04

Anonymous Communication

Kai Bu
kaibu@zju.edu.cn
http://list.zju.edu.cn/kaibu/netsec2022

Anonymous Communication

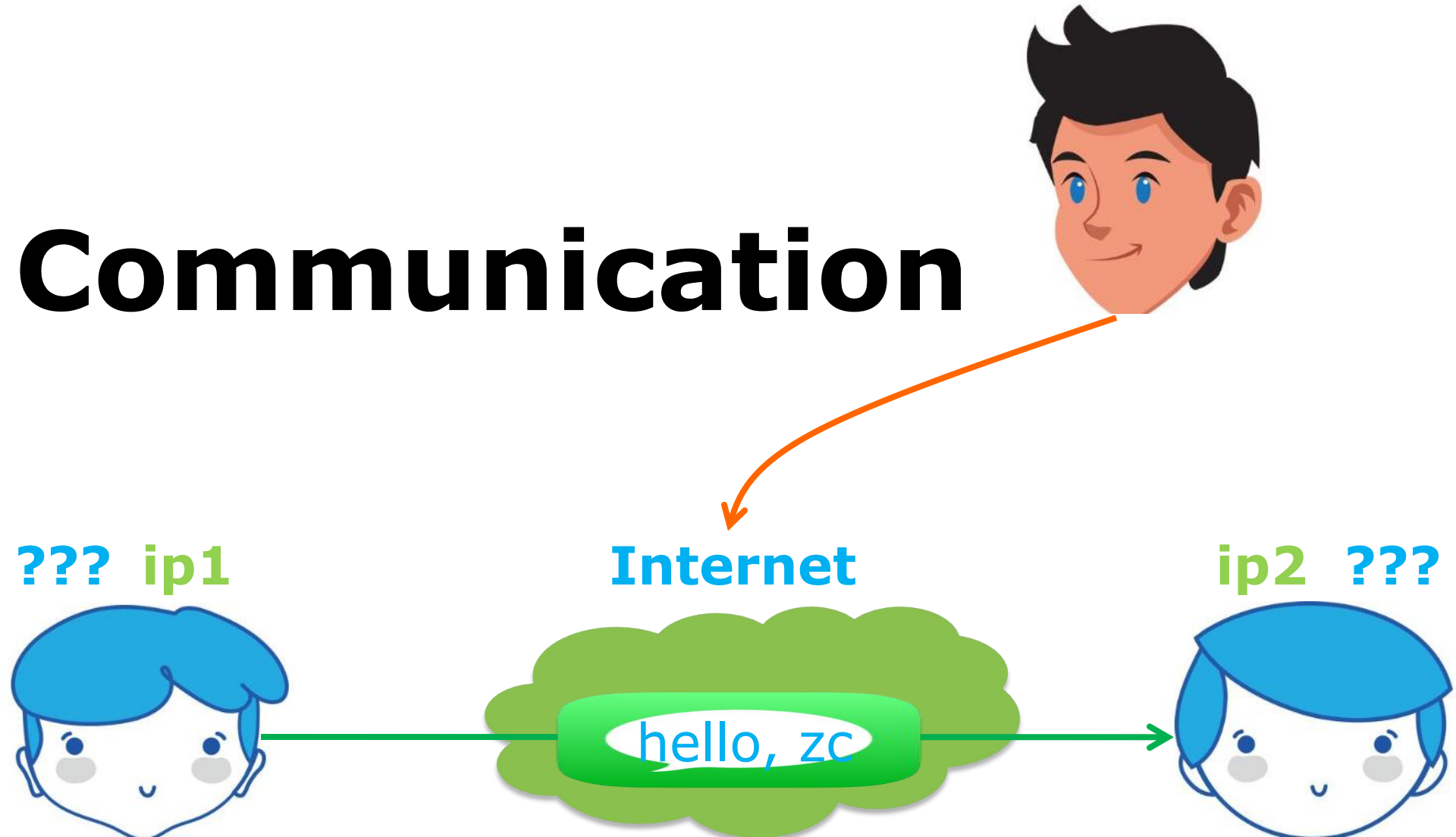
Disclaimer:
The content to be presented aims only for helping students understand principles of anonymous communication. It should not be used for abusive Internet activities.

Communication

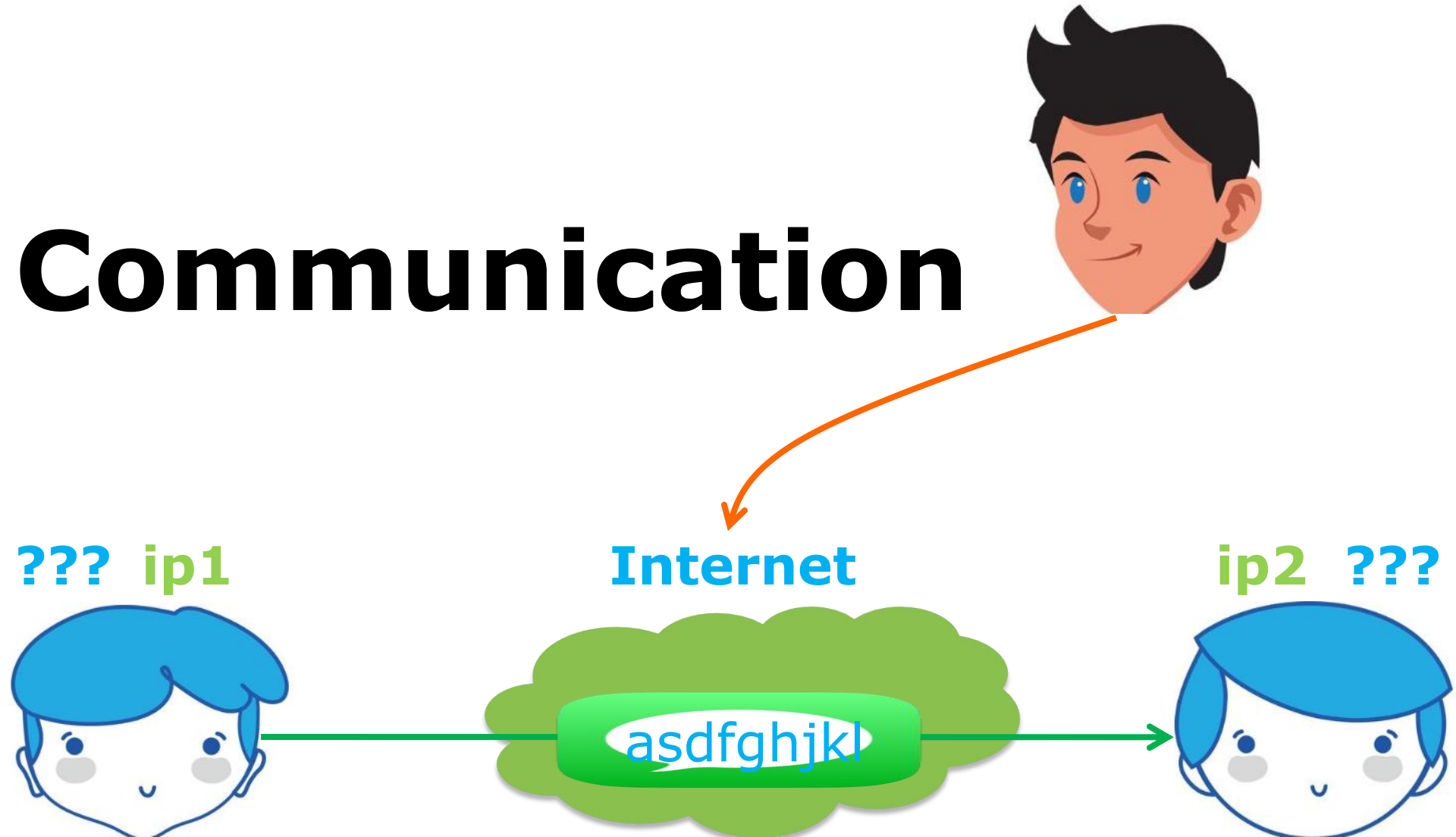
Communication

Communication

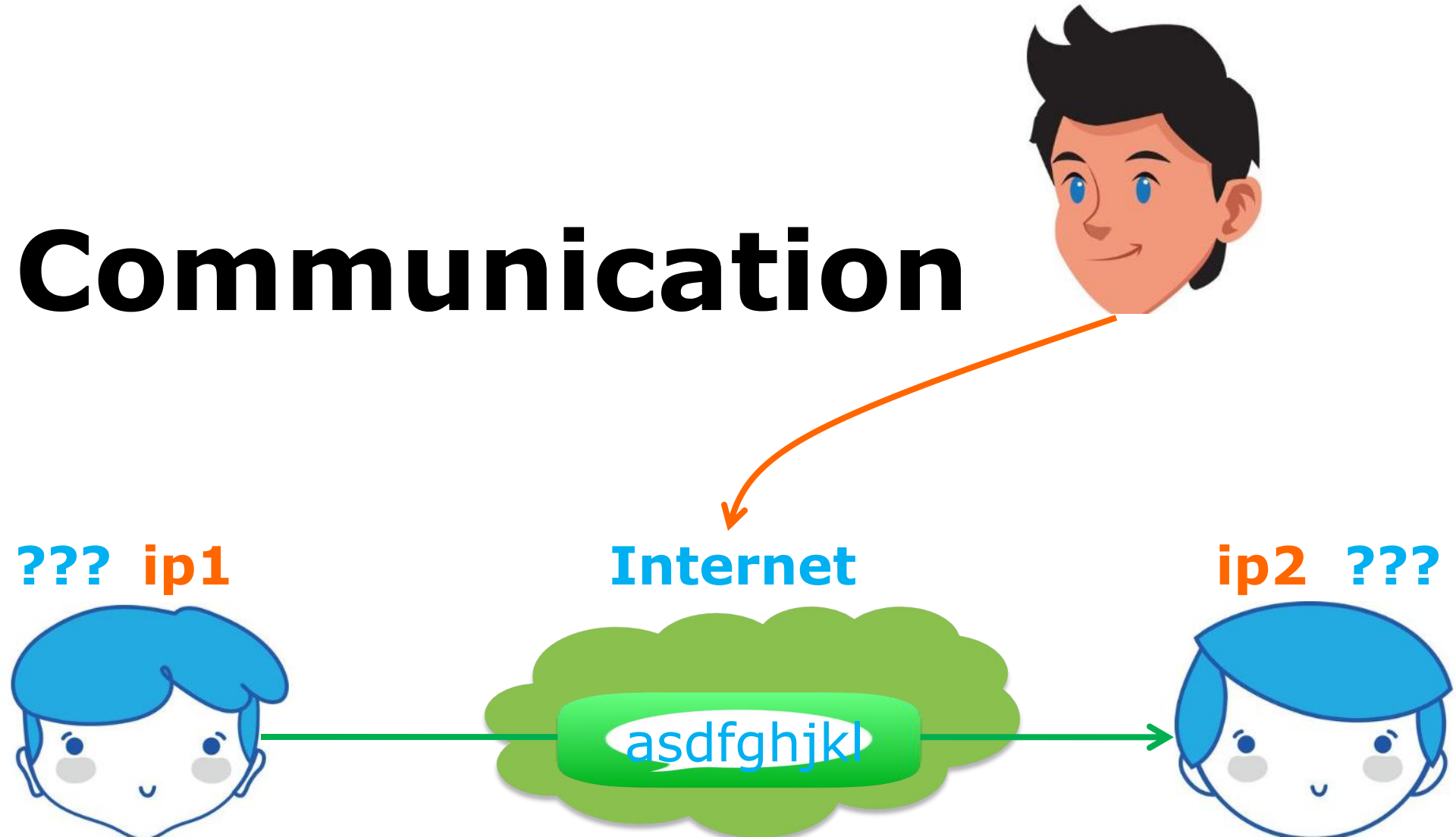
Communication



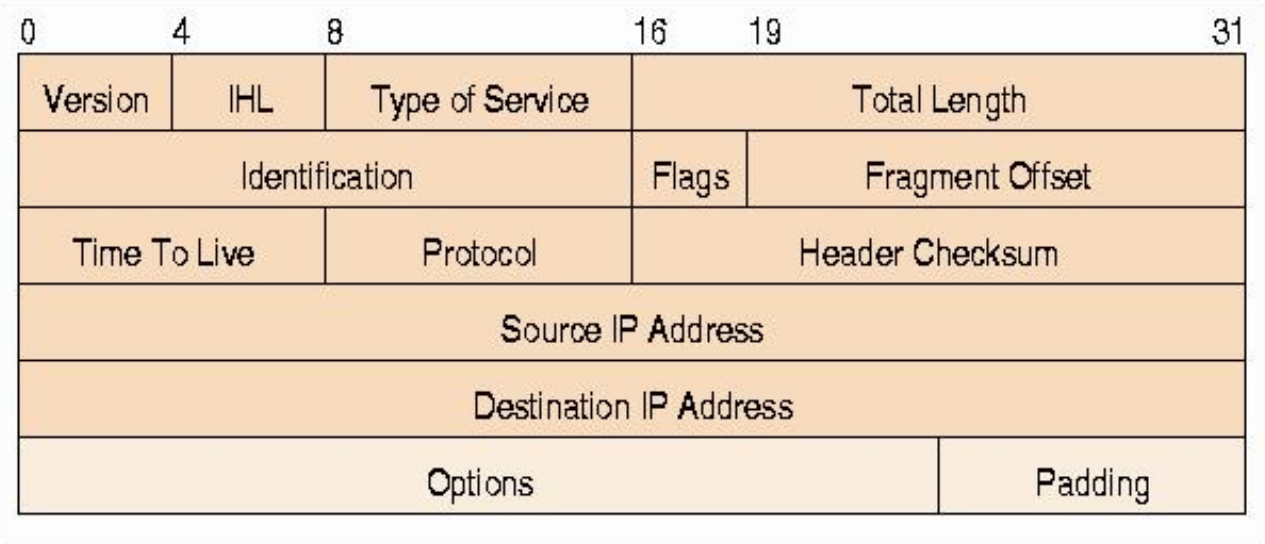
Communication



Communication



Communication



Communication

anonymity & privacy:

who is communicating?

who are you talking to?

what type of activities?

what type of information?

Anonymous Communication

why wanted?

Anonymity for Mortals

- Unmonitored access to health and medical information
- Preservation of democracy:

  anonymous election/jury
- Censorship circumvention:

  anonymous access to otherwise restricted information
- …

Anonymity for Attackers

Misbehaviors without getting caught:

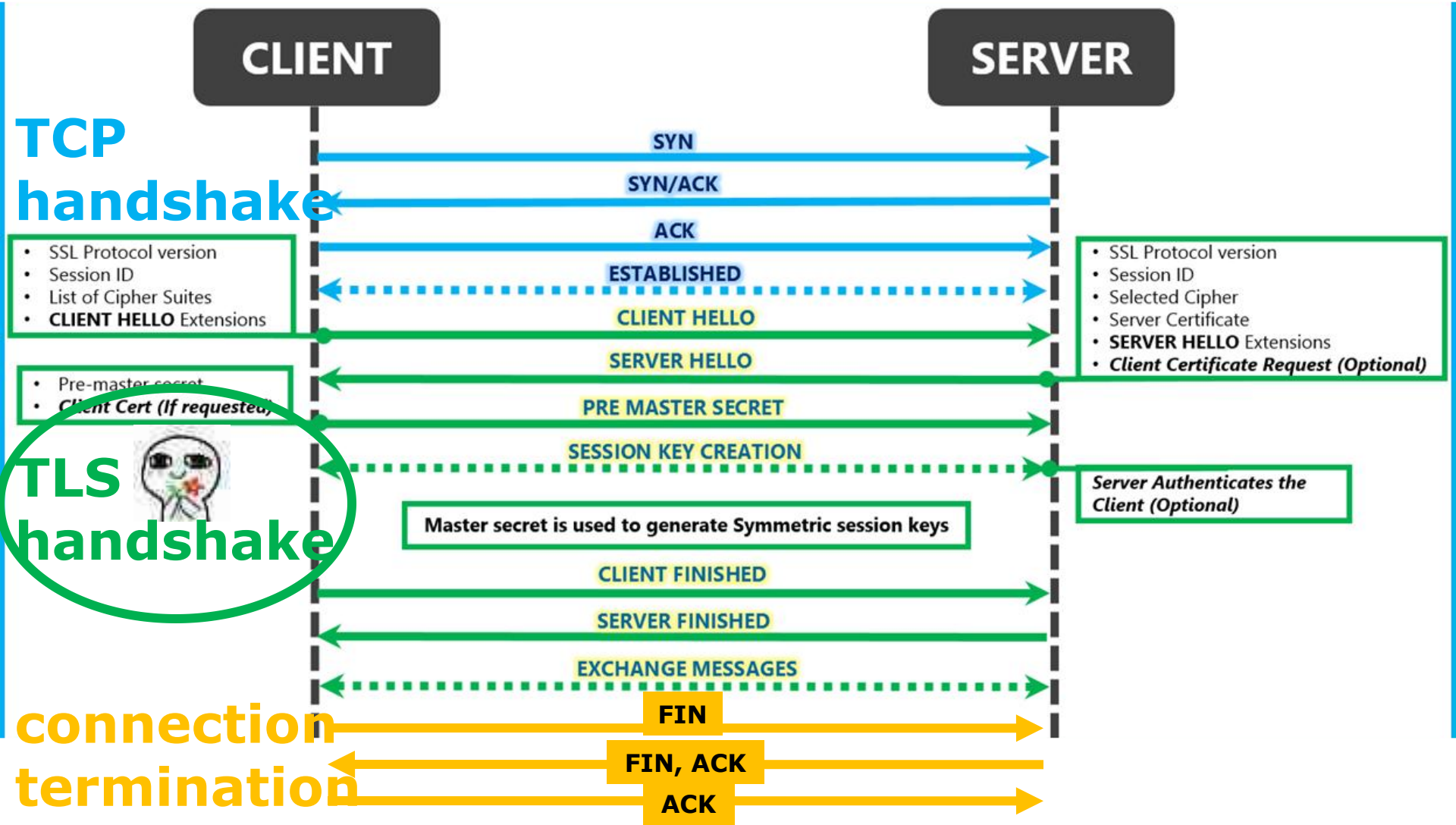
- Terrorism
- Darknet
- Spam
- Pirate
- …

Anonymous Communication

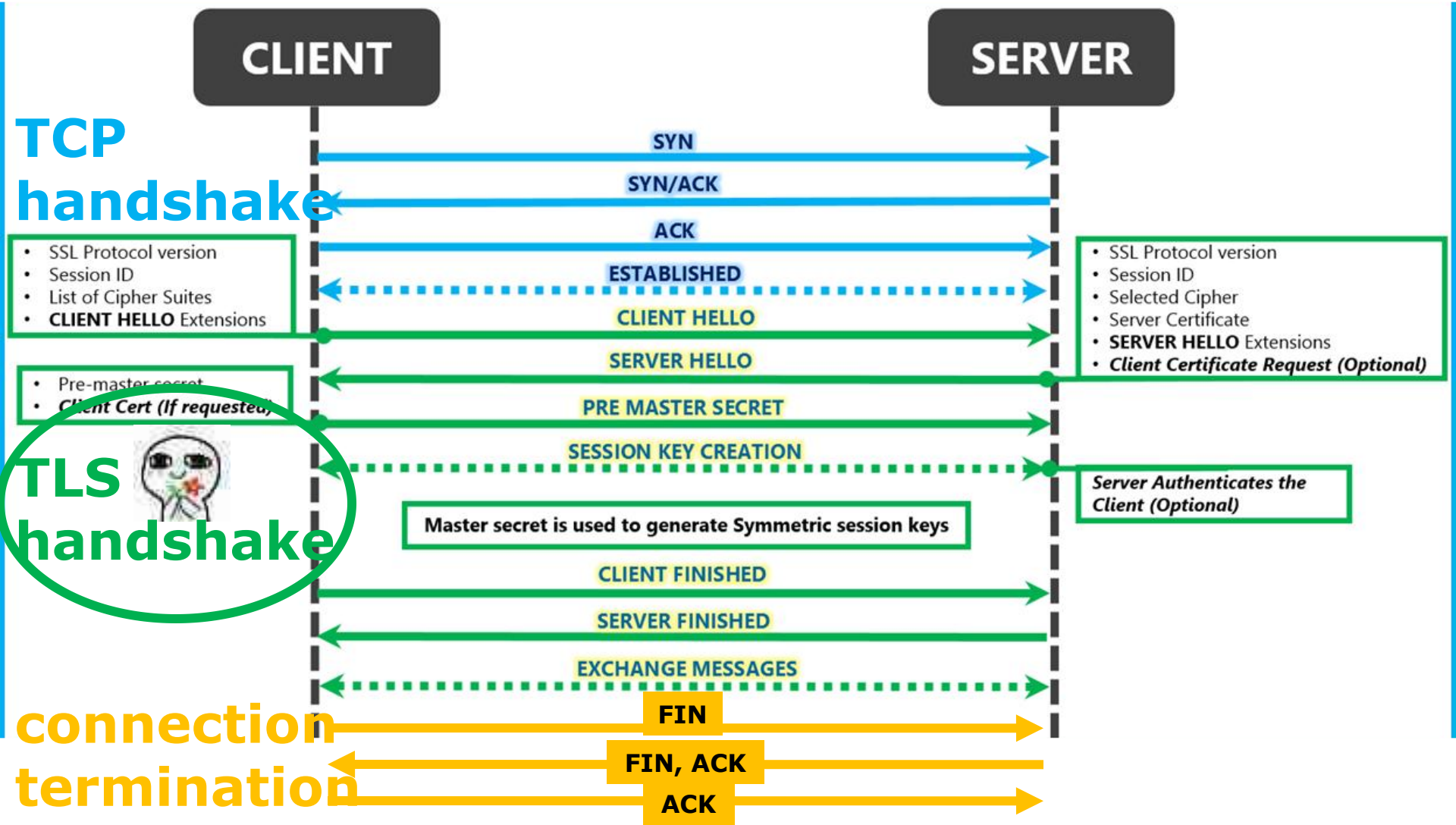
how to?

