Protecting Other Styles of Protocols

- Generally, how do you know you should believe another router?
- About distance to some address space
- About reachability to some address space
- About other characteristics of a path
- About what other nodes have told you

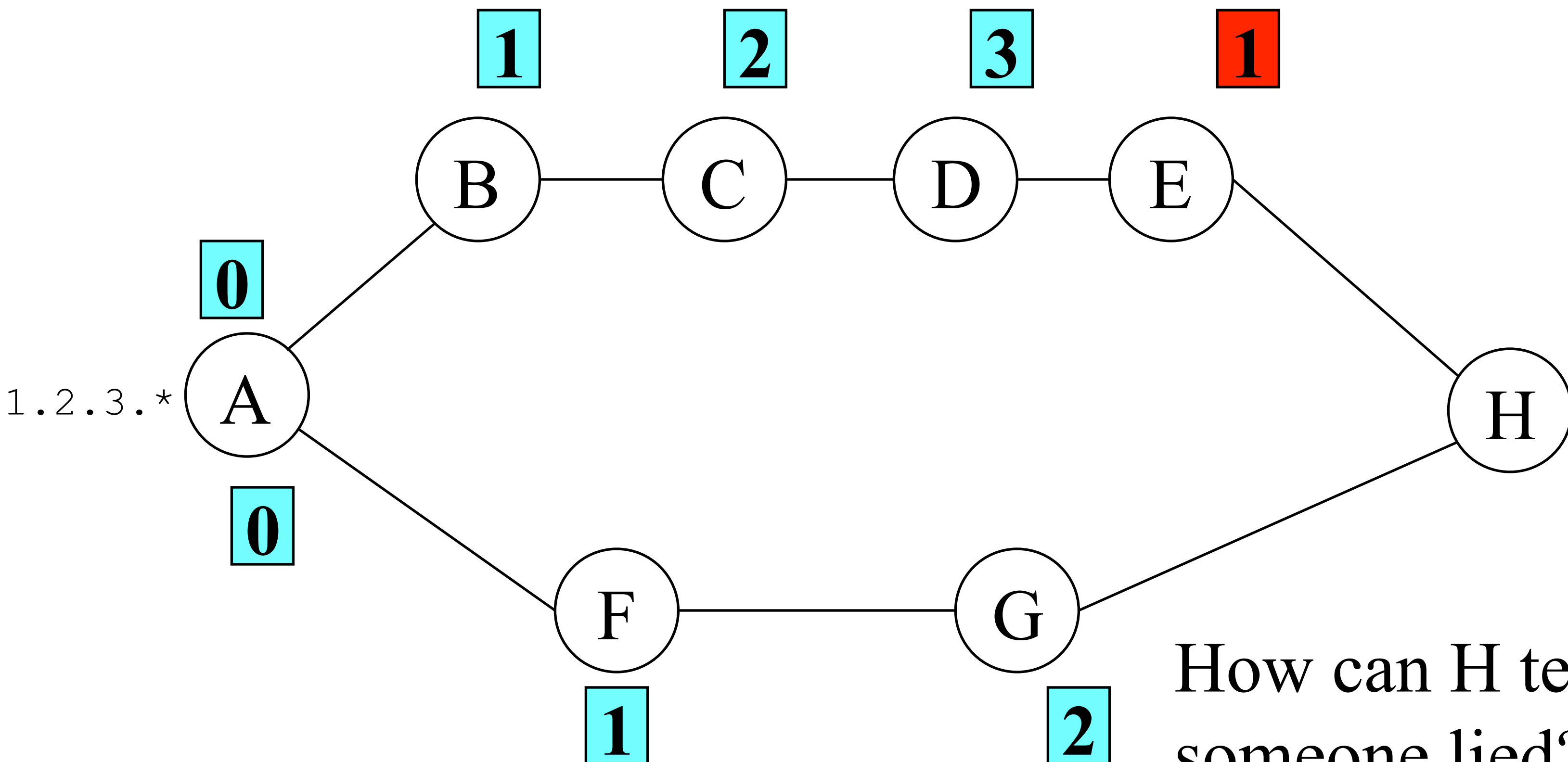
How Routing Protocols Pass Information

- Some protocols pass full information
  - E.g., BGP
  - So they can pass signed information
- Others pass summary information
  - E.g., RIP
  - They use other updates to create new summaries
  - How can we be sure they did so properly?

