Networking Review & Grand Challenges

Brighten Godfrey
CS 538 August 29 2013
Undergraduate Networking in Three Slides

(including this one)
Layering

A kind of modularity

Functionality separated into layers

- Layer n implements higher-level functionality by interfacing only with layer n-1
- Hides complexity of surrounding layers: enables greater diversity and evolution of modules
A kind of modularity

Functionality separated into layers

- Layer $n$ implements higher-level functionality by interfacing only with layer $n-1$
- Hides complexity of surrounding layers: enables greater diversity and evolution of modules
Layering

A kind of modularity

Functionality separated into layers

- Layer $n$ implements higher-level functionality by **interfacing only with layer $n-1$**
- Hides complexity of surrounding layers: enables greater diversity and evolution of modules
Layering

A kind of modularity

Functionality separated into layers

- Layer $n$ implements higher-level functionality by **interfacing only with layer $n-1$**
- Hides complexity of surrounding layers: enables greater diversity and evolution of modules
Layering

A kind of modularity

Functionality separated into layers

- Layer $n$ implements higher-level functionality by **interfacing only with layer $n-1$**
- Hides complexity of surrounding layers: enables greater diversity and evolution of modules
Layering

Tunnel
<table>
<thead>
<tr>
<th>Layer</th>
<th>Common functionality &amp; problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Anything you want...</td>
</tr>
<tr>
<td>Transport</td>
<td>Process-level communication</td>
</tr>
<tr>
<td>Network</td>
<td>Packets across domains</td>
</tr>
<tr>
<td>Data Link</td>
<td>Packets across networks</td>
</tr>
<tr>
<td>Physical</td>
<td>Packets on a ‘wire’</td>
</tr>
<tr>
<td></td>
<td>Encoding of bits</td>
</tr>
<tr>
<td></td>
<td>Life, the universe, and everything</td>
</tr>
<tr>
<td></td>
<td>Reliability, flow control, ordering, congestion, ...</td>
</tr>
<tr>
<td></td>
<td>Independent parties, scale, routing</td>
</tr>
<tr>
<td></td>
<td>Addressing, heterogeneity, routing</td>
</tr>
<tr>
<td></td>
<td>Framing, errors, addressing</td>
</tr>
<tr>
<td></td>
<td>Physics</td>
</tr>
</tbody>
</table>
Grand Challenges
Bismuth strontium calcium copper oxide (BSCCO)

Superconducts up to about -168°C (-271 °F)

High temperature superconductors are a “Grand Challenge” for condensed matter physics
Grand Challenges

Widely recognized as among the most important unsolved problems in a field

- P vs. NP
- natural language understanding
- bug-free programs
- moving society to carbon-neutral energy
- preventing cancer
- ...


Grand Challenges in networking?

Getting an A in this class?
GC’s in networking

An Informal Survey

1. “What I’m working on!”

2. High level objectives
   - Security & privacy
   - Reliability
   - Usability

   • Different than P vs. NP: hard to even define “security”; objectives involve tradeoffs
Unreliability: One Example
Internet Routing

AS 36561
YouTube

AS 7018
AT&T
eBGP

AS 11537
Internet2

AS 698
UIUC
iBGP
Border Gateway Protocol
Instability causes outages

- Link state changes
- Router failures
- Config. changes
- ...

Eventually, control message: CACBD

Loop detected!

Forwarding loop

- Loops
- Detection delay
- Black holes

FAIL
Instability causes outages

[F. Wang, Z. M. Mao, J. Wang, L. Gao, R. Bush SIGCOMM’06]
Instability causes outages

[Instability causes outages]

More outages

Longer outages

...and higher latency, packet reordering, router CPU load during instability
Many sources of unreliability

Congestion
  • no end-to-end bandwidth reservations in the Internet

Configuration or software bugs

Failures or delays
  • in network, DNS servers, caches, application servers, ...
Insecurity: one example
Prefix hijacking

Anyone can advertise routes for any IP prefix!

How can hijacker get the advertised routes to actually be used by other ASes?

- Announce more specific (longer) prefix than real owner
- Now everyone’s traffic is “blackholed”

Can protect against this (Secure BGP), but...

- it’s not deployed today
- and even then, can still cleverly (or accidentally) attract traffic and eavesdrop
Man in the Middle (MITM) attack

- Traffic to a destination redirected (not blackholed) through an attacker
- Attacker can watch everything you do without you noticing

What’s the key problem here?

How can attacker forward traffic to destination, if attacker is pretending to be the destination?
1. A finds legitimate path ABD for 128.2.0.0/16
1. A finds legitimate path ABD for 128.2.0.0/16

2. A sends semi-bogus announcement of path ABD for 128.2.0.0/17

3. Result:
   - ASes (here B) on real path keep using real path because of loop elimination
   - All other ASes use route through A (128.2.0.0/17 beats 128.2.0.0/16)

4. A forwards traffic to B
Hijacking + eavesdropping

Kapela & Pilosov also described how to spoof traceroute information to be even more undetectable.
1. “What I’m working on!”

2. Nebulous high level objectives
   - Security & privacy
   - Reliability
   - Usability
   - Complexity

3. Why does networking lack a crisp Grand Challenge?
   - Infrastructure needs to support highly diverse and dynamic goals, applications, and environments
Meta-challenge:

How do we make the Internet evolvable?
Reviews due by 11:59 pm Monday:

- A protocol for packet network intercommunication (Cerf and Kahn, 1974)
- The Design Philosophy of the DARPA Internet Protocols (Clark, 1988)