes (each node corresponds to one radio)
- Changes to maximum transmit power due to entity damage
- Disabling of EXata nodes due to entity damage and on/off toggling
- Modeling of network communications following receipt of ASRS interaction using contents of SignalData parameter (message size, timeout, optional unicast destination)
- Network traffic from CGF radio messages, live traffic and battlefield application traffic all sharing communication resources
- Effects of Computer Network Attacks and Defenses on network state and packet delivery

Application

With the integration of cyber warfare communication effects into a live virtual constructive environment, we are now able to better represent a Network Centric Battlespace subject to cyber attack. We have used our testbed to investigate the effect of communication network disruption on blue force command and control applications, resulting from red force cyber attack.

In one experiment, we created a hostage rescue scenario in VR-Forces. In this scenario, a commander uses combat net radio to give orders to dismounted soldiers located in an urban area to move to position, and rescue a set of hostages. All VR-Forces entities, blue and red, exhibit intelligent behavior based on information they are able to sense, behavioral rule sets, and communication messages they receive. Communication effects including the successful / unsuccessful or delayed delivery of messages are modeled in EXata.

We ran this experiment in two ways. In the first, the blue communications network is not subject to attack. Under these conditions, the dismounted soldiers receive their orders via radio and are able to carry out their mission with complete success, surprising the guard and rescuing the hostages.

In the second case, we kept rule sets and behavior of all VR-Forces entities unchanged from the first case, but made a change only in the communications model. The change was a penetration of the blue communications network due to a successful cyber attack from the red forces. The attack enabled a red entity to eavesdrop on the communications between the commander and the dismounted soldiers. When the same scenario was rerun, this time the eavesdropper was able to listen in to the blue orders, and communicate with other red entities to inform them. The informed red entities then moved to ambush positions and engaged the blue soldiers. In the ensuing gun battle, a blue soldier was killed. The blue soldiers still completed their mission, albeit with a loss.

As this example clearly indicates, without the inclusion of cyber warfare communications effects, battlefield modeling and simulation can be overly optimistic and negative training could ensue. With the integration of high fidelity communication models that include network attack and defense, the capability to analyze and train for the effects of cyber warfare on mission outcome is dramatically improved.

CONCLUSION

To date, most modeling and simulation systems assume perfect communications between simulated entities. Since real world constraints and cyber warfare limit the communications capability, however, the use of a perfect model creates negative training effects and provides substantially imperfect analysis.

The authors have, by integrating COTS tools, created a test bed for the attack/defense of networks that allows integration into a LVC environment. The result is a system which increases the fidelity level of modeling, which has been proven to provide better training and improved analysis capabilities for the vulnerability and resilience of net centric military systems to computer network attacks. The integration into a LVC environment provides an improved assessment of the impact of cyber warfare on operational systems and force effectiveness.

REFERENCES

Department of Defense. *The Implementation of Network-Centric Warfare*. Washington, DC: January 2005.

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.

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.