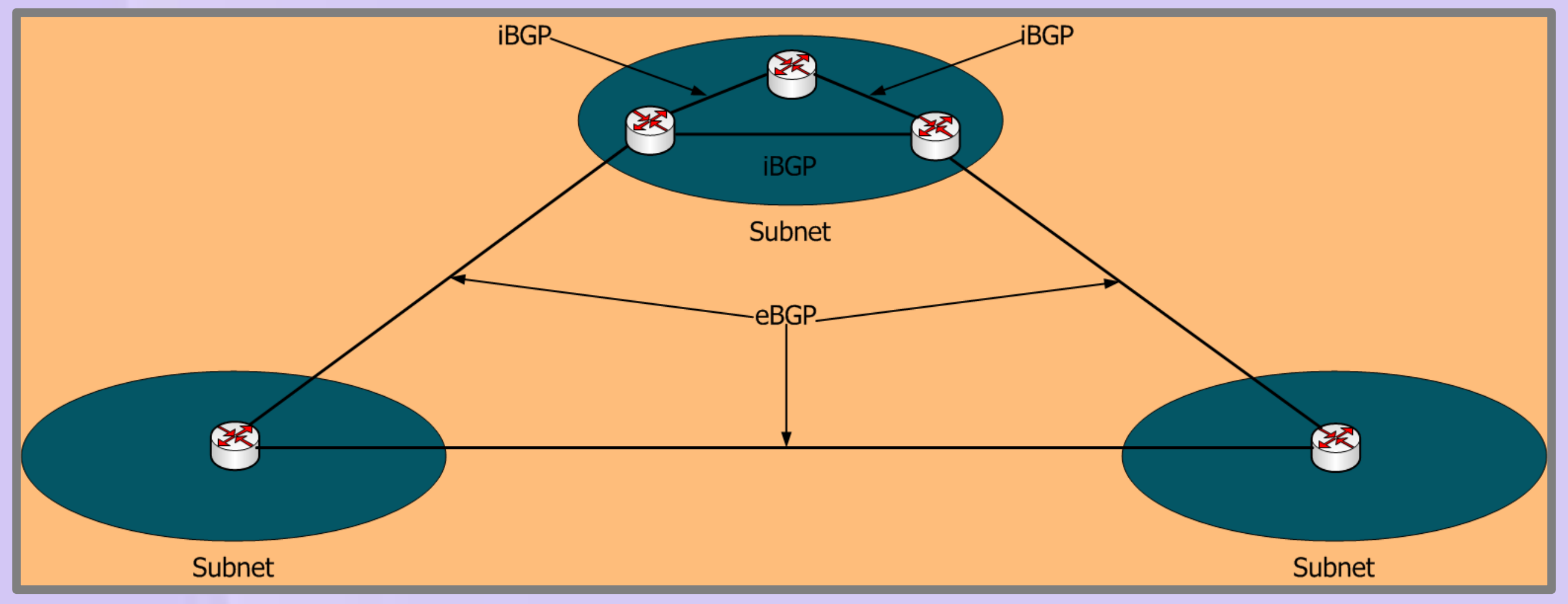
Improving the Internet Security using BGP Routing Information Base