HTTPS?

HTTPS for Confidentiality

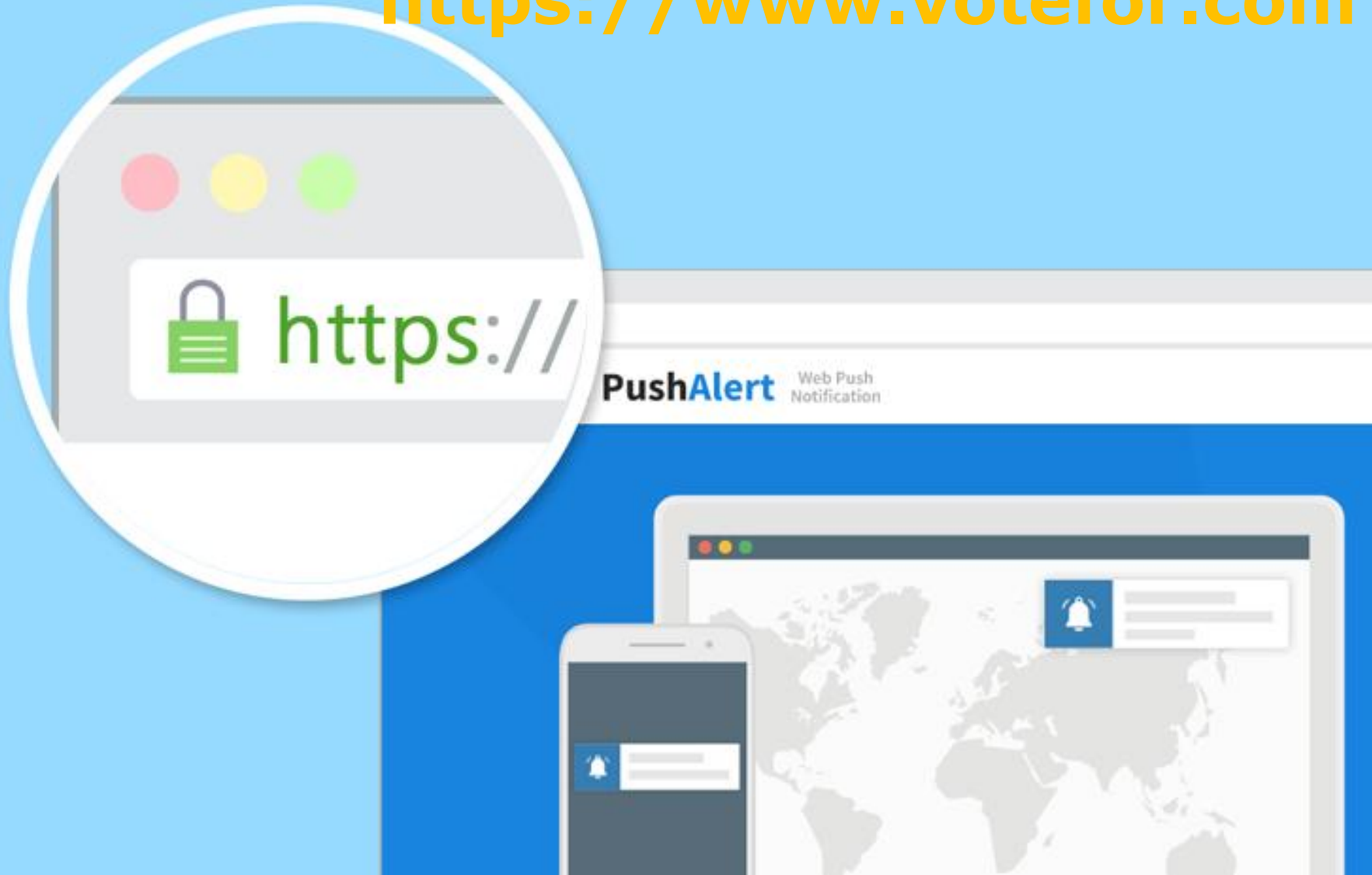


HTTPS Not for Anonymity



HTTPS?

https://www.votefor.com



Anonymous Communication

how to?

how to?

Anonymous Communication

hide destination address;

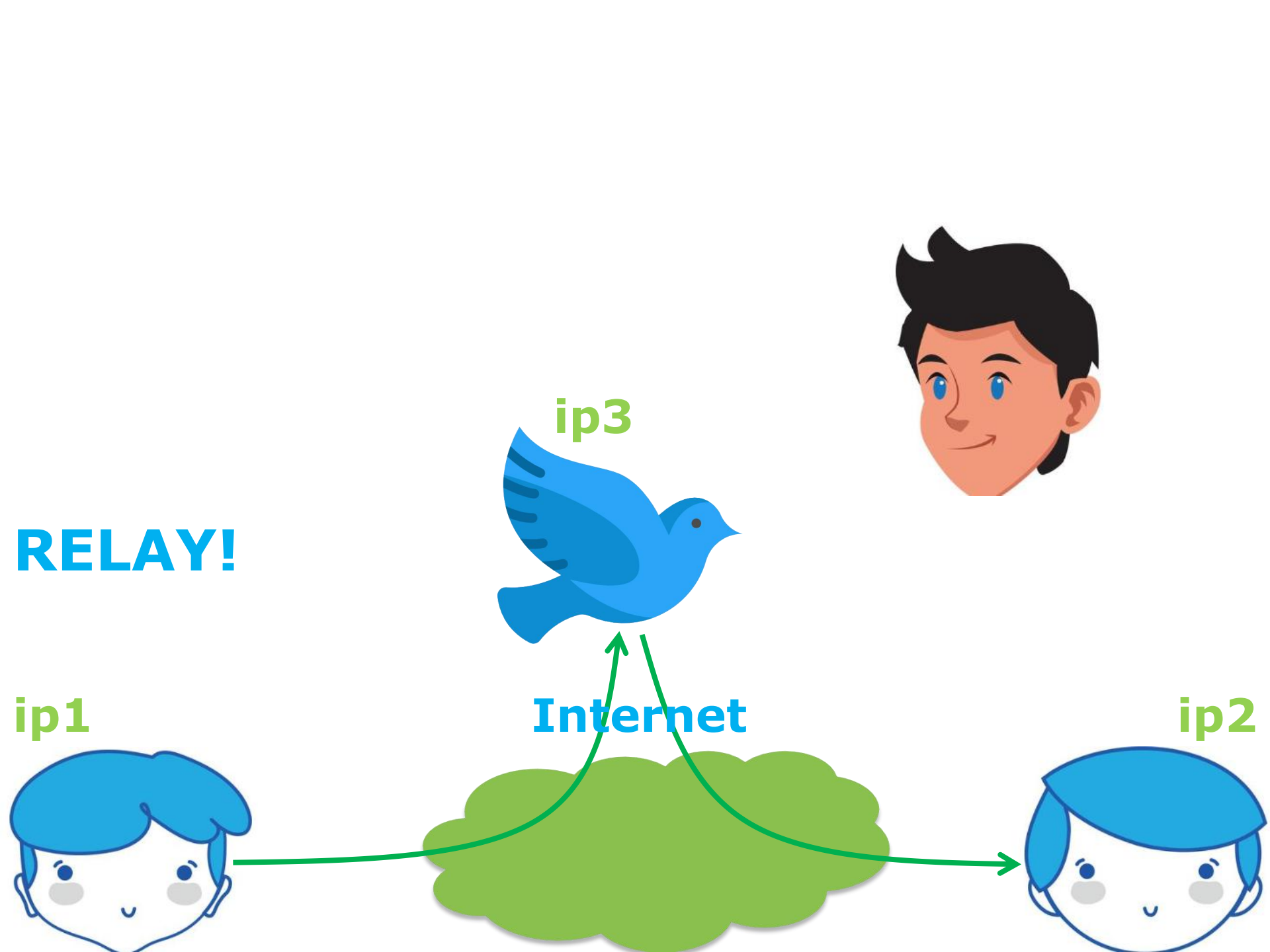
Anonymous Communication

hide destination address;

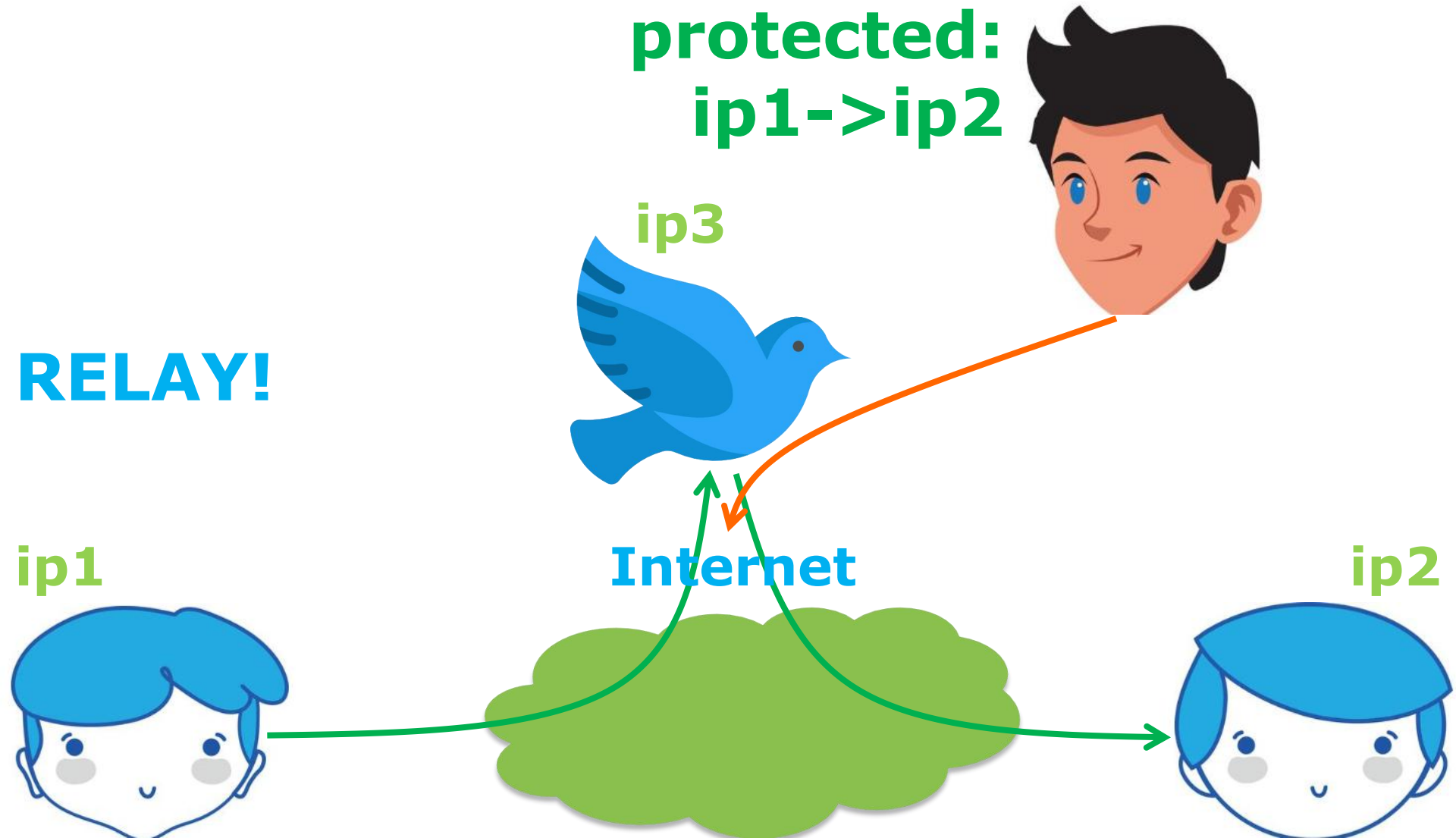
how to deliver packets to destination?

Anonymous Communication

RELAY!


RELAY!
ip3
ip1
Internet
ip2

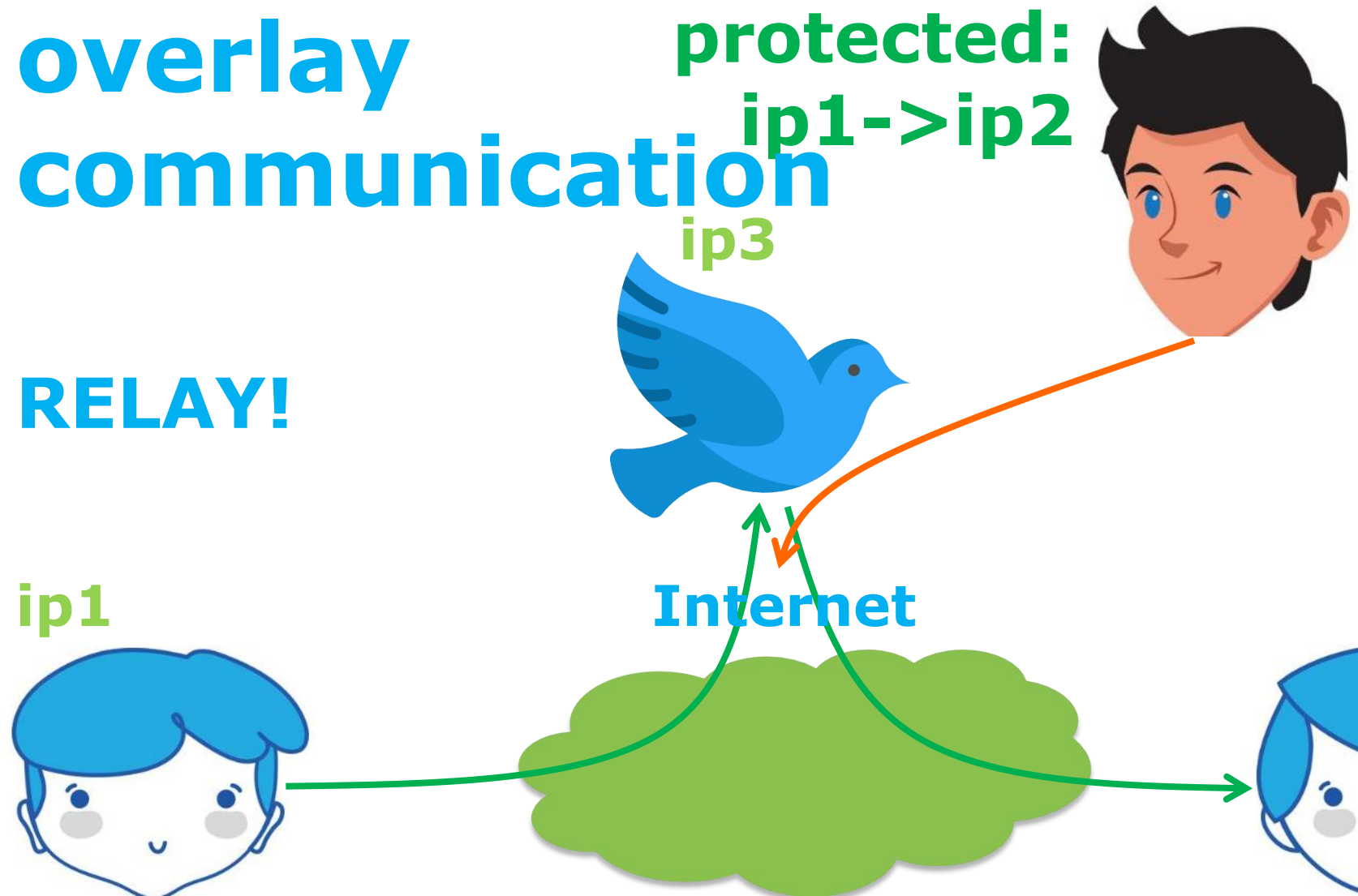
monitored:
ip1->ip3, ip3->ip2
protected:
ip1->ip2



monitored:
ip1->ip3, ip3->ip2

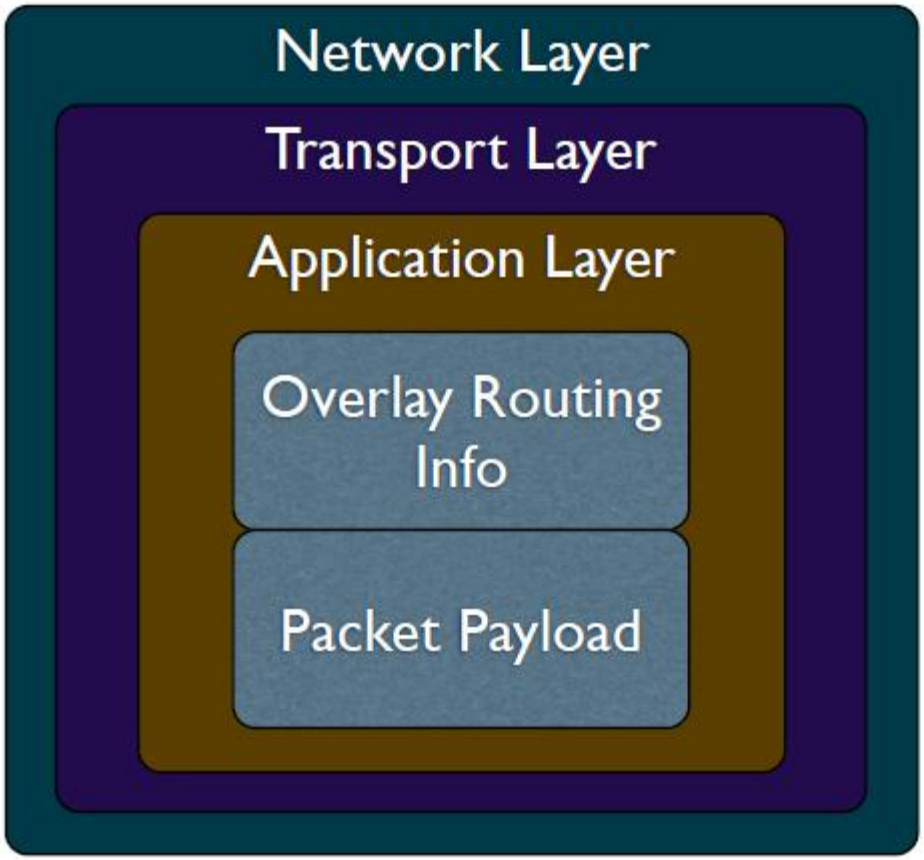
protected:
ip1->ip2

overlay communication

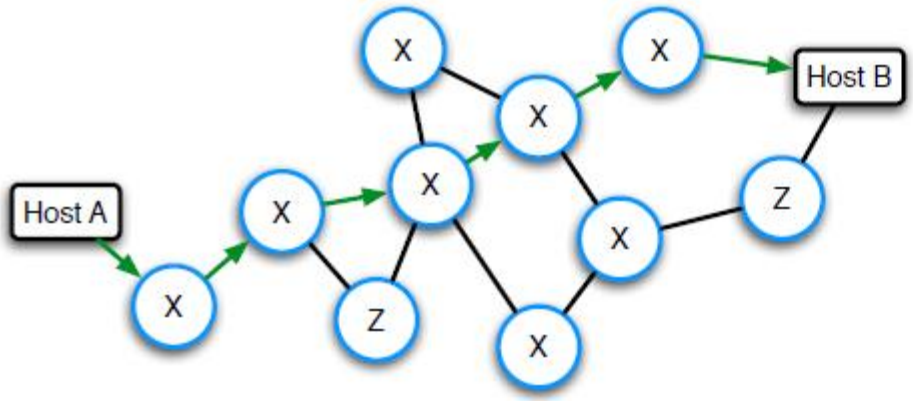


Overlay Network

- Handle routing at the application layer
- Tunnel messages inside other messages



