Secure Routing Measurement

Boaz Barak, Princeton (joint work with S. Goldberg, J. Rexford, E. Tromer, and D. Xiao)

Internet communication is conveyed through paths chosen by *routing protocols*. But current protocols can be easily manipulated by malicious hosts. These need not be hackers - such manipulation can occur by legitimate hosts for political or business reasons. In this work we designed lightweight protocols to enable secure measurement of routing path quality, even in the face of malicious manipulation.

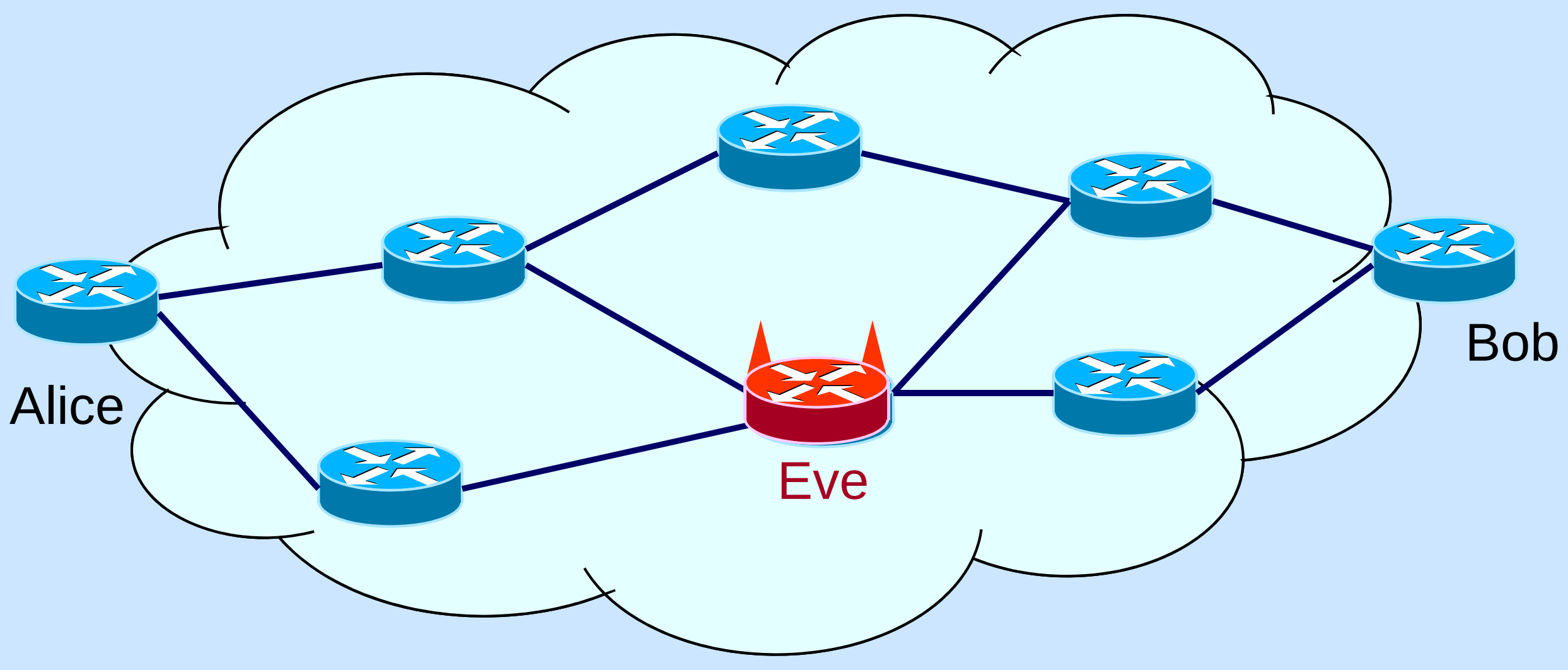
We consider two basic tasks –

1)Path Quality Monitoring (PQM) – detect if more than certain fraction of messages on a route fail to arrive to destination.

2)Failure localizing PQM (FL-PQM) – find the edge along the path where failures happened.

We give protocols and limitation results for both cases.

Work to appear in SIGMETRICS 08 (results on PQM) and EUROCRYPT 08 (results on PQM-FL).



A PQM protocol allows Alice to detect if her packets arrive to Bob even in presence of malicious intermediate Eve

Approach and Impact

New approach	Research Impact
• Rigorous definitions of security	• Protocols with *proven* security
• Proving impossiblity results	• Inform net design choices
• Using low storage sketches	• Extremely lightweight protocols

Our main results are:

1) Path Quality Measurement (PQM) protocols that are efficient enough to run in high-speed routers even for very strong threat model.
•Secure sketch PQM for lightweight packet loss monitoring.
•Secure sampling PQM for packet loss and delay monitoring
•Asymmetric sampling PQM for client-server setting
Protocols are incentive compatible because only the end points are involved.

2) Negative results for Fault Localization (FL): Very strong threat model for FL means that any FL protocol requires participation from all nodes on the path (i.e. keys and crypto): Protocols may be best for highly secure networks / important traffic

National Science Foundation
WHERE DISCOVERIES BEGIN

**NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT**