Listen and Whisper: Security Mechanisms for BGP

Lakshminarayanan Subramanian

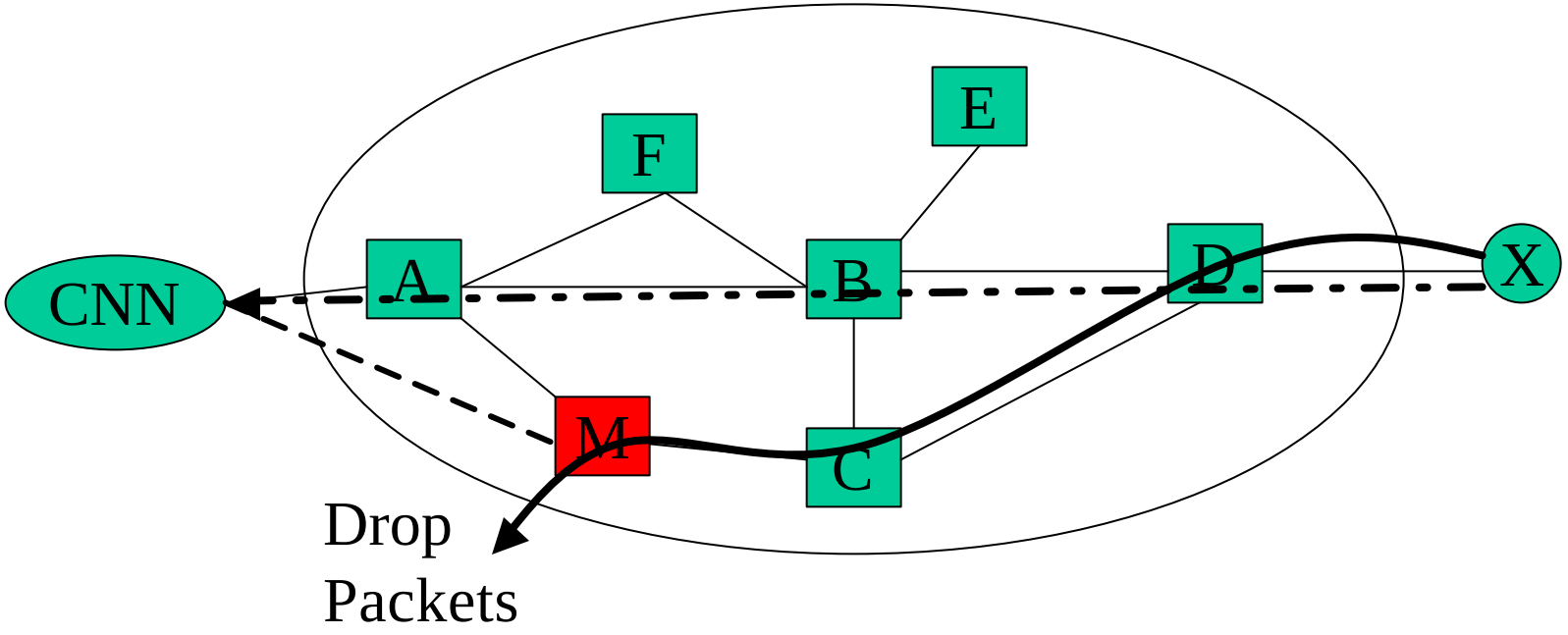
UC Berkeley

Joint work with: Volker Roth, Ion Stoica, Scott Shenker, Randy Katz

BGP Route Verification

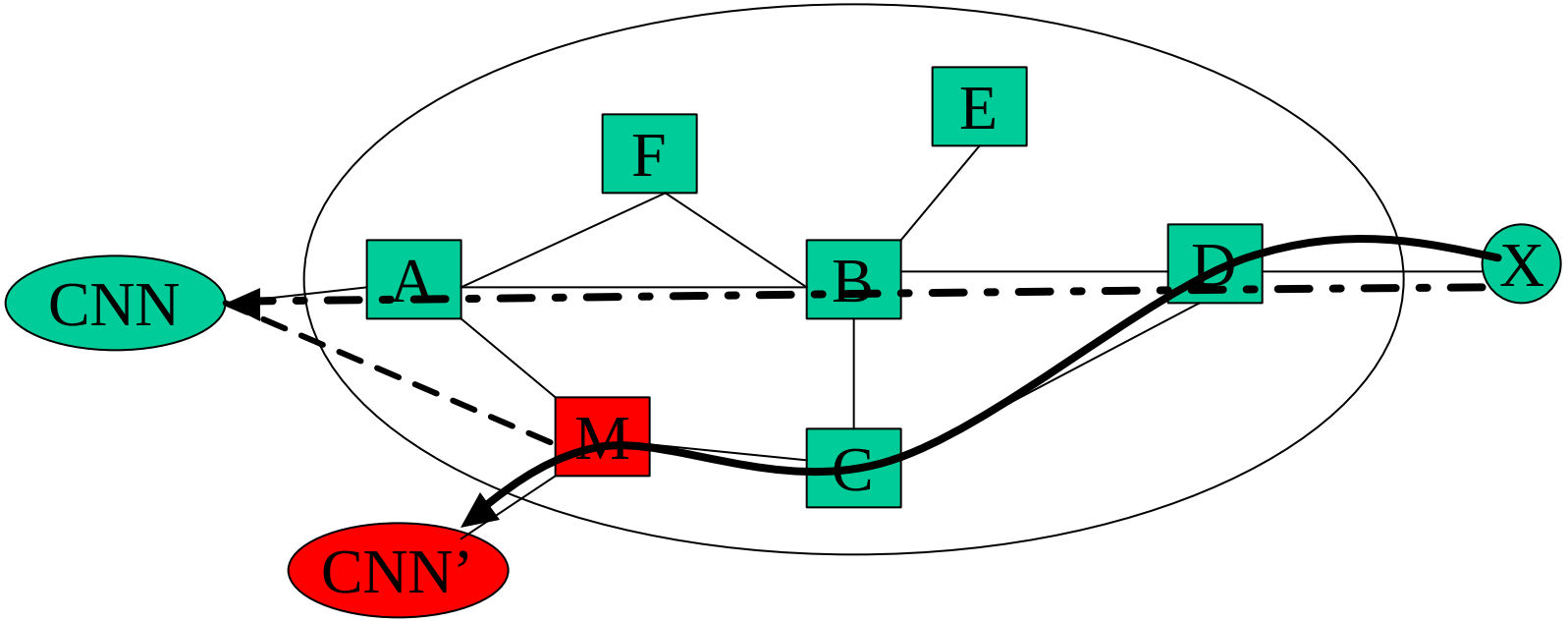
- BGP speakers blindly assume that routes advertised by neighboring nodes are correct
  - What if a router propagates spurious routes?
- Potential Causes
  - Router mis-configurations
  - Malicious behavior
- Potential Effects
  - Drop packets and render a destination ***unreachable***
  - ***Eavesdrop*** the traffic to a given destination
  - ***Impersonate*** the destination

