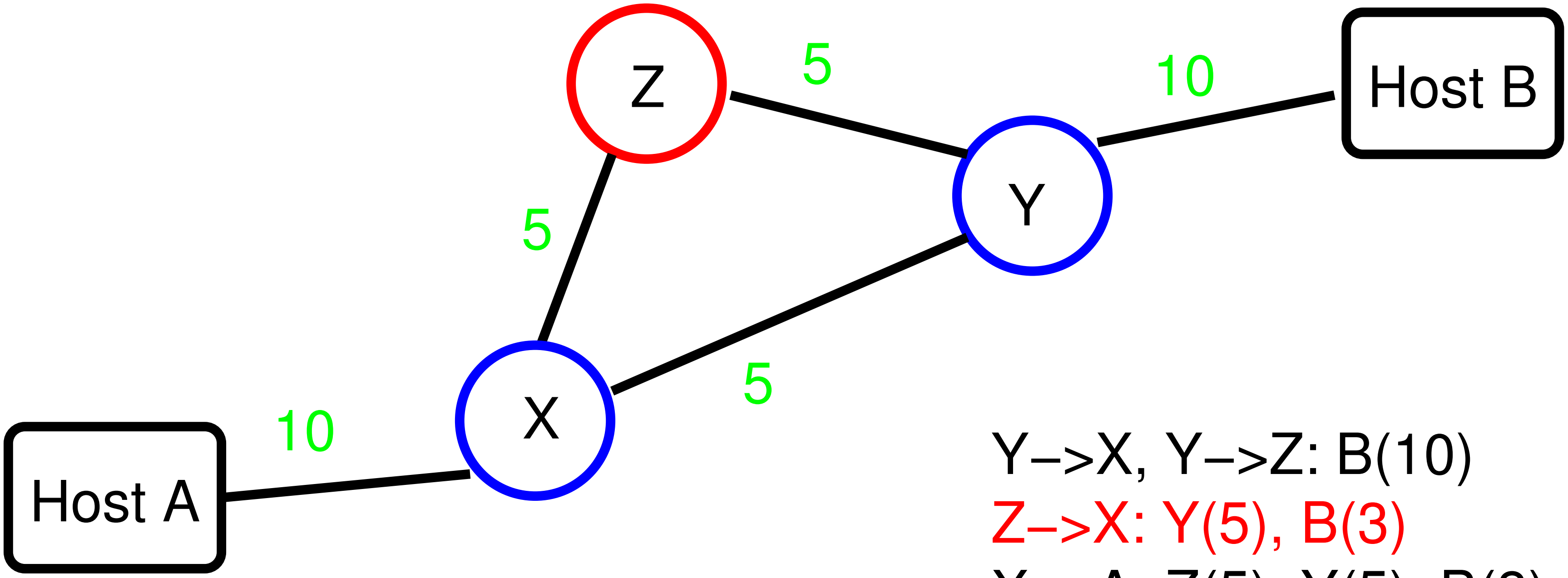
Link-Cutting Attacks

Steven M. Bellovin *Emden R. Gansner*
`smb@research.att.com` `erg@research.att.com`

AT&T Labs Research

Florham Park, NJ 07932

Classic Routing Attacks: Z Can Lie



Y–>X, Y–>Z: B(10)
Z–>X: Y(5), B(3)
X–>A: Z(5), Y(5), B(8)

Note that X is telling the truth as it knows it.

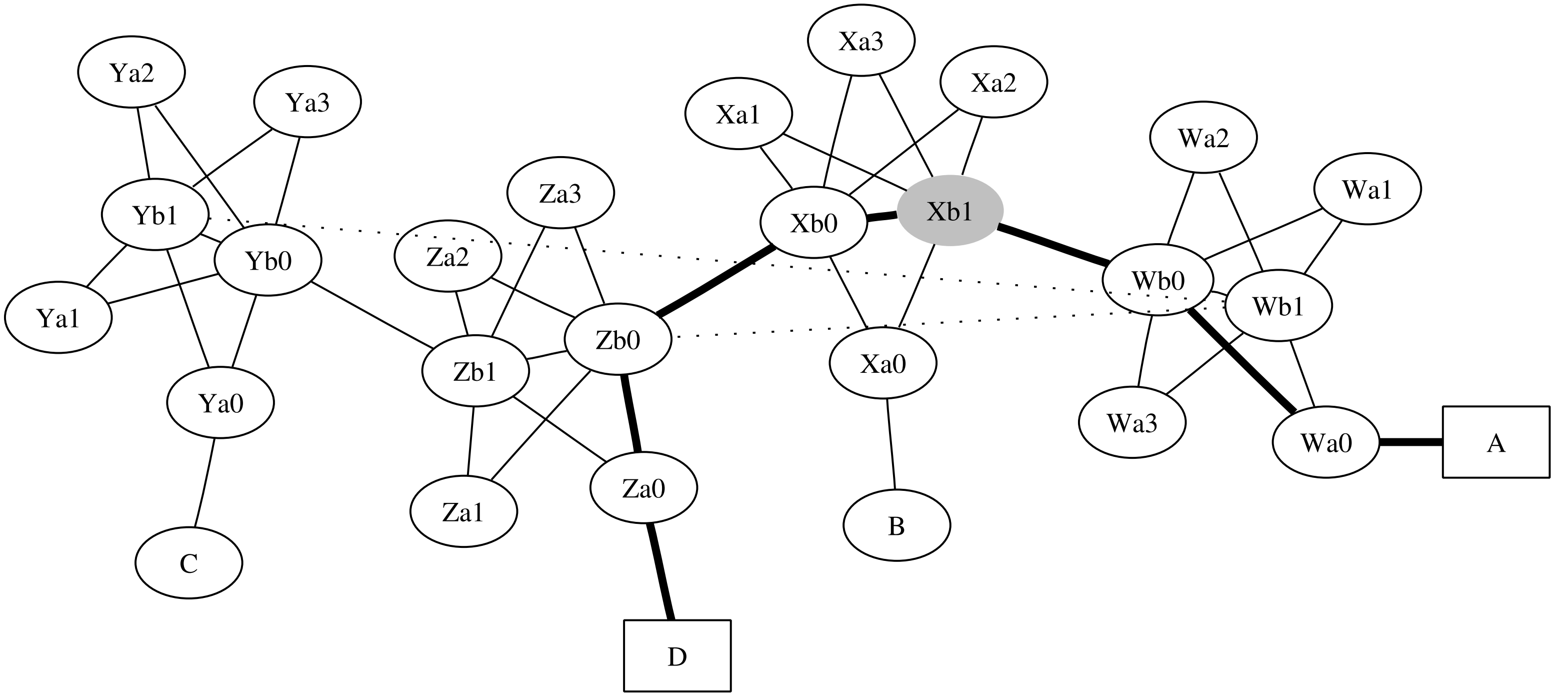
What Can We Do?

- In theory, we can secure routing protocols.
- SBGP uses digitally signed paths; there’s also a Secure OSPF design.
- But. . .

A New Attack

- Suppose that we've deployed secure routing protocols
- Suppose the attacker controls some links or nodes, and has a map of the topology.
- It's computationally feasible for the attacker to calculate what links to cut to force traffic past the controlled points.

The Attacker Has Compromised Node X1



The dotted lines are the cut links.

Results

- In hundreds of trials on intra- and inter-ISP topologies, we had a success rate of 80-90%.
- Each calculation takes at most a few seconds, even on very large topologies.

Link-Cutting Attacks

http://www.research.att.com/~smb/papers/reroute.ps

http://www.research.att.com/~smb/papers/reroute.pdf