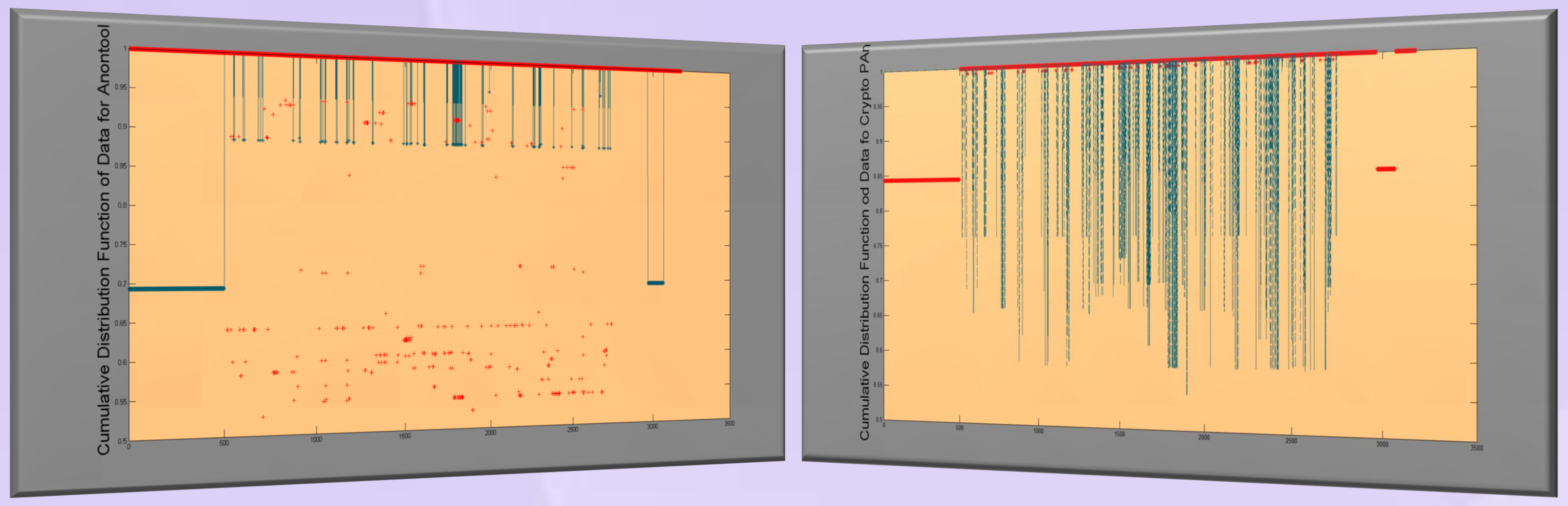
Nabil Al-Rousan, Khaled Alutaibi, Tanjila Farah, Rajvir Gill, Soroush Haeri, Sukhchandan Lally, Ravinder Paul, Reza Sahraei, Don Xu, and Ljiljana Trajković
Communication Networks Laboratory, Simon Fraser University, Vancouver, British Columbia, Canada

