

CEWAS (Cyber Early WArning System): Evaluation on DETER

ARDA Program: P2INGS (Proactive And Predictive
Information Assurance For Next Generation Systems)

**Abhrajit Ghosh
Sudha Ramesh
Scott Alexander,
Giovanni DiCrescenzo
PI: Rajesh Talpade**

Outline

- CEWAS background
- DETER Experimentation
- Experiences & Issues
- Conclusion & Future work

CEWAS: problem scope

- Large proportion of Internet-based attacks involve use of “spoofed” IP packets i.e. packets with incorrect source IP address
 - Use of spoofed packets provides anonymity to attacker, and reduces effectiveness of defense mechanisms
 - Slammer (worm: some instances) TFN (ddos) nmap idlescan (scanning) all utilize spoofed source IP addresses

- We focus on detection of attacks that use spoofed IP packets, and facilitate attack traceback to the administrative boundary of the target IP network
 - Leverage existing capabilities of IP routers

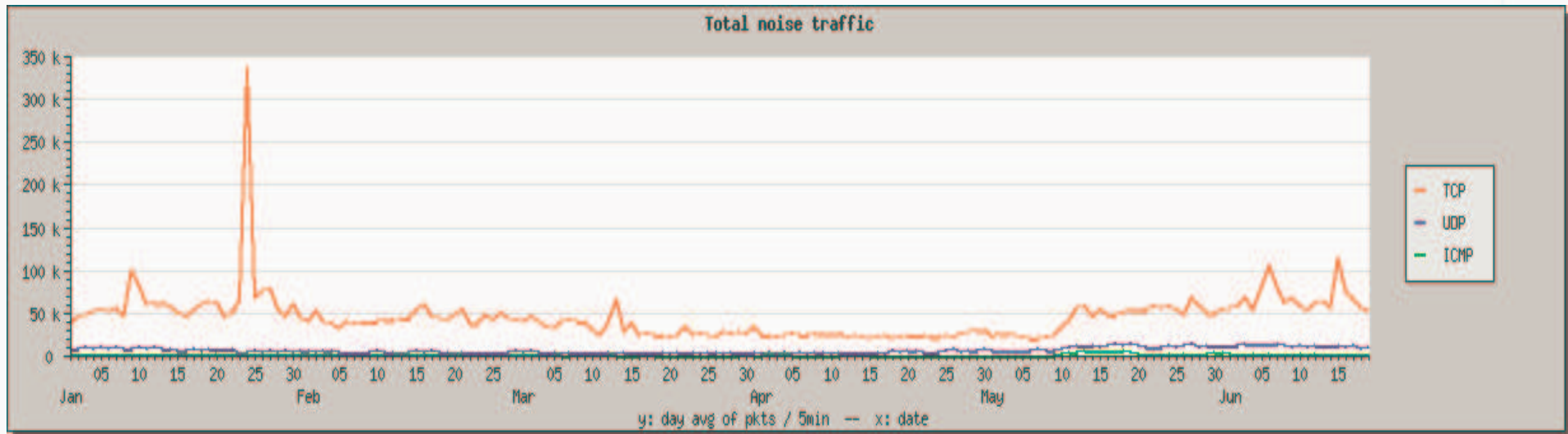
Spoofer attacks & impact

* Tested with CEWAS

Attack Type	Impact	Instances/tools
Worm*	Malicious access, propagation	Slammer
Router spoofing	Eavesdropping, VPN compromise	ICMP router advertisement
DNS spoofing	Traffic redirection, phishing	DNS birthday attack
Idle scanning*	Scan host for vulnerabilities, without traceability	nmap -I
Background noise generation	Hard to pinpoint malicious activity	nmap -D
Zombie control*	Data pilfering, Network unavailability	TFN
TCP connection spoofing	Reset/Hijack TCP connection, compromise BGP based routing	http://www.osvdb.org/4030
Network Stack attack*	System instability/unavailability	Teardrop, Land
DDoS attacks*	Network unavailability	Smurf, TFN

Spoofed Activity

- Internet telescopes (IUCC/IDC, SWITCH/IBN) show significant amount of spoofed activity