Threat Model

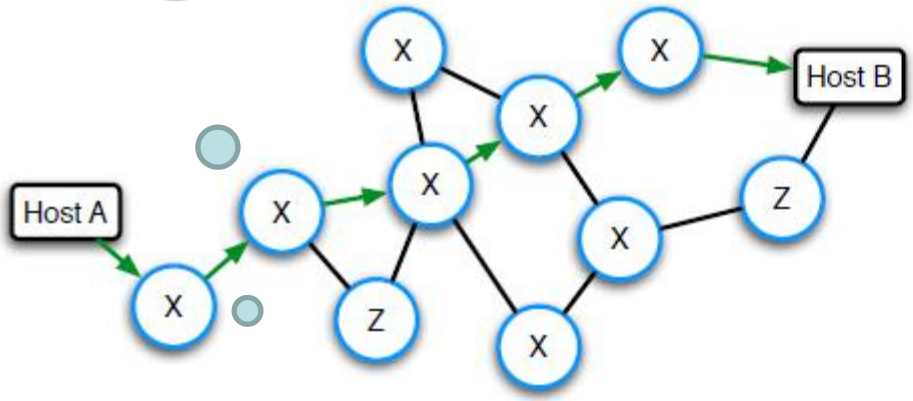


vs

- Insider Byzantine attacker
  with limited view of network:
  an attacker might have tight control over a network (e.g., Z ASes),
  yet unlikely to observe entire Internet

Threat Model

Attacker is part of the network



vs

- Insider Byzantine attacker

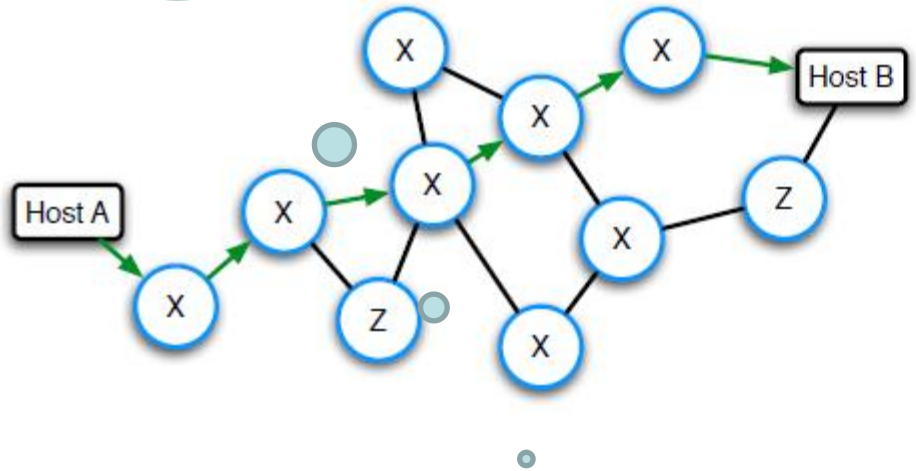
  with limited view of network:

  an attacker might have tight control over a network (e.g., Z ASes),

  yet unlikely to observe entire Internet

Threat Model

Attacker may or may not attack



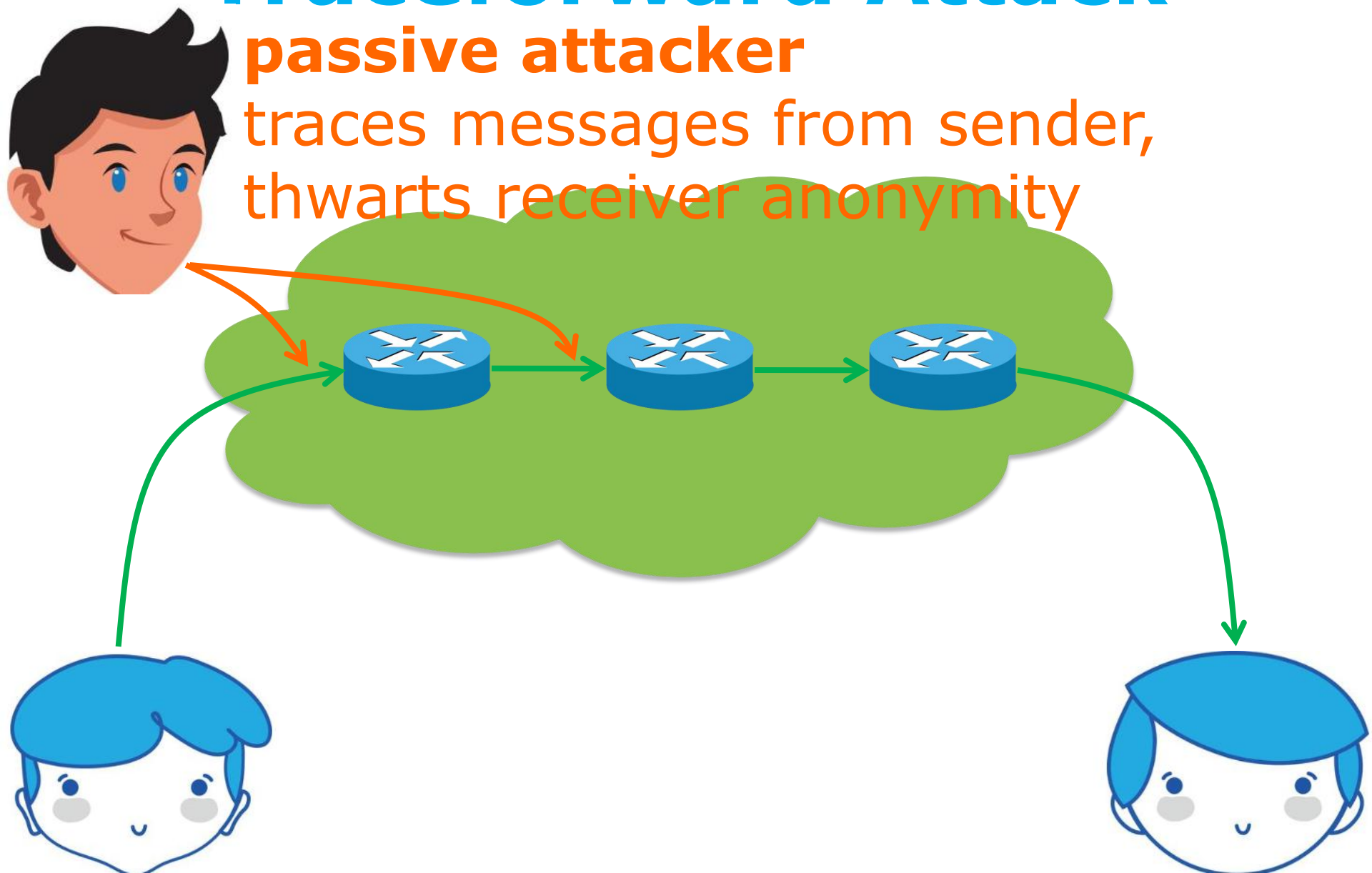
vs

- Insider Byzantine attacker
  with limited view of network:
  an attacker might have tight control over a network (e.g., Z ASes),
  yet unlikely to observe entire Internet

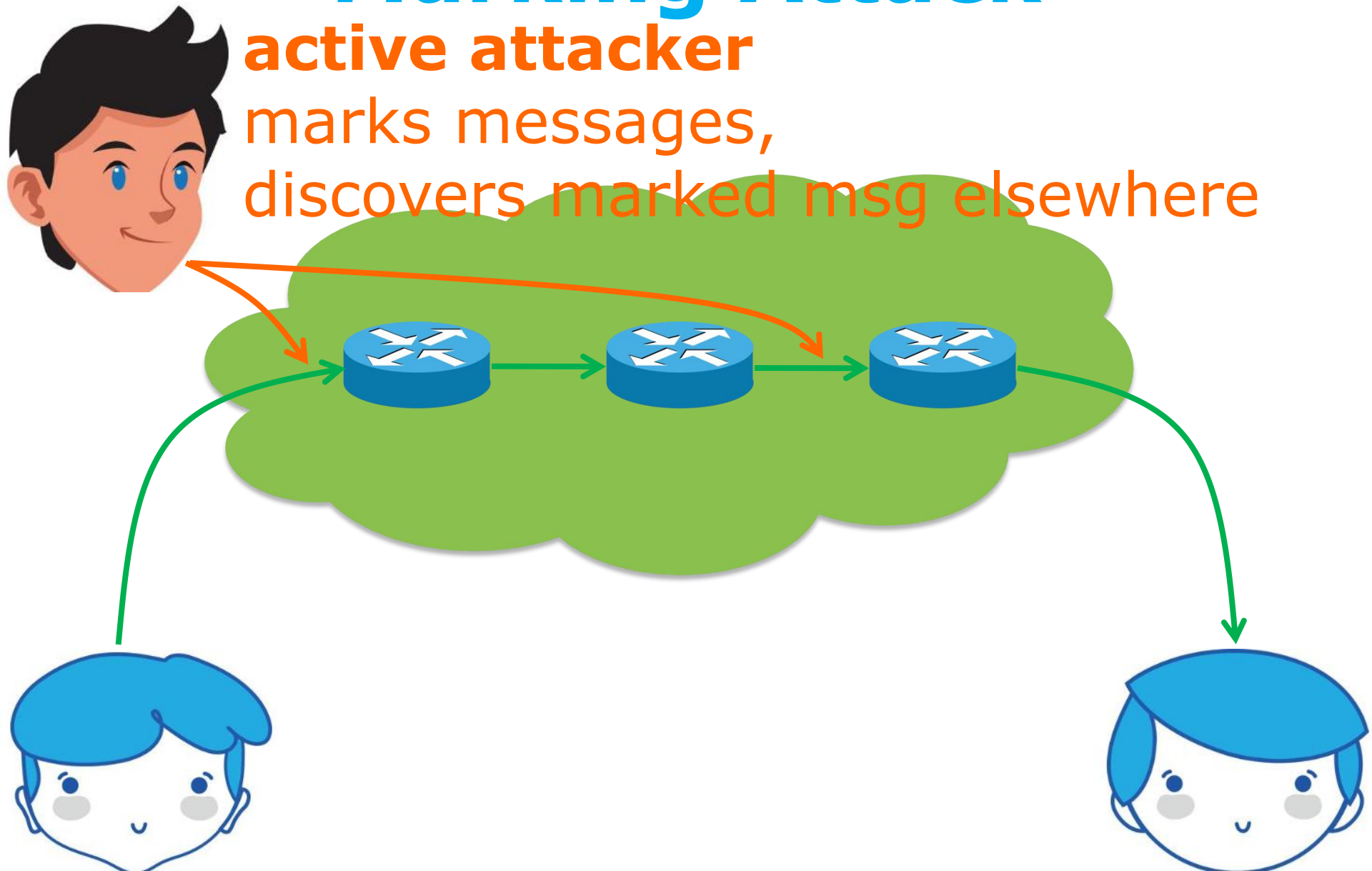
Traceforward Attack

passive attacker

traces messages from sender, thwarts receiver anonymity



Marking Attack



Anonymous Communication

anonymizing proxy

Anonymizing Proxy

PROXIFY

Anonymouse.org

hidemyass!
FREE WEB PROXY

Zend2.com
Freedom of Speech

FREEPROXY.CA
Anonymous, free and proudly Canadian.

Anonymizing Proxy

- intermediary between sender & receiver
- Sender relays all traffic through proxy
- Encrypt destination and payload

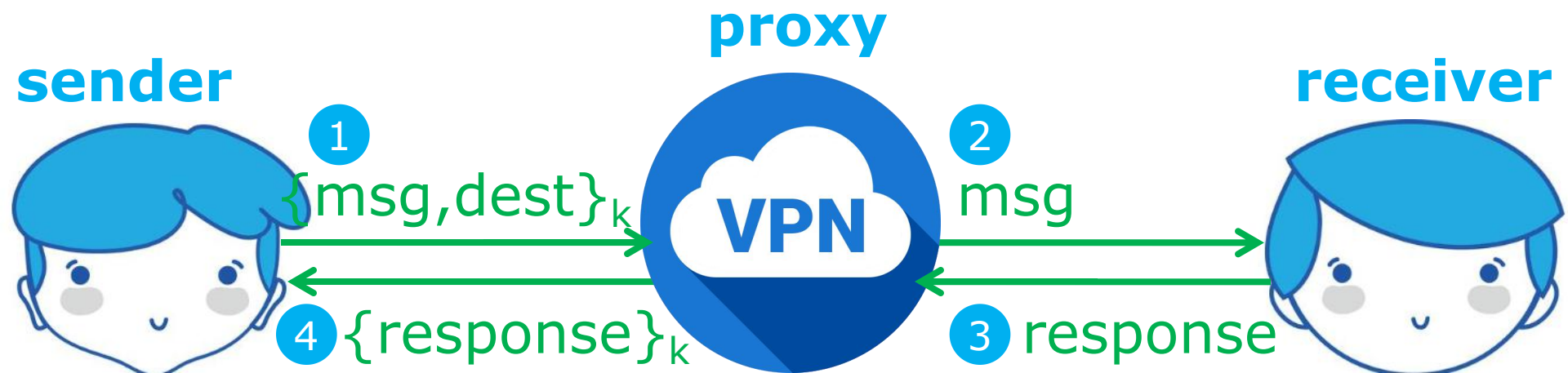
Anonymizing Proxy

- intermediary between sender & receiver
- Sender relays all traffic through proxy
- Encrypt destination and payload
- Asymmetric technique:

  receiver not involved (or informed of) anonymity

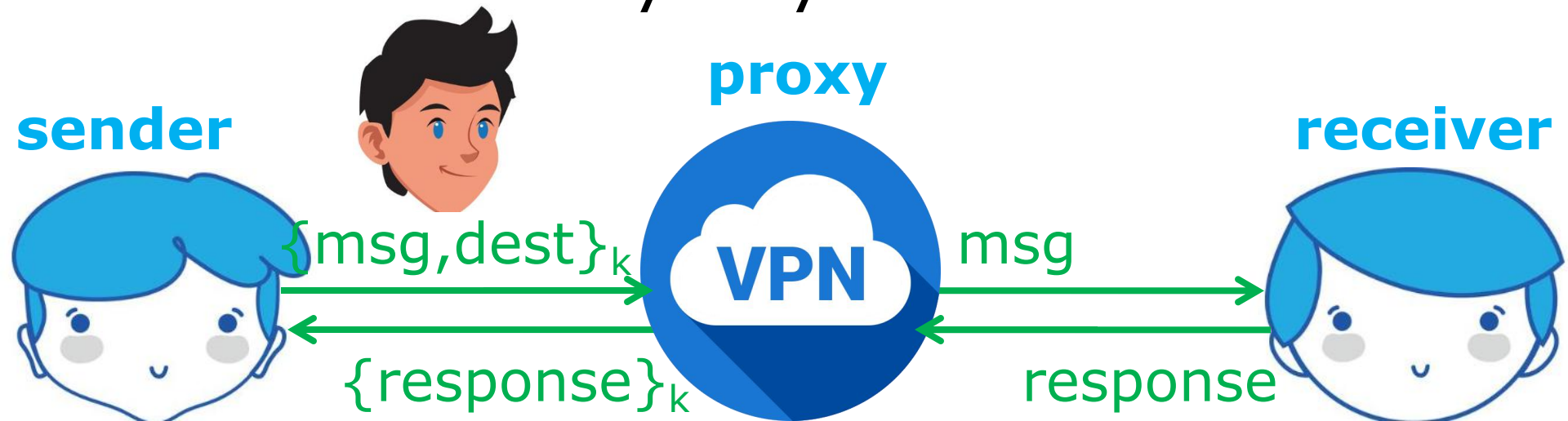
Anonymizing Proxy

- k: shared key of sender and proxy



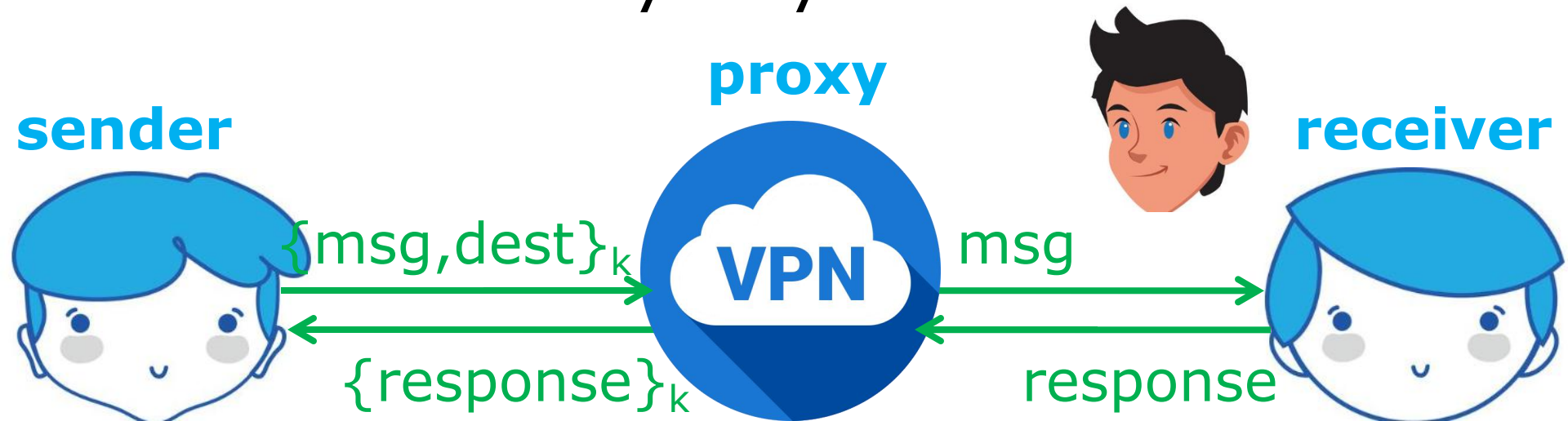
Anonymizing Proxy

- k: shared key of sender and proxy
- if attacker is located between sender and proxy:
  sender anonymity: 0
  receiver anonymity: 1



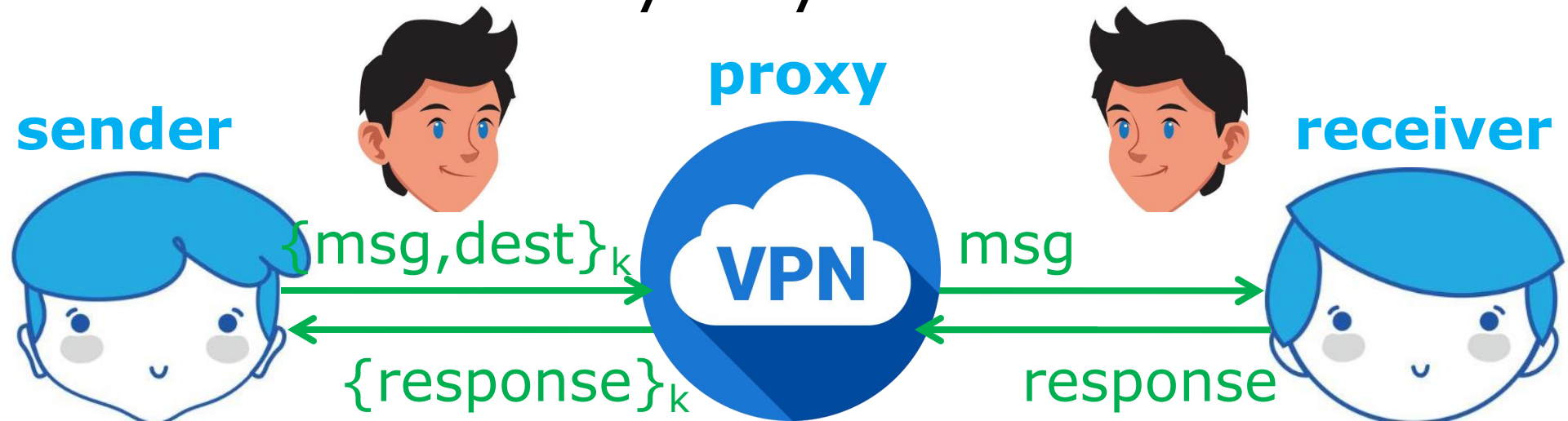
Anonymizing Proxy

- k: shared key of sender and proxy
- if attacker is located between proxy and receiver:
  sender anonymity: 1
  receiver anonymity: 0



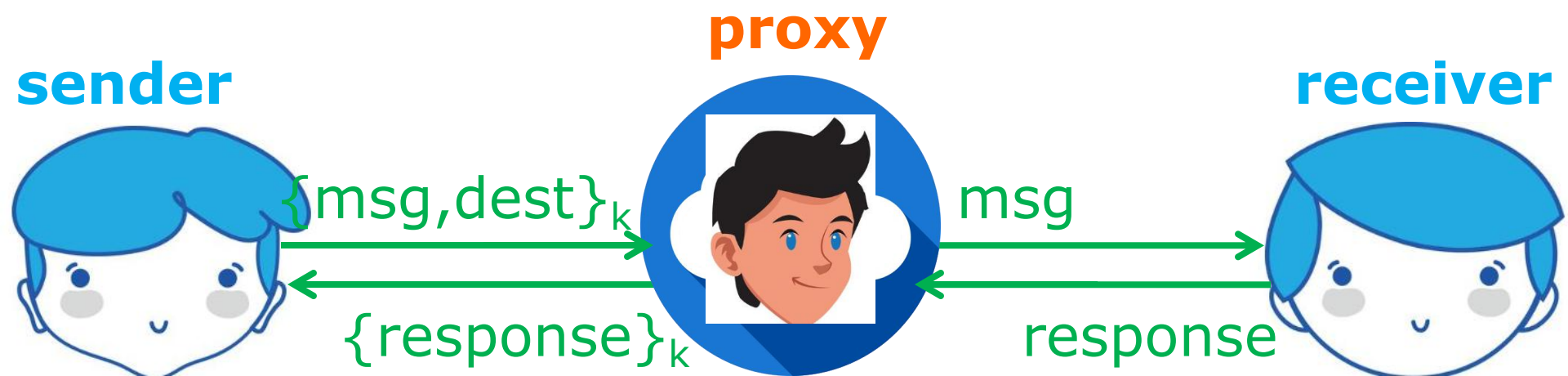
Anonymizing Proxy

- k: shared key of sender and proxy
- if two attackers collude to correlate ingress and egress proxy traffic:
  sender anonymity: 0
  receiver anonymity: 0



Anonymizing Proxy

- If attacker is the proxy per se:
  decrypt all messages;
  crack both confidentiality & anonymity;
  sender anonymity: 0
  receiver anonymity: 0



what if receiver is attacker?

what if receiver is attacker?

