

# Security Topics in Networking and Distributed Systems CS 590D

## **Lecture 12: BGP Security (cont.)**

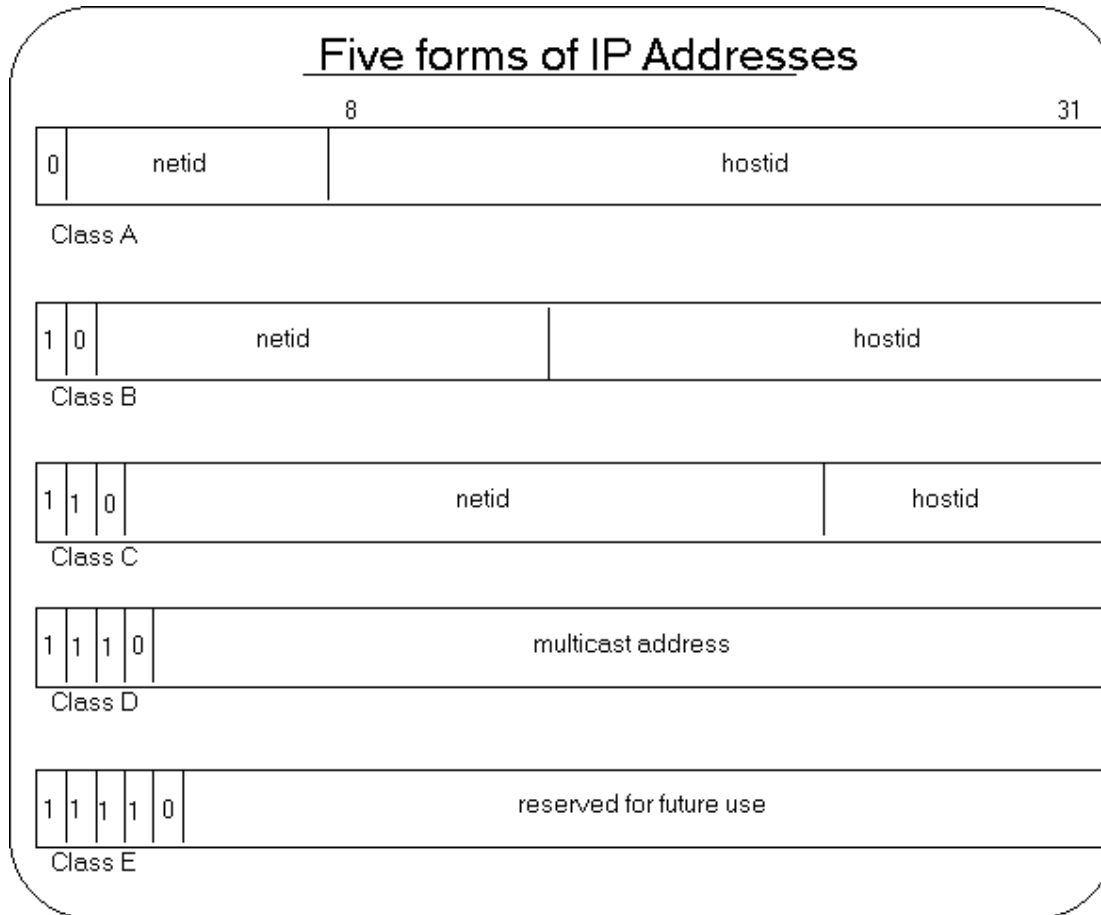
Department of Computer Sciences  
Purdue University

# References

- Detection of Invalid Routing Announcement in the Internet. Xiaoliang Zhao, Dan Pei, Lan Wang, Dan Massey, Allison Mankin, S. Felix Wu, Lixia Zhang, DSN 2002.
- Topology-based detection of anomalous BGP messages. C. Kruegel, D. Mutz, W. Robertson, F. Valeur, RAID 2003.