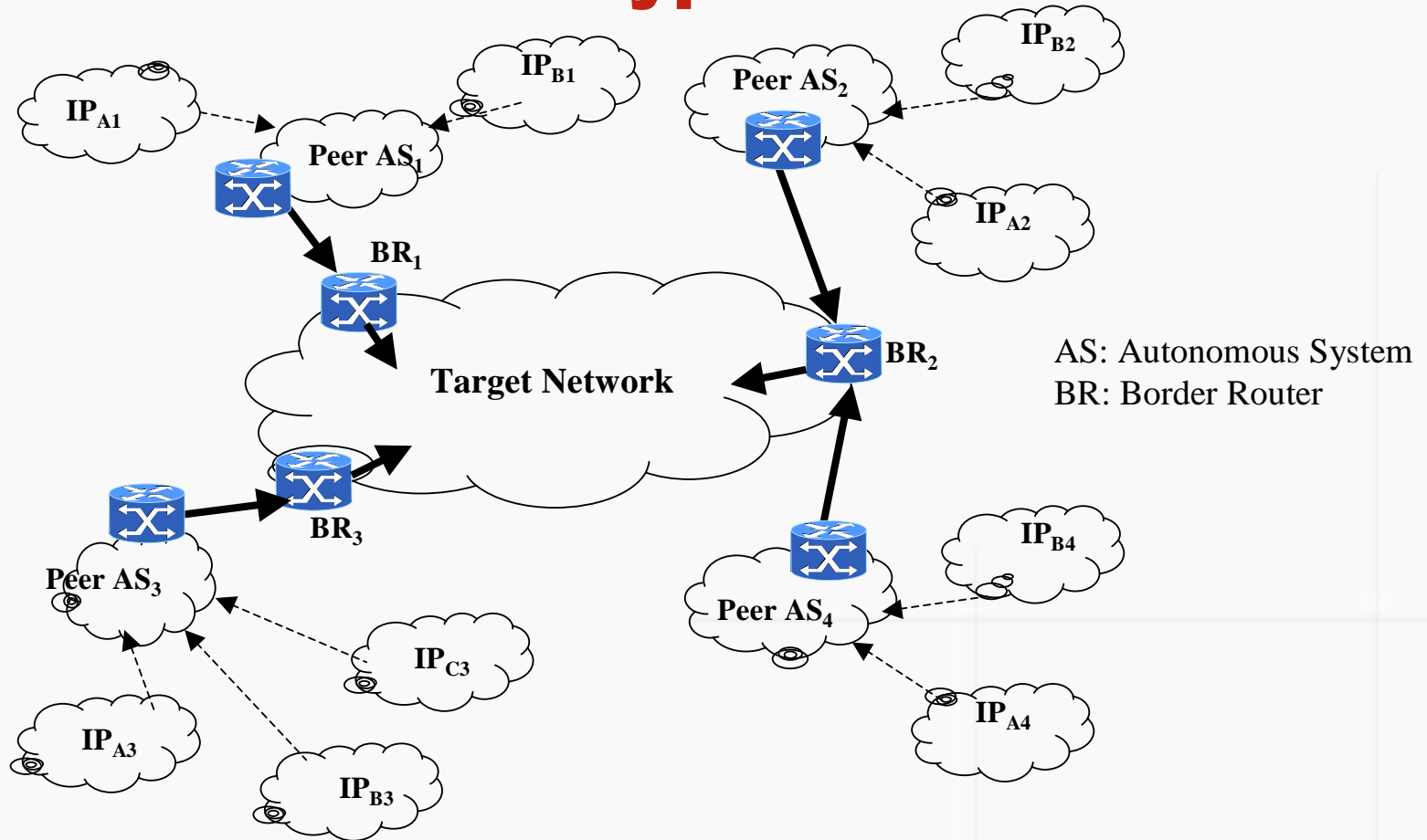
- Readings from IBN (Internet Background Noise) sensor at SWITCH
- Y-axis is day average of packets/5 min for 1st half of 2005
- IBN receives ~ 70K unsolicited traffic packets/5 min
 - Since the Telescope uses 3 /17s of IP address space, this corresponds to 2B packets/min for the Internet

Why detect spoofing ?

- Detection of spoofed packets effectively detects a whole range of attacks
 - No packet signatures needed
 - Stealthy single packet attacks are detectable

