Assessment of Network Vulnerabilities Using Virtual and Constructive Simulation

J. Harikumar, R. Hartley, and G. Pineda

January 2017

Issues

Networks are vulnerable to threats at

- system level
- network level

Live exercises of cyber attacks and defense

- Are cost driven (time and resources)
- May conflict with other test objectives
- May create security issues
- Generally capture only the immediate effect of an event (eg., loss of communication because link was taken down

Loss or degradation of communications is only part of the problem; *instead we require understanding a range of possible impacts*

Objectives

Provide a virtual and constructive modeling and simulation (M&S) environment

to assess vulnerabilities

- In wired and wireless networks
- In a mission context with varying terrains

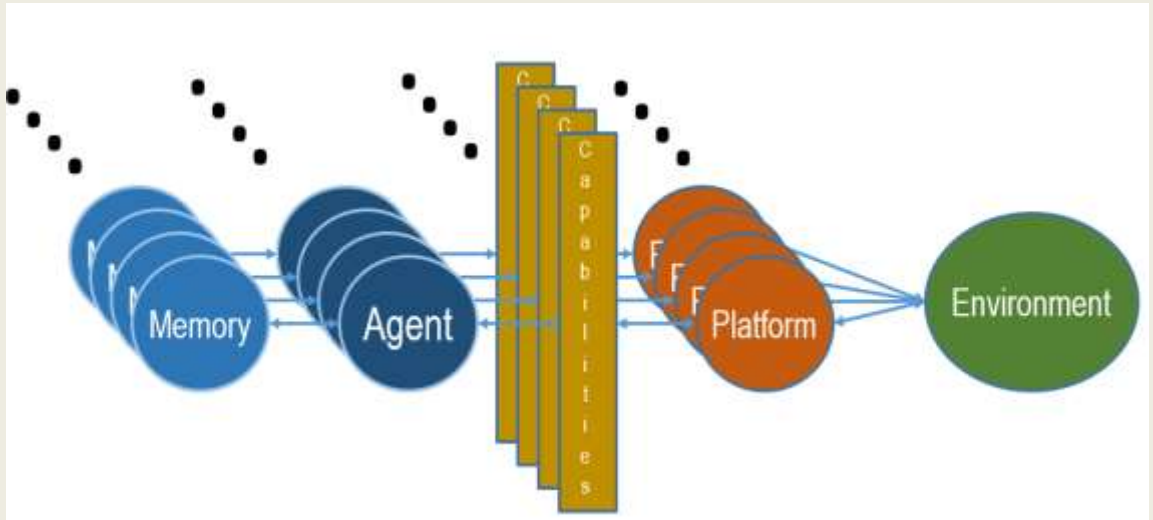
to enable

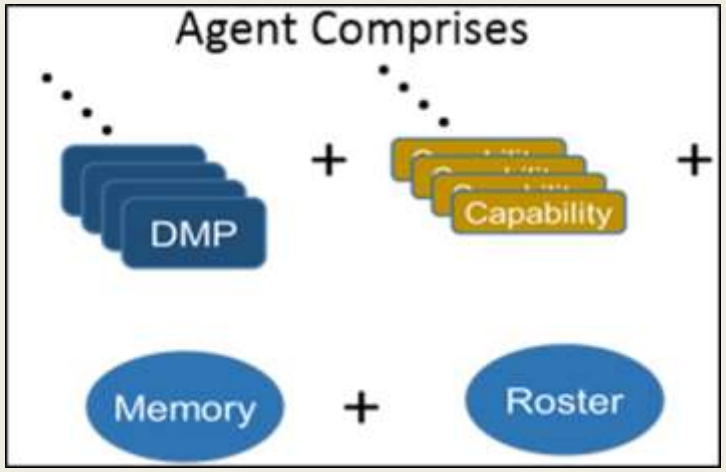
- the “so-what” of cyber attacks
- “what if” analysis
- tactical impact analysis
- understanding of multi-variate network vulnerability threat vectors in a mission context
- analysis of cyberspace vulnerability, survivability, and lethality risks and opportunities through large-scale data analytics

