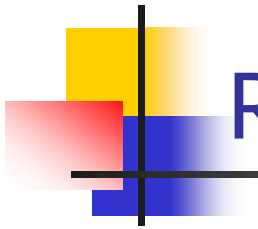
TCP session analysis and modeling of hybrid satellite-terrestrial Internet traffic

Savio Lau
saviol@cs.sfu.ca

Communication Networks Laboratory
http://www.ensc.sfu.ca/cnl
School of Engineering Science
Simon Fraser University

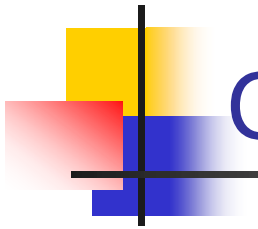


Roadmap

- Introduction:
  - satellite links
  - ChinaSat Network
- Analysis of user behavior from:
  - billing data
  - tcpdump
- Current work:
  - analysis of TCP connections
- Conclusions
- References

Characteristics of satellite links

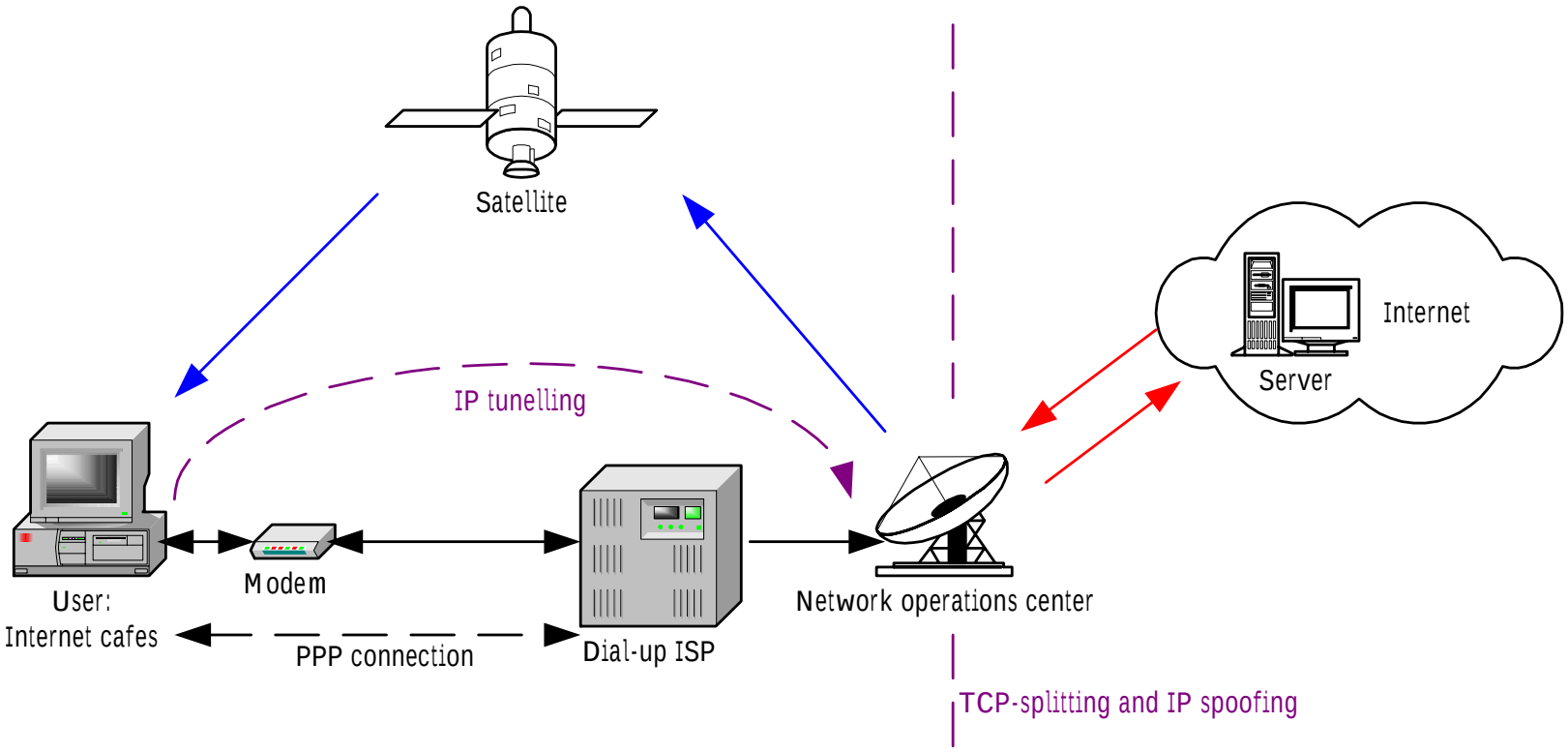
- Satellite links:
  - large coverage area
  - long link propagation delay (~250 ms)
  - high bandwidth-delay product
  - high bit error rates (~10^{-6} without error correction)
- Wired links:
  - bit error rates (~10^{-9})
  - short link propagation delay (< 1 ms)
- Wireless links:
  - bit error rates (~10^{-5})
  - variable link propagation delay



