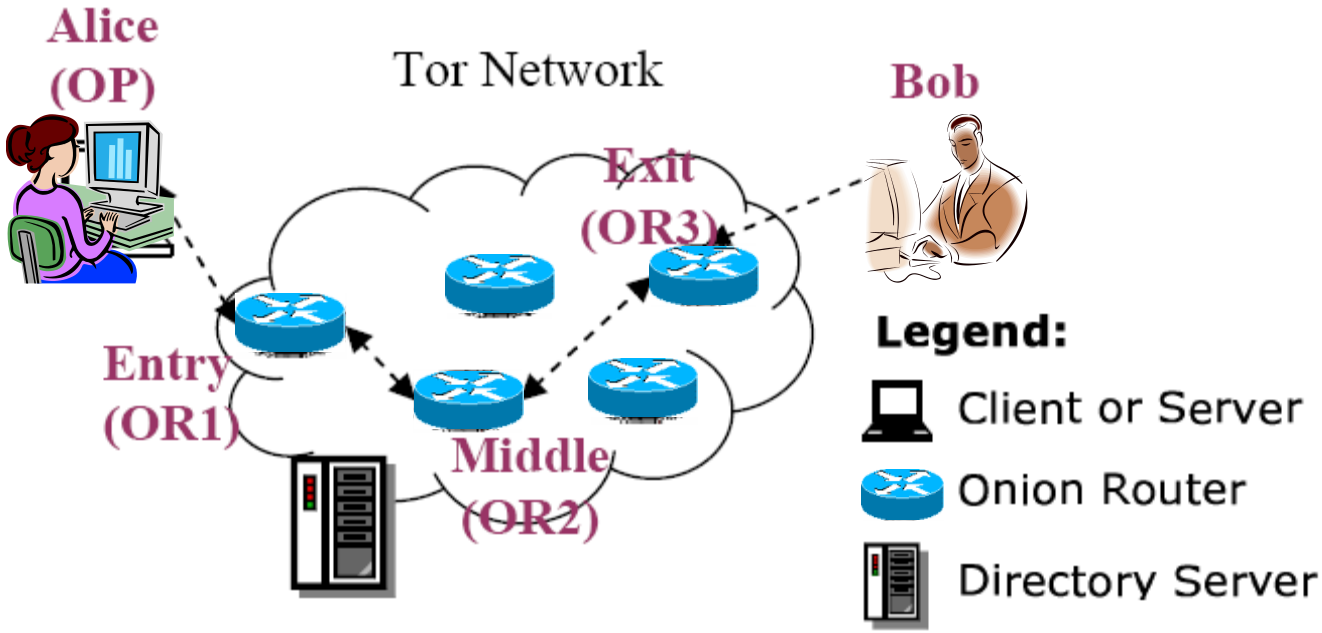
Example of Traffic Analysis Attacks

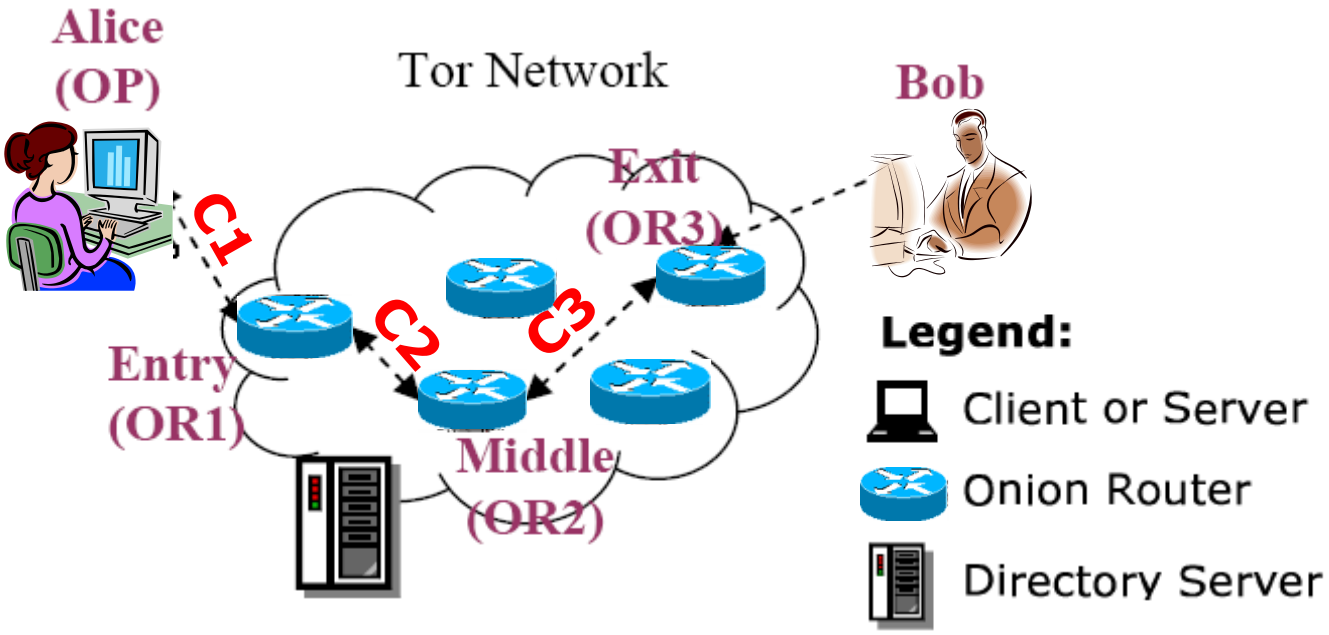
Components of Tor



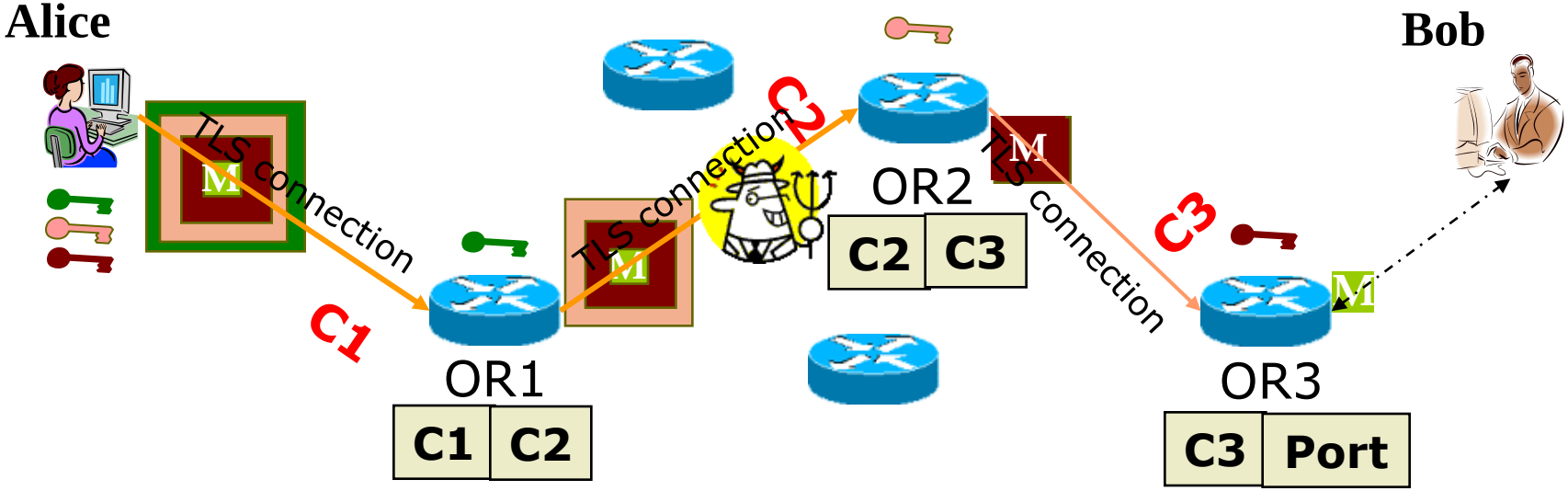
- **Client**: the user of the Tor network
- **Server**: the target TCP applications such as web servers
- **Tor (onion) router**: the special proxy relays the application data
- **Directory server**: servers holding Tor router information