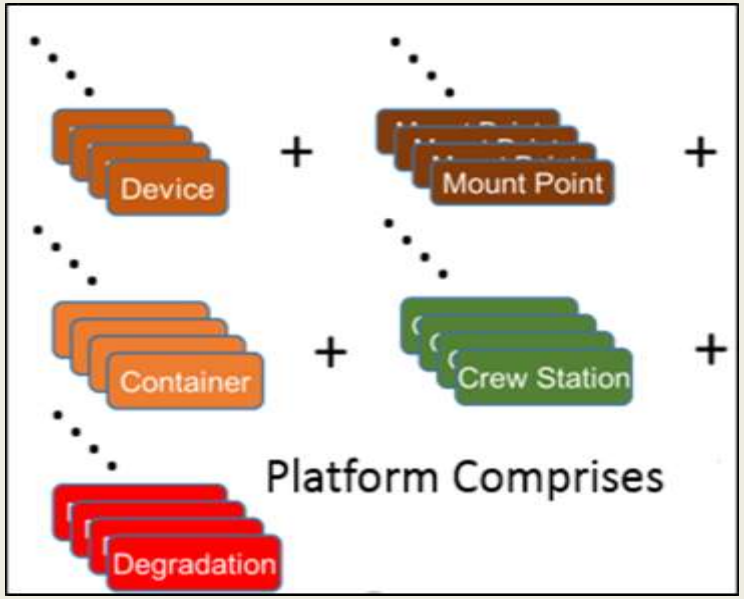
Software Package

S4 Simulation: Abstractions and Models

S4 simulation allows for visualization of and interaction with different scenarios involving agents interacting with each other in a mission context.







Network Simulator: NS-3

Open-Source Discrete Event Network Simulator

- NSF, INRIA, GaTech, Univ. of Washington, etc.
- Development and contributions from users world-wide (C++, Python)
- Comprehensive simulation of network layers 3, 4, and above
- *Event scheduler that can be accessed and controlled externally*

Plugin interface to Layer-3 encourages growth to the library of layer-2 models that already include CSMA, 802.11 (WiFi), etc.

Network emulation support for “System-in-the-Loop” and Linux tap device supporting interface to external virtualized and hardware networks

Support for native Linux application integration via Direct Code Execution (DCE)

Approach

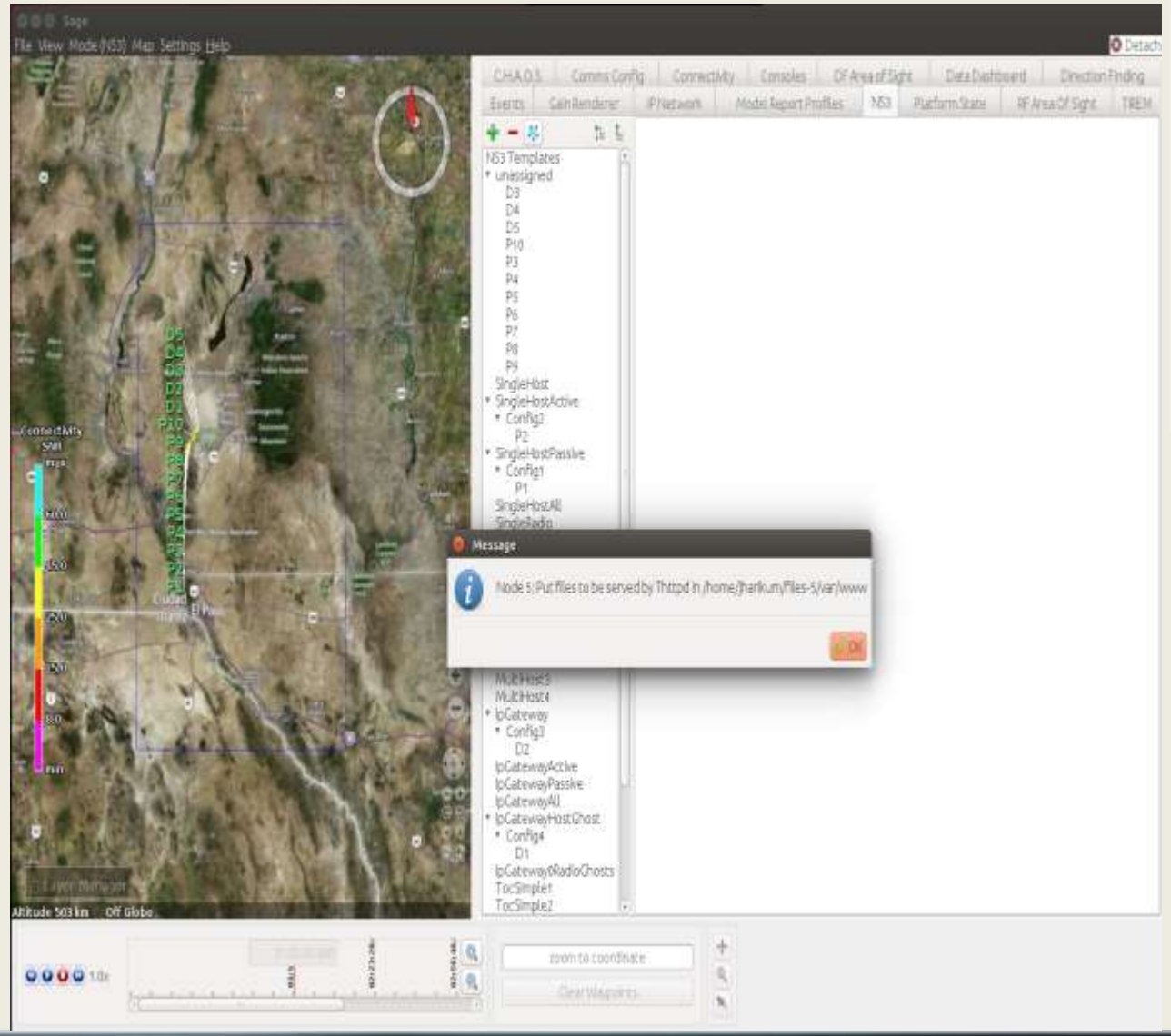
- S4 models entities on the battlefield with respect to their network communications, movement, engagement, and sensing, and decision making associated with these areas of emphasis
- Network communications model in S4 enables information to be passed between entities