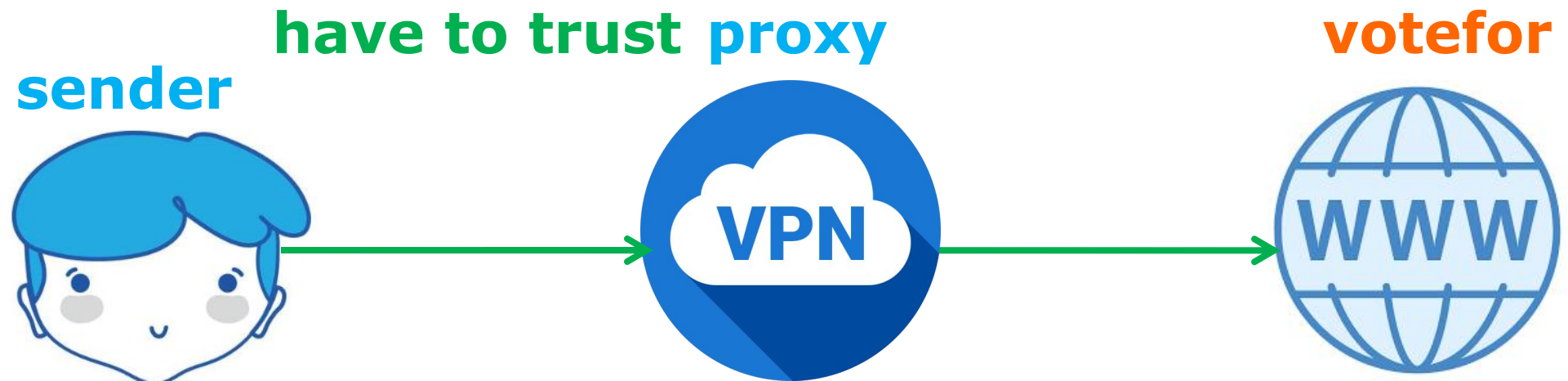
protect sender anonymity from receiver

Receiver as Attacker

- Known-location attacker
- Use proxy to protect sender anonymity:
  do not vote for letting votefor website
  know that I accessed votefor /wink

Receiver as Attacker

- Known-location attacker
- Use proxy to protect sender anonymity:
  do not vote for letting votefor website
  know that I accessed votefor /wink



Anonymizing Proxy

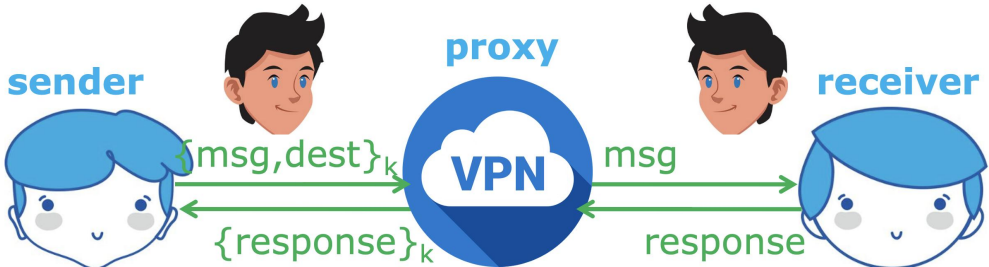
Advantages

- Easy to configure
- Require no active participation of receiver, which need not be aware of anonymity service
- Have been widely deployed on Internet

Anonymizing Proxy

Disadvantages

- Require trusted third party
  proxy may release logs,
  or sell them,
  or blackmail sender
- Anonymity largely depends on the (likely unknown) location of attacker



how to evade attacker?

how to evade attacker?

dynamize proxy location

Crowds Algorithm

- Basic idea:

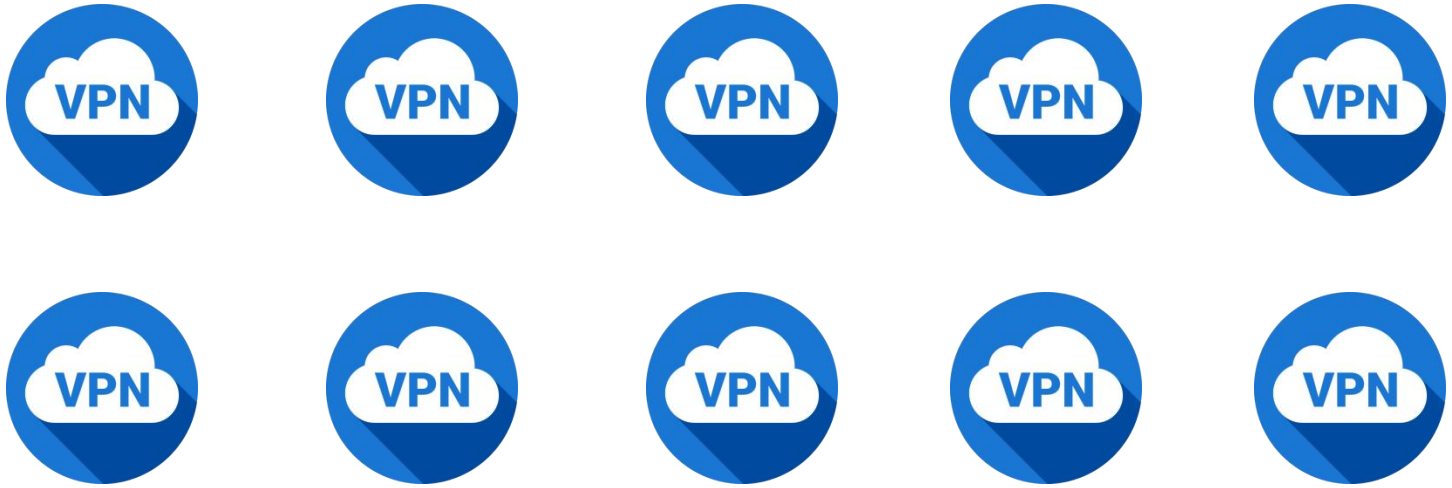
  get lost in a crowd
- Jump from one crowd to another
- Members of a crowd called Jondos

Crowds Algorithm

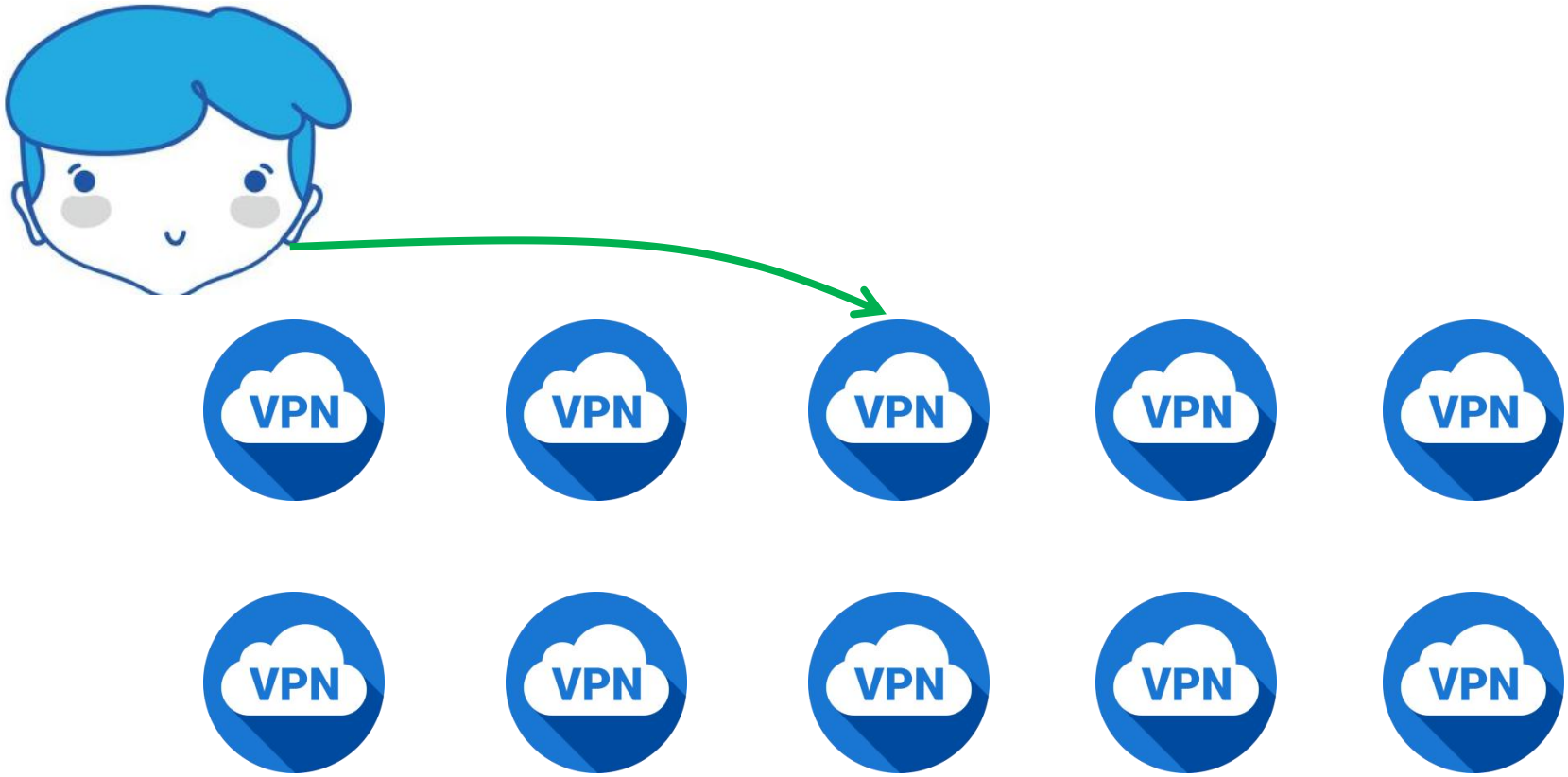
Algorithm:

- Relay message to random jondo
- With probability p, jondo forwards message to another jondo
- With probability 1-p, jondo delivers message to its intended destination