- Knowledge of ingress point will assist traceback

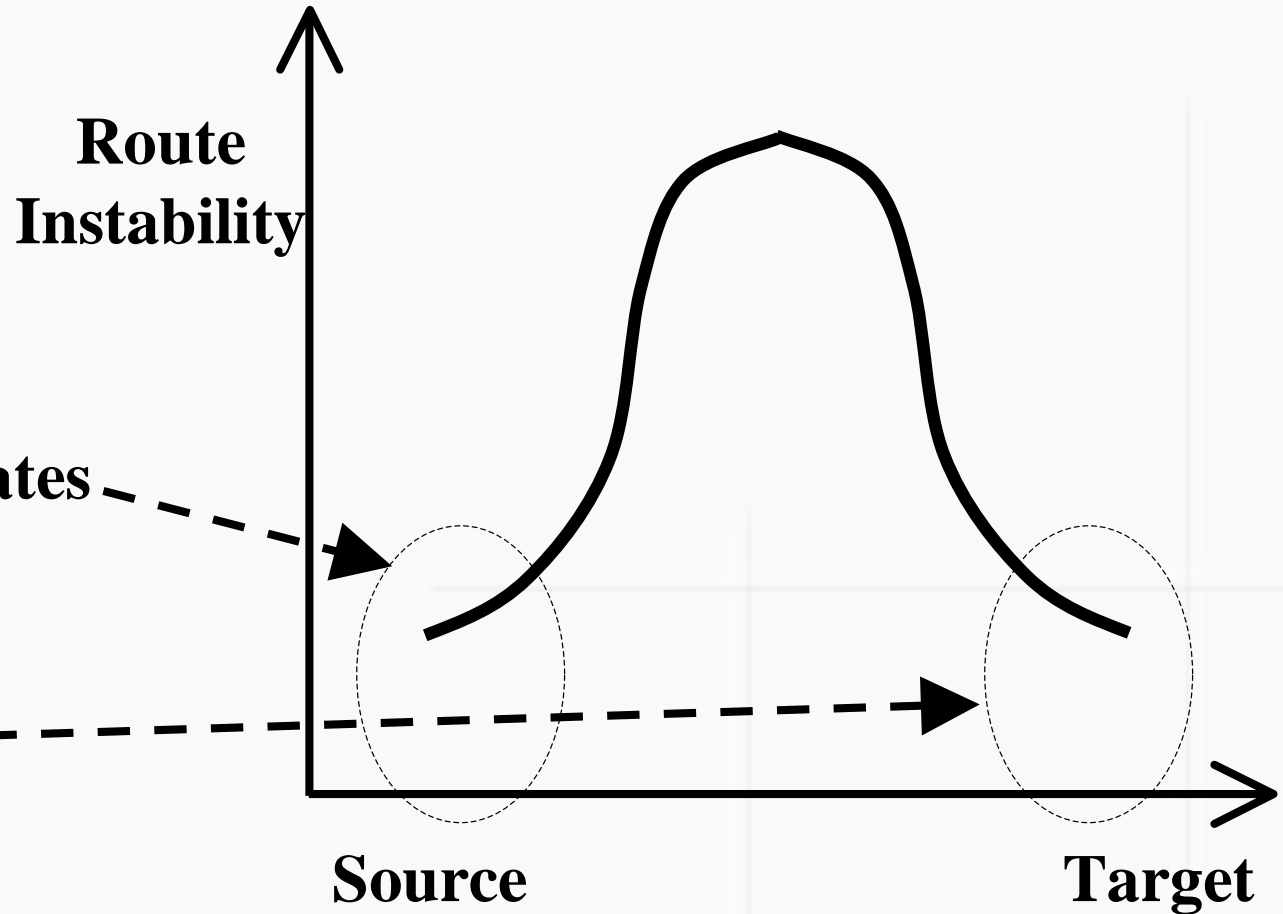
CEWAS Hypothesis



	Expected IP Addresses
Peer AS ₁ – BR ₁	IP _{A1} , IP _{B1}
Peer AS ₂ – BR ₂	IP _{A2} , IP _{B2}
Peer AS ₄ – BR ₂	IP _{A4} , IP _{B4}
Peer AS ₃ – BR ₃	IP _{A3} , IP _{B3} , IP _{C3}

- Peer AS-BR pair (last AS hop) used by traffic from any IP address to enter the “Target Network” remains relatively static.