Approach taken takes advantage of

- S4 communications models that provide MANET routing/waveform *effects (*data link layer)
- S4 propagation models (physical layer) that can be further enhanced to provide support for EW attacks beyond basic jamming
- NS-3's ability to simulate nodes in either real-time or simulation modes
- NS-3 model fidelity at the transport and internet/network layers
- NS-3 support of direct code execution and the ability to connect simulation nodes to virtual and real nodes

Network Vulnerability Example: Stealing Web Traffic

Build the network via Sage



SingleHostPassive: P1

Config1

radio routing	RIPD
host routing	STATIC
stack type	NS3
PCAP tracing	☐

PktSink

Thttpd

enabled

http port	80
htdocs	/var/www
start	1.0

SingleHostActive: P2

Config2

radio routing	RIPD
host routing	STATIC
stack type	NS3
PCAP tracing	☐

Ping

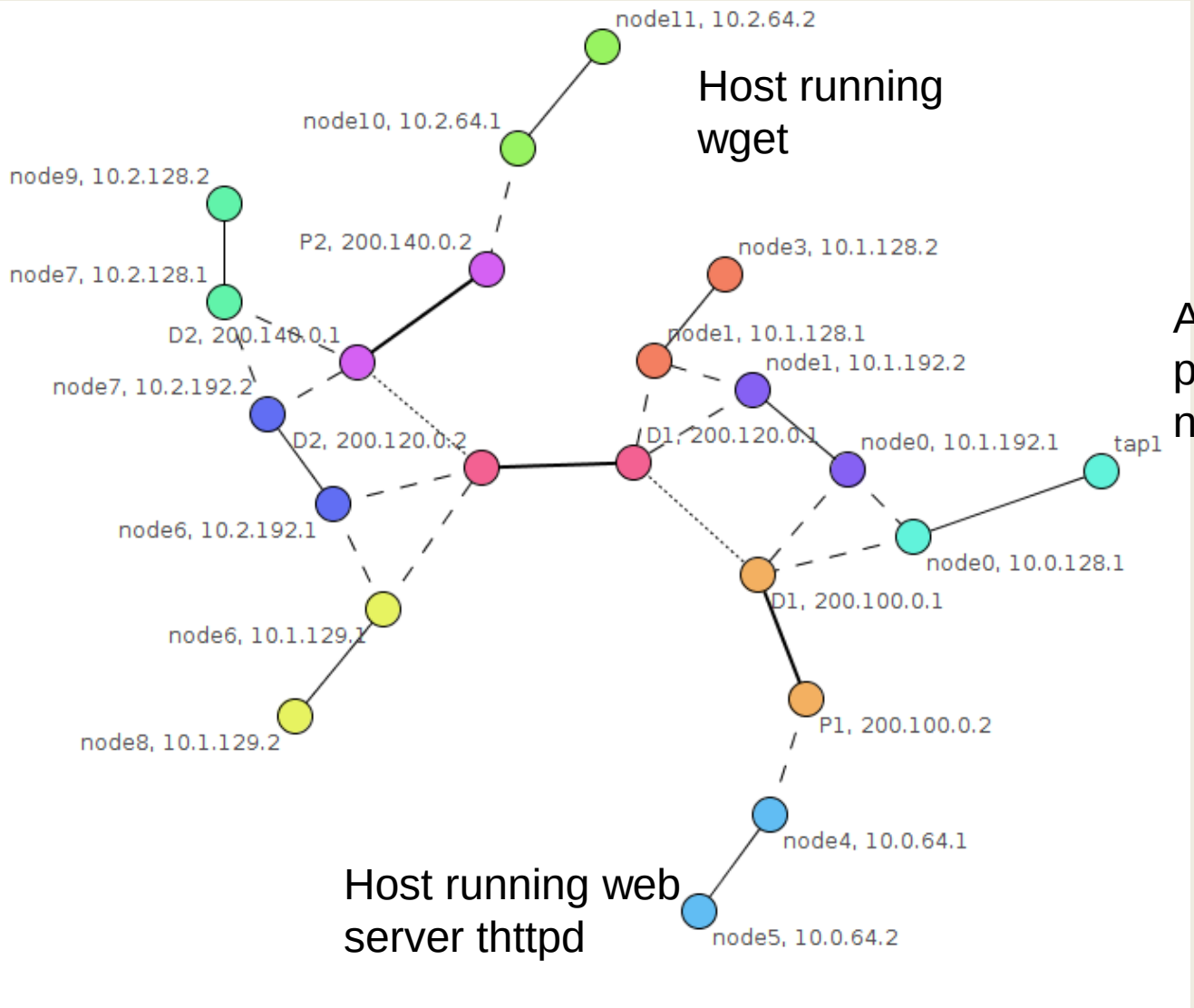
OnOff

Wget

enabled

remote	P1/0
http port	80
number of commands	100
interval between commands	5.0
