Amplification Attacks

draft-mattsson-t2trg-amplification-attacks

T2TRG, John Preuß Mattsson

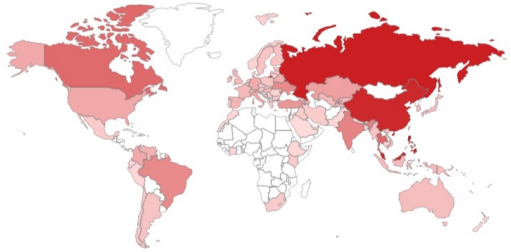
Critical Infrastructure Under Attack

- DDoS attacks is a huge, costly, and growing problem for services and critical infrastructure (including IoT deployments).
  - DDoS attacks can be done with small amounts of cleverly chosen traffic, e.g., the TCP SYN flood attack.
  - Most DDoS attacks are done with large amounts of not so cleverly chosen data using compromised devices, or amplification attacks using a spoofed source address.
  - In an amplification attack, the amplification factor is the ratio between the total size of the data sent to the target and the total size of the data sent by the attacker.
- draft-mattsson-t2trg-amplification-attacks and this presentation talks about amplification attacks exemplified with CoAP.
  - When transported over UDP, the CoAP NoSec mode is susceptible to source IP address spoofing.
  - Powerful CoAP amplification attacks made headlines in 2018, the biggest reaching 320 Gbps. But in 2019, they were hardly seen anymore.
  - The open CoAP servers are mostly concentrated to a few countries and a few implementations (numbers are shrinking, was 546,795 in July 2021).