Leverage Route Stability near Target

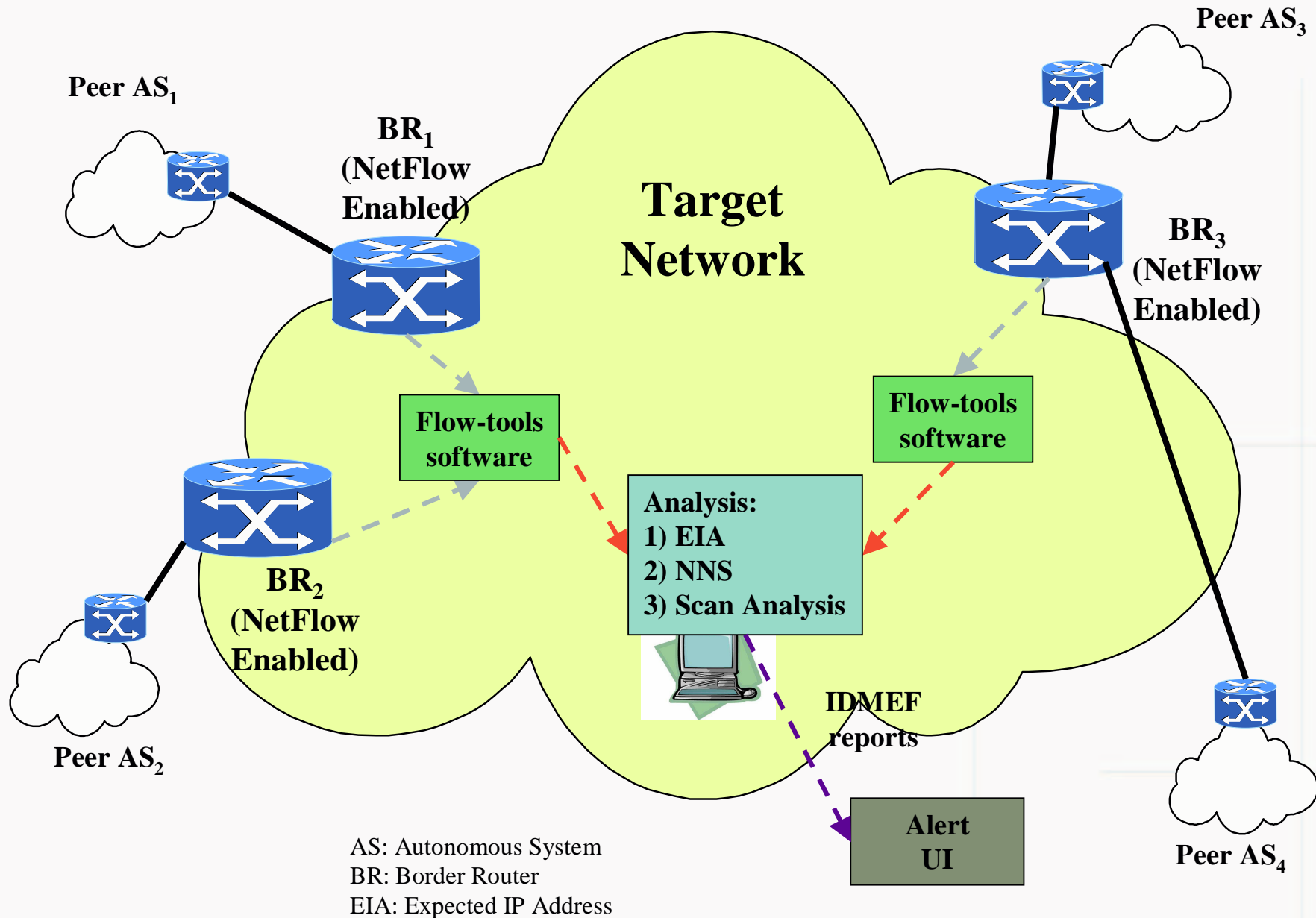


- Egress Filtering operates in this region

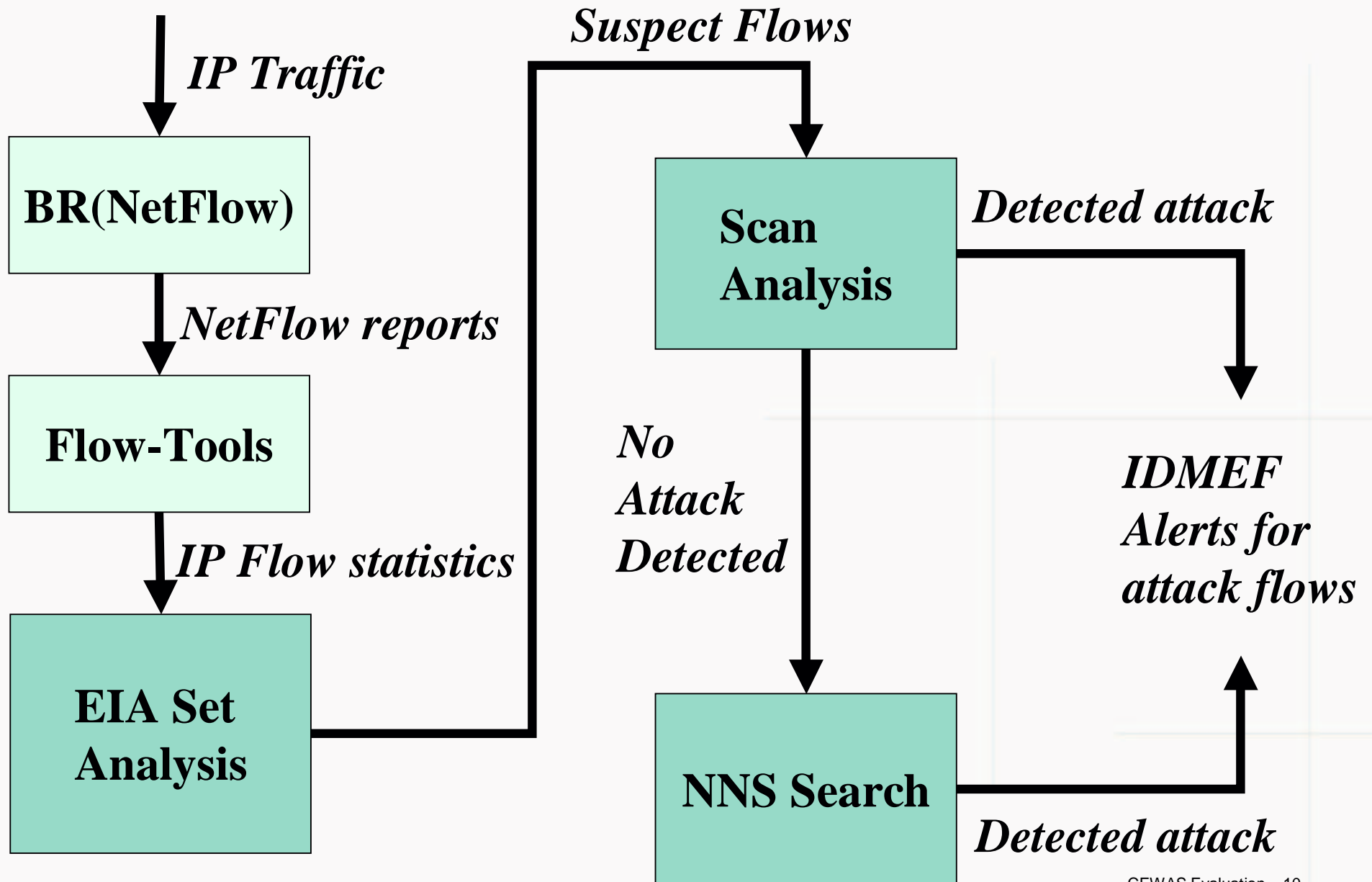
- CEWAS operates in this region



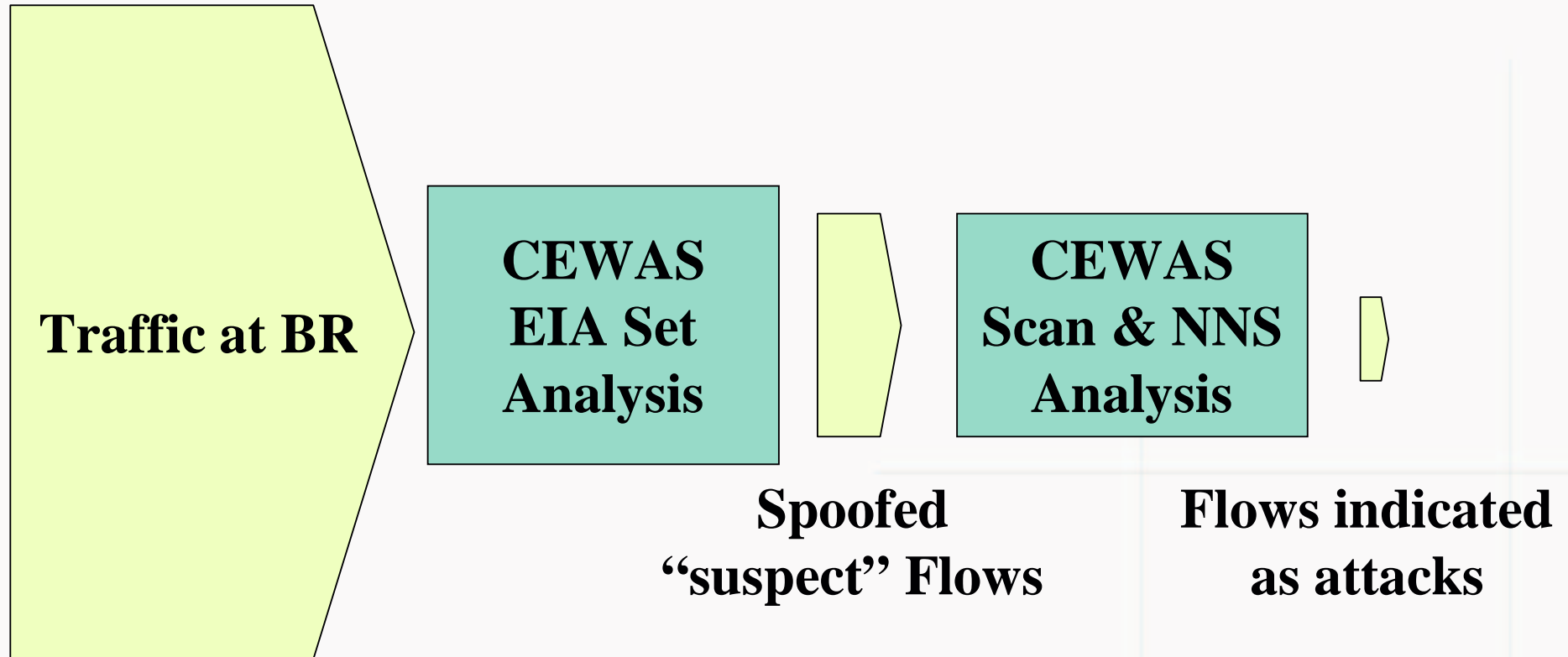
Deployment Architecture



Normal Processing



Improving Detection Accuracy

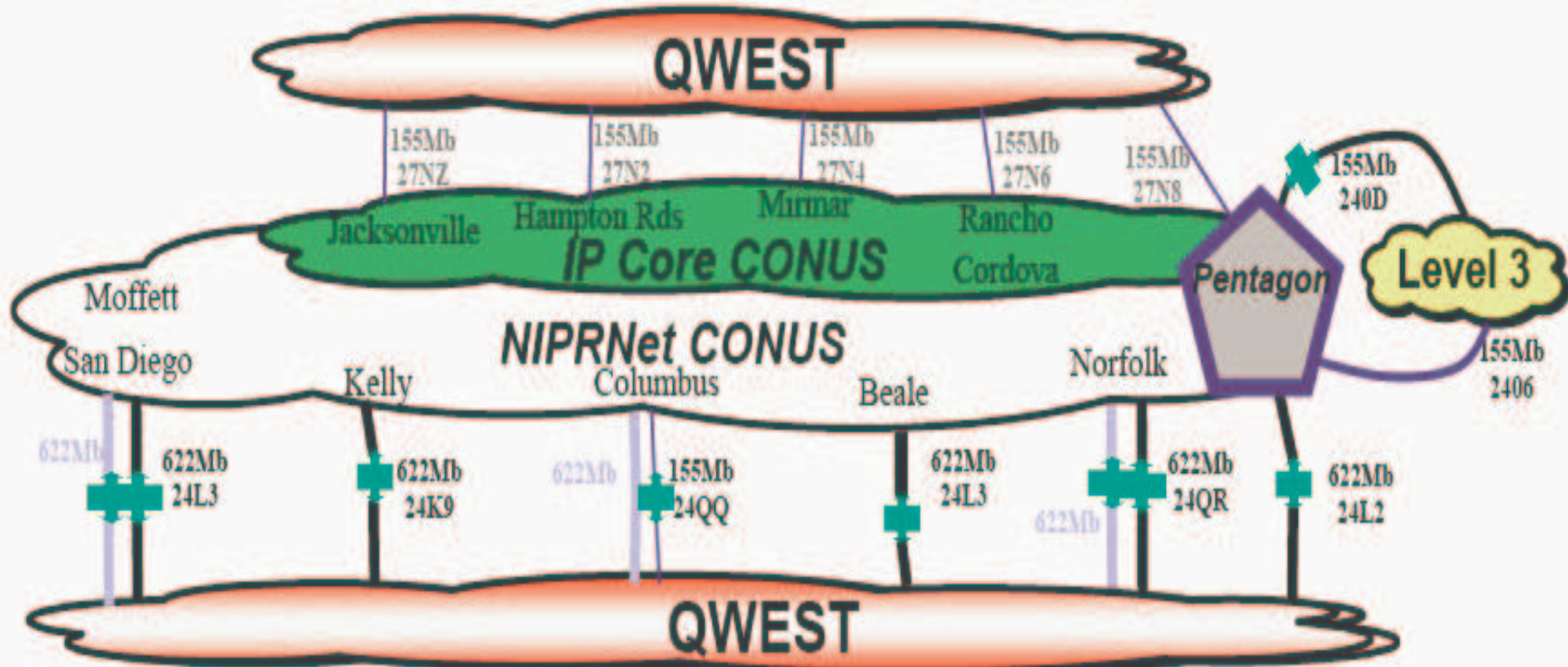


Route changes can lead to false positives

NIPRNet Emulation

- Examine CEWAS performance in a large network topology that emulates portions of NIPRNet
- Introduce routing changes by randomly failing network links
 - Route changes, in response to link failures, will be effected by dynamic routing protocols
 - Estimate false positive rates in the context of true route changes
- Randomly generate attack traffic in the network
 - Estimate impact of attack generation rate on detection rate