Effect: Blackhole Attack



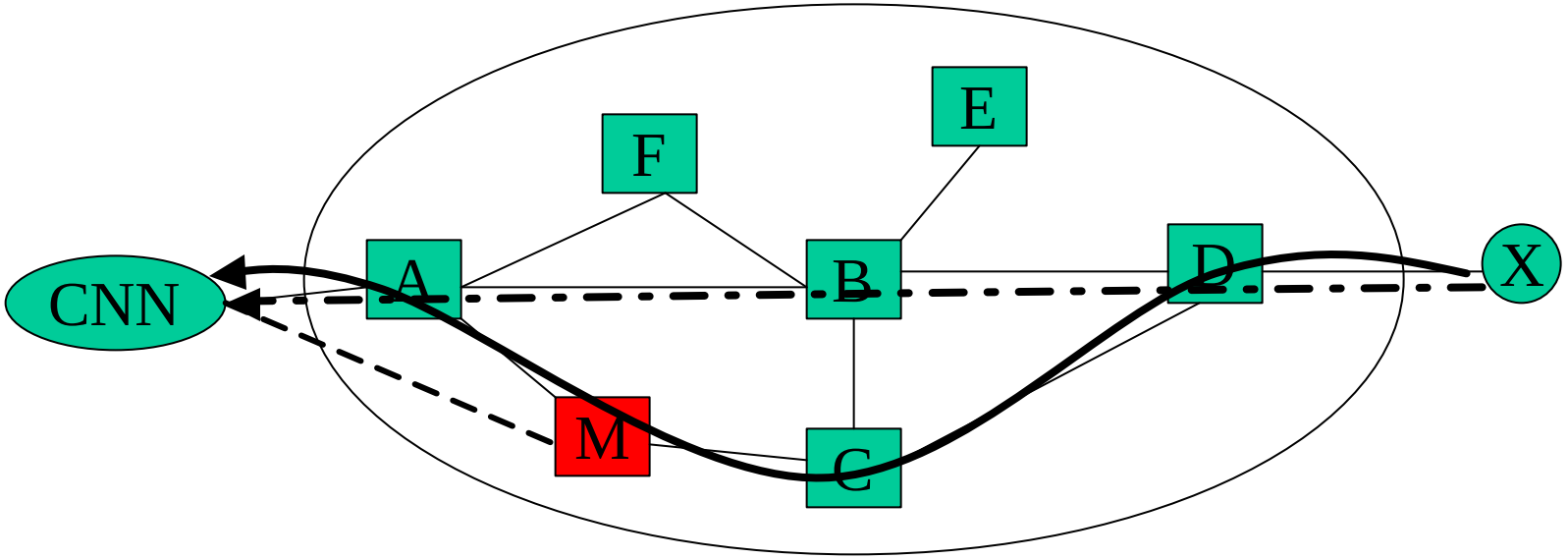
Renders Destination Network Unreachable

Effect: Impersonation



Impersonates end-hosts in destination network

Effect: Eavesdropping



Eavesdrop on the traffic: Hard to detect

Some Real-world examples

- Examples of Misconfigurations
  - A single misconfigured router in AS7007 claims ownership for many IP addresses in April 1997
    - Caused an outage lasting 2 hours
  - AS3561 propagates 5000 improper announcements in April 2001
  - Minor misconfigurations are common [Mahajan02]
- Malicious adversaries: a potential threat
  - Routers with default passwords [Rob Thomas, NANOG]
  - Cisco IOS security advisories
  - What if we have a large scale worm attack on routers?

What are Invalid Routes in BGP?

- Invalid Routes in the Control Plane
  - Route advertisements with an invalid AS path
    - 200-1200 prefixes affected every day [Mahajan02]
    - Causes: Misconfigurations, malicious nodes
- Invalid routes in the Data Plane
  - Data plane path does not match the path advertised in control plane
    - Covers 8% of Internet routes [Mao03]
    - Causes: Stale routes, Forwarding problems, route aggregation, Blackhole attacks
- Need a combination of control plane and data plane verification