TOTAL RESULTS

379,385

TOP COUNTRIES

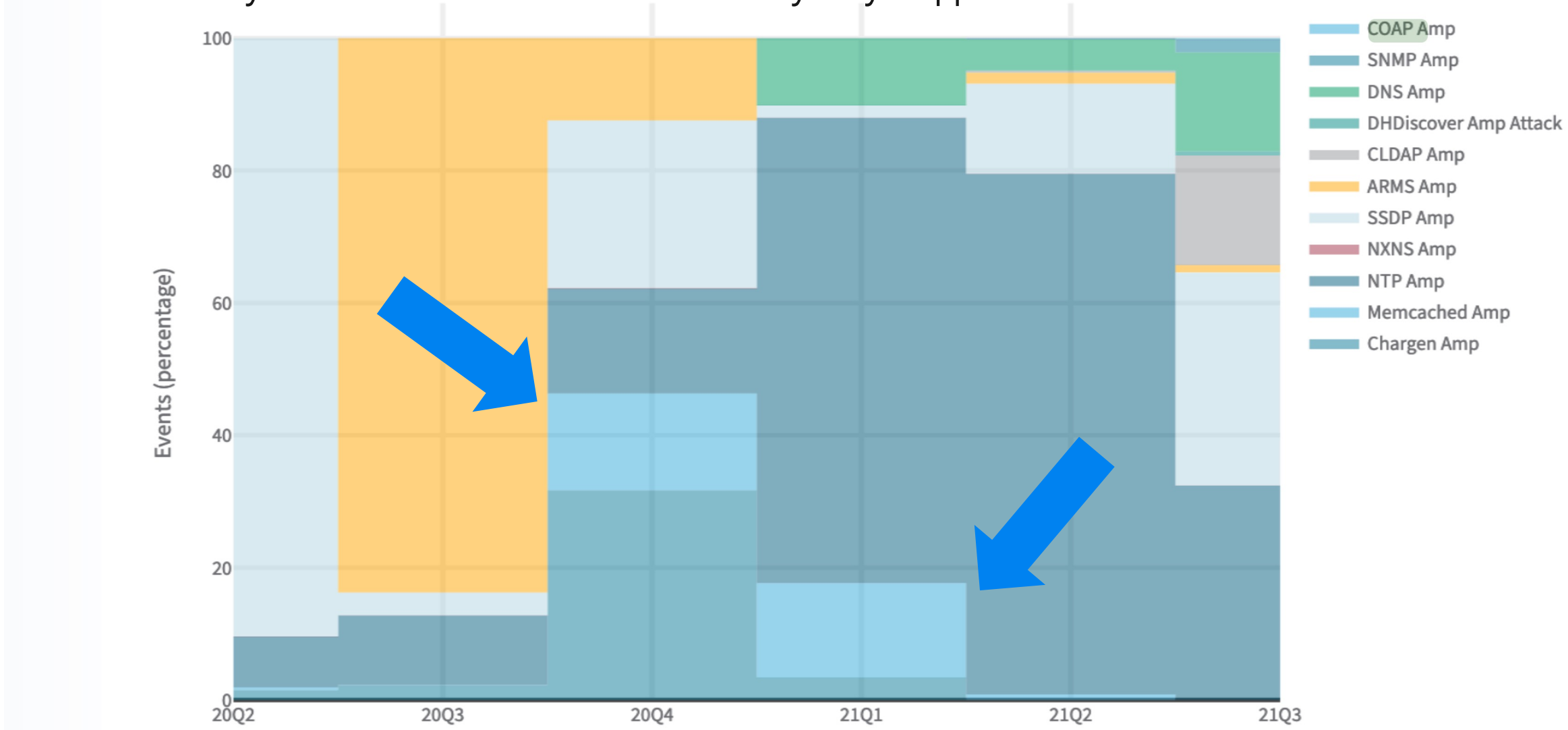


Philippines	121,489
Russian Federation	83,484
Malaysia	73,949
China	66,629
Thailand	10,142

More...

CoAP Amplification Attacks (Radware report)

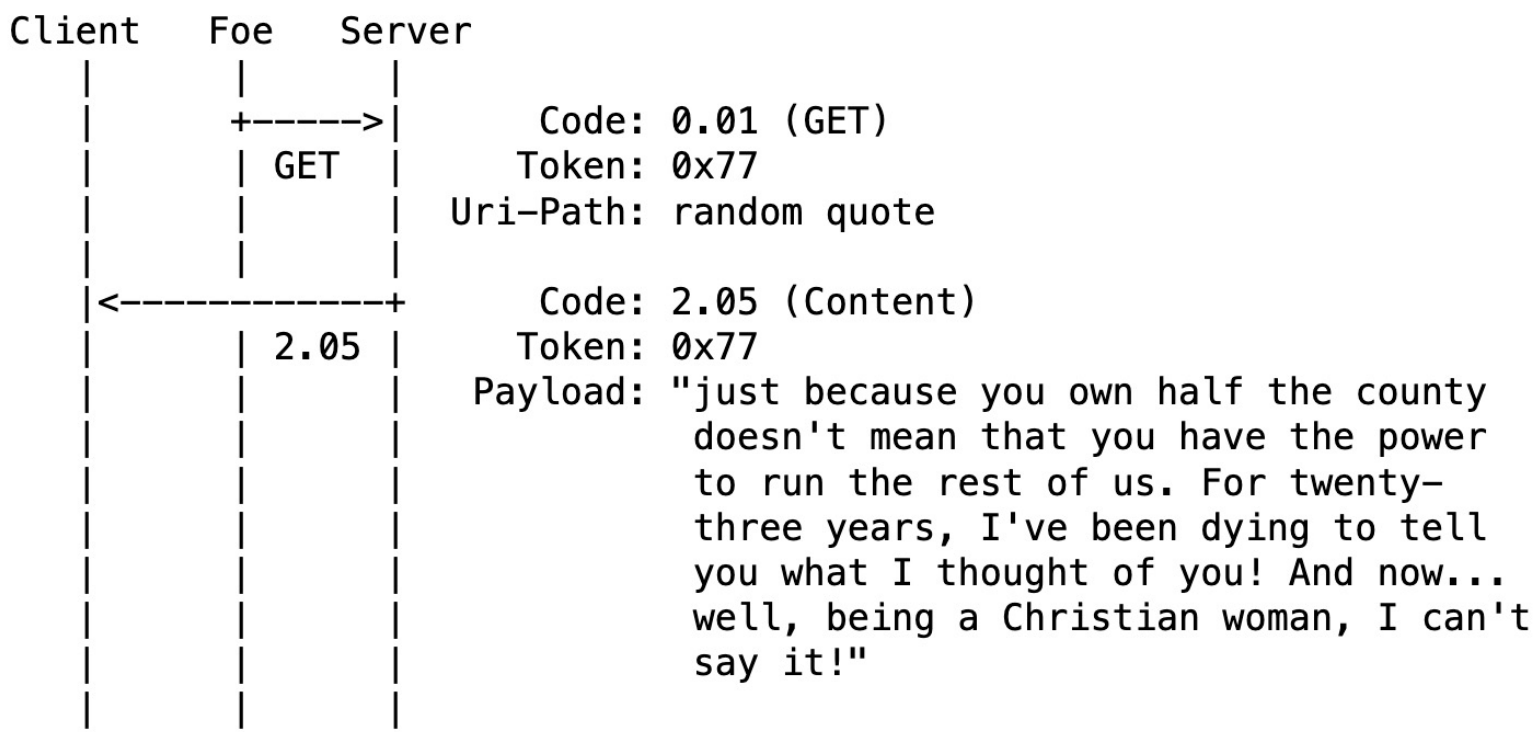
— CoAP amplification attacks seems to have made a major comeback in Q4 2020 and Q1 2021*
Unclear exactly how the attacks were done and why they stopped.



