Onion Routing

- Meant to handle issue of people knowing who you're talking to
- Basic idea is to conceal sources and destinations
- By sending lots of crypo-protected packets between lots of places
- Each packet goes through multiple hops

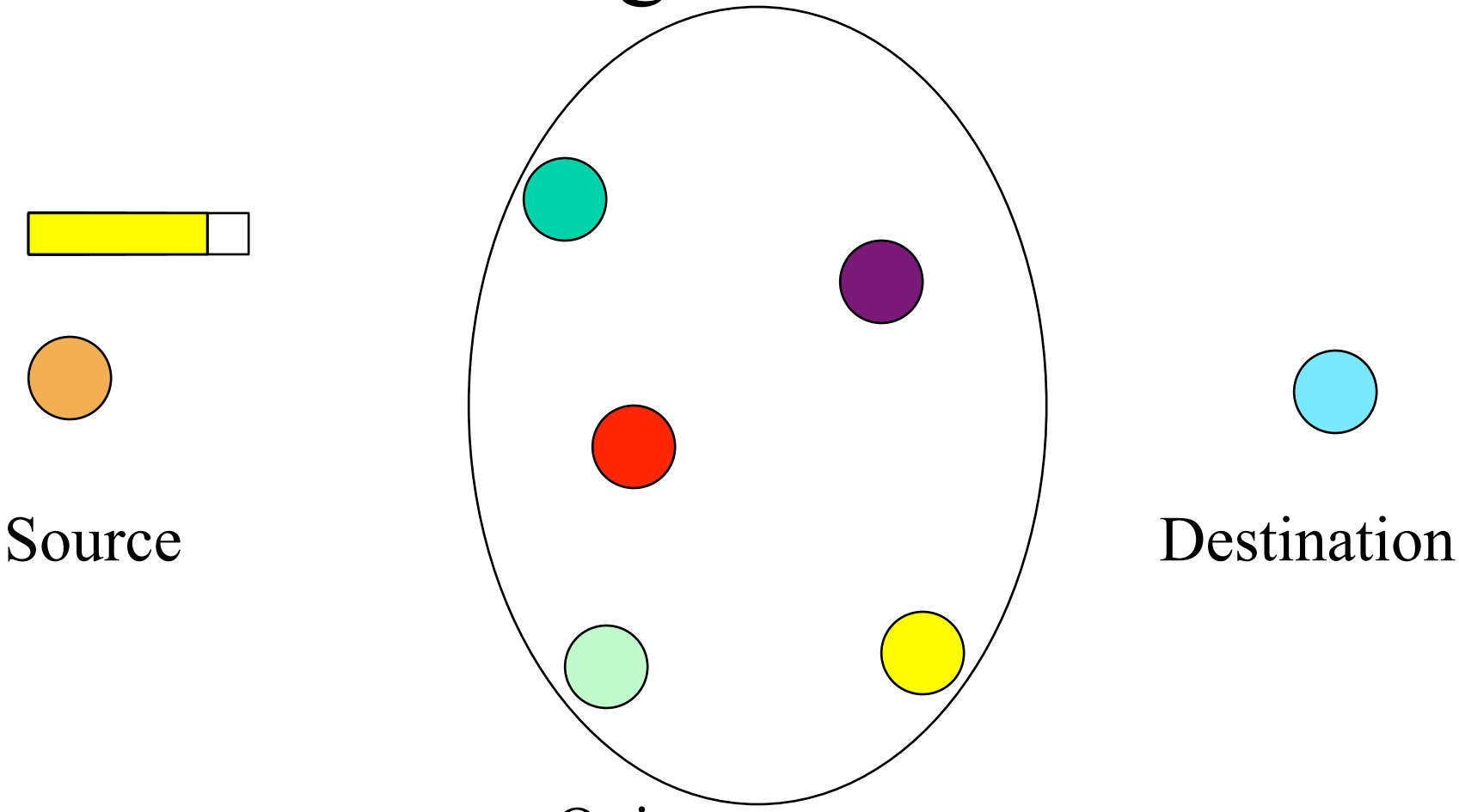
A Little More Detail

- A group of nodes agree to be onion routers
- Users obtain crypto keys for those nodes
- Plan is that many users send many packets through the onion routers
  - Concealing who's really talking