path to resource	/myfiles/file.txt
relative target path	home/myfiles/gotit.txt
log file	☐
start	2.0

The IP Network displayed in Sage



Attachment point for CORE network

Thick Continuous lines connect interfaces on the same subnet. They are all on the same channel. The nodes are labeled with their name and their IP address from that subnet.

Dashed lines connect interfaces within the same computing device. Each radio has two interfaces; each gateway radio has three.

Thin Continuous lines that are not bold connect interfaces in different devices. These are external wired links (pieces of Ethernet cable if you like).

Dotted lines connect the two radios of a gateway. This is not a signal connection, but an indication of a two-channel radio.

Node Colors denote members of the same IP subnet

The traffic flow before the redirection:

P2: wget
http://10.0.64.2/tmp/file.txt

P1: thttpd

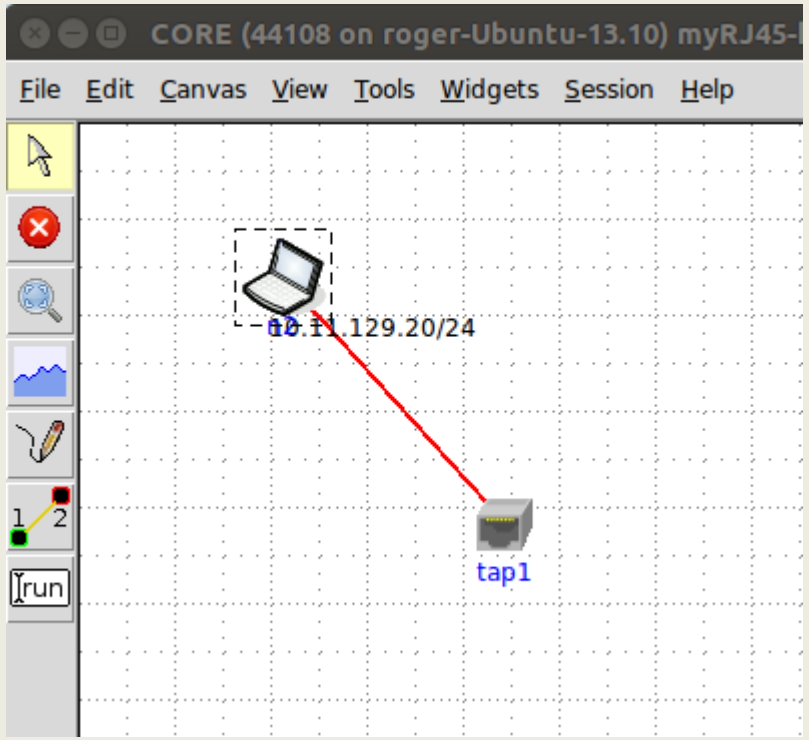
200.100.0.0/24 | 200.120.0.0/24 | 200.140.0.0/24