ChinaSat hybrid satellite network

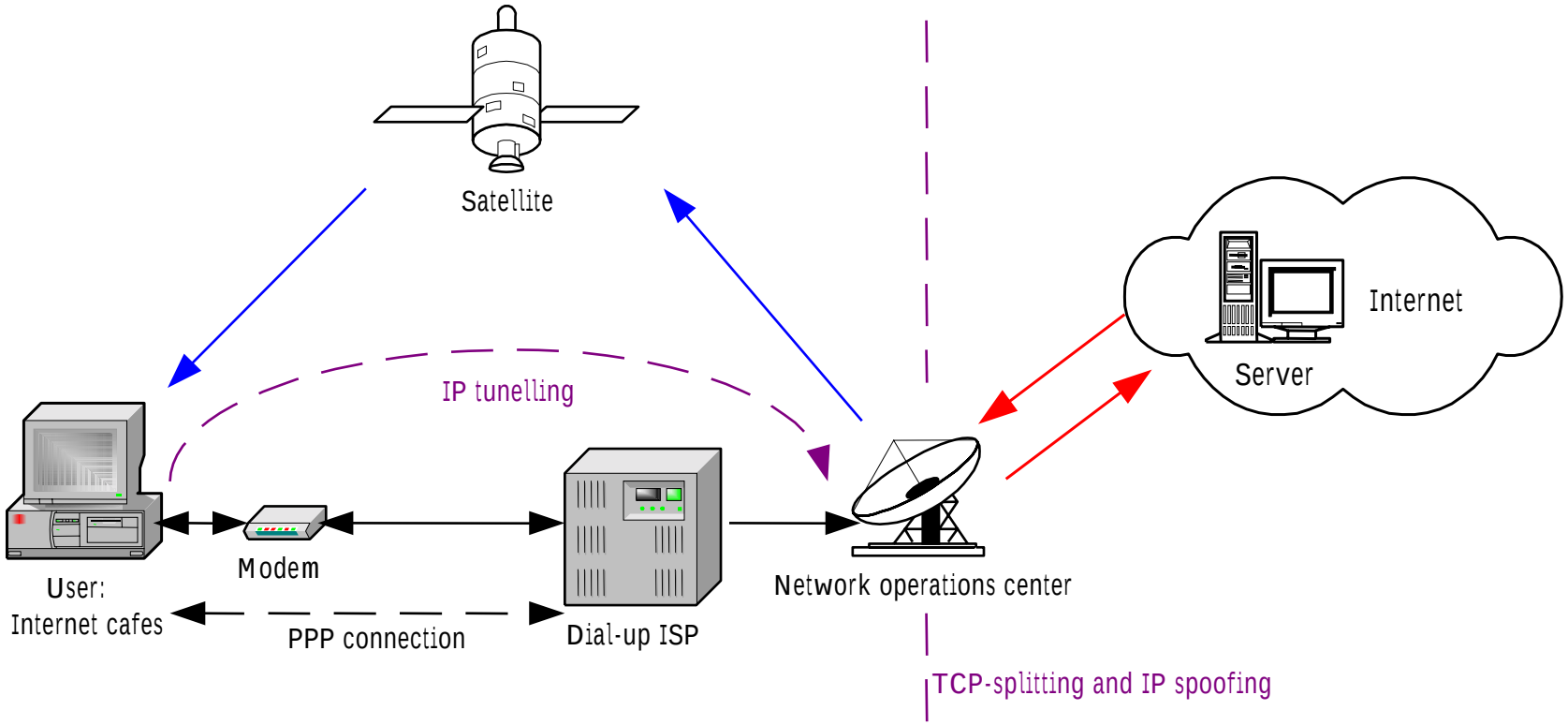
- Employs geosynchrous satellites deployed by Hughes Network Systems
- Provides data and television services:
  - DirecTV: satellite television service
  - DirecPC (Classic): unidirectional satellite data service
  - DirecWay (Hughnet): new bi-directional satellite data service that replaces DirecPC
- Collected ChinaSat DirecPC data:
  - continuous billing data from October 31, 2002 to January 10, 2003
  - 35 GBytes of data from tcpdump traces from December 14, 2002 to January 10, 2003