How Tor Works? --- Circuits

- Alice herself chooses the relay routers and creates circuits through the relay routers
  - Source routing
  - Circuit: communication tunnel from Alice to Bob
  - These circuits are dedicated for Alice

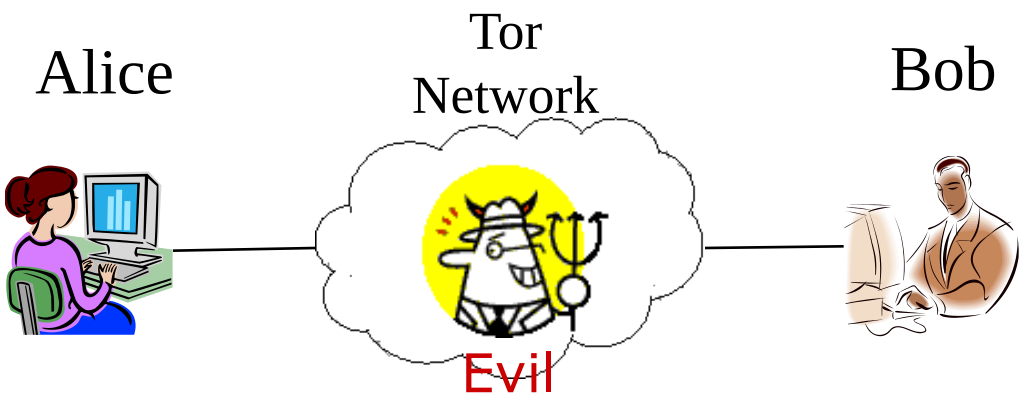


How Tor Works? --- Onion Routing



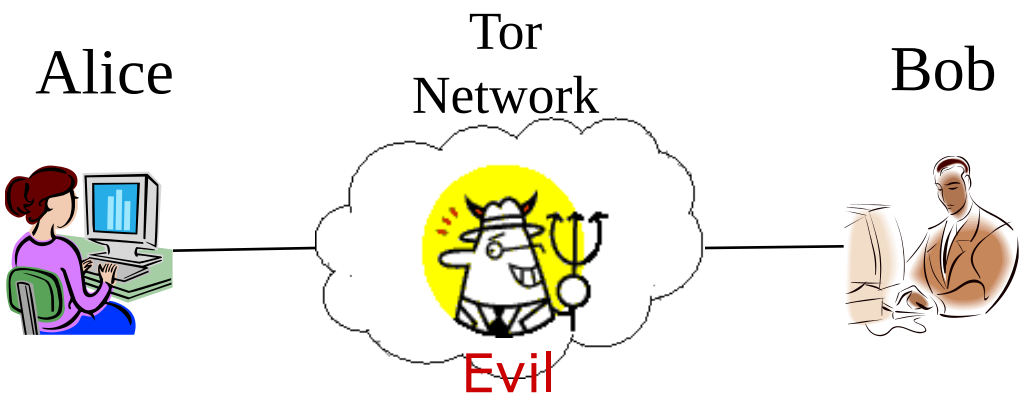
- A circuit is built incrementally one hop by one hop
- Onion-like encryption
  - Alice negotiates an AES key with each router
  - Messages are divided into equal sized cells
  - Each router knows only its predecessor and successor
  - Only the Exit router (OR3) can see the message, however it does not know where the message is from

Traffic Analysis Attack against Tor



- Alice is sending messages to Bob through an encrypted and anonymous circuit, how can Evil confirm the communication relationship between Alice and Bob?