Amplification attack using a single response

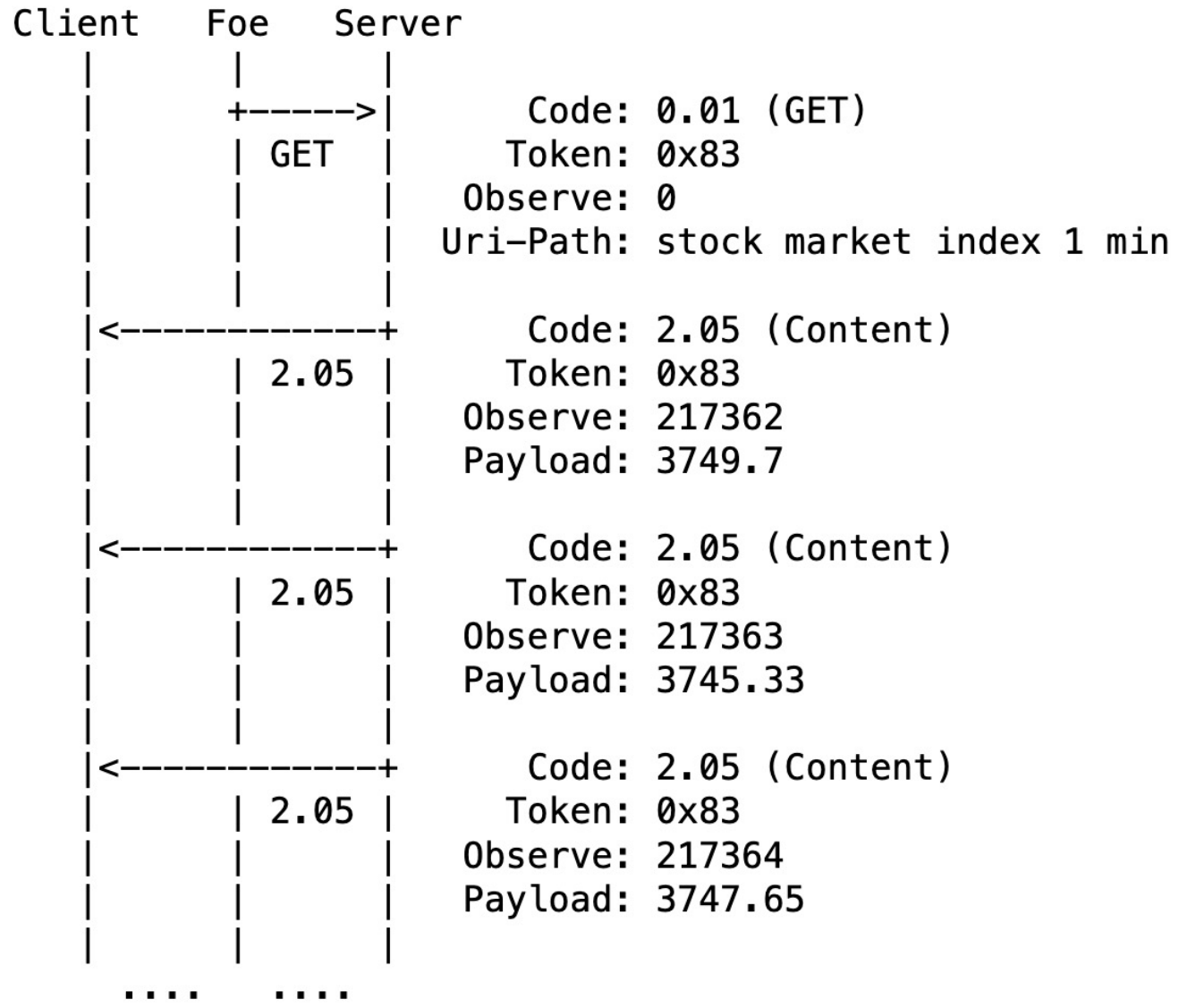
— If the response is a times larger than the request, the **amplification factor is a.**

— Amplification factors can be significantly worse when combined with observe [RFC7641] and multicast [I-D.ietf-core-groupcomm-bis].