DirecPC system diagram



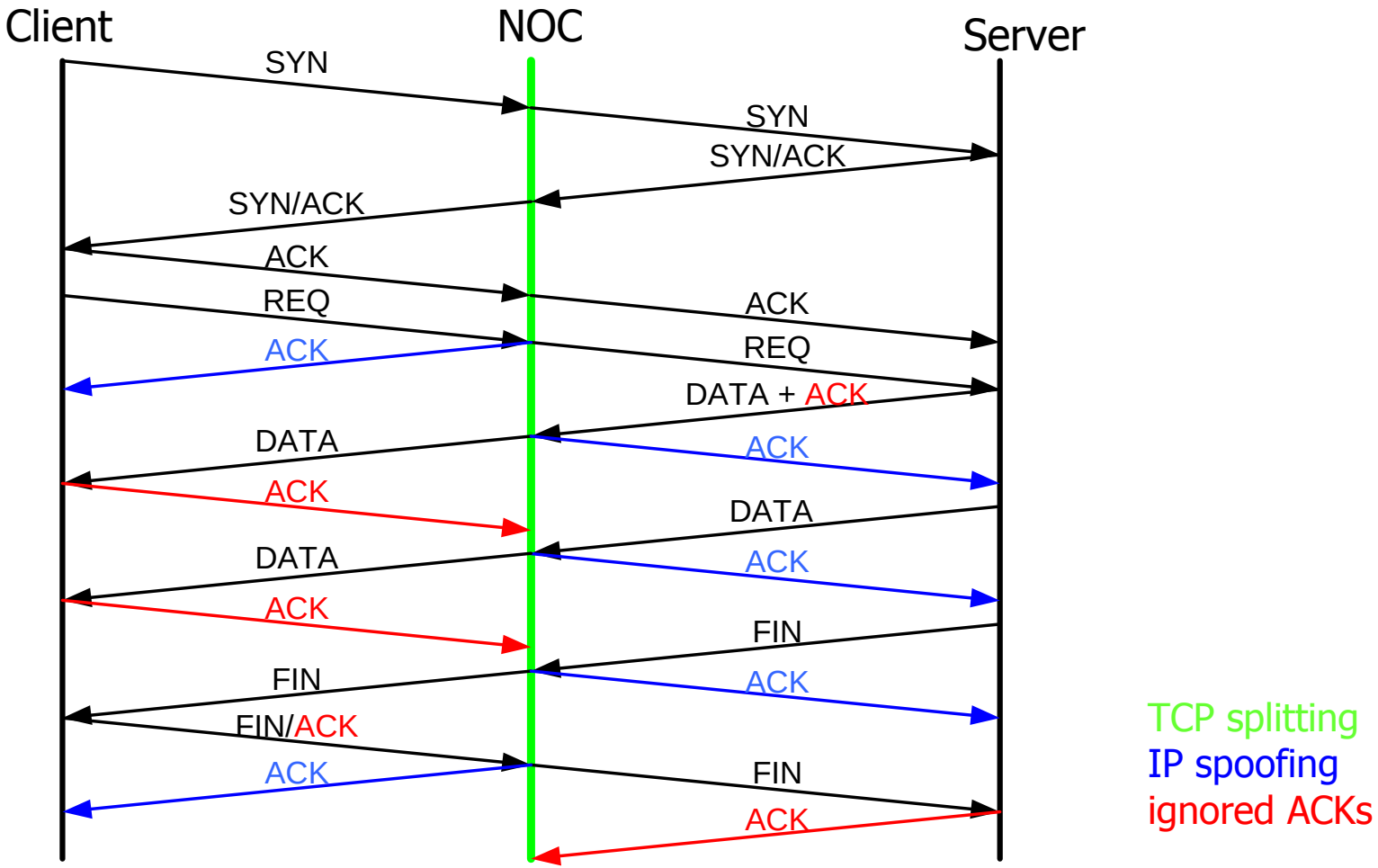
NOC: Network Operations Center
PPP: Point-to-point protocol