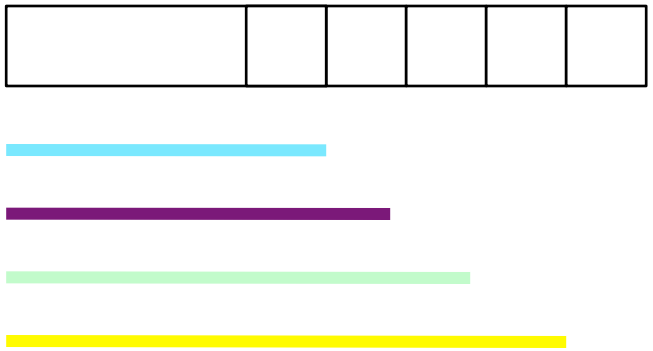
Sending an Onion-Routed Packet

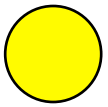
- Encrypt the packet using the destination's key
- Wrap that with another packet to another router
  - Encrypted with that router's key
- Iterate a bunch of times

In Diagram Form

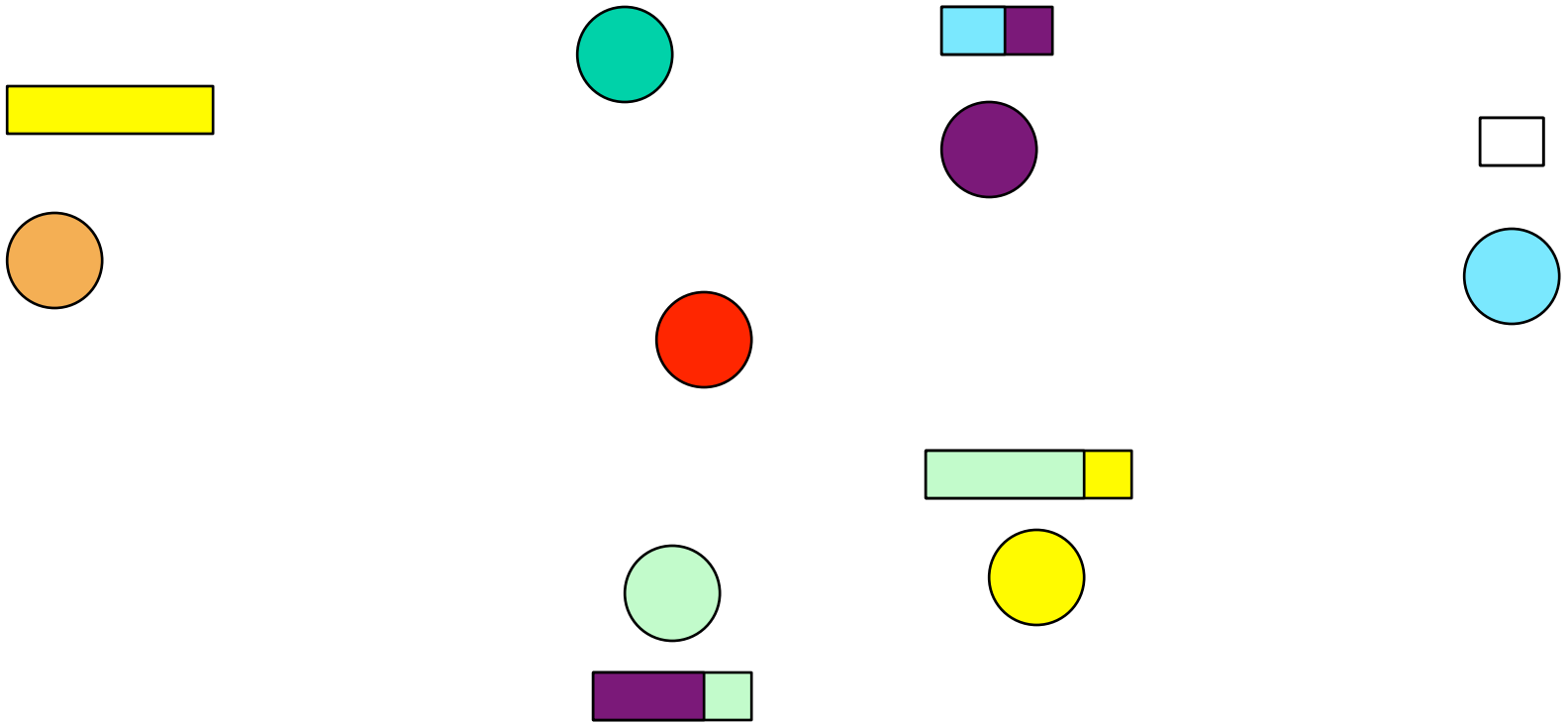


What's Really in the Packet



An unencrypted header to allow delivery to 

Delivering the Message



What's Been Achieved?

- Nobody improper read the message
- Nobody knows who sent the message
  - Except the receiver
- Nobody knows who received the message
  - Except the sender
- Assuming you got it all right

Issues for Onion Routing

- Proper use of keys
- Traffic analysis
- Overheads
  - Multiple hops
  - Multiple encryptions

Tor

- The most popular onion routing system
- Widely available on the Internet
- Using some of the original onion routing software
  - Significantly altered to handle various security problems
- Usable today, if you want to
- IETF is investigating standard for Tor

Why Hasn't Tor Solved This Privacy Problem?

- First, the limitations of onion routing
- Plus usability issues
  - Tor's as good as it gets, but isn't that easy to use
- Can't help if a national government disapproves
  - China and other nations have prohibited Tor's use
- NSA (and others) keep attacking Tor's privacy techniques

Can't I Surreptitiously Run Tor?

- Can't I get around government restrictions by just not telling them?
- No
  - Tor routers must know each others' identities
  - Traffic behavior of Tor routers "glows in the dark"
  - Tor developers keep trying

Privacy-Preserving Data Mining

- Allow users access to aggregate statistics
- But don't allow them to deduce individual statistics