# IP address: a reminder



Class A:  
1.0.0.0 - 126.0.0.0

Class B:  
127.0.0.0 - 191.255.0.0

Class C:  
192.0.0.0 - 223.255.255.0

Class D:  
224.0.0.0 - 240.0.0.0

Class E:  
241.0.0.0 - 248.0.0.0

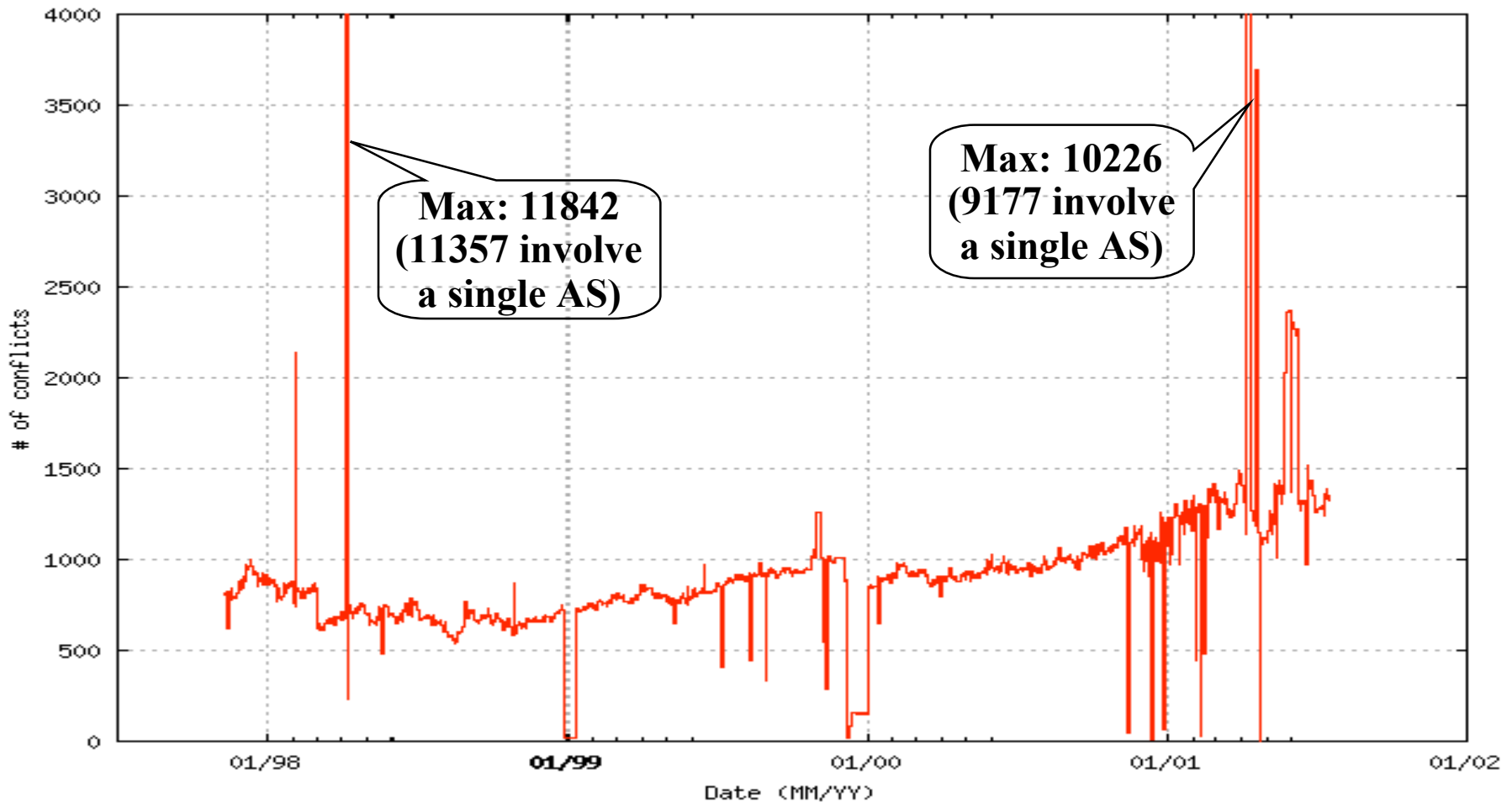
# What Are Invalid Announcements?