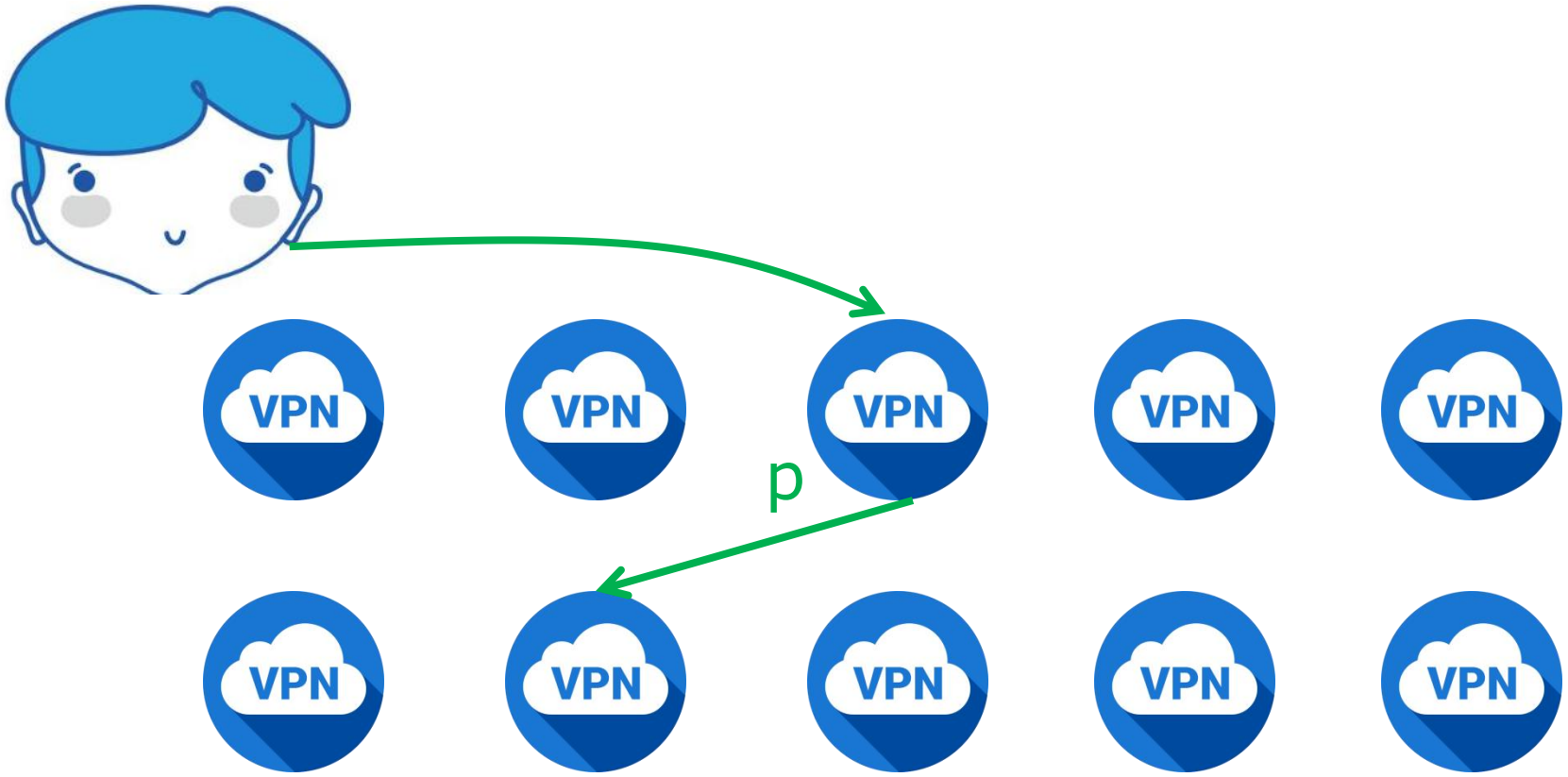
Crowds Algorithm



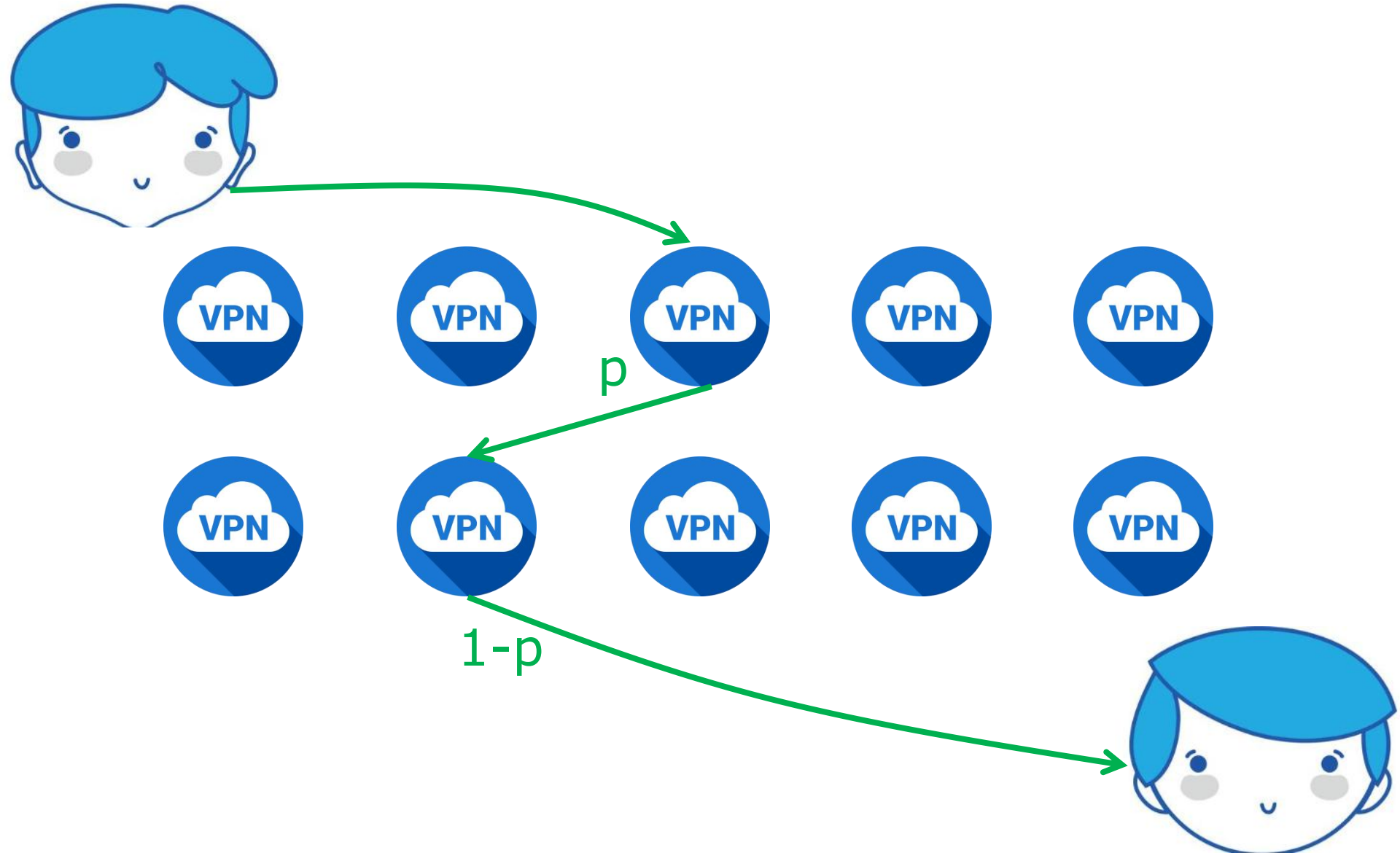
Crowds Algorithm



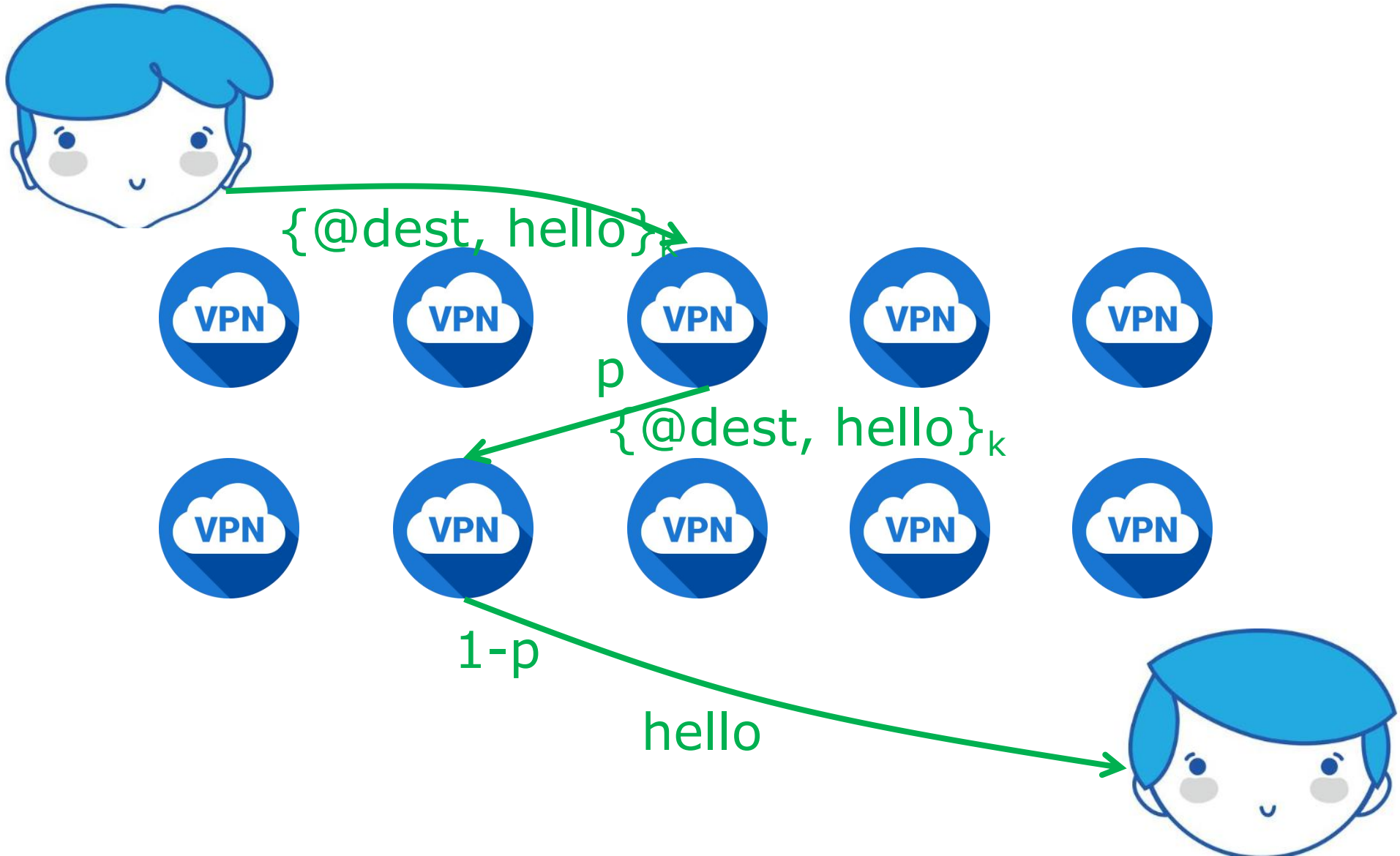
Crowds Algorithm



Crowds Algorithm

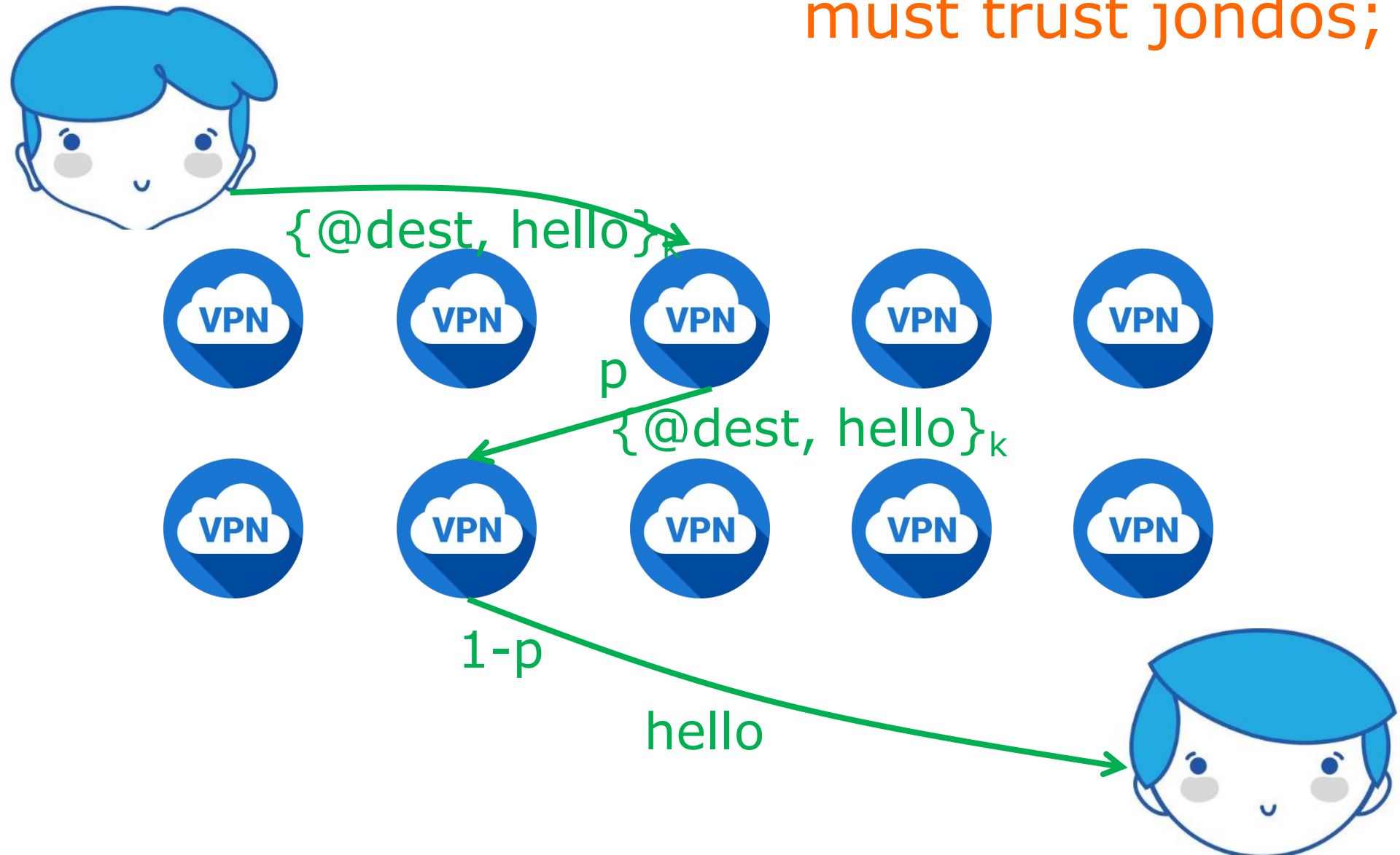


Crowds Algorithm



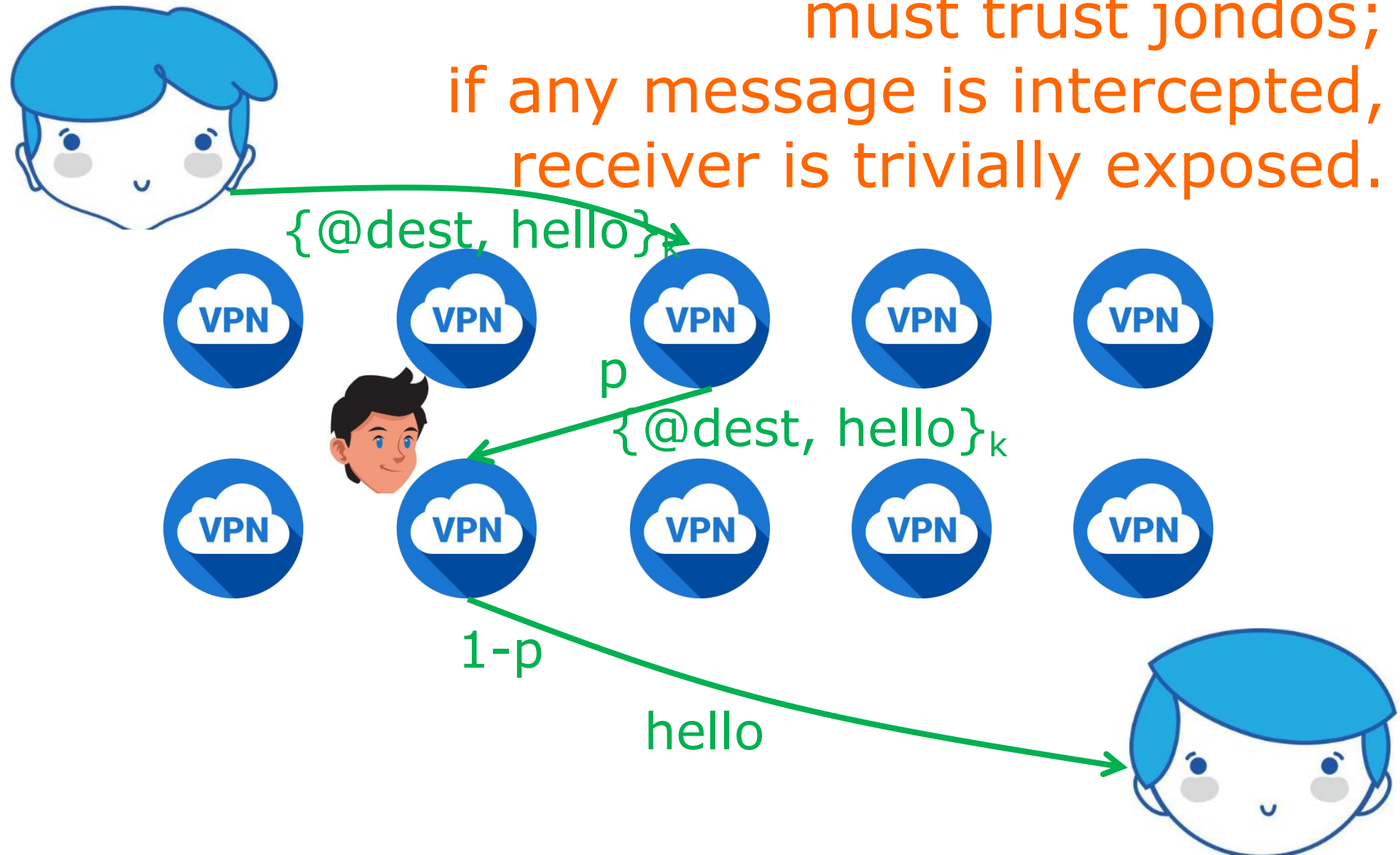
Crowds Algorithm

must trust jondos;



Crowds Algorithm

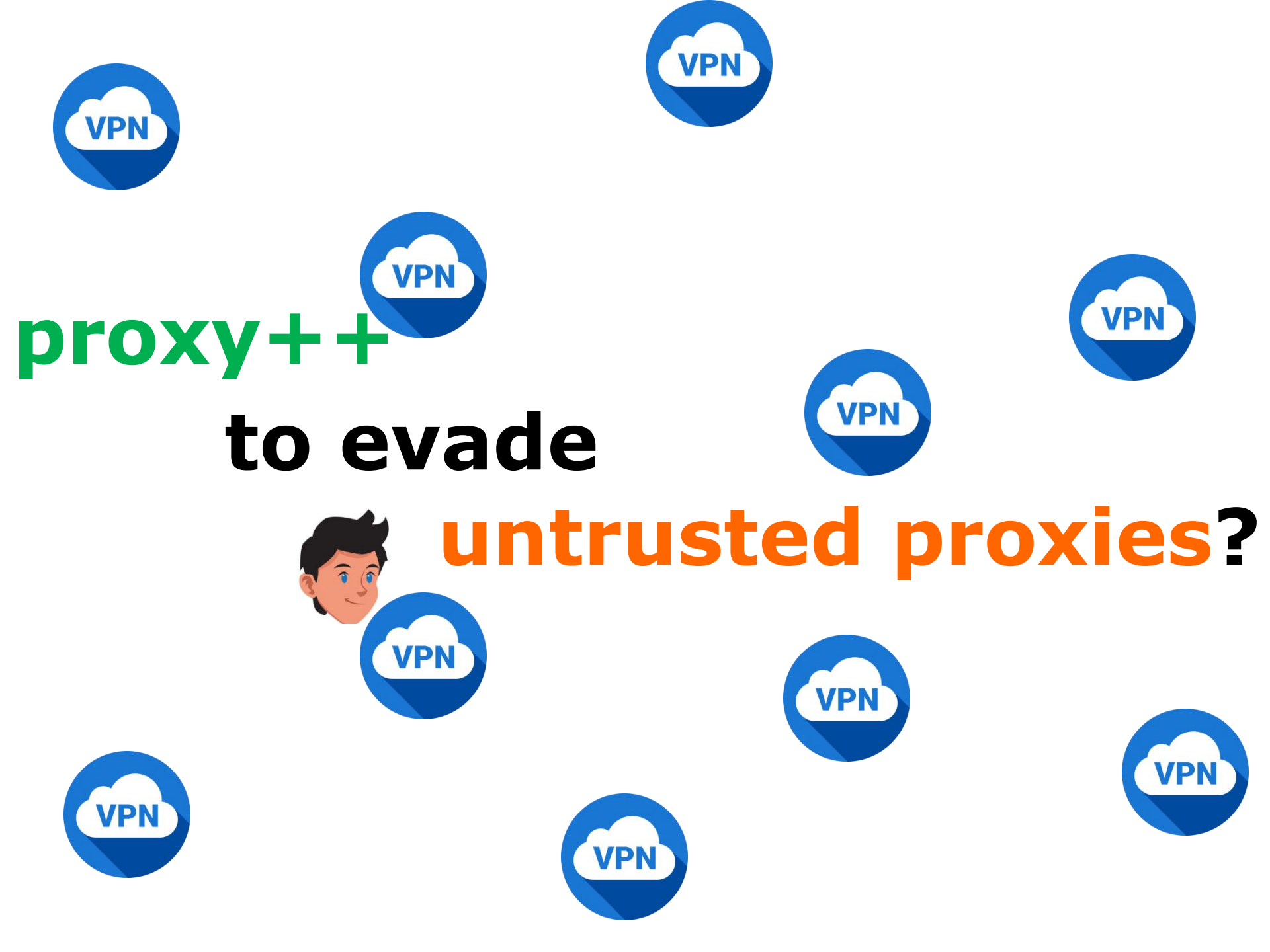
must trust jondos;
if any message is intercepted,
receiver is trivially exposed.

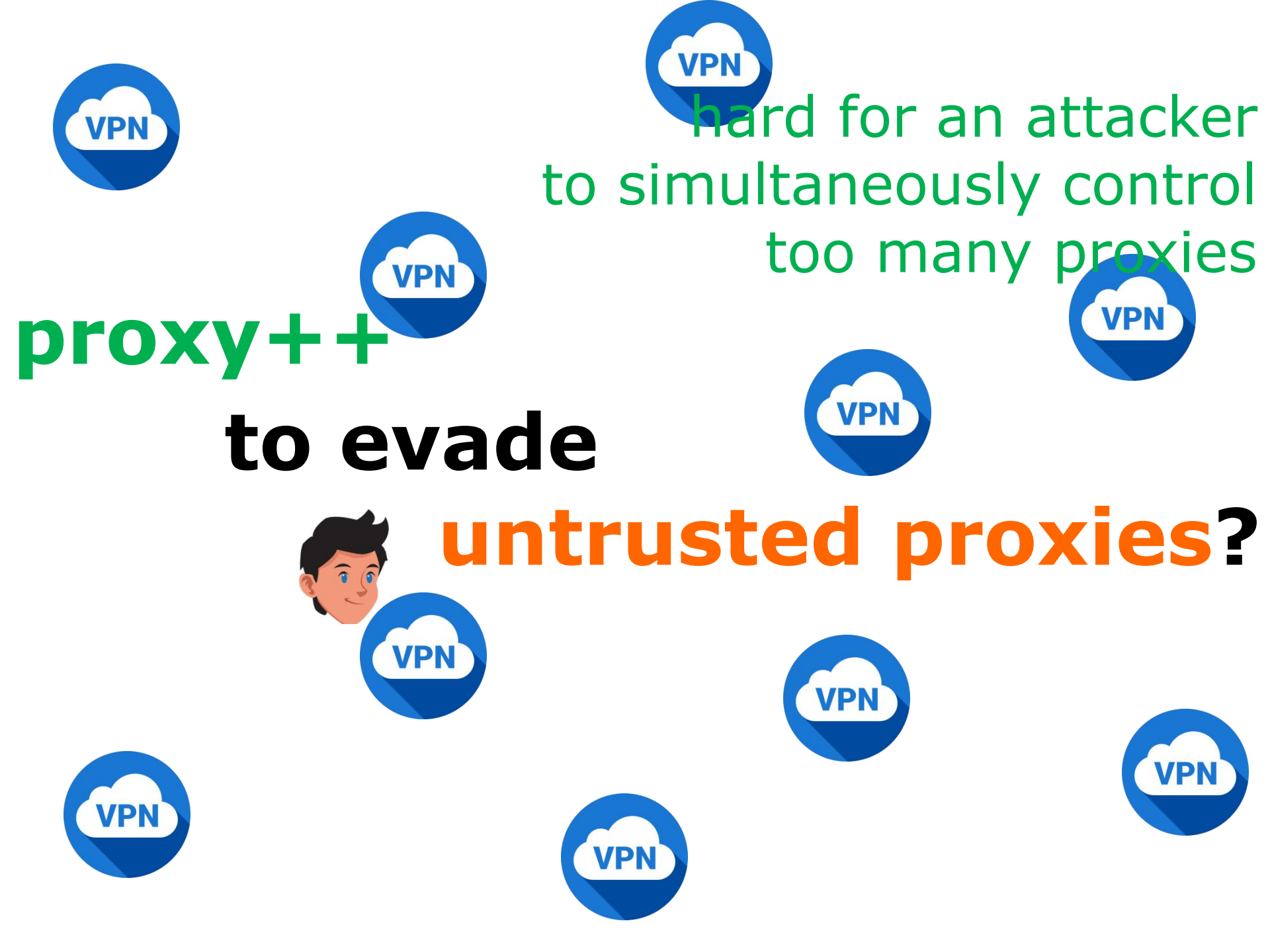


how to evade

untrusted proxies?

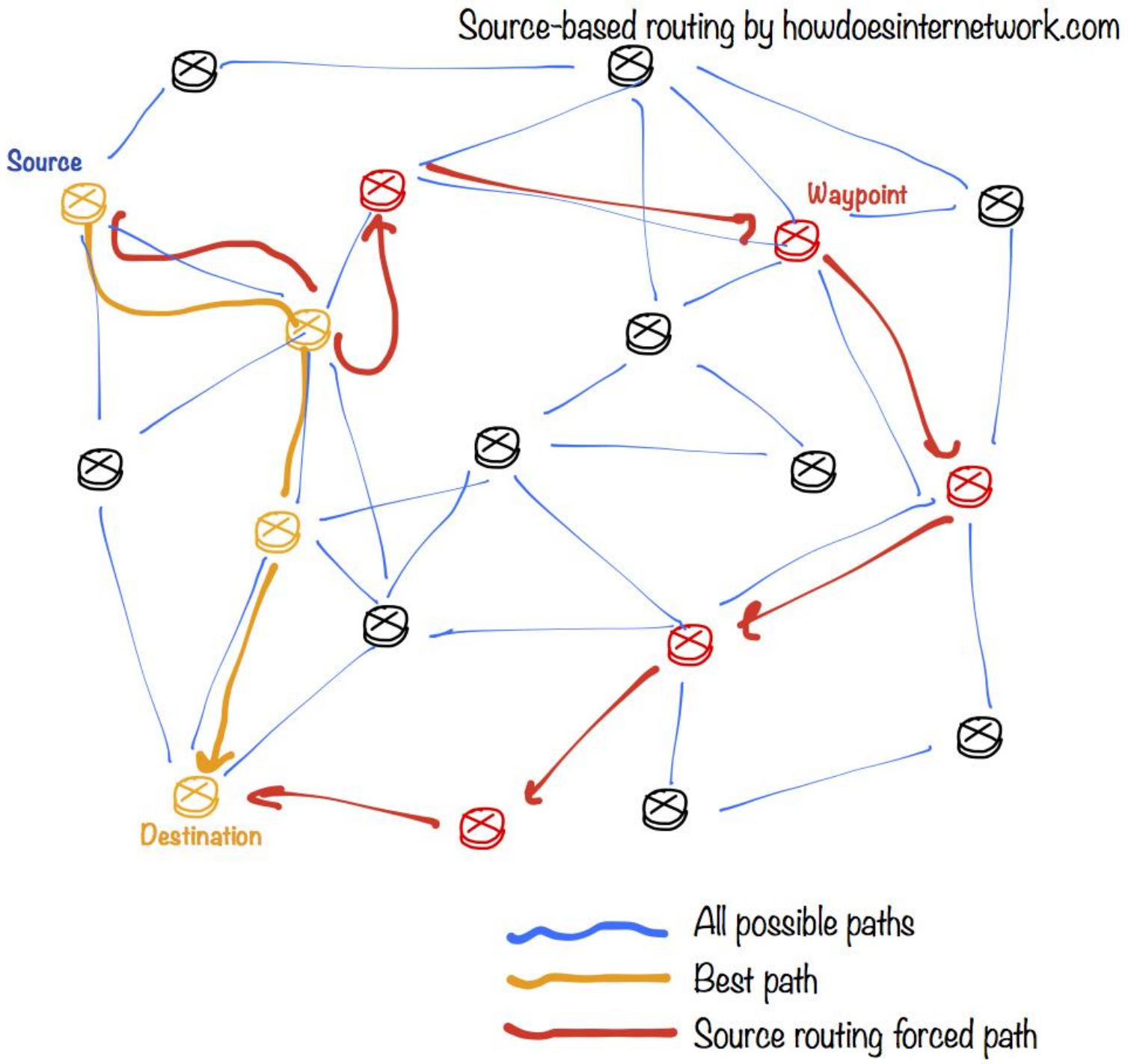
how to evade untrusted proxies?


proxy++
to evade
untrusted proxies?
VPN


hard for an attacker
to simultaneously control
too many proxies
proxy++
to evade
untrusted proxies?