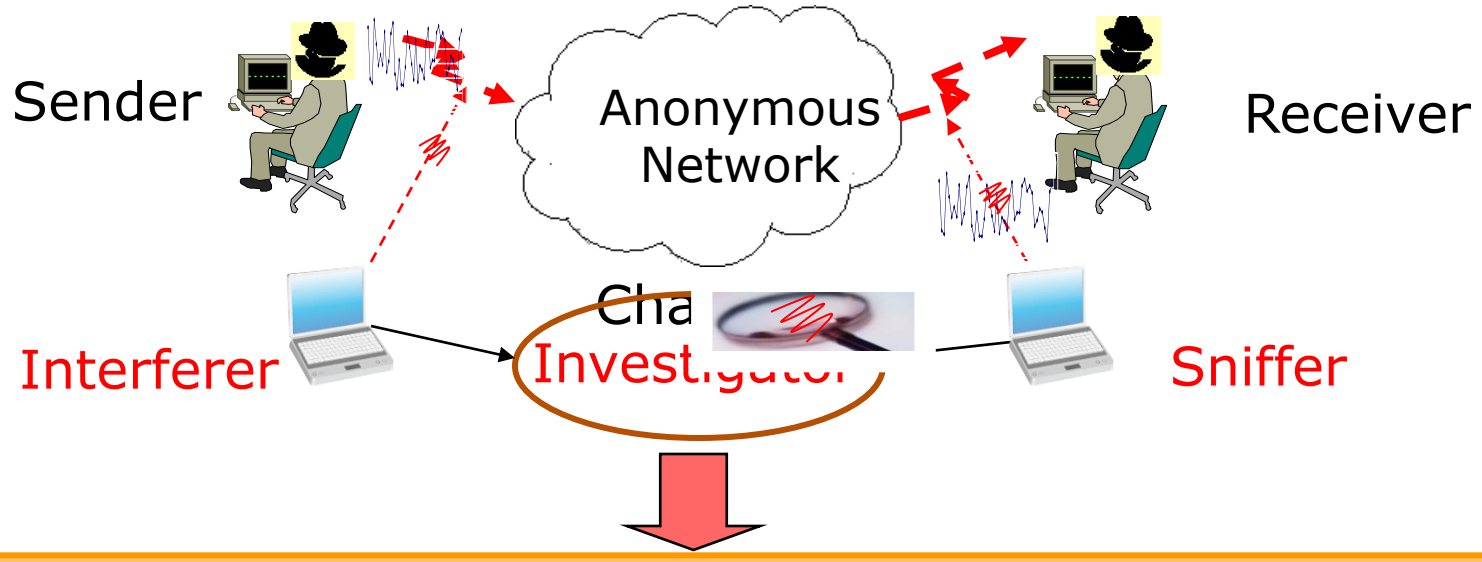
Traffic Analysis Attack?