Who Are You Worried About?

- Random attackers?
  - Generally solvable by encrypting/ authenticating routing updates
- Misbehaving insiders?
  - A much harder problem
  - They're supposed to make decisions
  - How do you know they're lying?

A Sample Problem



Assume a distance vector protocol

How can H tell someone lied?

How can H tell that E lied?

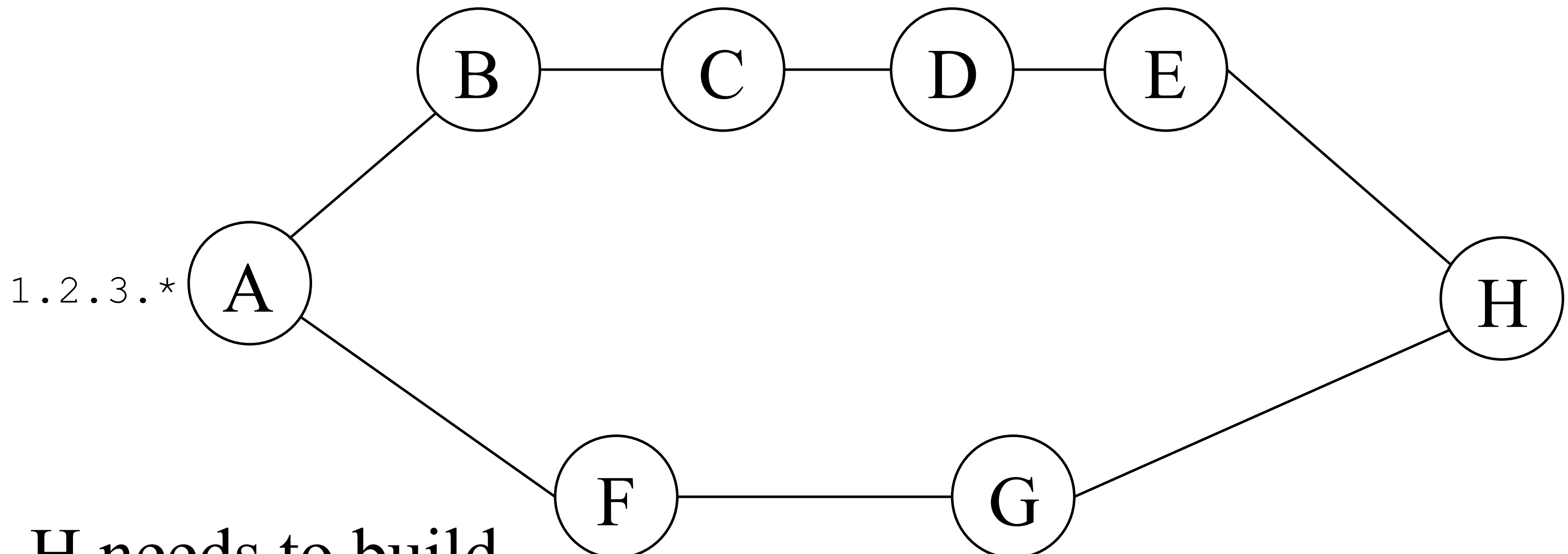
Types of Attacks on Distance Vector Routing Protocols

- Blackhole attacks
  - Claim short route to target
- Claim longer distance
  - To avoid traffic going through you
- Inject routing loops
  - Which cause traffic to be dropped
- Inject lots of routing updates
  - Generally for denial of service

How To Secure a Distance Vector Protocol?