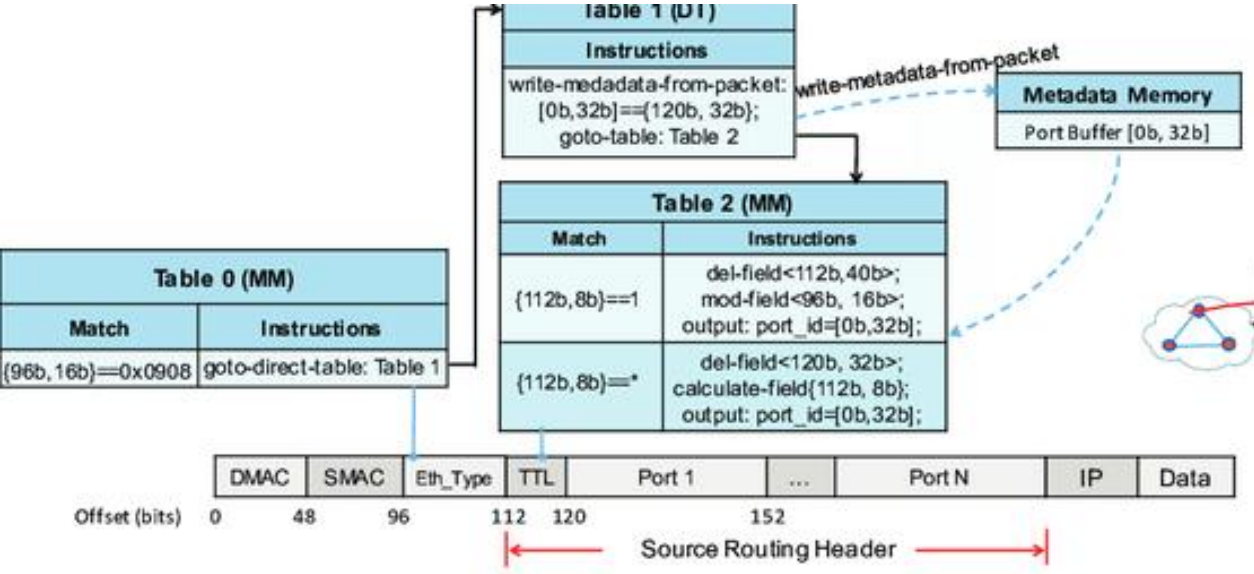
source routing

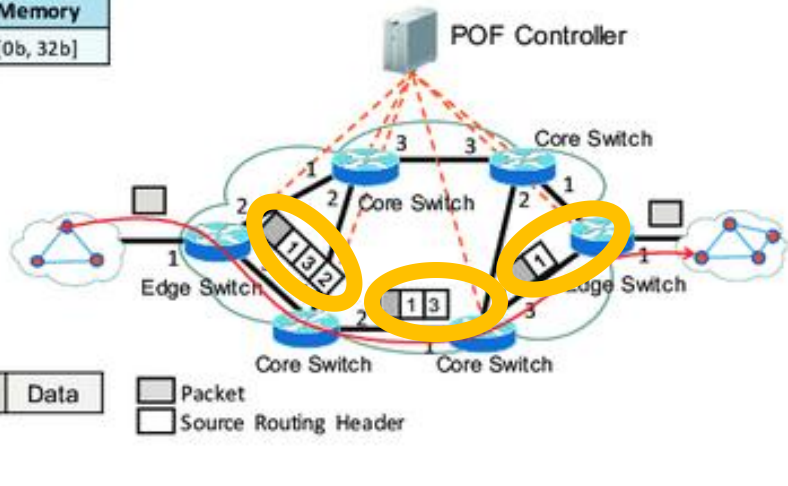
specify on-path routers by source


Source-based routing by howdoesinternetwork.com
Source
Waypoint
Destination
All possible paths
Best path
Source routing forced path

POF-based Source Routing

- POF: Protocol Oblivious Forwarding
- Port bound



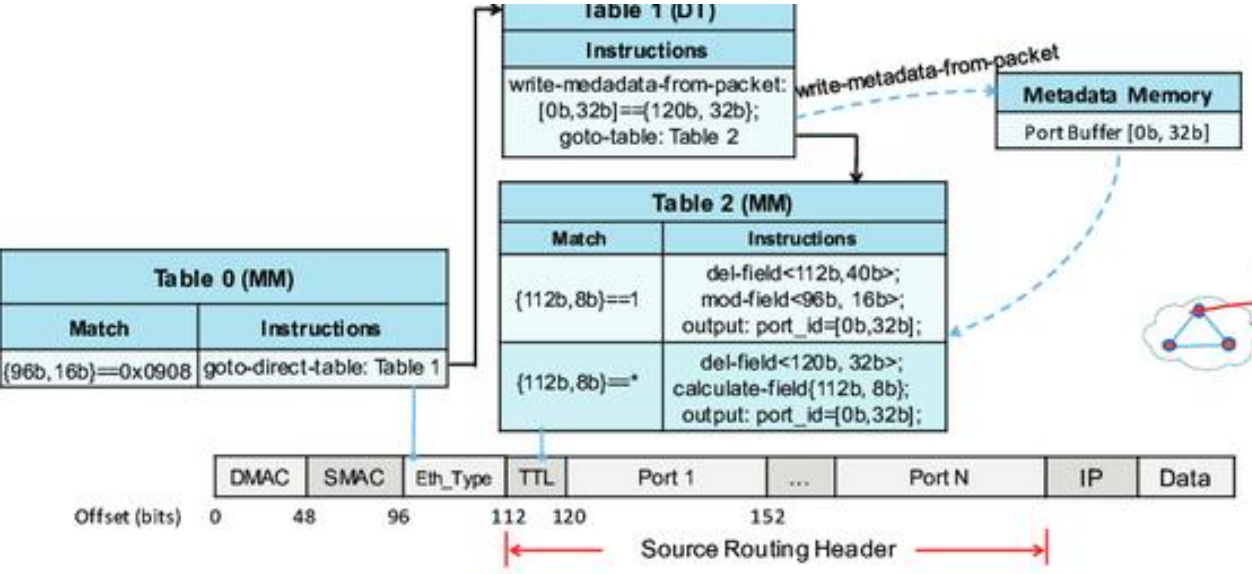


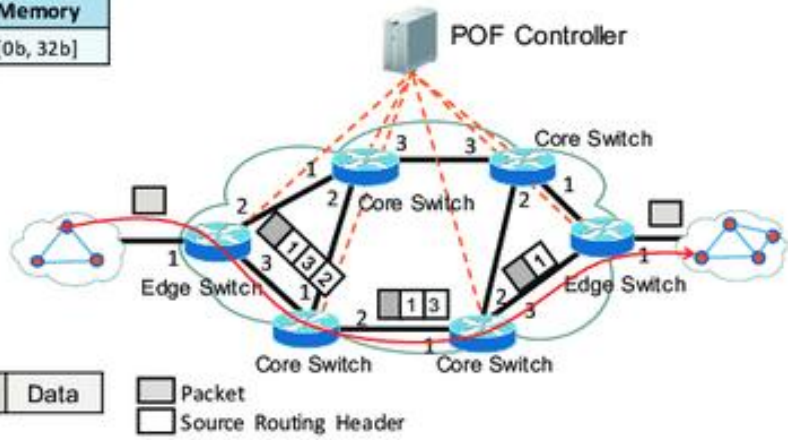
forwarding table

forwarding process

POF-based Source Routing

- POF: Protocol Oblivious Forwarding
- Port bound





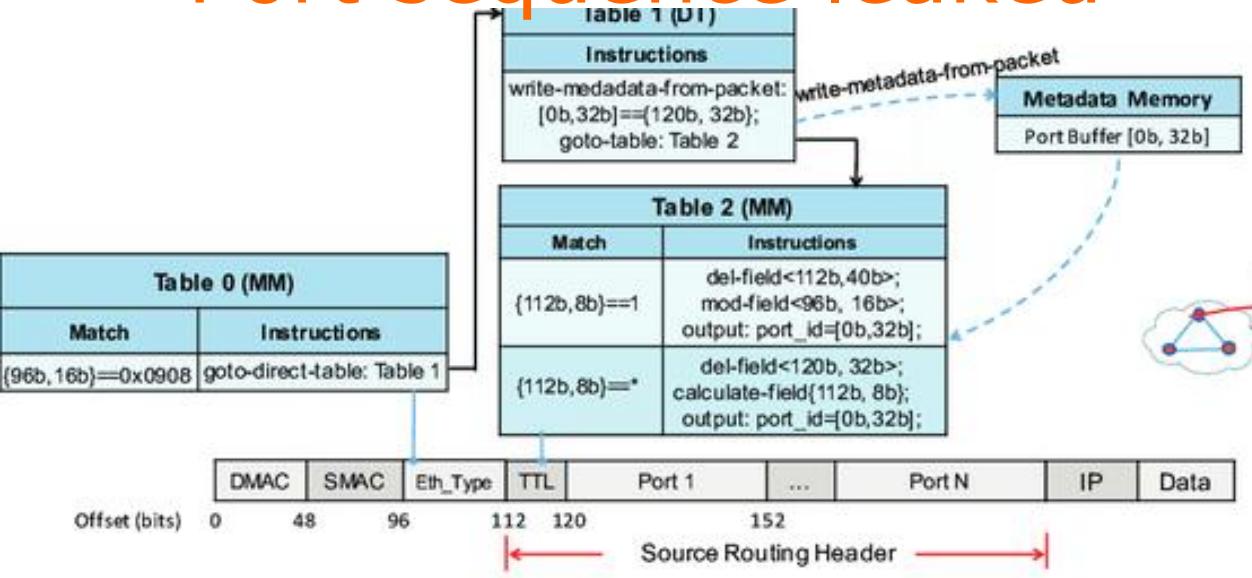
forwarding table

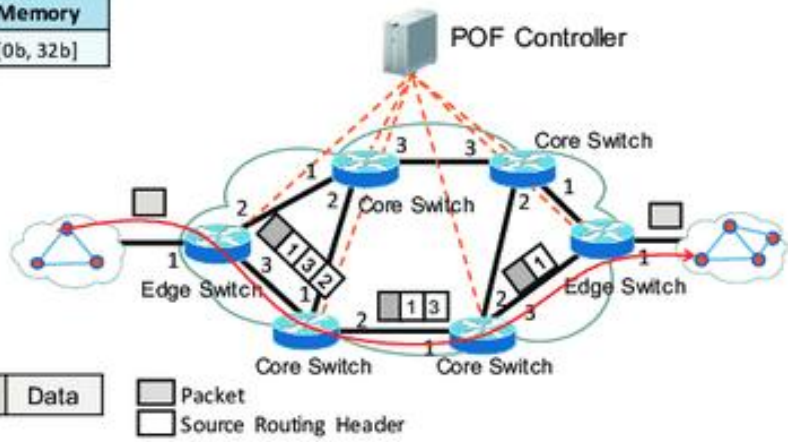
forwarding process

anonymity protected?

POF-based Source Routing

- POF: Protocol Oblivious Forwarding
- Port sequence leaked





forwarding table

forwarding process

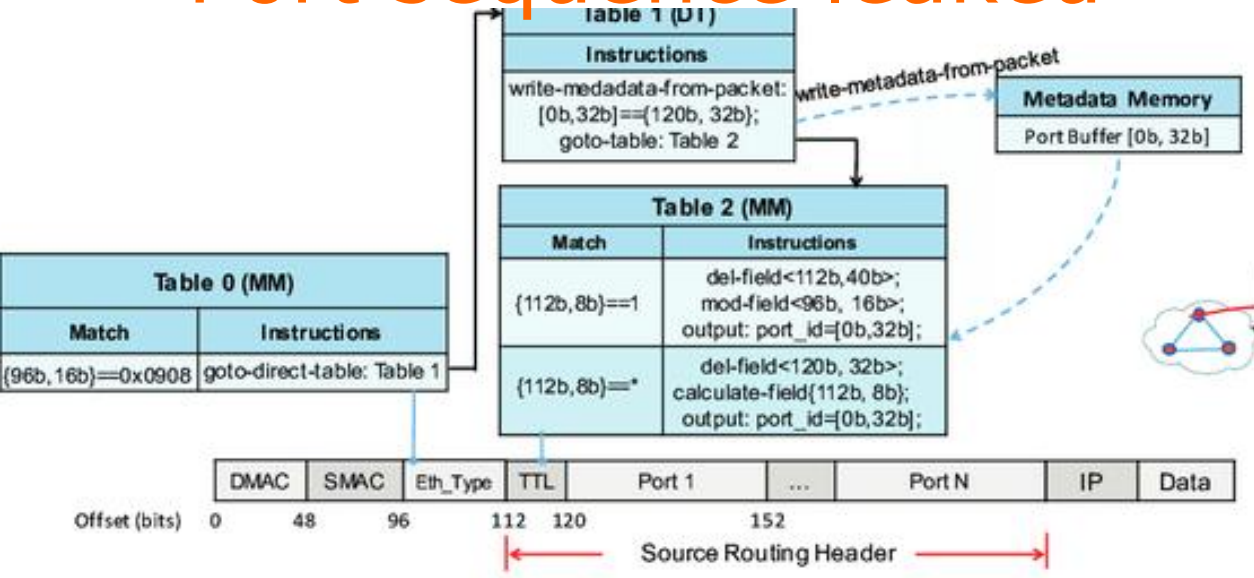
anonymity protected? nah!

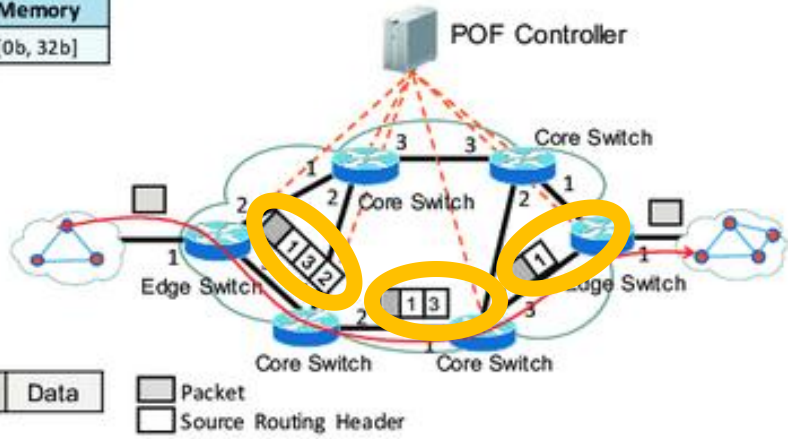
source routing

how to anonymize?