NIPRNet CONUS topology

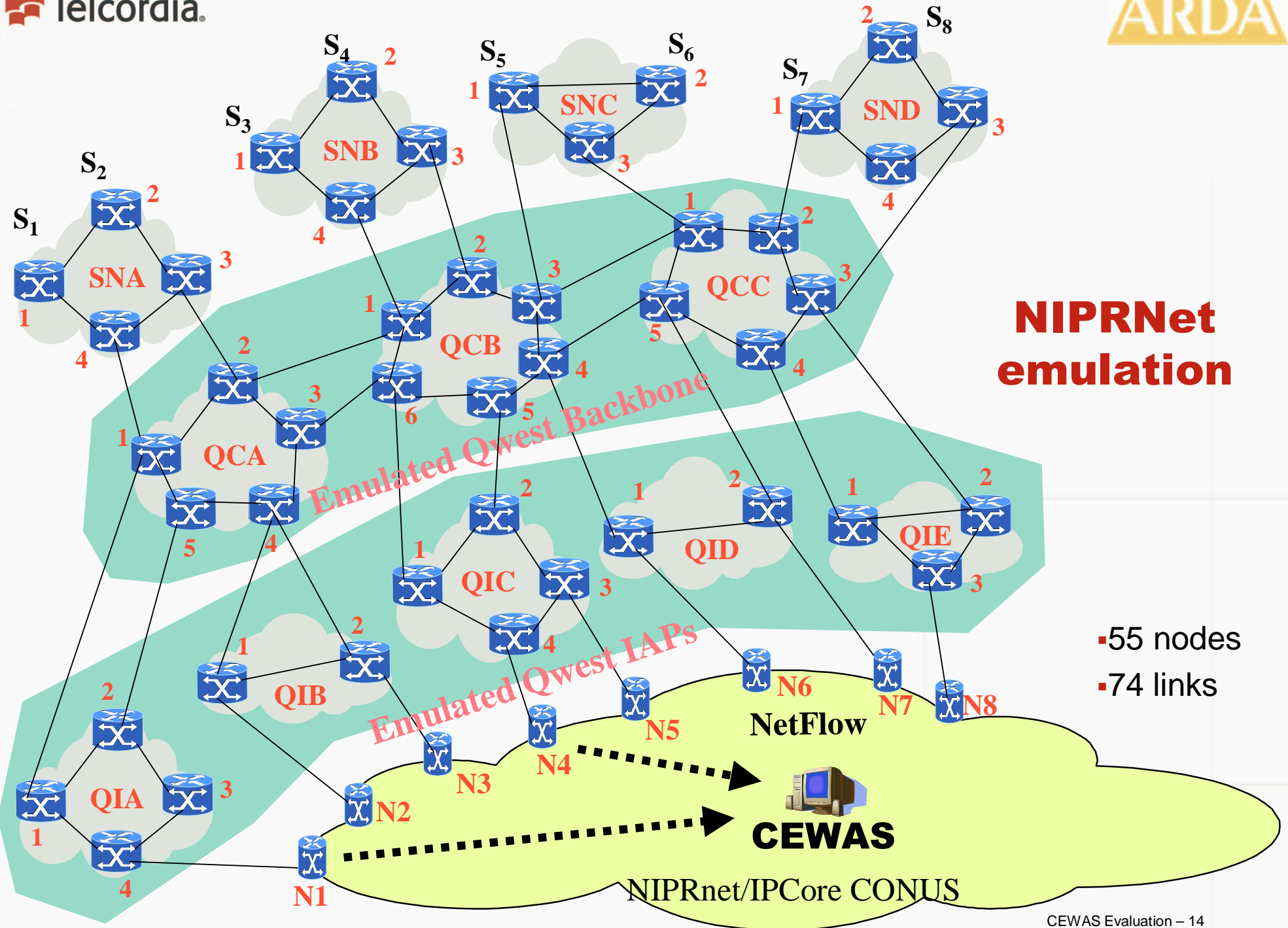


Internet Bandwidth
Total Internet BW 5385Mb

Updated 8 Mar 05

Key

- Operational OC-3 (solid black line)
- To be Deactivated in 8-12 months (dashed black line)
- Planned OC-12 (dashed purple line)
- Operational OC-12 (solid black line)
- Juniper ISR Deployed (green cross symbol)
- 155Mb 27N8 IP Core Circuits (purple line)



NIPRNet emulation

- 55 nodes
- 74 links

NIPRNet emulation: Tools used

- Dagreplay
 - Replays traffic from input trace file
 - Used for generating normal & attack traffic
 - Takes source and destination IP address ranges as input
 - Developed in-house
 - Runs on all source nodes (S_1 - S_8)
- Fprobe
 - Linux based NetFlow generation tool
 - Listens on network interface for incoming traffic
 - Runs on all Border routers (N1-N8)
 - Generates NetFlow v5 records as per Cisco specifications
 - Available under GNU GPL
- Gated
 - Dynamic routing software for OSPF