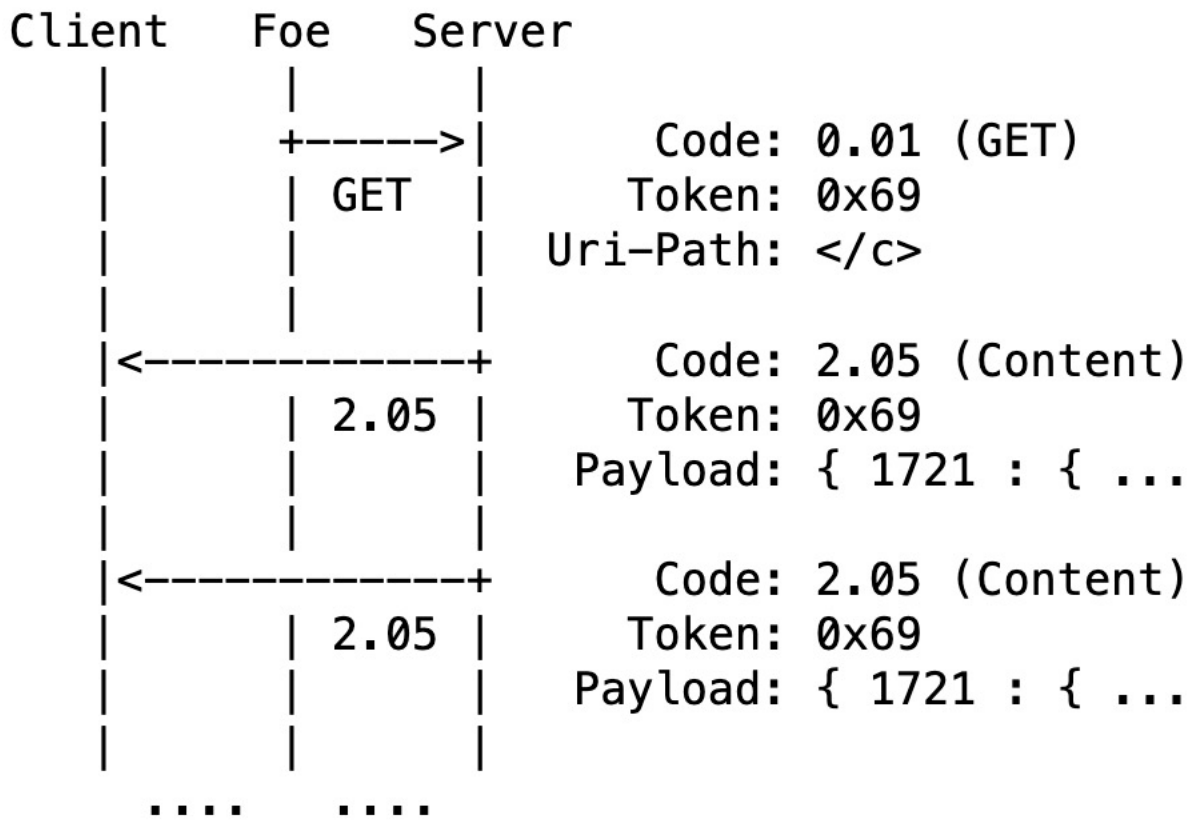
Amplification attack using observe

— If each response have an amplification factor of a, and the server sends n responses, the total **amplification factor is an.**