BGP Routing: Autonomous Systems



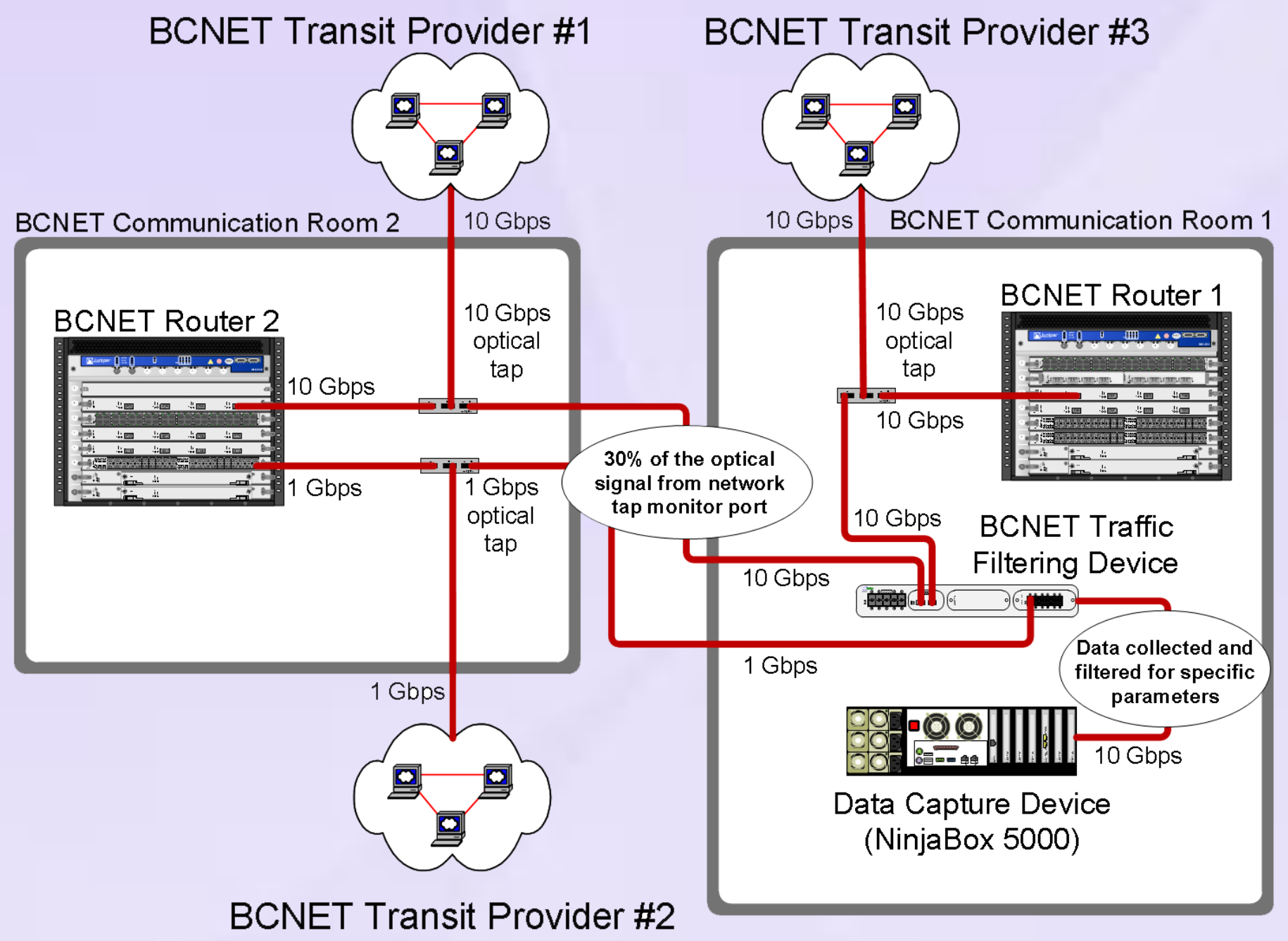
- Border Gateway Protocol (BGP) is de facto Inter-Autonomous System (AS) routing protocol
- Operates over a reliable transport protocol (TCP)
- Exchanges network reachability information among BGP systems
- Employs the Best Path Selection algorithm to select the routing path
- Supports Classless Inter Domain Routing
- Permits aggregation of routes