DirecPC system diagram



NOC: Network Operations Center
PPP: Point-to-point protocol

TCP splitting and IP spoofing



Previous work

- Performance enhancing proxies (J. Border et al., RFC 3135):
  - TCP-splitting and IP spoofing
  - increasing initial TCP congestion window
- Analysis of HTTP over satellite (H. Kruse and M. Allman)
- Prediction and analysis (long-range dependence) of ChinaSat traffic data (Q. Shao and Lj. Trajkovic)

J. Border, M. Kojo, J. Griner, G. Montenegro, and Z. Shelby, "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations," *RFC 3135*, June 2001.

H. Kruse and M. Allman, "Experimentation and modeling of HTTP over satellite channels," *International Journal of Satellite Communications*, vol. 19, no. 1, pp. 51–68, Feb. 2001.

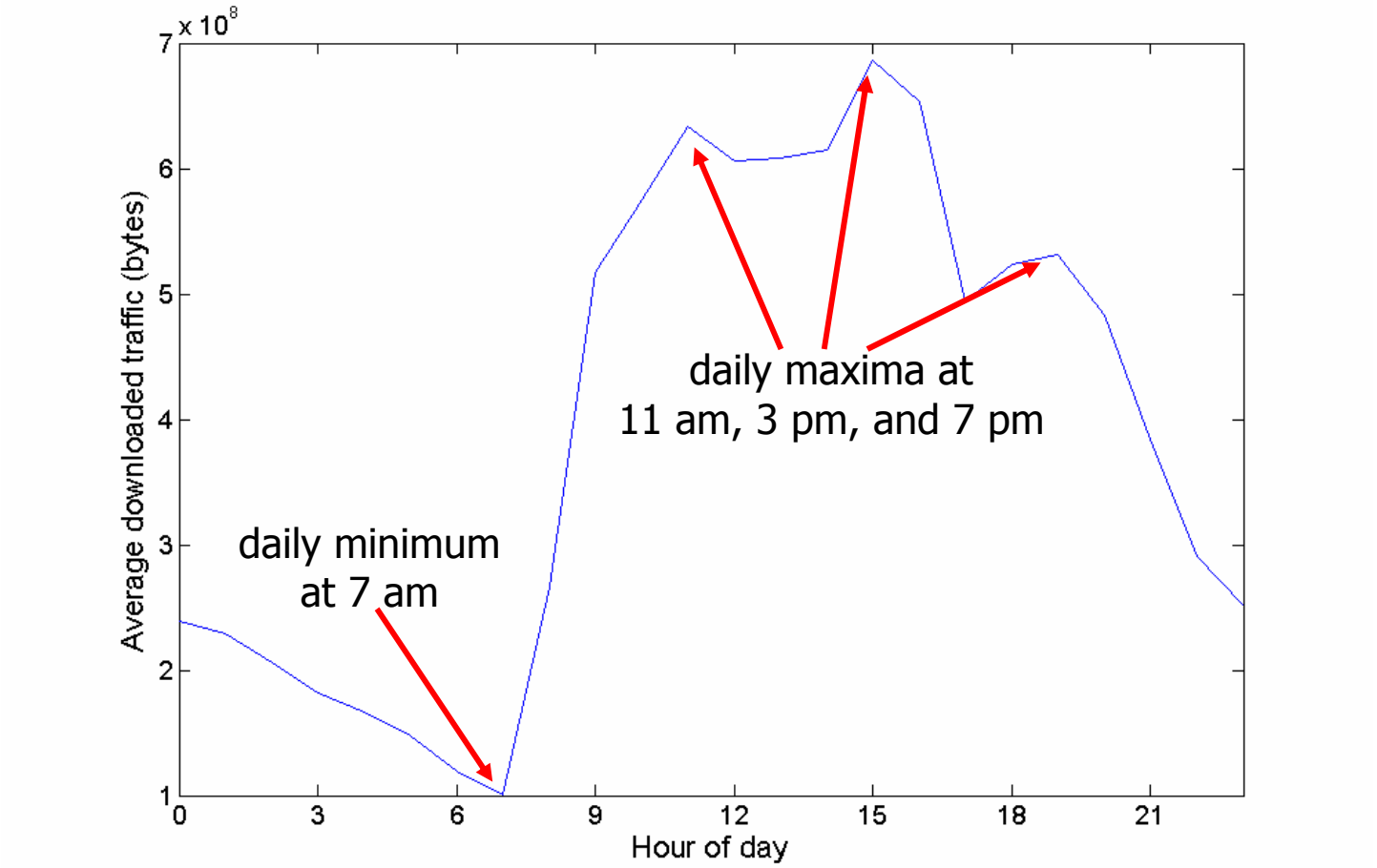
Q. Shao and Lj. Trajković, "Measurement and analysis of traffic in a hybrid satellite-terrestrial network," *Proc. SPECTS 2004*, San Jose, CA, July 2004, pp. 329–336.