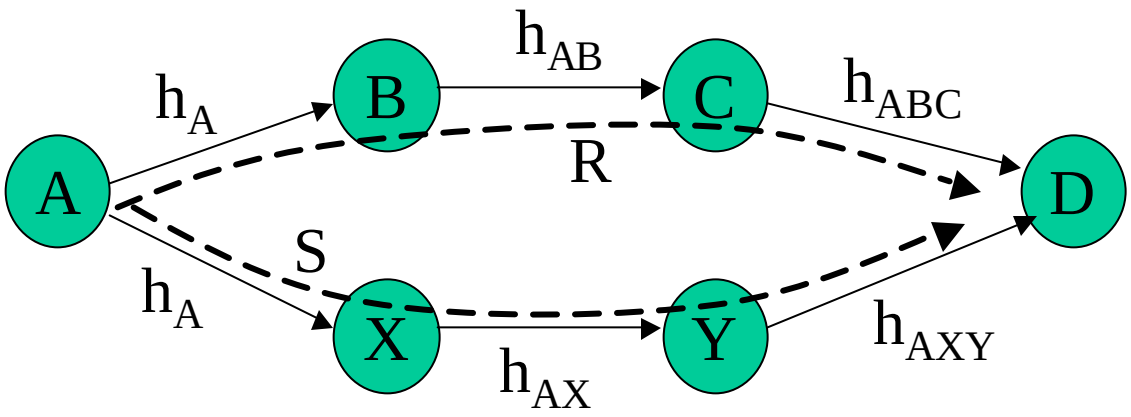
Our Approach: Listen and Whisper

- What best security can one provide without a PKI or the support of a centralized infrastructure?
- Whisper: Control plane verification
  - checks for consistency of routes using cryptographic signatures
  - Can ensure that any invalid route from a misconfigured router or isolated adversary will raise an alarm
  - Can isolate and contain the effects of independent adversaries propagating many invalid announcements
- Listen: Data plane verification
  - checks for reachability problems in the data plane
  - Useful for detecting problems due to stale routes, forwarding errors, adversaries performing blackhole attacks

Comparison to Related Work

	Control Plane Verification	Data Plane Verification
Key-distribution based approaches	Good security; hard to deploy	Not applicable
Using centralized databases	Incomplete, no security properties	Not applicable
Configuration checking tools	Useful for misconfigurations	Not applicable
Data-plane Route probing tools	Not applicable	Useful for our work
Listen and Whisper	**Trigger alarms + Containment**	**Notify existence of data-plane problems**

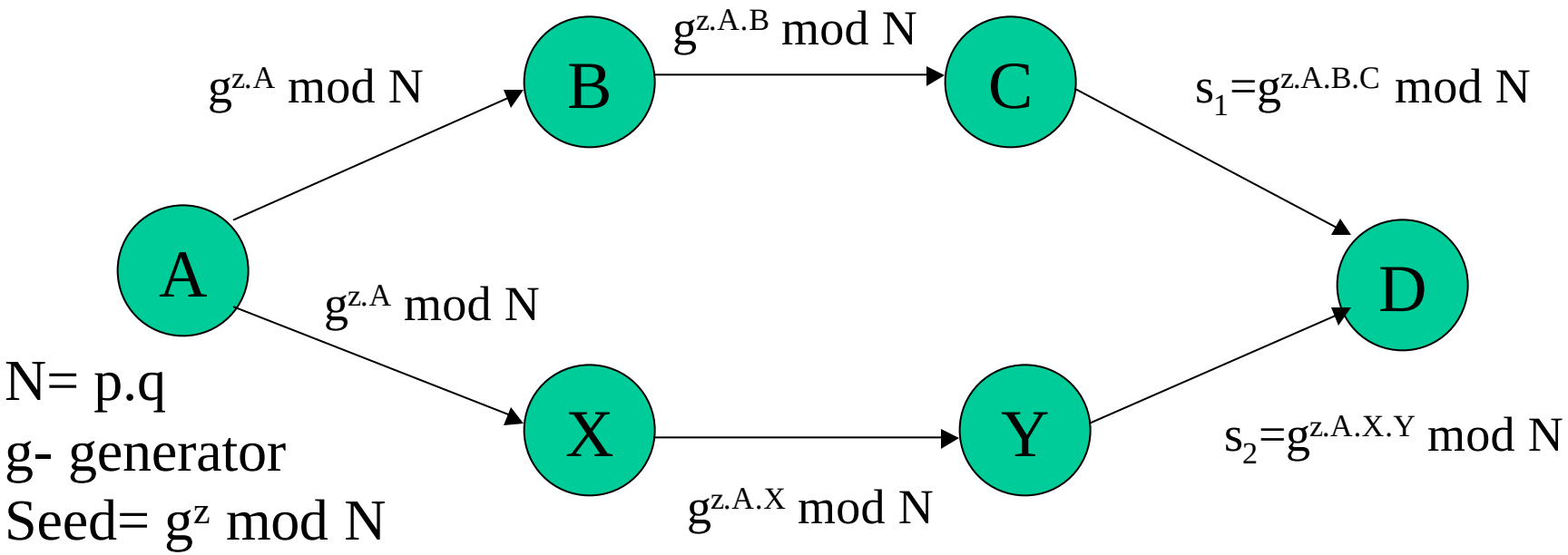
Whisper: Route Consistency Test



- Every path P is associated with a hash value h_P
- A route consistency test compares two routes R and S to a common destination:
  - R and S are genuine routes => consistent
  - R genuine, S spurious => inconsistent
  - R and S spurious => consistent or inconsistent
- ***Route consistency provides the ability to trigger alarms if any node generate spurious update.***