Anonymization: Anontool and Crypto-PAn



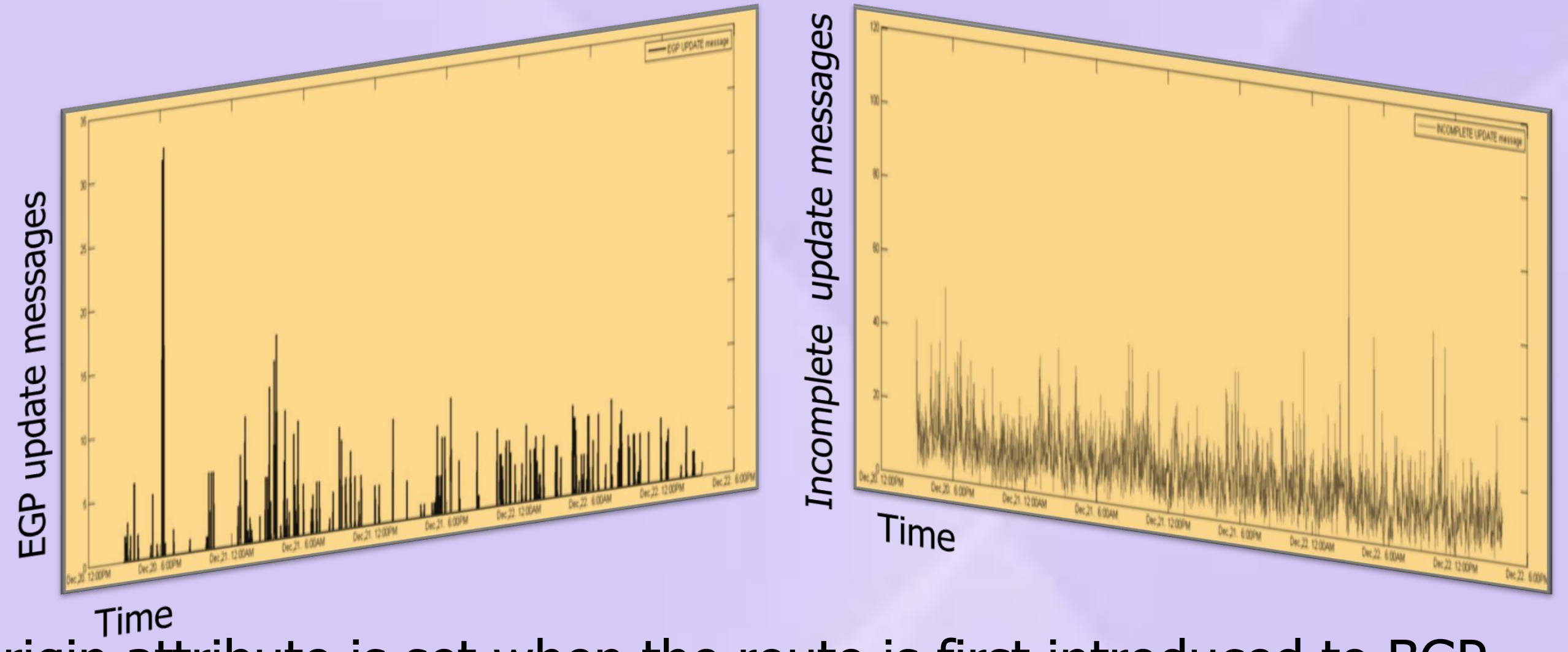
- Multiple tools are available for anonymizing traffic traces
- They modify traffic trace to suppress sensitive information
- Their goal is to provide balance between privacy and trace content
- Anontool and Crypto-Pan graphs show that they preserve structure of traffic trace

Packet Capture: BCNET Architecture


BCNET Transit Provider #1
BCNET Transit Provider #3
BCNET Communication Room 2
10 Gbps
10 Gbps
BCNET Communication Room 1
BCNET Router 2
10 Gbps optical tap
BCNET Router 1
10 Gbps optical tap
10 Gbps
10 Gbps
1 Gbps
1 Gbps optical tap
30% of the optical signal from network tap monitor port
10 Gbps
BCNET Traffic Filtering Device
10 Gbps
1 Gbps
Data collected and filtered for specific parameters
1 Gbps
10 Gbps
Data Capture Device (NinjaBox 5000)
BCNET Transit Provider #2