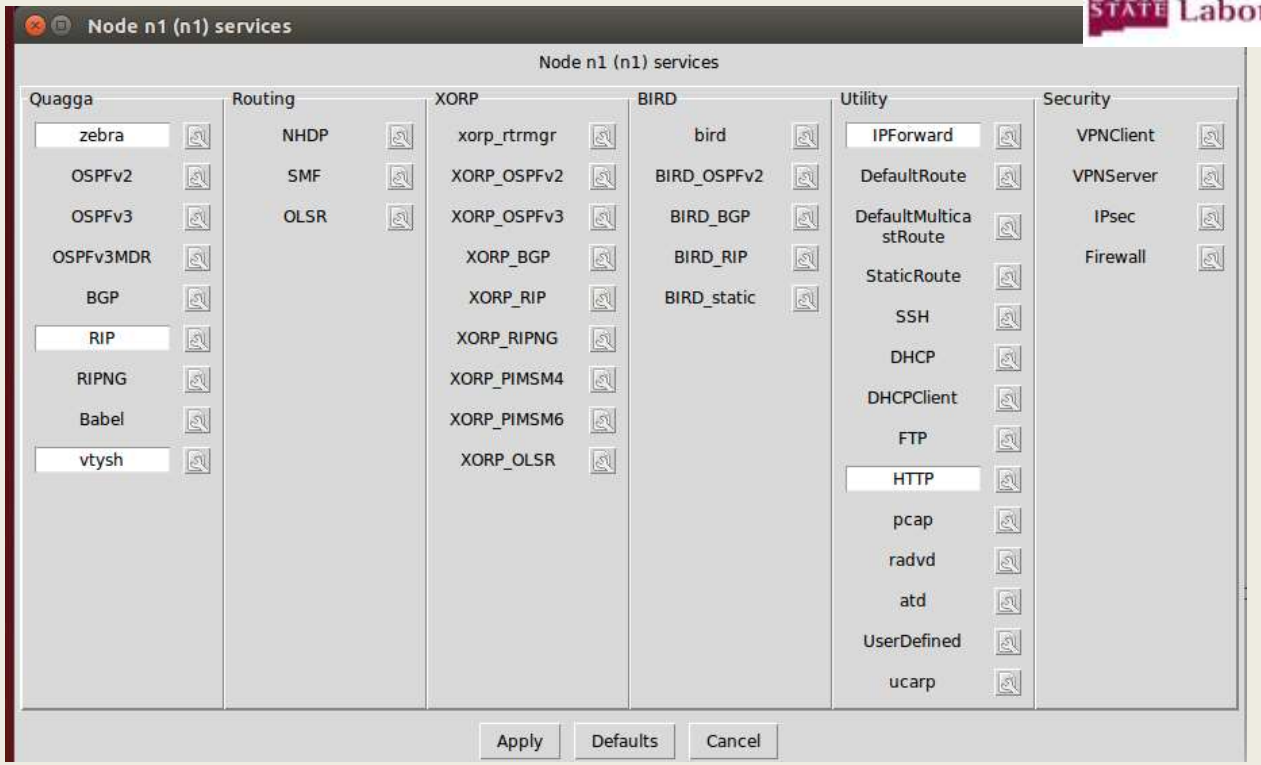
Enable display | Row Limit 1,000 | Clear table | Enable TooTipText

No.	Time	Sender	Sender IP	Receiver	Receiver IP	Protocol	Length	Info
1	6.000113	D1	200.100.0.1:520		224.0.0.9:520	RIPv2	70	RREQ
2	7.0001444	D1	200.100.0.1:520		224.0.0.9:520	RIPv2	90	RREP:10.0.128.0/24,0.0.0.0(1...
3	7.5022232	D1	200.100.0.1:520		224.0.0.9:520	RIPv2	130	RREP:10.0.128.0/24,0.0.0.0(1...
4	8.0001142	P1	200.100.0.2:520		224.0.0.9:520	RIPv2	70	RREQ
5	8.231216599	D1	200.100.0.1	P1	200.100.0.2	ARP	64	REQUEST
6	8.456318998	P1	200.100.0.2	D1	200.100.0.1	ARP	64	REPLY
7	8.681526998	D1	200.100.0.1:520	P1	200.100.0.2:520	RIPv2	130	RREP:10.0.128.0/24,0.0.0.0(1...
8	9.000112998	P1	200.100.0.2:520		224.0.0.9:520	RIPv2	70	RREP:10.0.64.0/24,0.0.0.0(1);
9	10.502159397	D1	200.100.0.1:520		224.0.0.9:520	RIPv2	90	RREP:10.1.129.0/24,0.0.0.0(3...
10	13.166696692	P2	10.1.64.2:49155	P1/0	10.0.64.2:80	TCP	74	SYN
11	14.227337794	D1	200.100.0.1:520		224.0.0.9:520	RIPv2	110	RREP:10.1.64.0/24,0.0.0.0(3);...
12	14.777271457	P2	10.1.64.2:49156	P1/0	10.0.64.2:80	TCP	74	SYN
13	15.015397534	P1	200.100.0.2	D1	200.100.0.1	ARP	64	REQUEST
14	15.240499933	D1	200.100.0.1	P1	200.100.0.2	ARP	64	REPLY
15	15.465618333	P1/0	10.0.64.2:80	P2	10.1.64.2:49156	TCP	74	SYN,ACK
16	15.707469414	P2	10.1.64.2:49155	P1/0	10.0.64.2:80	TCP	74	SYN
17	15.936612492	P1/0	10.0.64.2:80	P2	10.1.64.2:49155	TCP	74	SYN,ACK
18	16.155030291	P2	10.1.64.2:49156	P1/0	10.0.64.2:80	TCP	70	ACK
19	16.15799837	P2	10.1.64.2:49156	P1/0	10.0.64.2:80	HTTP	193	GET HTTP/1.1 /myfiles/file.t...
20	16.38715345	P1/0	10.0.64.2:80	P2	10.1.64.2:49156	TCP	70	ACK
21	16.390147529	P1/0	10.0.64.2:80	P2	10.1.64.2:49156	HTTP	316	HTTP/1.1 200 OK abcde
22	16.40286125	P1/0	10.0.64.2:80	P2	10.1.64.2:49155	TCP	74	SYN,ACK
23	16.62000197	P2	10.1.64.2:49155	P1/0	10.0.64.2:80	TCP	70	ACK
24	16.622492049	P2	10.1.64.2:49155	P1/0	10.0.64.2:80	HTTP	193	GET HTTP/1.1 /myfiles/file.t...
25	16.851647129	P1/0	10.0.64.2:80	P2	10.1.64.2:49155	TCP	70	ACK
26	16.854311208	P1/0	10.0.64.2:80	P2	10.1.64.2:49155	HTTP	316	HTTP/1.1 200 OK abcde
27	16.887153129	P1/0	10.0.64.2:80	P2	10.1.64.2:49156	TCP	70	FIN,ACK
28	17.274000649	P2	10.1.64.2:49156	P1/0	10.0.64.2:80	TCP	70	ACK
29	17.352153129	P1/0	10.0.64.2:80	P2	10.1.64.2:49155	TCP	70	FIN,ACK
30	17.394252842	P2	10.1.64.2:49154	P1/0	10.0.64.2:80	TCP	74	SYN
31	17.570534929	P2	10.1.64.2:49156	P1/0	10.0.64.2:80	TCP	70	ACK
32	17.572971048	P2	10.1.64.2:49156	P1/0	10.0.64.2:80	TCP	70	FIN,ACK