POF-based Source Routing

- POF: Protocol Oblivious Forwarding
- Port sequence leaked





forwarding table

forwarding process

should hide ports from non-neighbors

onion routing

source-routing based

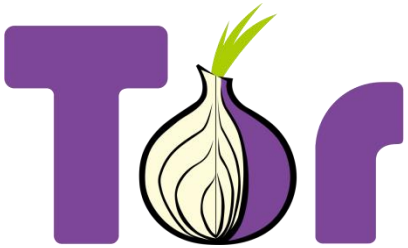
anonymous overlay communication

onion routing

source-routing based

anonymous overlay communication

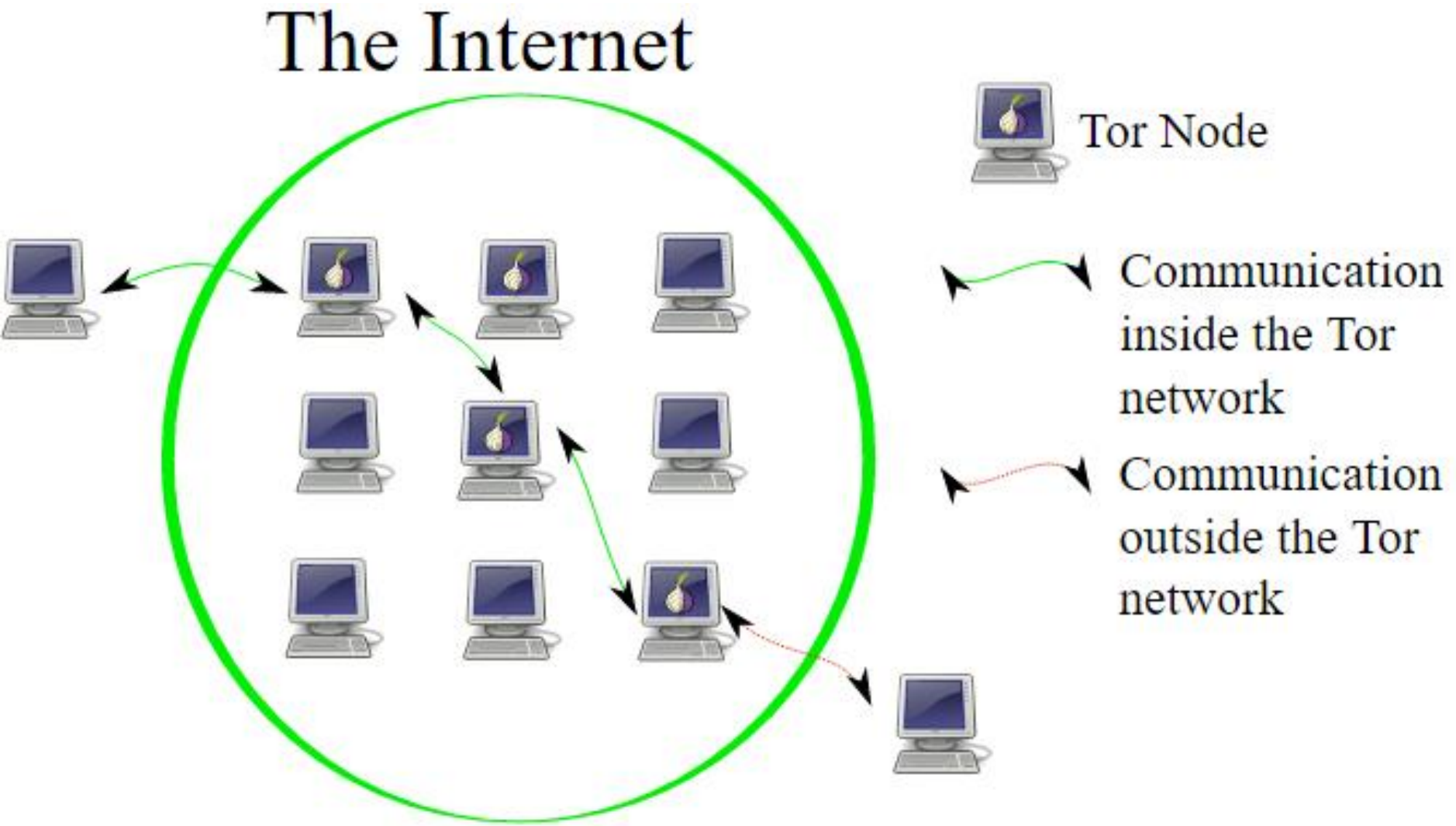
onion routing



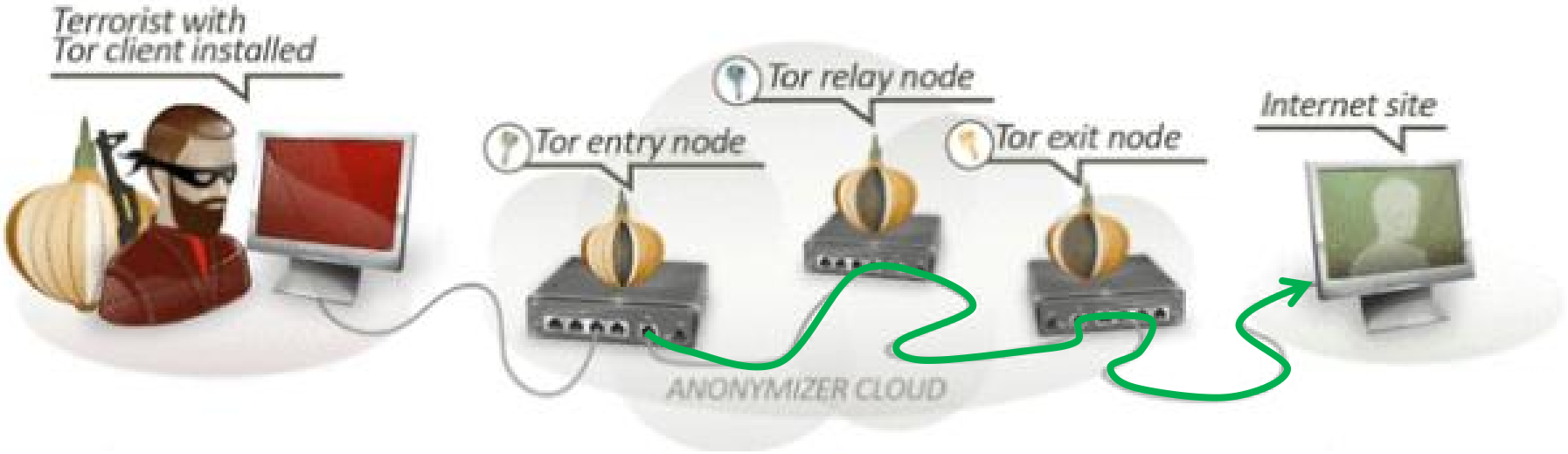
source-routing based

anonymous overlay communication

Onion Routing

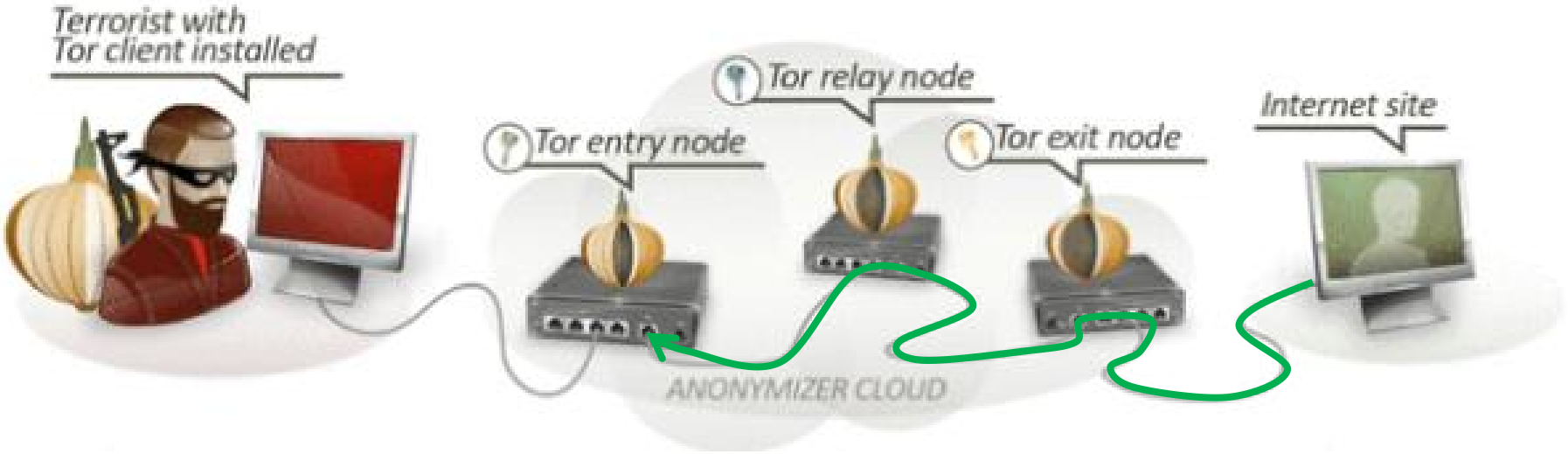


Onion Routing



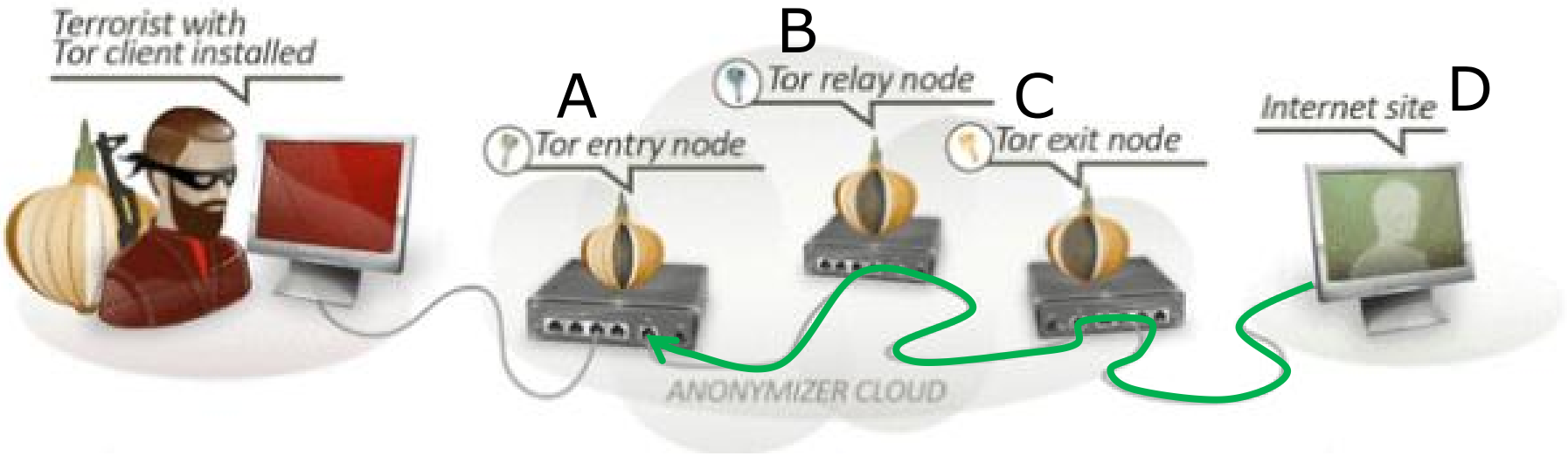
- Connect to Tor entry
- Randomly select a series of Tors
- Relay messages across them
- Tor exit relays messages to destination

Onion Routing



- Reply traffic from destination traverses the reverse path
- Maintains a bidirectional persistent multi-hop path between source and destination

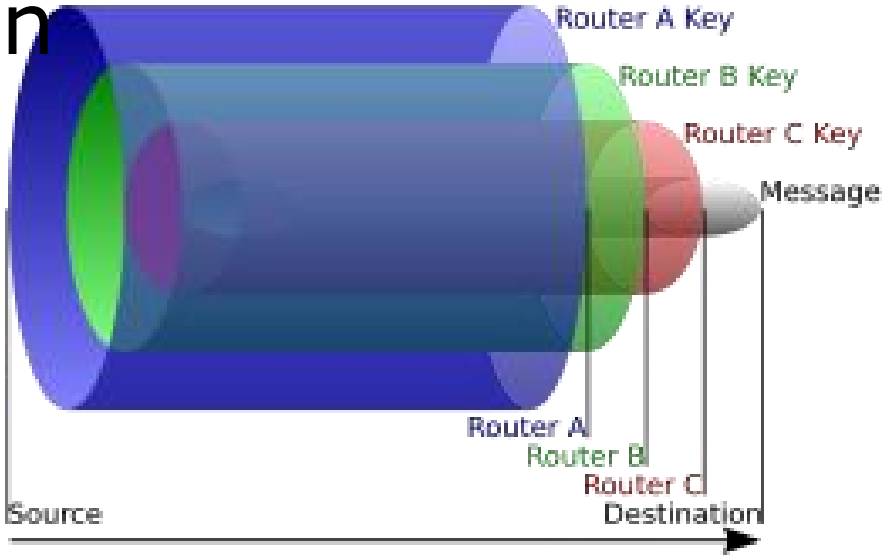
Onion Routing



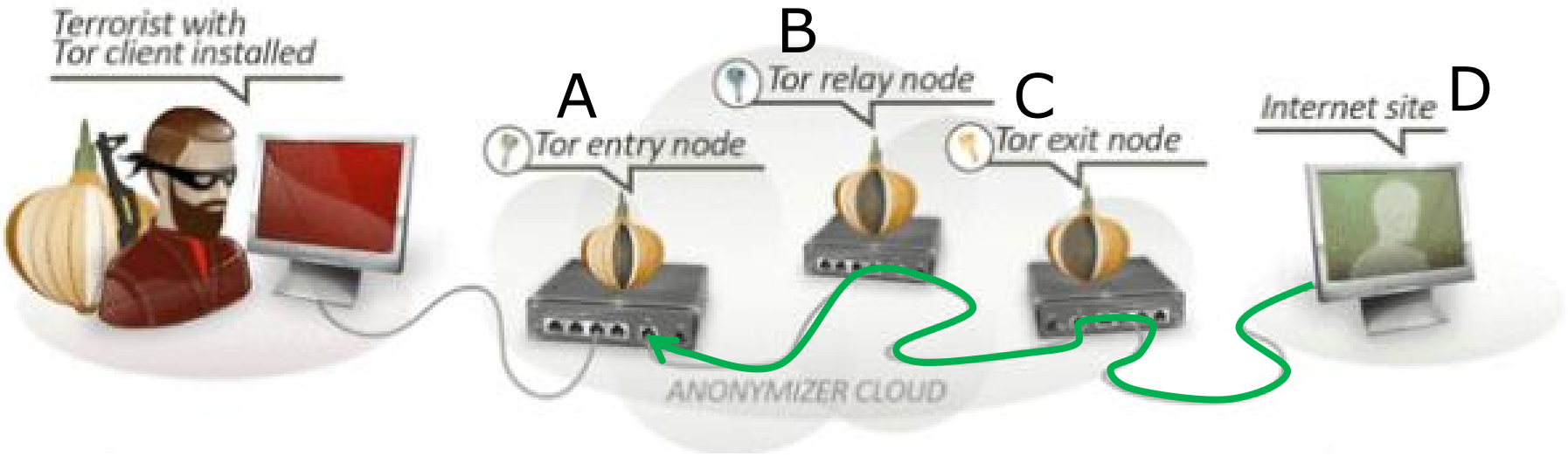
- Layered Encryption

  $\{\{\{\{msg\}_D\}_C\}_B\}_A$

  sufficient?



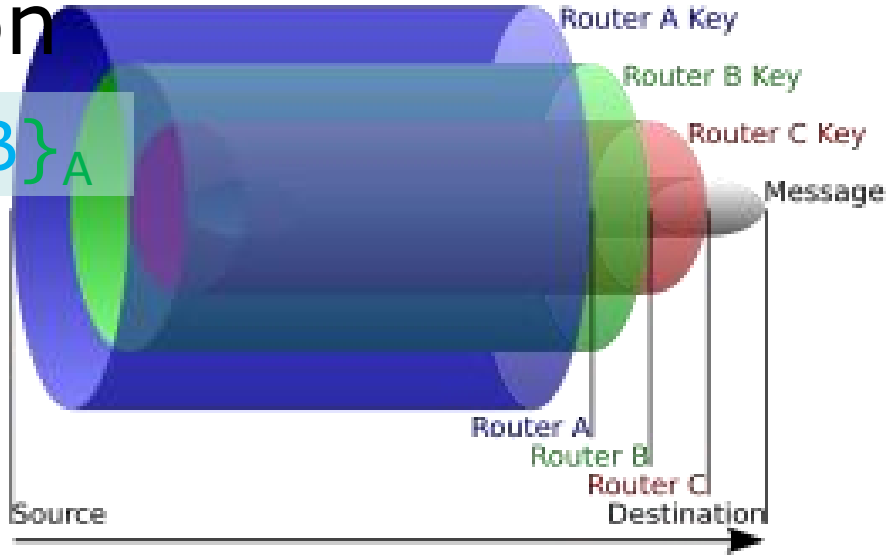
Onion Routing



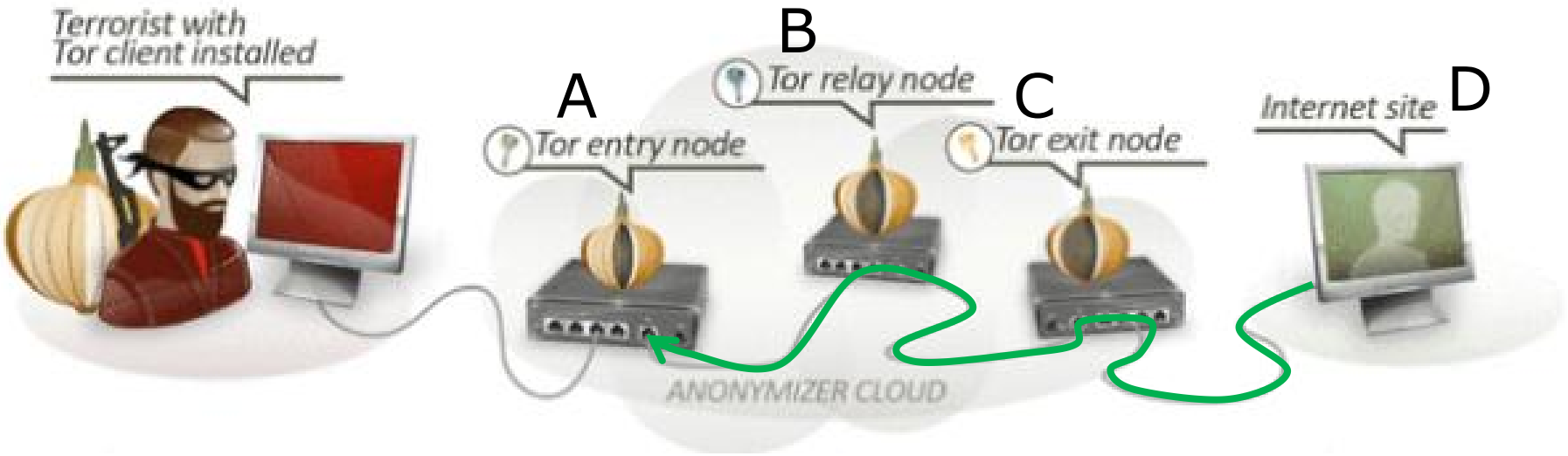
- Layered Encryption

  $\{\{\{\{msg\}_D, D\}_C, C\}_B, B\}_A$

  sufficient



Onion Routing

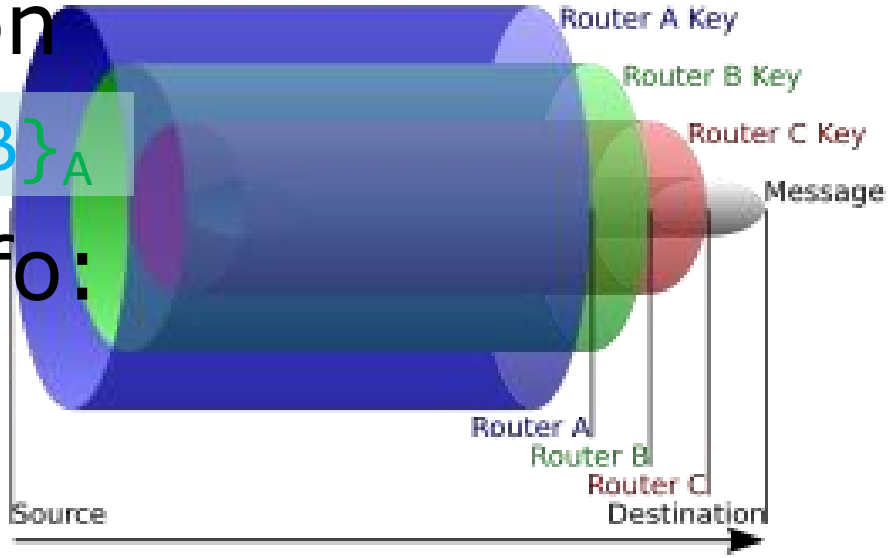


- Layered Encryption

  $\{\{\{\{msg\}_D, D\}_C, C\}_B, B\}_A$

- Leaked routing info:

  neighborship only



onion routing

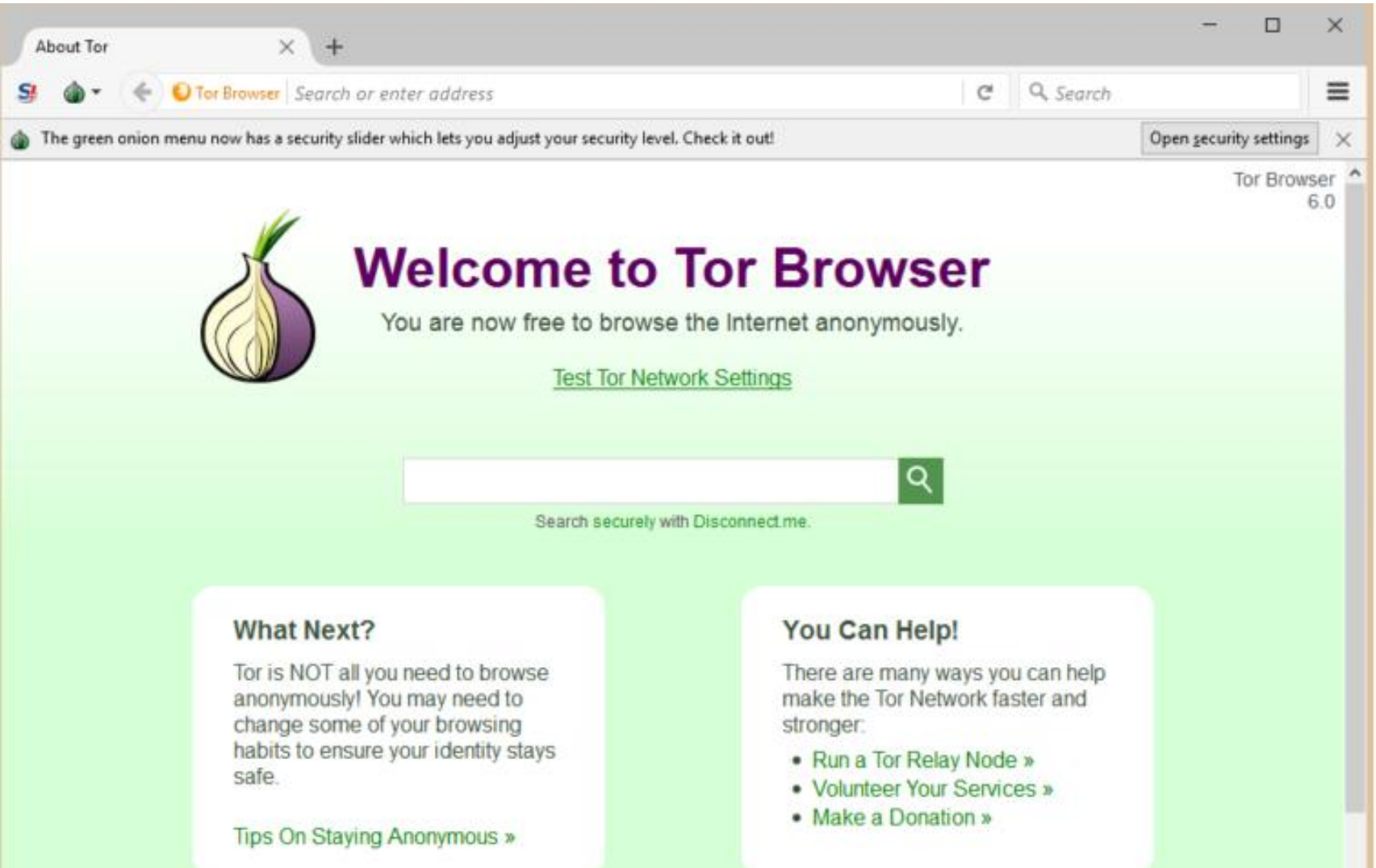
applications?

Darknet

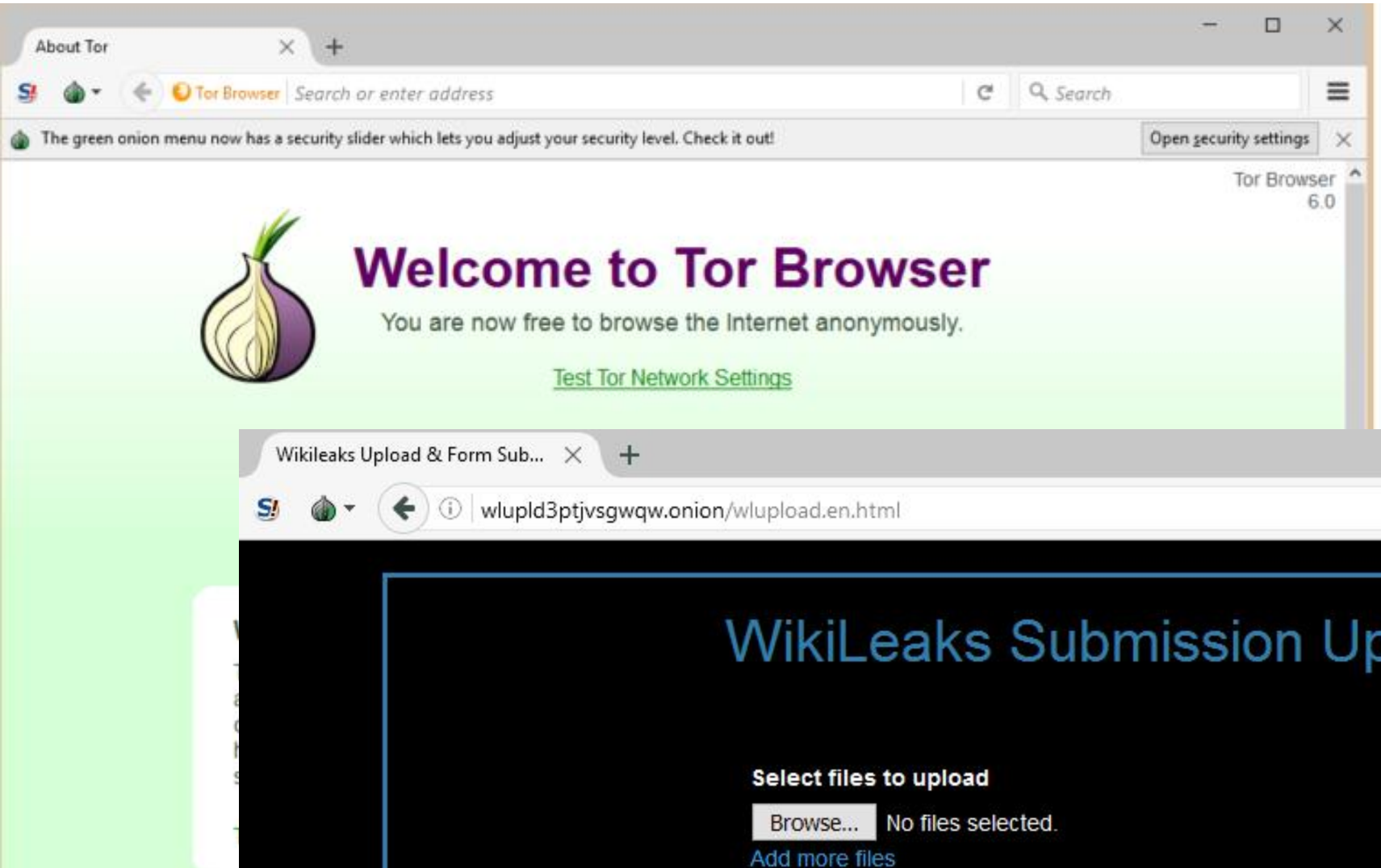
- Portions of the Internet purposefully not open to public view
  or hidden networks whose architecture is superimposed on that of Internet.