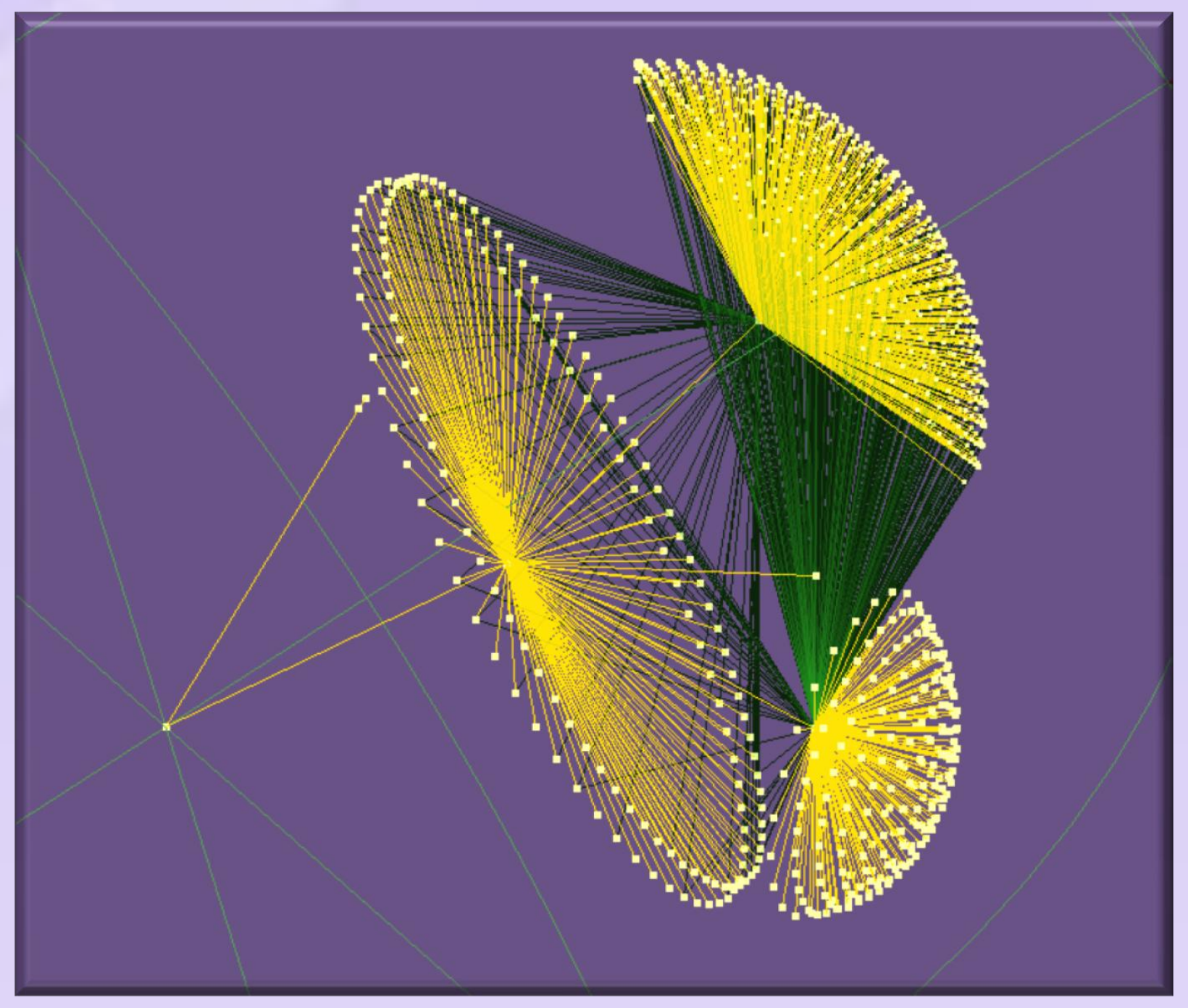
- Primary BCNET backbone is a 10 Gbps Ethernet network with 1 Gbps links for backup
- Data are sent to Traffic Filtering Device (Net Optics Director 7400) and to Data Capture Device (NinjaBox 5000)
- Optical Test Access Point (TAP) splits the signal into two distinct paths
- 30% of the split is sent to the Traffic Filtering Device that filters packets and sends filtered data to the Data Capture Device
- Transit providers are connected to BCNET via 1 Gbps and 10 Gbps links