Preliminary billing data results

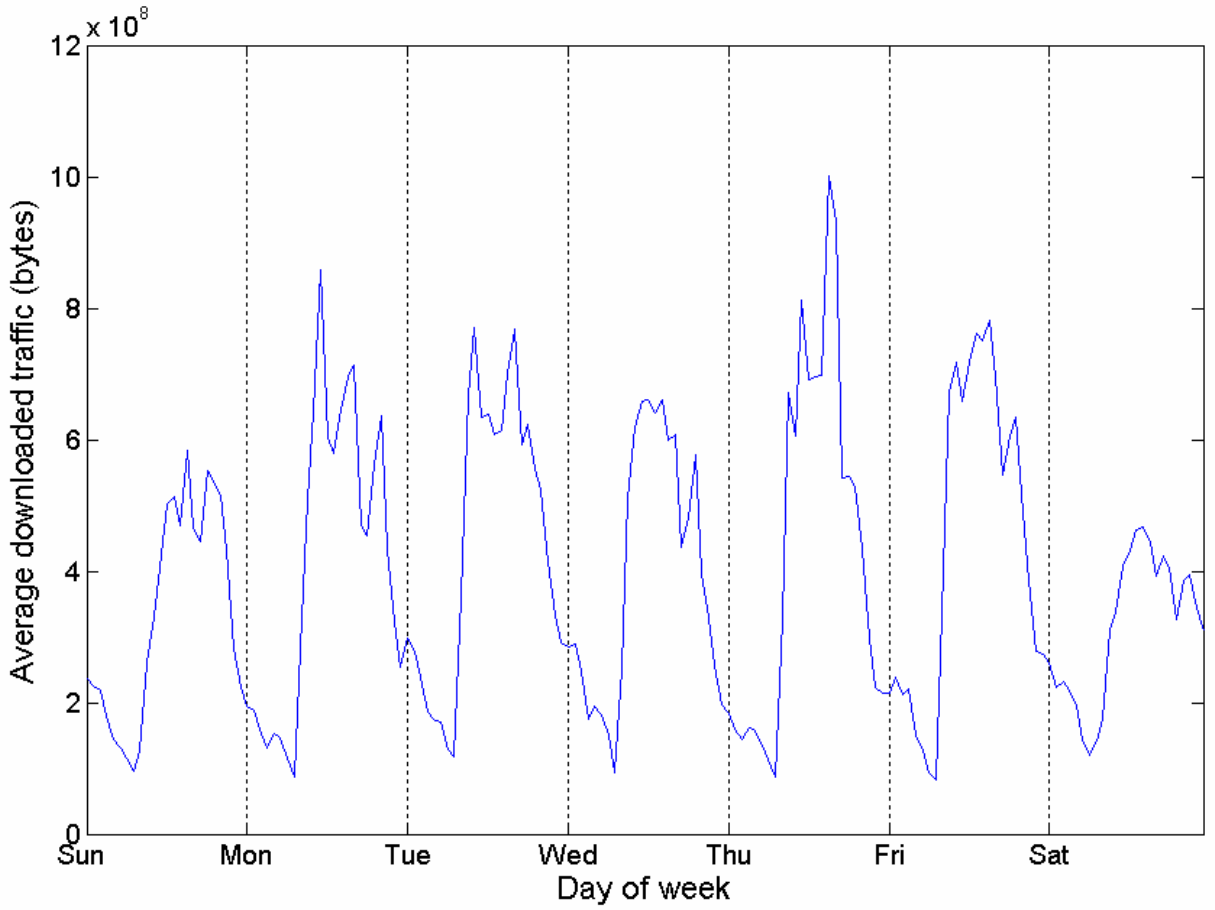
- Daily (diurnal) traffic pattern:
  - averaged over recorded period (October 31, 2002 to January 10, 2003)
  - traffic pattern similar to previous research results (Thompson, Miller, and Wilder)
- Weekly traffic pattern:
  - averaged over recorded period
  - lower traffic volume on Saturdays and Sundays