- Install Tor
- Access darknet.onion through it

Darknet


About Tor
Tor Browser
Search or enter address
Search
The green onion menu now has a security slider which lets you adjust your security level. Check it out!
Open security settings
Tor Browser 6.0
Welcome to Tor Browser
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Disconnect.me.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »

Darknet


About Tor
Tor Browser
Search or enter address
Search
The green onion menu now has a security slider which lets you adjust your security level. Check it out!
Open security settings
Tor Browser
6.0
Welcome to Tor Browser
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Wikileaks Upload & Form Sub...
wlupld3ptjvsgwqw.onion/wlupload.en.html
WikiLeaks Submission Upload
Select files to upload
Browse...
No files selected.
Add more files

how to de-anonymization?

in it to win it!

Tor Traffic Correlation

- Passive monitoring
- Active attraction:

  deploy a Tor router;

  attract Tor traffic;

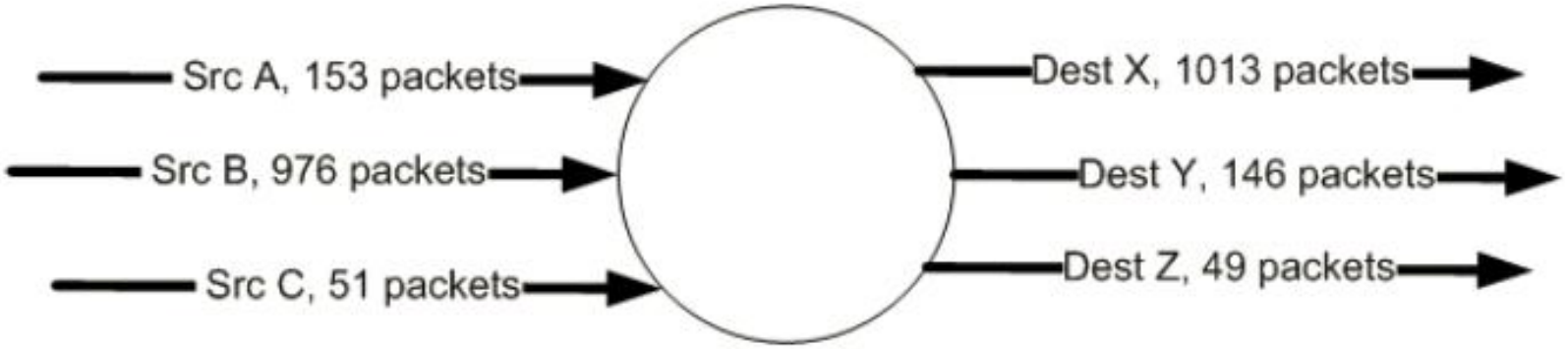
  perform traffic analysis and correlation;

Path Selection Attack

- Tor path selection algorithm:
  weight nodes by selfreported bandwidth
  select each node using weighted probability distribution;
- Attack:
  malicious relay reports very high bw to increase selection probability;
  if it controls the first hop, de- sender;
  if it controls the last hop, de- receiver;

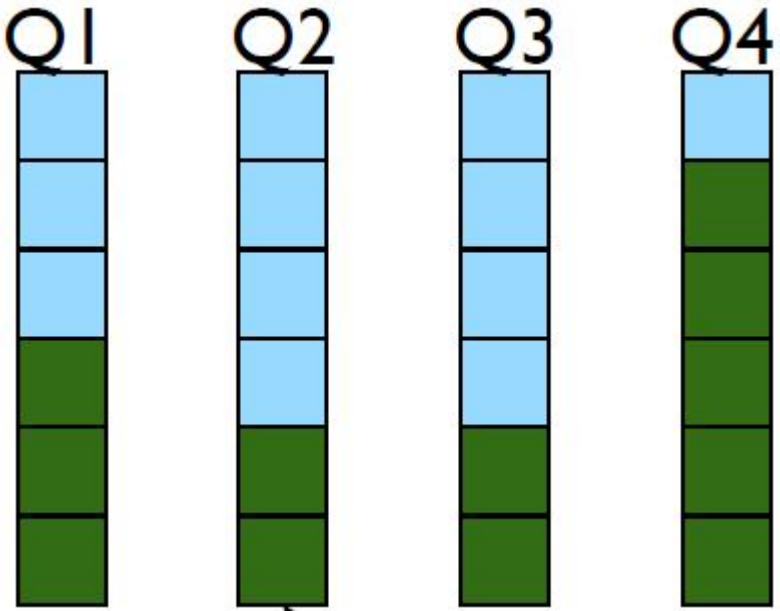
Counting Attack

- Correlate incoming and outgoing flows by counting the number of packets



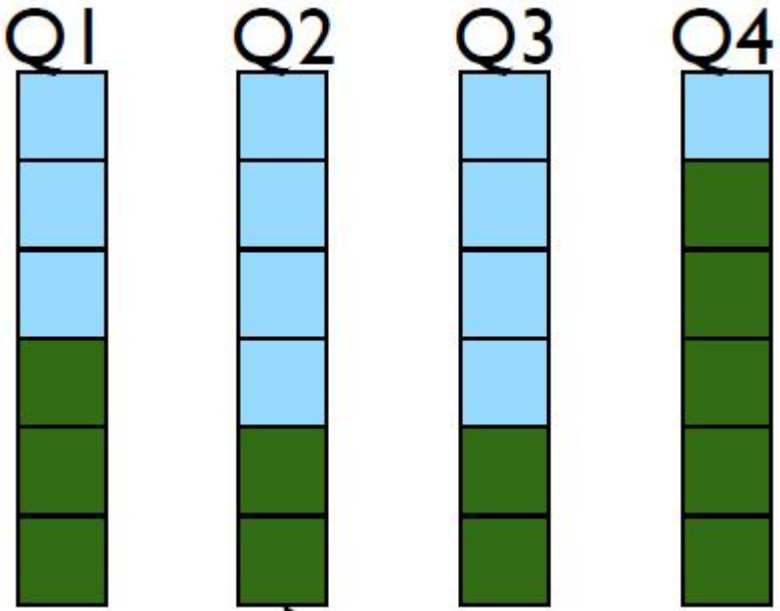
Low Latency Attack

- Tor router assigns each anonymous circuit its own queue
- Dequeue one packet from each queue in round-robin fashion



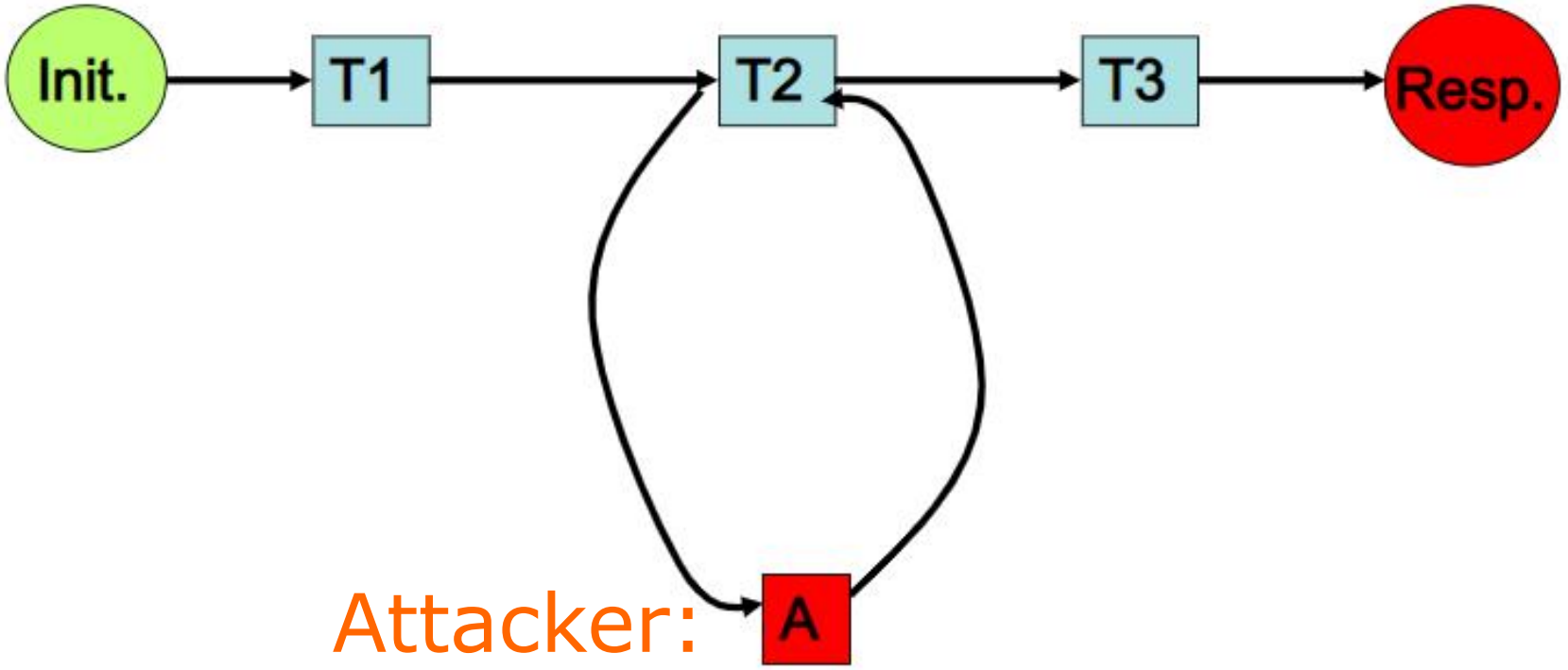
Low Latency Attack

- Tor router assigns each anonymous circuit its own queue
- Dequeue one packet from each queue in round-robin fashion



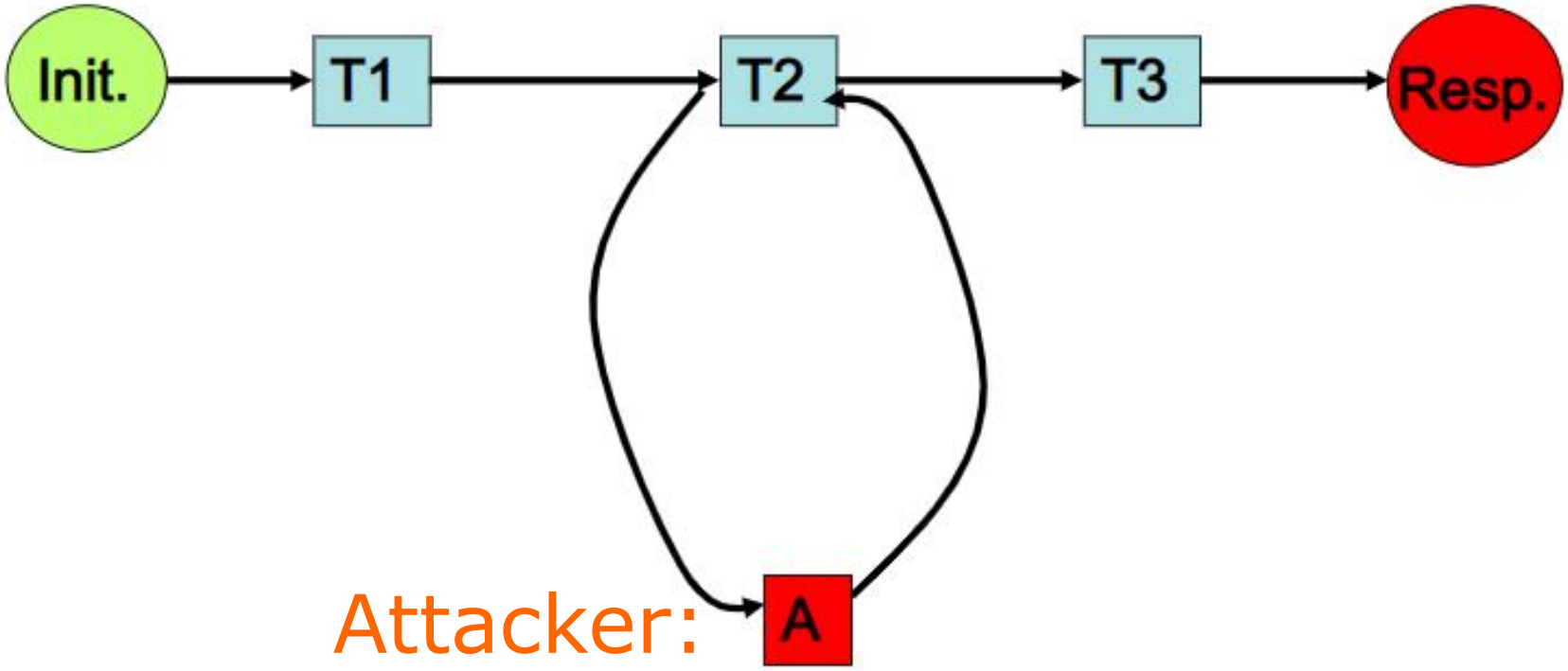
new queue affects latencies of all other queues;

Low Latency Attack



Attacker:
intends to infer Init's activity

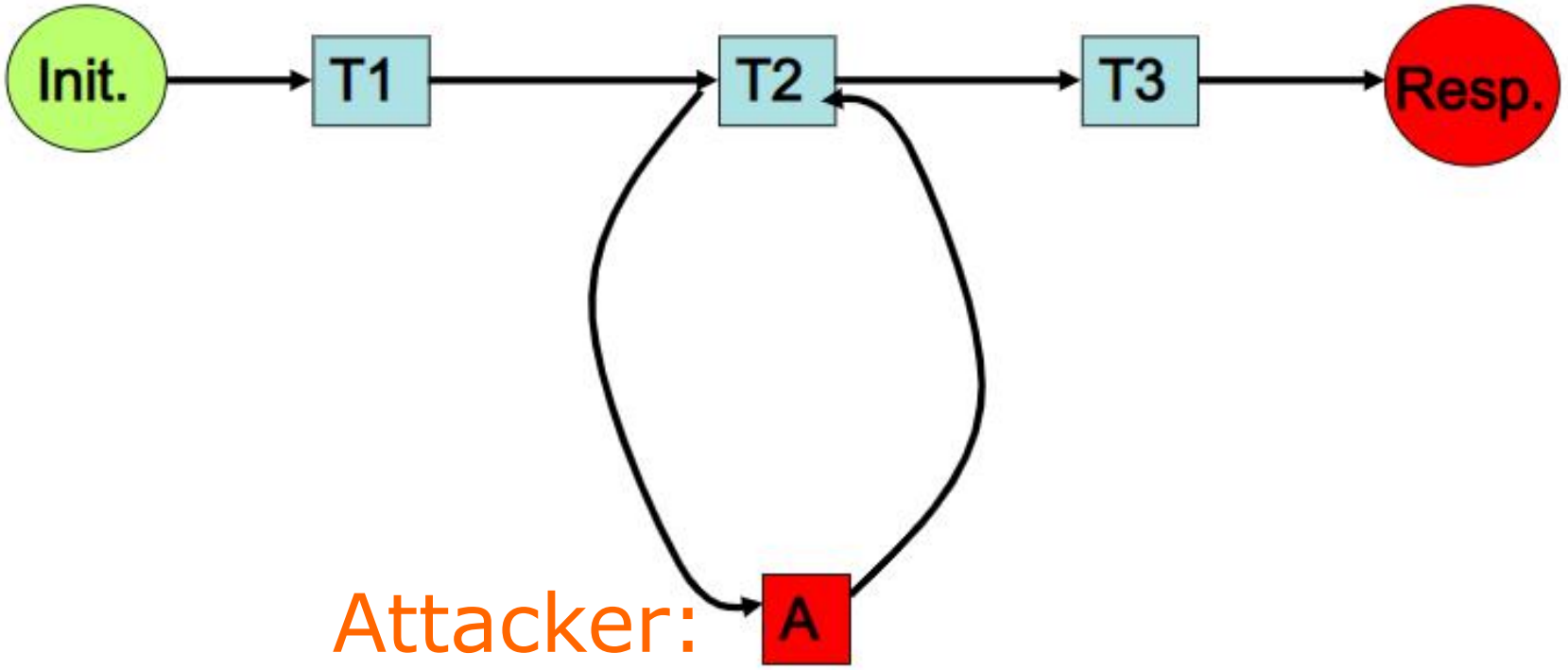
Low Latency Attack



Attacker:
intends to infer Init's activity

Assumption:
only Init and A occupy T2

Low Latency Attack



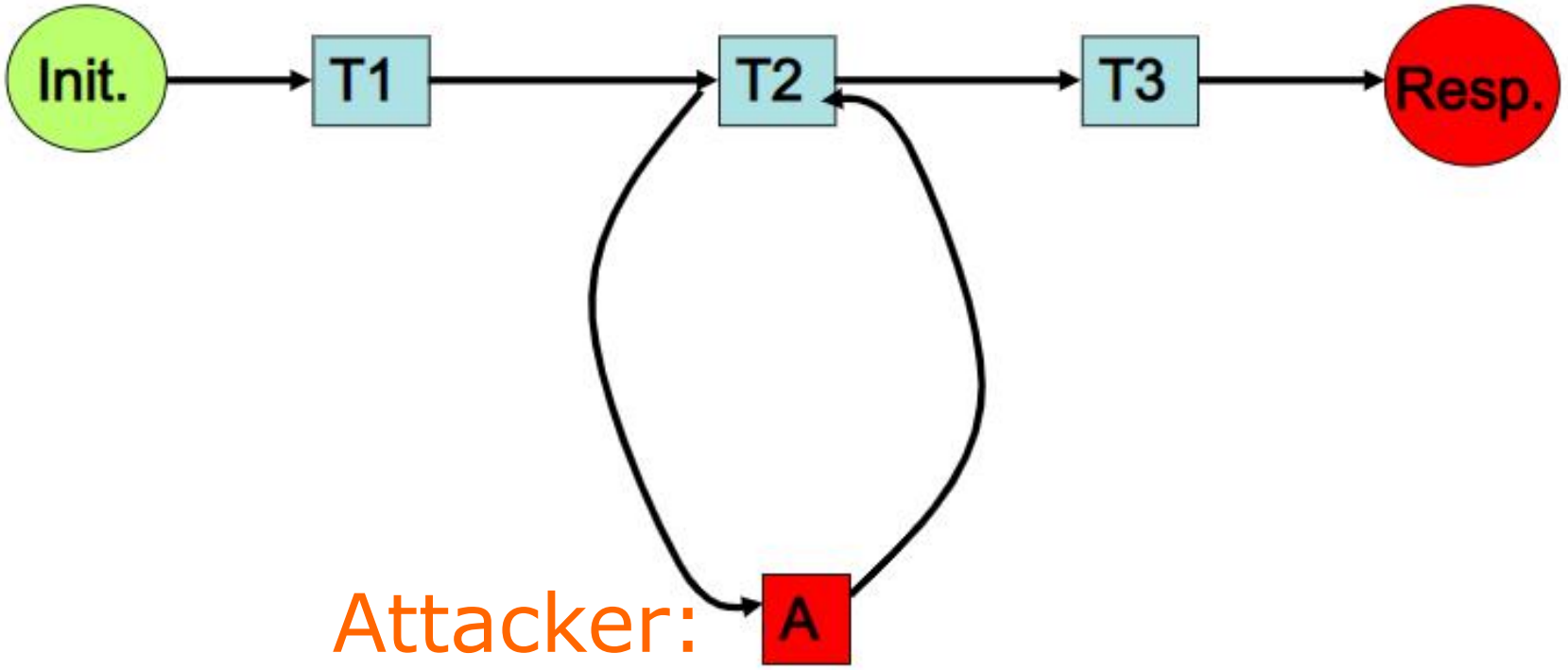
Attacker:

loop:

send packets to T2;
measure latency;

Low Latency Attack

larger latency indicate Init's traffic!



Attacker:

loop:

send packets to T2;

measure latency;

Cross Site Attack

Crawling:

- Deploy Tor routers
- Access darknet
- Crawl transaction information
- Extract Bitcoin accounts of interest

Correlation:

- Search the accounts on public websites

Readings

- Anonymous Communication
  by Nick Mathewson
- Tor: The Second-Generation Onion Router (2012 DRAFT)
  by Dingledine *et al.*

Disclaimer:

The content aims only for helping students understand principles of anonymous communication. It should not be used for abusive Internet activities.

Thank You