Amplification attack using multicast

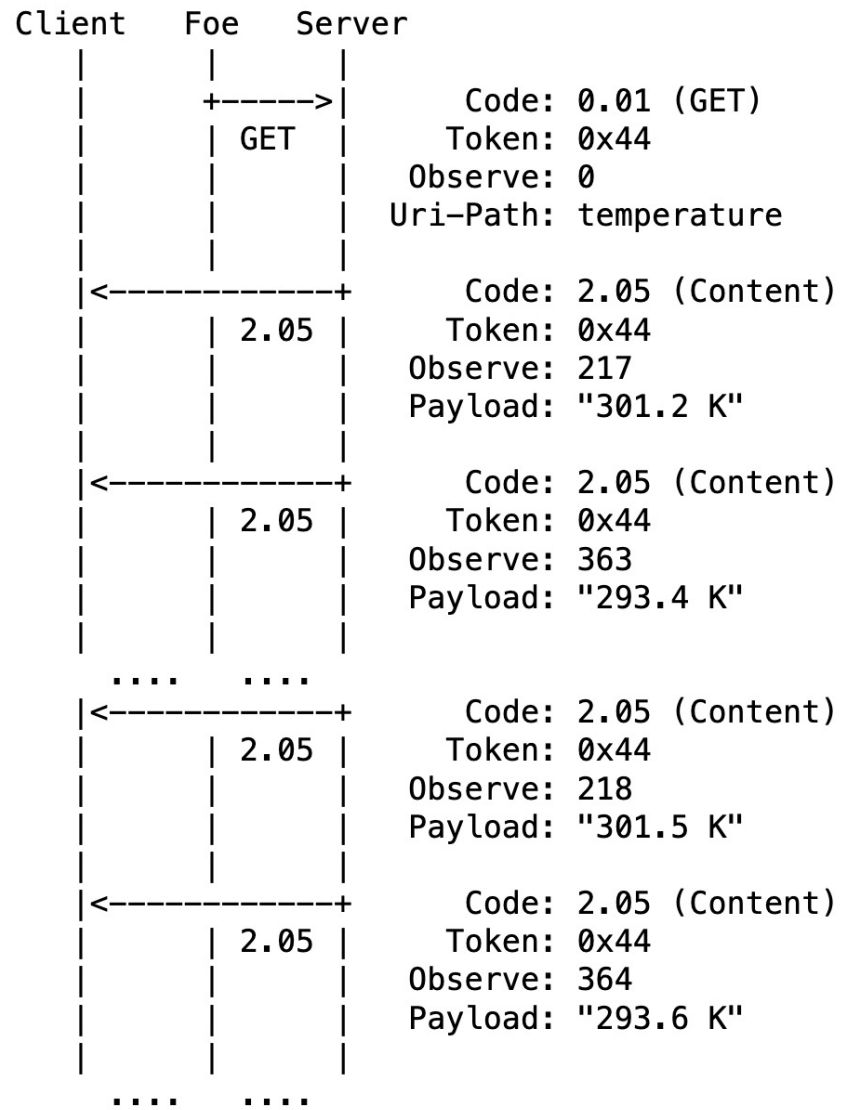
- If each response have an amplification factor of a, and there there are m servers, the total **amplification factor is am.**
- Note that the servers usually do not know the variable m.
- Cannot be used from the Internet but an attacker on a local network (e.g., a compromised node) can use local CoAP servers to attack targets on the Internet or on the local network.



Amplification attack using multicast and observe

— If each response have an amplification factor of a, and there there are m servers, and each server sends n responses, the total **amplification factor is amn.**

— Note that the servers usually do not know the variable m.



DoS - Perfect activity for T2TRG SecCORE

— DDoS is a major problem. Networks and services are targeted by Distributed Denial-of-Service attacks. Mitigations are costly. We don't want IoT to be used for DDoS and we also don't want actuators and sensors to be vulnerable to denial-of-service attacks. Unacceptable that services and critical infrastructure (including IoT deployments) need to take large costs because of too much cost saving in devices.

— QUIC [RFC9000] mandates "*an endpoint MUST limit the amount of data it sends to the unvalidated address to three times the amount of data received from that address"* without exceptions. This approach should be seen as current best practice for non-constrained devices.

— IETF/IRTF should make sure to not make it worse. If IETF is not taking care of its DDoS hygiene, likely nobody else will. If the industries do not act themselves, regulators are likely to step in and in that case, we want them to have IETF/IRTF documents to read.

— DoS is a perfect activity for T2TRG as part of SECCORE. Need to raise awareness, increase understanding, and hopefully suggest mitigations suitable for constrained devices and networks. Could look at Denial-of-Service for constrained devices and networks in general.