- Bogus route announcements from false origins
- Undetected faults can create black-holes
- Multiple Origin AS (MOAS): a prefix is announced by more than one AS.
  - Some of these announcement are legitimate
  - Some are configuration errors
  - Some are malicious

# Possible Solution

- Using cryptographic mechanisms (authentication, data integrity, attestations, based on PKI)
- Exploit the dense connectivity existing in the Internet
- Based on observations about the topology of the Internet: core nodes vs. periphery nodes

# How Often Do IA Occur ?



# Agreement on the Origin

- Create a list of the multiple ASes allowed to originate a particular IP prefix and attach the list to the route announcements
- Exploit the distributed nature of the Internet to spread the correct information
- A richly connected network contains multiple paths between a particular source and destination
- It will be very difficult for a particular node to block all paths.

# Does it Work?

- What if there exists only one path from one originating AS to the rest of the network?
- Do we need cryptographic mechanisms to protect the list?
- How difficult is for an attacker to block or modify the origin AS list?
- False alarms?

# What About in Practice?

- Effectiveness at preventing the propagation of false information
- Scaling to large networks
- How effective is if only partially deployed?
- How many router are affected (adopt the bad path) by an attack?

# Numbers

- 96% of all prefixes have a path of only 2 AS and 2.7% have a path of 3.
- Simulations network of 46 AS:
  - Original protocol 4% of AS inject false data, 36% of AS adopt;
  - With agreement on origin, 4% of AS inject false, 0.15% adopt false path;
  - 30% inject false data, 9.8 routers adopt false paths

# Other Approach

- Exploiting topology, classify ASes:
  - **Core nodes**: large ISPs, well connected
  - **Periphery nodes**: local providers, companies and universities
- Periphery nodes
  - Few links with core nodes
  - When they are connected to each other, they are also close geographically

# More Observations

- How does a path in the BGP UPDATE look like?
- **For a valid UPDATE, list of cored nodes, once the path leaves the core nodes, does not come back**

# Solution

- Construct the connectivity graph
- Classify nodes as core and peripheral
- How? Use the node degree and pruning. 10 to 15 % AS are labeled as core nodes.
- Decompose the complete AS graph in clusters of periphery nodes

# Solution (cont.)

- Subsequence of AS in the path list may only contain a subsequence of core nodes
- All consecutive pairs of periphery nodes must either be part of the same cluster, or when a link is established between two previously unconnected clusters, must be in close geographical distance
- Threshold distance set to 300 Km

# Limitations

- What happens when a core node announces a new prefix, whose propagation stops also in a core node
- What about a peripheral node announcing has direct connection with other peripheral node (path does not traverse core nodes).
- If network topology changes and/or IP address allocation, how valid remains the classification of peripheral and core nodes?

# To Summarize (1)...

- BGP provides information routing between AS
- No security mechanisms
- Malfunctions of BGP translated into large-scale problems: big parts of the Internet can become unreachable
- Problems?
  - IP ownership
  - Intermediate path validation
  - Multiple origin
  - Injection/modification of BGP specific packets

# To Summarize (2)...

- **SBGP:**
  - Secure the BGP traffic by using IPSEC, ESP mode with no encryption (provides authentication and integrity)
  - Uses Public Key Infrastructure to provide an authorization for the mapping between address space and AS
  - Uses digital signatures to bind authorization information to UPDATE messages

# To Summarize (3)...

- Include a list of possible origins and attach it to UPDATE messages; use the high interconnectivity of the Internet to distribute this info (multiple-paths)
- Topology based: core nodes and periphery nodes; examine the order of the AS in the list in the UPDATE message; only one sequence of core nodes should exist