- Can't just sign the hop count
  - Not tied to the path
- Instead, sign a length and a "second-to-last" router identity
- By iterating, you can verify path length

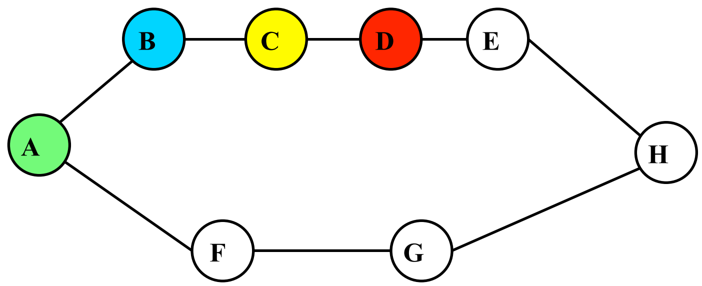
An Example



H needs to build a routing table entry for 1.2.3.*

Should show hop count of 3 via G, 5 via E

One Way to Do It



H directly verifies that it's one hop to E

H gets signed info that D is 2 hops through E

Then we iterate

E	1	-	
D	2	E	
C	3	D	
B	4	C	
A	5	B	

Now we can trust it's five hops to A

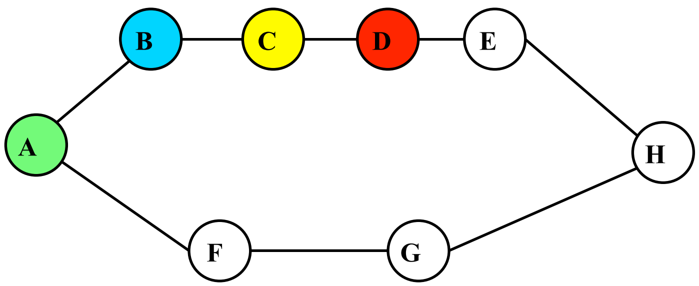
Who Does the Signing?

- The destination
  - A in the example
- It only signs the unchanging part
  - Not the hop count
- But an update eventually reaches H that was signed by A

What About That Hop Count?

- E could lie about the hop count
- But he can’t lie that A is next to B
- Nor that B next to C, nor C next to D, nor D next to E
- Unless other nodes collude, E can’t claim to be closer to A than he is

What If Someone Lies?



E	1	-	
D	2	E	
C	3	D	
B	4	C	
A	5	B	

There's limited scope for effective lies

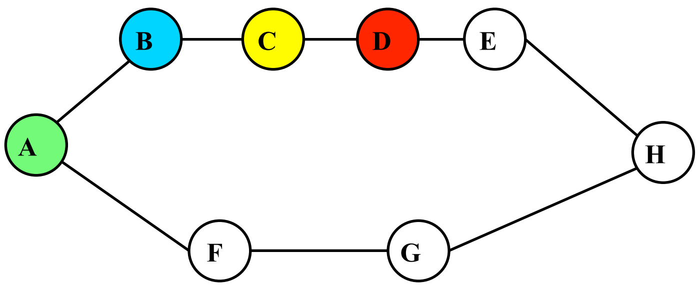
E can't claim to be closer to A

Since E can't produce a routing update signed by A that substantiates that

A Difficulty

- This approach relies on a PKI
- H must be able to check the various signatures
- Breaks down if someone doesn’t sign
  - That’s a hole in the network, from the verification point of view
  - Consider, in example, what happens if C doesn’t sign

What If C Doesn't Sign?



E	1	-	
D	2	E	
C	3	D	
B	4	C	
A	5	B	

A message coming through D tells us that it's three hops to C

But H can't verify that

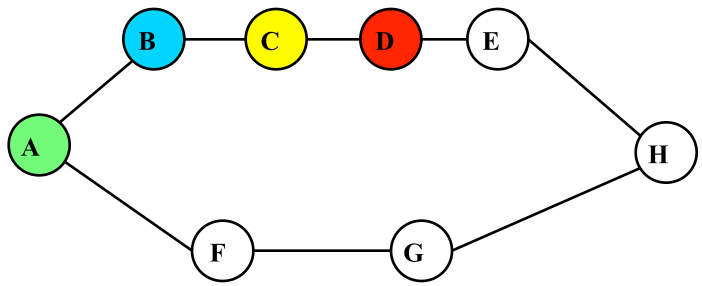
H knows C is next to B

And that B is next to A

But how can he be sure D is next to C?

Other than trusting D . . .

What's the Problem?



E	1	-	
D	2	E	
C	3	D	
B	4	C	
A	5	B	

For this graph, no problem

But how about for this one?