K. Thompson, G. J. Miller, and R. Wilder, "Wide-area Internet traffic pattern and characteristics," *IEEE Network*, vol. 11, no. 6, pp. 10–23, Nov. 1997.

Daily (diurnal) traffic pattern: average downloaded bytes



Weekly traffic pattern: average downloaded bytes



Preliminary tcpdump results

- Majority of traffic (> 90%) is TCP
  - TCP traffic mostly uses the HTTP protocol
- Considerable volume of traffic is illegitimate:
  - TCP packets with invalid TCP flag combinations
  - port scans originating from the ChinaSat network users
  - port scans directed to the ChinaSat network users

Port scans are generated packets designed to search for open ports (and exploit vulnerabilities) on a network host

TCP SYN/RST/FIN/PSH analysis

TCP flag	Count	% of Total
SYN only	19,050,849	48.5%
RST only	7,440,418	18.9%
FIN only	12,679,619	32.3%
SYN+FIN	408	0.001%
RST+FIN (no PSH)	85,571	0.2%
RST+PSH (no FIN)	18,111	0.05%
RST+FIN+PSH	8,329	0.02%
Total number of packets with illegitimate TCP flag combinations	112,419	0.3%
Total packet count	39,283,305	

Port scans originating from the ChinaSat network users

192.168.2.30:137 - 195.x.x.98:1025
192.168.2.30:137 - 202.x.x.153:1027
192.168.2.30:137 - 210.x.x.23:1035
192.168.2.30:137 - 195.x.x.42:1026
192.168.2.30:137 - 202.y.y.226:1026
192.168.2.30:137 - 218.x.x.238:1025
192.168.2.30:137 - 202.y.y.226:1025
192.168.2.30:137 - 202.y.y.226:1027
192.168.2.30:137 - 202.y.y.226:1028
192.168.2.30:137 - 202.y.y.226:1029
192.168.2.30:137 - 202.y.y.242:1026
192.168.2.30:137 - 61.x.x.5:1028
192.168.2.30:137 - 219.x.x.226:1025
192.168.2.30:137 - 213.x.x.189:1028
192.168.2.30:137 - 61.x.x.193:1025
192.168.2.30:137 - 202.y.y.207:1028
192.168.2.30:137 - 202.y.y.207:1025
192.168.2.30:137 - 202.y.y.207:1026
192.168.2.30:137 - 202.y.y.207:1027
192.168.2.30:137 - 64.x.x.148:1027

Client (192.168.2.30) using source port (137) scans external network addresses with UDP packets at destination ports (1025-1040):

- > 100 are recorded within a three hour period
- scanned IP addresses are variable
- multiple ports are scanned per IP
- corresponds to Bugbear (Sept. 2002), OpaSoft (Sept. 2002), or other worms