Strong Split Whisper (SSW)

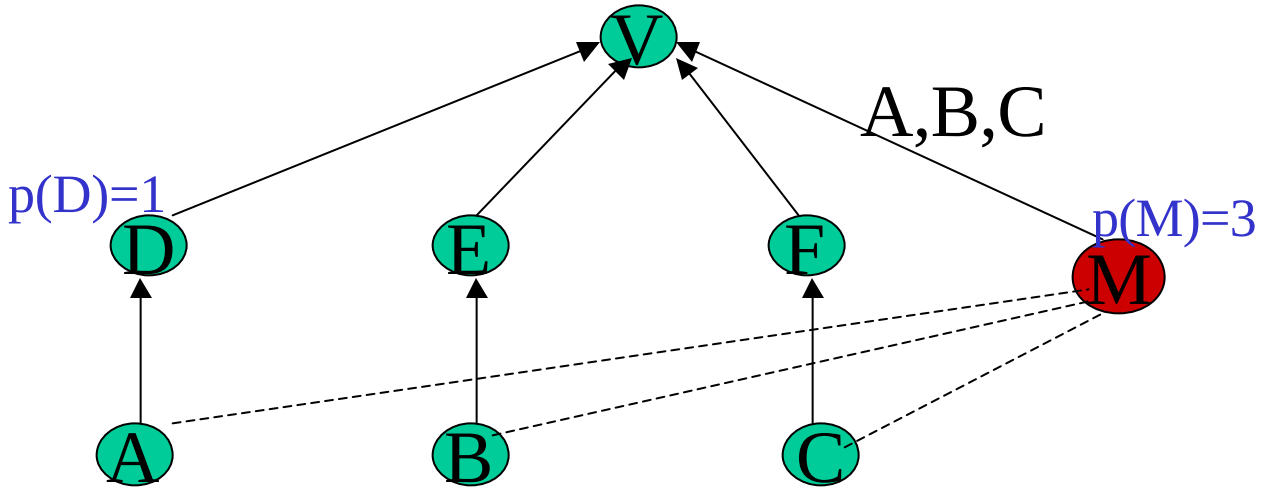
An Example route consistency test construction



Consistency Checking of Routes (C,B,A) and (Y,X,A)