Contents of the real file.txt -- **abcde**

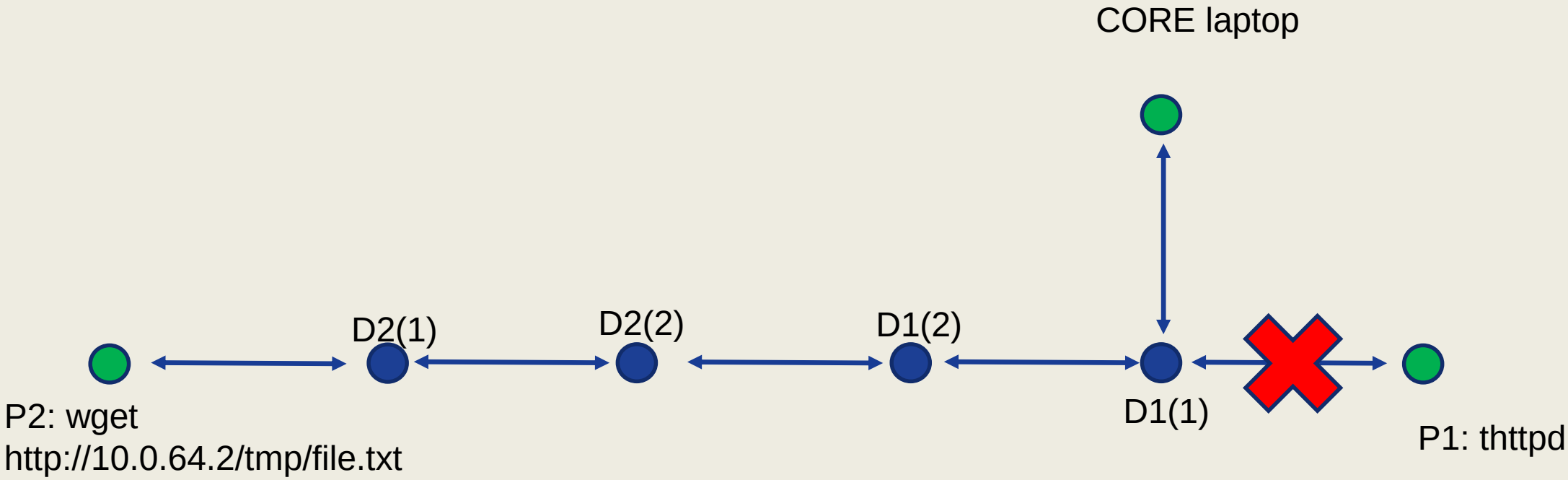
Attack Using CORE: CORE network and services





- CORE is on the NS3 network.
- Use nmap or another tool get the web server address
- Have the CORE laptop pose itself as the server using the web server address

Traffic flow after redirection



Conclusions

Types of vulnerability assessments
- Outside looking in (web & email servers, devices accessible to internet traffic)
- Inside looking around (print servers, file servers, databases)

Vulnerability assessment is dependent on user expertise to
- configure and monitor network and/or system resources
- patch and update services efficiently
- define and implement ways to minimize the consequences of threats

M&S helps in vulnerability assessments
- map and assess the entire network
- examine host and radio individually
- examine security *tools* for wired & wireless networks, Windows & Linux systems

Testing (Exploiting a vulnerability) on production resources can adversely impact the productivity of the systems and network

Backup

Cover Page

Title of Paper : Assessment of Network Vulnerabilities Using Virtual and Constructive Simulation

Authors: Jayashree Harikumar, Roger Hartley, and George Moreno Pineda

Places(s) of Employment, Phone and email address (es)

Jayashree Harikumar

- **Physical Science Laboratory, 575-646-9464, jharikum@psl.nmsu.edu**

Roger Hartley

- **Physical Science Laboratory, 575-646-9485, rhartley@psl.nmsu.edu**

George Moreno Pineda

- **US Army Research Laboratory, 575-678-0359, george.o.morenopineda.civ@mail.mil**

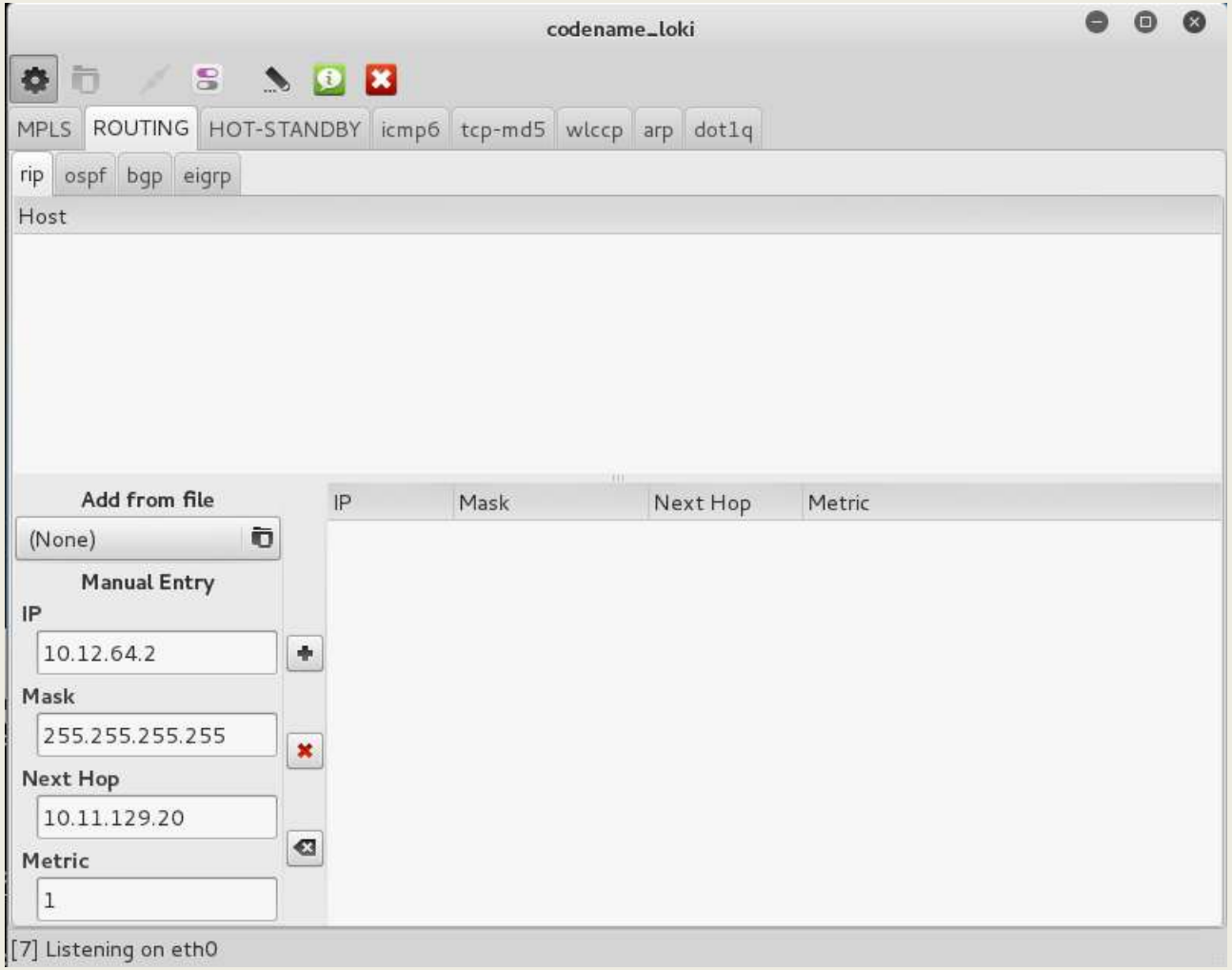
Abstract

Networks are vulnerable to threats at the system and network level. Traditional methods often do not capture engineering level details such as the impact of an attack on a standard routing protocol. Large scale live test of emerging technology is neither cost effective nor feasible when cyber activities can conflict with other test objectives. In this paper, we show through examples, a methodology for an analyst to configure a variety of networks using different tactical radios to integrate and understand