- Idea?????
  - Passive based
  - Active based

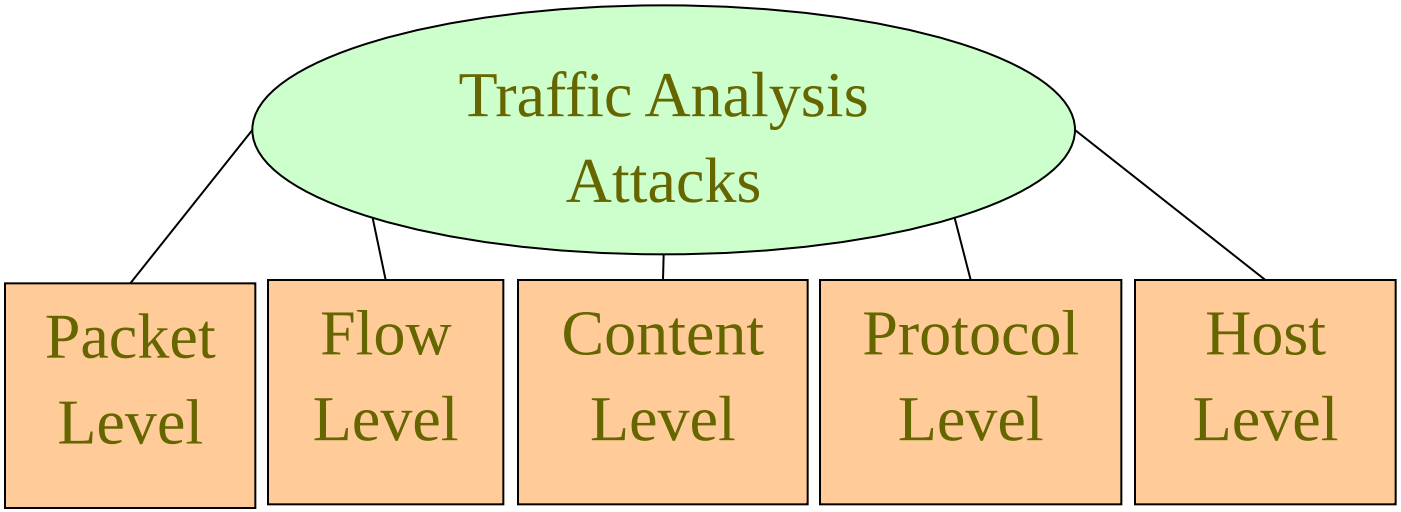
Active Traffic Marking

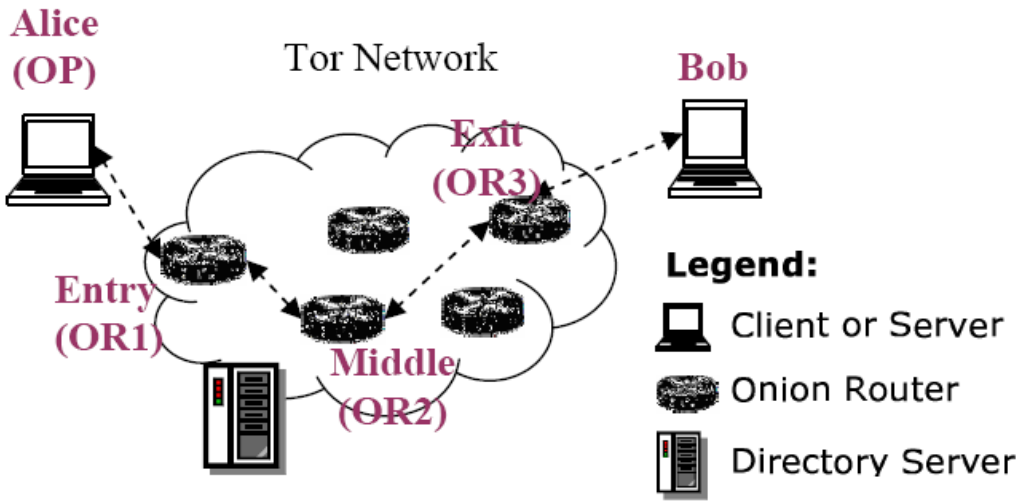
- Change traffic flow rates, packet timing, packet size
- Traffic rate changes represent a "mark", i.e. a special secret code



Investigator knows that Sender communicates with Receiver!