BCNET Traffic: Analysis



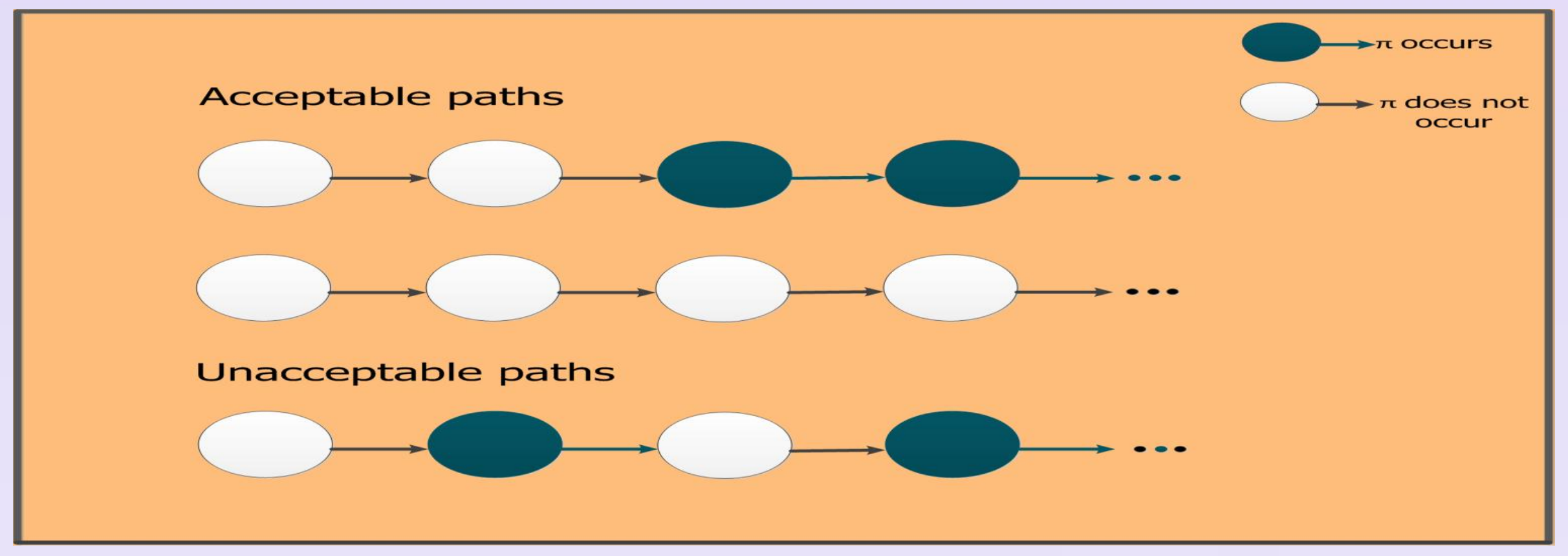
- Origin attribute is set when the route is first introduced to BGP
- Defines the origin of the path information
- Types of the origin attribute: Exterior Gateway Protocol (EGP), Interior Gateway Protocol (IGP), and incomplete
- 822 EGP packets and 33,932 incomplete packets were identified