NIPRNet emulation: Experiment 1

Initialization of EIA sets

- Topology is created, all links are activated, routing protocol establishes routes
 - OSPF based Dynamic routing in effect
- CEWAS is initialized in training mode
- Each source S_i generates normal traffic using Dagreplay
- Each normal Dagreplay instance selects its source IP addresses from a set SIP_i which is unique for S_i
- CEWAS computes EIA sets for NIPRNet
- At this point no link failures are introduced
- The objective is to create EIA sets that may be used as input to experiments 2 & 3

NIPRNet Emulation: Experiment 1 Results

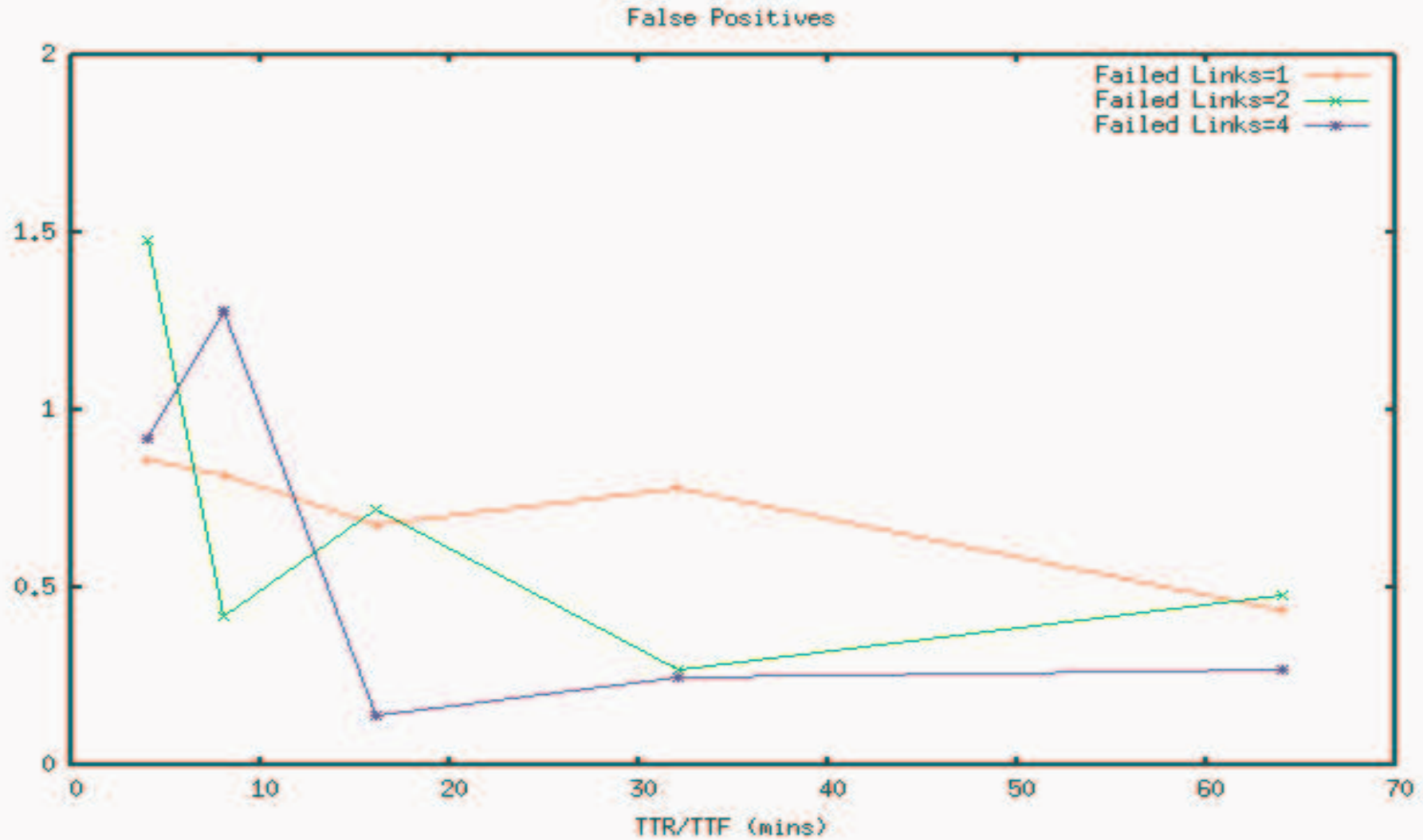
Border Router	EIA Set
N1	SIP ₁ , SIP ₂
N4	SIP ₃
N6	SIP ₄ , SIP ₅ , SIP ₆
N7	SIP ₇
N8	SIP ₈

NIPRNet emulation: Experiment 2

Link Failures

- Each source S_i generates normal traffic with source IP addresses selected from SIP_i
- Random link failures generated to effect routing changes
 - Every f minutes select k links that will fail
 - Each failure lasts for f minutes
 - During the failure OSPF computes new routes
 - At the end of failure period, links are restored
- Measure the number of false positives raised as a result of route changes induced by link failures
- The EIA set computed in Experiment 1 is an input to Experiment 2
 - EIA sets change during the course of the experimentation as route changes stabilize.