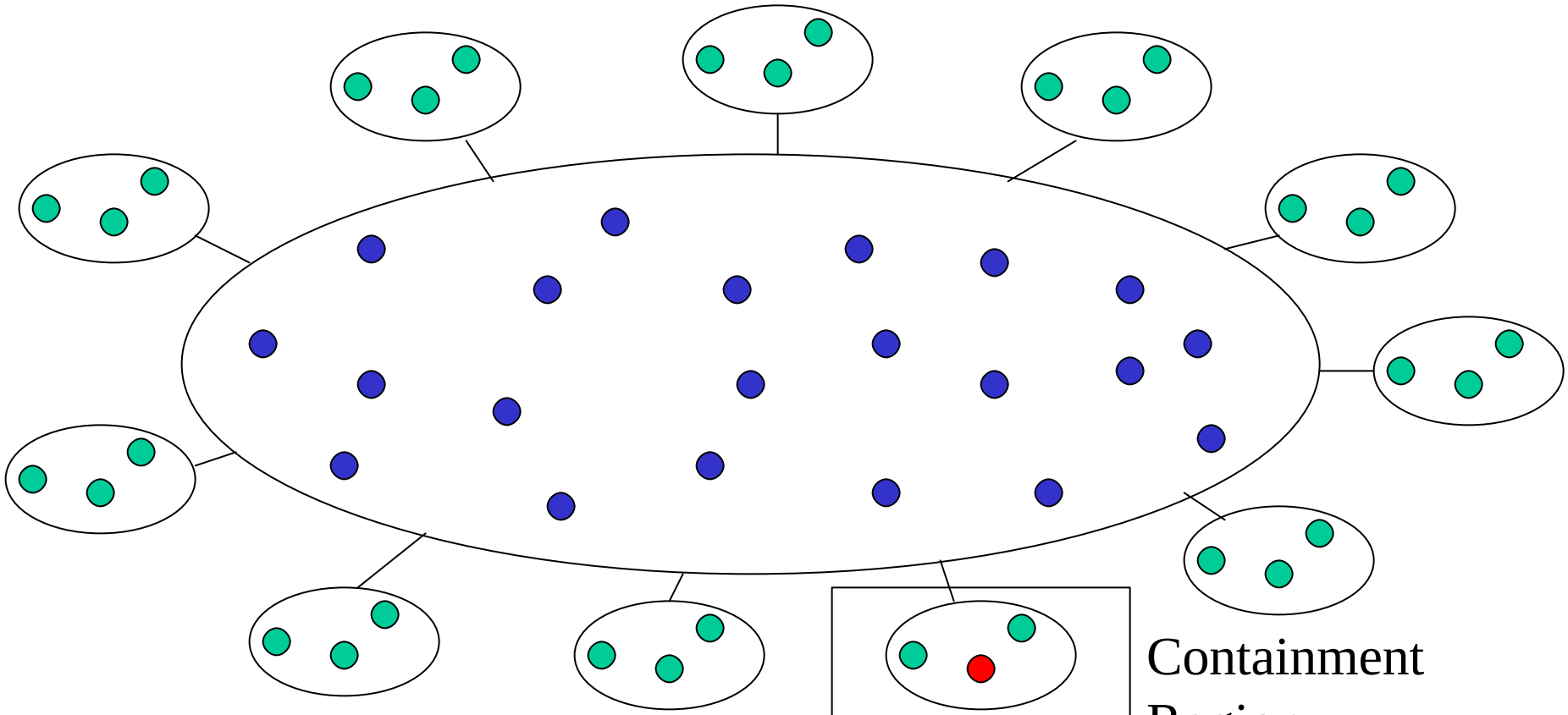
$$s_1^{X.Y} = s_2^{B.C} = g^{z.A.B.C.X.Y}$$

Containment Strategy



- Consistency check: (DA,MA), (EB,MB), (FC,MC)
  - Assign penalty of 1 to each intermediary node in a pair of inconsistent paths
- Penalty based Filtering: Choose routes with least penalty value
  - Contains the effect of an isolated adversary
  - Not applicable when #(adversaries) is large