- How to stop that?

Approaches to Privacy for Data Mining

- Perturbation
  - Add noise to sensitive value
- Blocking
  - Don't let aggregate query see sensitive value
- Sampling
  - Randomly sample only part of data

Preserving Location Privacy

- Can we prevent people from knowing where we are?
- Given that we carry mobile communications devices
- And that we might want location-specific services ourselves

Location-Tracking Services

- Services that get reports on our mobile device's position
  - Probably sent from that device
- Often useful
  - But sometimes we don't want them turned on
- So, turn them off then

But . . .

- What if we turn it off just before entering a “sensitive area”?
- And turn it back on right after we leave?
- Might someone deduce that we spent the time in that area?
- Very probably

Handling Location Inferencing

- Need to obscure that a user probably entered a particular area
- Can reduce update rate
  - Reducing certainty of travel
- Or bundle together areas
  - Increasing uncertainty of which was entered

So Can We Have Location Privacy?

- Not clear
- An intellectual race between those seeking to obscure things
- And those seeking to analyze them
- Other privacy technologies (like Tor) have the same characteristic

The NSA and Privacy

- 2013 revelations about NSA spying programs changed conversation on privacy
- The NSA is more heavily involved in surveillance than previously believed
- What are they doing and what does that mean for privacy?

Conclusion

- Privacy is a difficult problem in computer systems
- Good tools are lacking
  - Or are expensive/cumbersome
- Hard to get cooperation of others
- Probably an area where legal assistance is required