BCNET: AS Topology Graph



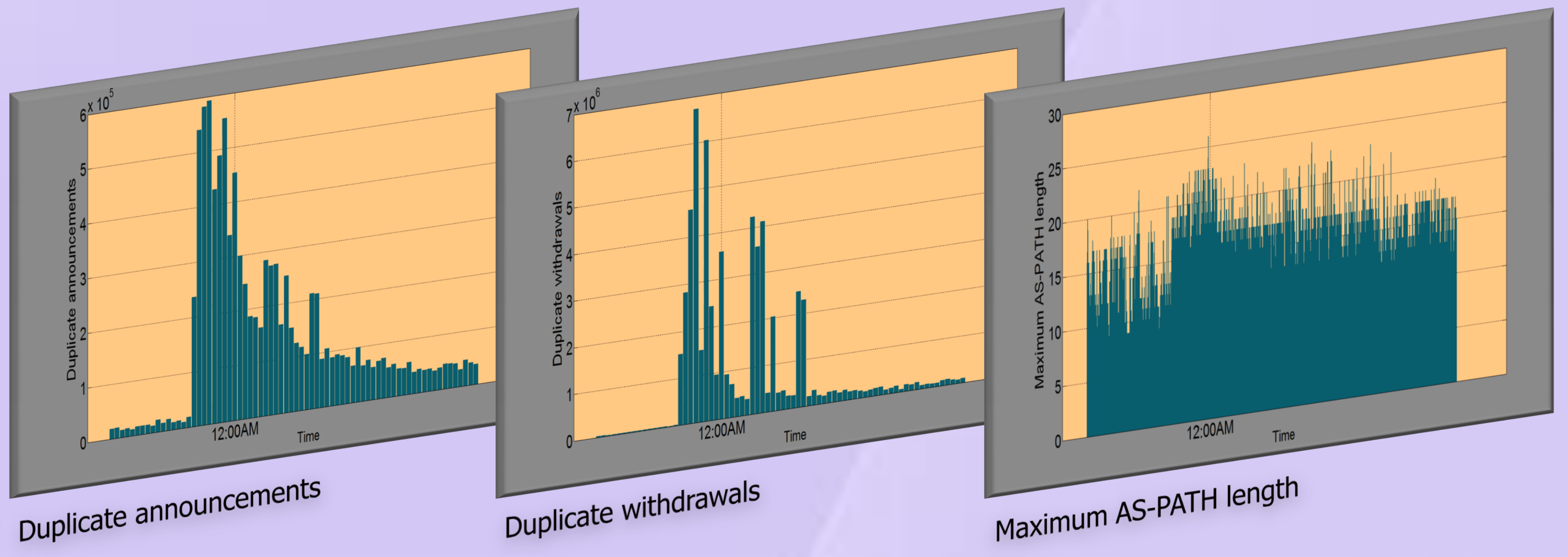
- 230,424 BGP update messages were found
- The graph: 982 nodes, 981 tree-links, and 441 non tree-links
- Clusters: 155, 683, and 588 AS nodes
- Created using BGP AS_path attribute from BGP update messages
- Graph links reflect a policy relationship between BCNET transit providers
- Centers of the three clusters correspond to BCNET transit providers: Telus Advanced Communications, Shaw Communications, and Peer 1 Network Inc.

BGP Convergence: Probabilistic Verification



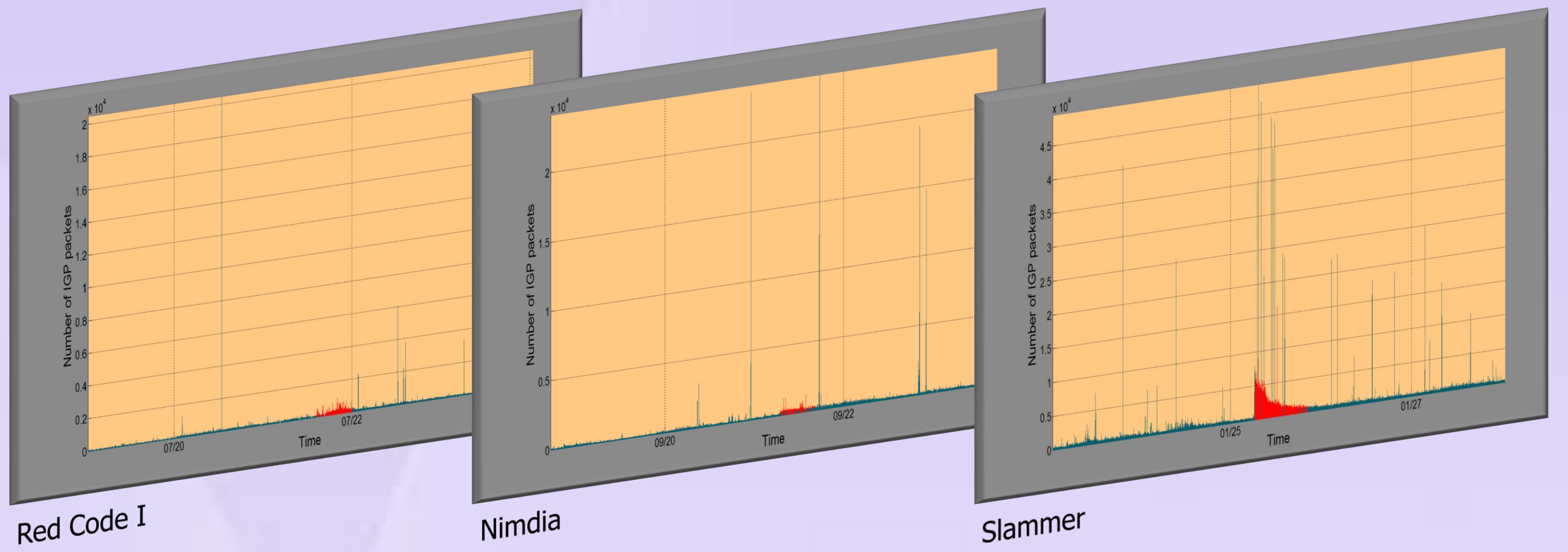
- An instance of BGP execution is safe with respect to an initial state π_0 if and only if there is no cyclic state.
- Probabilistic Computation Tree Logic: $P_{\geq 1}[\mathbf{GF}\ \pi \rightarrow \mathbf{FG}\ \pi]$, for all states $\pi \in Q(S)$, where Q(S) denotes set of all states
- Convergence time is calculated based on a rewarding function $\rho(\pi) = 1$, $\forall \pi \in Q(S)$
- The number of transitions until convergence is reached at a unique absorbing state δ is $R_{=?}[\mathbf{F}\ \delta]$