NIPRNet Emulation: Experiment 2 Results

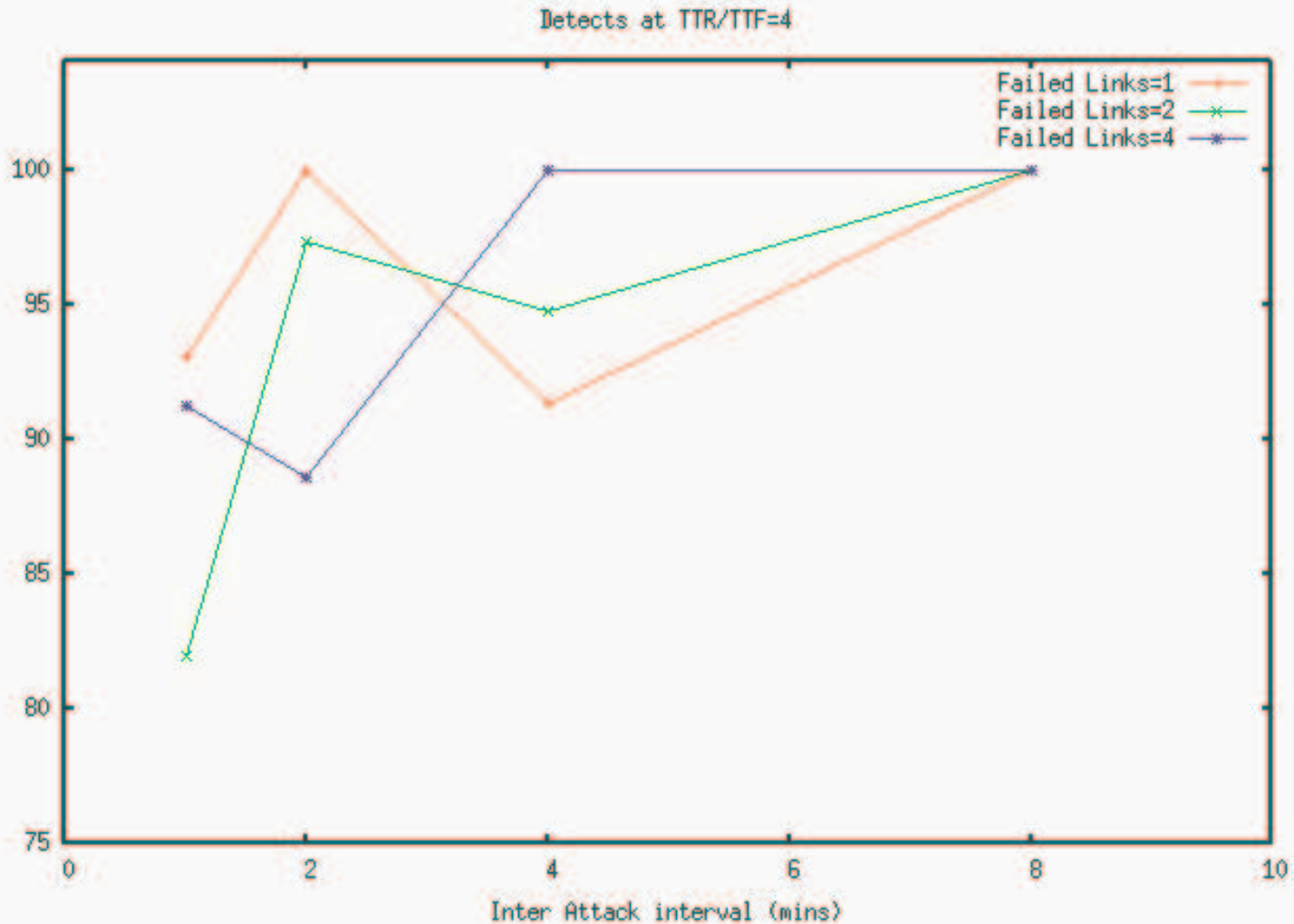


NIPRNet emulation: Experiment 3

Link Failures & Random Attacks

- Each source S_i generates normal traffic with source addresses in SIP_i
- Route changes are induced via link failures as in Experiment 2
- The EIA sets from Experiment 1 are an input to this Experiment.
- In addition, attack traffic is generated every t seconds
 - A source node S_k is selected for the purposes of launching the attack
 - An attack trace is selected randomly from the available set of attack traces
 - Dagreplay is used to launch the attack packets, source IP addresses for the attack are selected randomly from $U_{i \neq k} SIP_i$ emulating an attack with spoofed source IP addresses
- The number of attacks detected by CEWAS is measured

NIPRNet Emulation: Experiment 3 Results - II



Experiences and issues

- DETER use resulted in significant savings:
 - No hardware setup issues: nodes managed by DETER support staff
 - Hardware error issues were resolved by support staff
 - Most system software issues were resolved by DETER support as well
- Remote access features were very useful
 - Remote power cycling capability allowed experiments to be progressed, without staff intervention, even when nodes “froze up”.
 - Access to serial console allowed us to resolve problems when reconfiguring operating system

Experiences and issues

- Telcordia helped identify several testbed problems
 - Bug on inter-switch connection (VLAN creation failure across switches)
 - Problem with port speeds (dead links, Linux e1000 driver issue)
 - Inter-switch trunk bandwidth (assign script issue)
 - QoS on Nortel switch disabled (inadvertent ToS byte modification)
 - Close cooperation from DETER staff in resolving the above
- Node failure issues
 - Experiments needed repeating since source nodes froze up every now and then

Conclusion & Future work

- As a result of our experimentation we found that
 - CEWAS exhibited a detection rate of between 85 and 100% depending on the attack frequency
 - The false positive rate for CEWAS was typically seen to be around 1.6% of all observed traffic in the target network.
- As part of our future work we plan to examine the following issues:
 - Technology transition to ARDA customers
 - Enhance CEWAS to perform distributed analysis to address fault tolerance and scalability issues
 - Incorporate techniques for inline CEWAS training (instead of requiring a separate training phase)
 - Evaluate future CEWAS versions on DETER