An Isolated Adversary



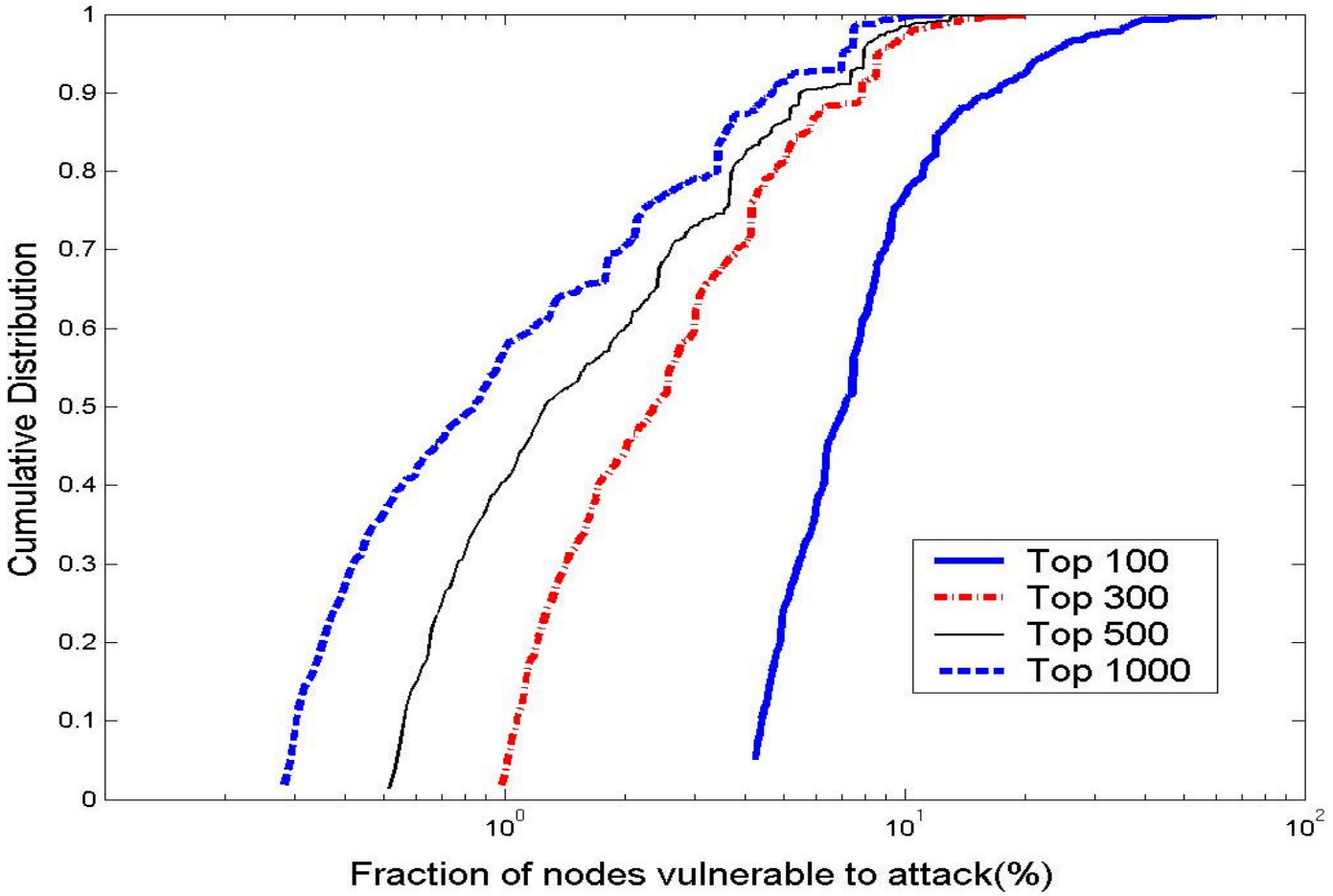
Uses penalty based Filtering

Malicious

Normal node

Only nodes within the containment region are vulnerable to an isolated adversary

Dealing with an Isolated Adversary



Containment region of an isolated adversary is reduced to roughly 1% of the nodes in the Internet topology

Whisper Implementation

	512-bit	1024-bit	2048-bit
VerifySign	0.18 msec	0.45 msec	1.42 msec
UpdateSign	0.25 msec	0.6 msec	1.94 msec
GenSign	0.4 sec	8.0 sec	68 sec

- Our Implementation:
  - Hash library uses RSA-like signatures using OpenSSL library
  - Whisper library integrated with Zebra version 0.93b bgpd
  - Overhead of Whisper operations is small
    - For 1024-bit keys, process rate >100,000 adv/minute
    - BGP maximum update rate is 9300 adv/min (avg=130)

Listen: Summary of Results

- Basic approach: A router passively observes a TCP flow for SYN and DATA packets
  - If so, the ACK has been received by sender => Route to destination is verifiable
- Challenge: Dealing with false positives and false negatives
  - Have developed techniques to reduce the probability of false positives and negatives to less than 1%
- Implementation results:
  - Deployed in the local area /24 network (KatzNet consisting of 40 machines) for over 2 months
  - Determined 571 routing problems with a false negative ratio of 0.93% (verified using active probing)

Summary: Listen and Whisper

- We identified three forms of threats to BGP
  - Mis-configurations, isolated adversaries, colluding adversaries
- Remedies
  - Whisper flags control plane route inconsistencies
  - Listen is necessary for flagging data plane anomalies
  - A single isolated node (compromised or mis-configured) propagating several bogus announcements can be isolated and contained
- Limitations
  - Does not work well when the number of adversaries is large
  - Limited protection against colluding adversaries

Deployment Issues/ Concerns

- Listen is a stand-alone tool which is incrementally deployable for detecting data-plane problems
- Whisper issues:
  - Are community attributes/ BGP options the right place to put these signatures?
  - Can we have 256 bits of a signature field?
    - Need not send signature for repetitive announcements
  - What is the right deployment strategy?