BGP Features: Selection



- Feature selection algorithms improve classification accuracy
- They were used to select the most relevant features in order to identify two BGP traffic classes: Anomaly and Regular
- Feature statistics were computed based on one-minute time intervals
- Selected features are used to train the Naive Bayes (NB), Support Vector Machine (SVM), and Hidden Markov Model (HMM) classifiers
- Graphs show extracted features during the Slammer worm attack on January 25, 2003

Detection of Worms: Machine Learning



- Anomalies such as Slammer, Nimda, and Code Red I affect BGP performance
- NB, SVMs, and HMMs classifiers are used as detection mechanisms by introducing new features
- Models are tested using BGP traffic collected from RIPE and BCNET
- Multi-classification models are developed to classify the correct anomaly type in test datasets
- The best achieved classification F-scores: NB (69.7%), SVM (86.1%), and HMM (84.4%)
- Graphs show correctly classified anomaly traffic (red) for Red Code I (July 19, 2001), Nimda (Sept. 8, 2001), and Slammer (Jan. 25, 2003)

References

- BCNET [Online]. Available: http://www.bc.net.
- Walrus - Graph Visualization Tool [Online]. Available: http://www.caida.org/tools/visualization/walrus.
- N. Al-Rousan and Lj. Trajković, "Comparison of machine learning models for classification of BGP anomalies," *HPSR 2012*, Belgrade, Serbia, June 2012 (to be presented).
- T. Farah, S. Lally, R. Gill, N. Al-Rousan, R. Paul, D. Xu, and Lj. Trajković, "Collection of BCNET BGP traffic," in *Proc. 23rd International Teletraffic Congress*, San Francisco, CA, USA, Sept. 2011, pp. 322–323 (students poster session paper).
- S. Haeri, D. Kresic, and Lj. Trajković, "Probabilistic verification of BGP convergence," in *Proc. IEEE International Conference on Network Protocols, ICNP 2011*, Vancouver, BC, Canada, Oct. 2011, pp. 127–128 (students poster session paper).
- Lj. Trajković, "Analysis of Internet topologies," *IEEE Circuits and Systems Magazine*, vol. 10, no. 3, pp. 48–54, Third Quarter 2010.

Communication Networks Laboratory
http://www.ensc.sfu.ca/~ljilja/cnl/