Port scans directed to the ChinaSat network users

210.x.x.23:1035 - 192.168.1.121:137
210.x.x.23:1035 - 192.168.1.63:137
210.x.x.23:1035 - 192.168.2.11:137
210.x.x.23:1035 - 192.168.1.250:137
210.x.x.23:1035 - 192.168.1.25:137
210.x.x.23:1035 - 192.168.2.79:137
210.x.x.23:1035 - 192.168.1.52:137
210.x.x.23:1035 - 192.168.6.191:137
210.x.x.23:1035 - 192.168.1.241:137
210.x.x.23:1035 - 192.168.2.91:137
210.x.x.23:1035 - 192.168.1.5:137
210.x.x.23:1035 - 192.168.1.210:137
210.x.x.23:1035 - 192.168.6.127:137
210.x.x.23:1035 - 192.168.1.201:137
210.x.x.23:1035 - 192.168.6.179:137
210.x.x.23:1035 - 192.168.2.82:137
210.x.x.23:1035 - 192.168.1.239:137
210.x.x.23:1035 - 192.168.1.87:137
210.x.x.23:1035 - 192.168.1.90:137
210.x.x.23:1035 - 192.168.1.177:137
210.x.x.23:1035 - 192.168.1.39:137

External address (210.x.x.23) employs UDP packets to scans port (137) for NETBIOS response within the ChinaSat network from source port (1035):

- > 200 are recorded within a 3 hour period
- scanned IP addresses are not sequential
- corresponds to Bugbear (Sept. 2002), OpaSoft (Sept. 2002), or other worms

Current work

- Compare the volume of illegitimate and total traffic
- Use tcptrace to identify and analyze individual connections
- Use analysis results to model the TCP traffic (connection inter-arrival times, connection duration, number of bytes)
- Examine effects of:
  - HTTP pipelining
    - clients can send multiple HTTP requests at a time
    - servers can send multiple HTTP replies per connection
  - concurrent HTTP connections
  - HTTP 1.0 vs. HTTP 1.1

Conclusions

- Satellite data traffic have:
  - daily (diurnal) traffic patterns
  - weekly periodic traffic patterns
  - similar to wide-area Internet traffic patterns
- Illegitimate data traffic is found in the trace:
  - packets with invalid TCP flags
  - port scans originating from the ChinaSat network users
  - port scans directed to the ChinaSat network users

References

[1] Q. Shao and Lj. Trajkovic, "Measurement and analysis of traffic in a hybrid satellite-terrestrial network," *Proc. SPECTS 2004*, San Jose, CA, July 2004, pp. 329–336.

[2] T. R. Henderson and R. Katz, "Transport protocols for Internet-compatible satellite networks," *IEEE J. Select. Areas Commun.*, vol. 17, no. 2, pp. 326–344, Feb. 1999.

[3] H. Kruse and M. Allman, "Experimentation and modeling of HTTP over satellite channels," *International Journal of Satellite Communications*, vol. 19, no. 1, pp. 51–68, Feb. 2001.

[4] K. Thompson, G. J. Miller, and R. Wilder, "Wide-area Internet traffic pattern and characteristics," *IEEE Network*, vol. 11, no. 6, pp. 10–23, Nov. 1997.

[5] M. Arlitt and C. Williamson, "An analysis of TCP reset behaviour on the Internet," *Computer Communications Review*, vol. 35, no. 1, pp.37–44, Jan. 2005.

[6] W. R. Stevens, *TCP/IP Illustrated, Vol. 1: The Protocols*, Reading, MA: Addison Wesley, 1994.

[7] D. E. Comer, *Internetworking with TCP/IP: Principles, Protocols and Architectures, 4th ed.* Upper Saddle River, NJ: Prentice Hall, 2000, pp. 209–254.

References: RFCs

[8] Information Sciences Institute, "Transmission control protocol," *RFC 793*, Sept. 1981.

[9] Information Sciences Institute, "TCP and IP bake off," *RFC 1025*, Sept. 1987.

[10] M. Allman, D. Glover, and L. Sanchez, "Enhancing TCP over satellite channels using Standard Mechanisms," *RFC 2488*, Jan. 1999.

[11] M. Allman, S. Dawkins, D. Glover, J. Griner, D. Tran, T. Henderson, J. Heidemann, J. Touch, H. Kruse, S. Ostermann, K. Scott, and J. Semke, "Ongoing TCP research related to satellites," *RFC 2760*, Feb. 2000.

[12] J. Border, M. Kojo, J. Griner, G. Montenegro, and Z. Shelby, "Performance enhancing proxies intended to mitigate link-related degradations," *RFC 3135*, June 2001.

[13] S. Floyd, "Inappropriate TCP resets considered harmful," *RFC 3360*, Aug. 2002.