cyber effects in an operational environment. These networks can be embedded in a credible mission scenario based on unit objectives. The proposed methodology allows an analyst to (a) configure real applications or code that is faithful to the behavior of the real application at a packet level in NS-3 nodes, (b) use Sage-Cyber simulation to get to the “so-what” of cyber-attacks in simulated or in real time, and (c) use MulVAL to assess vulnerabilities in the wired or wireless MANET.

Stealing Web Traffic: External Version

NS-3 on one machine, linked to another machine running Kali/loki

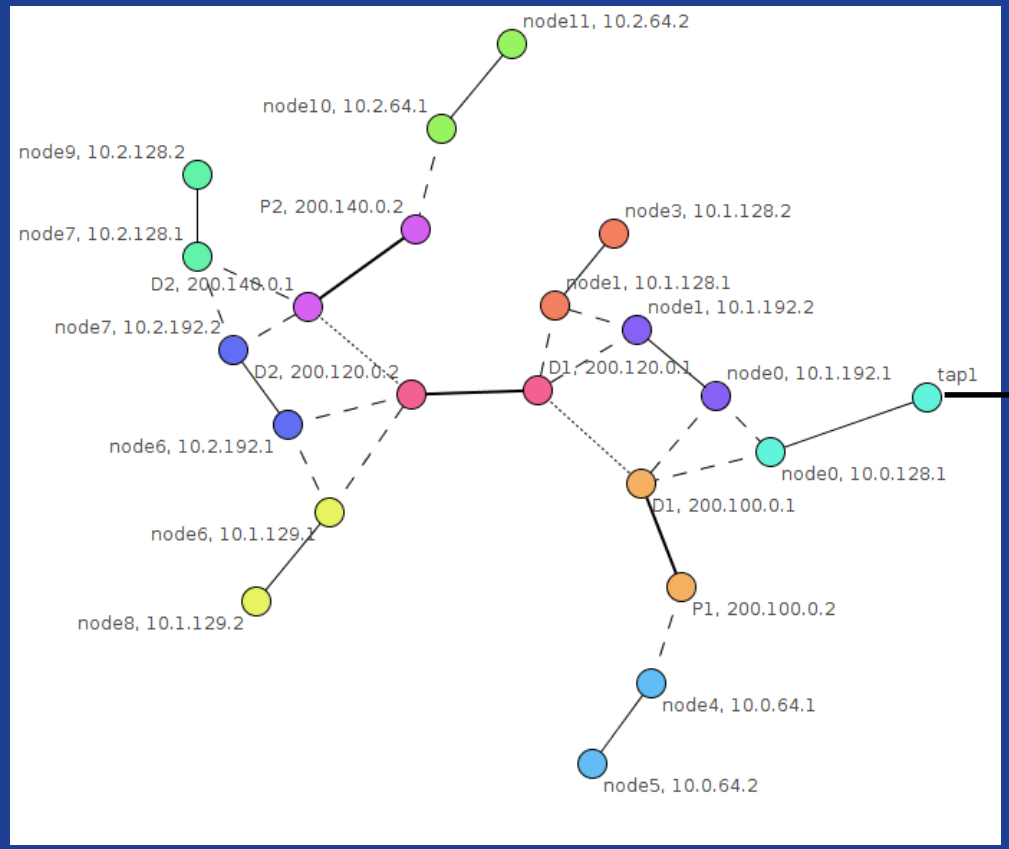
The Kali machine running loki and apache2




```
root@kali:~# ps ax |grep apache
 7987 ?        Ss     0:00 /usr/sbin/apache2 -k start
 7989 ?        S      0:00 /usr/sbin/apache2 -k start
 7990 ?        S      0:00 /usr/sbin/apache2 -k start
 7991 ?        S      0:00 /usr/sbin/apache2 -k start
 7992 ?        S      0:00 /usr/sbin/apache2 -k start
 7993 ?        S      0:00 /usr/sbin/apache2 -k start
 7994 ?        S      0:00 /usr/sbin/apache2 -k start
 8065 ?        S      0:00 /usr/sbin/apache2 -k start
 8311 ?        S      0:00 /usr/sbin/apache2 -k start
 8312 ?        S      0:00 /usr/sbin/apache2 -k start
 8425 pts/0    S+     0:00 grep apache
root@kali:~#
```

Kali linked to Sage/NS3 through the tap

Ubuntu VM (Sage)



eth1

br1

tap1

VMWare switch

eth0

Kali VM