Problem Space of Active Traffic Analysis





Traffic Camouflage in Networking Security

Camouflage – A General Principle

- Camouflage
  - Conduct covert acts or operations
- Broad Applications

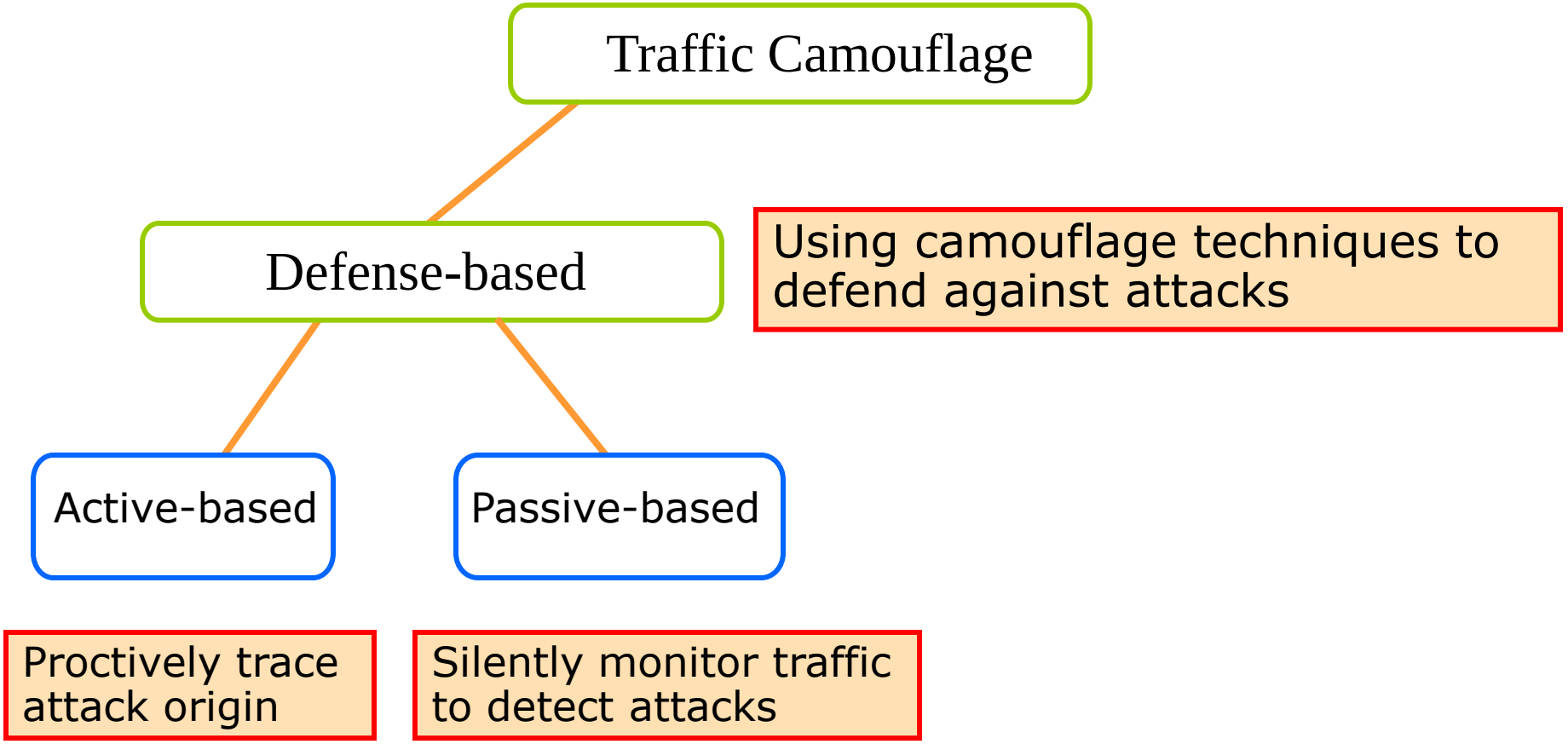
Tiger exhibits mimicry to remain indiscernible from the surrounding

