Distinguishing DDoS and Flash Crowd Traffic by Using Packet's Geolocation

Phetchai Ponpat <phetchai.ponpat.ph2@is.naist.jp>

iplab Laboratory for Cyber Resilience

Nara Institute of Science and Technology NAIST

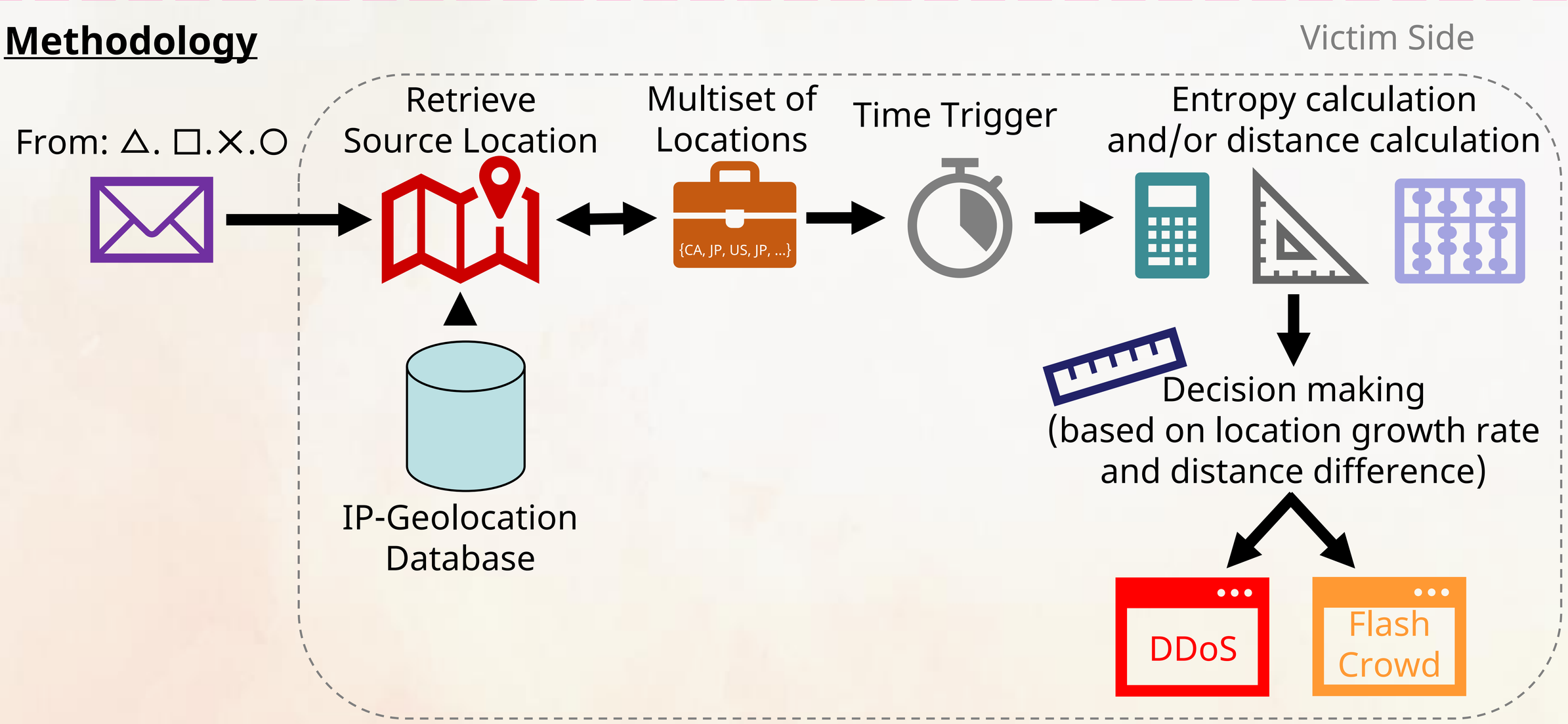
What is DDoS Attack?

- A kind of attack through a network with an intent to block the legitimate traffics to access a network or an end device by flooding a huge amount of traffic to the target entity.
- Example: Mirai Botnet
- Intention: To block the legitimate traffics to access. The response information does NOT matter
- Packet characteristics:
  - Forge source IP address to ensure that the packet does not get blocked.
  - May or may not contain payloads
- When retrieving the geolocation from source IP address there is no any specific pattern.

What is Flash Crowd Incident?

- There is a outside factor that cause many legitimate users to access a target network or end device in a short time. This will cause a huge surge in the traffic at target. It might also lead to target inaccessible.
- Example: The public goes to the news website to get latest information about COVID-19
- Intention: To access to the specific highly-demanded contents. The response information does matter
- Packet characteristics:
  - Legitimate source IP address to ensure reply packets arrival
  - Usually with payloads
- When retrieving the geolocation from source IP address some definable pattern can be found.

Methodology



Contribution

- To proof that the geolocation information is one of the characteristics can be used for differentiate DDoS and flash crowd traffic
- Implement the proposed method and define the related calculations
- Propose possible DDoS and flash crowd incident based on geolocation factors
- Complete an exhaustive analysis and testing on the proposed method