Army cadets put on camouflage clothing and face paint

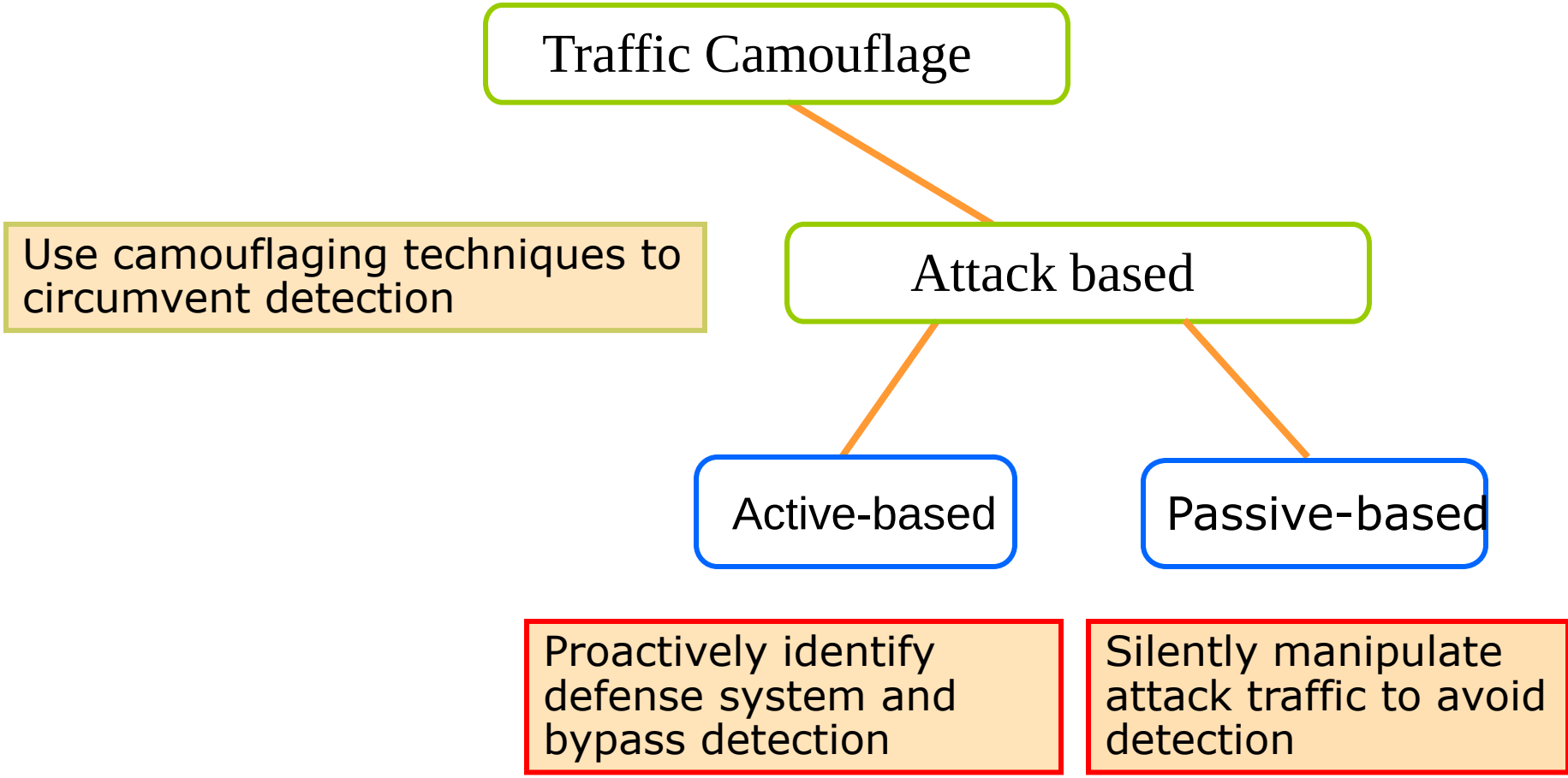
Motivation

- In cyberspace networking systems, a large number of attacks and defenses exist
  - Attacks: worms, critical infrastructure identification, denial-of-service
  - Defenses: detection of attacks, traceback of malicious origins
- Existing attacks and defenses have limitations
  - A worm can propagate fast, but can easily be detected
  - A defender traces attackers, but alarms them
- Sophisticated attacks and intelligent defenses are more effective
  - In hiding the propagation, a worm can ultimately infect more computers
  - In hiding itself, a defender can secretly identify attackers

Classification of Traffic Camouflage



Classification of Traffic Camouflage (cont.)



Classification of Traffic Camouflage (cont.)