Amplifying IoT honeypots with dynamic traffic replay

**Motivation:**
- Intensified attacks on IoT devices
  - BrickerBot, IoTReaper
- Plenty of vulnerable IoT devices deployed
- Honeypots can detect such large-scale attacks

**Limitations of honeypots:**
- Contain a few devices
  - limited vulnerability discovery
- Attack traffic targeted to single device
  - Device may not be vulnerable

**Our goals:**
- Greater attacker engagement even with untargeted IoT devices - Traffic amplification
- Discover vulnerabilities in large number of IoT devices - Traffic replay

**Traffic amplification in honeypot:**
- Proxy to handle real-time traffic
- Classify malicious incoming traffic
- Cache – impede repetitive attacks
- Oracle – Identify vulnerabilities

**Vulnerable devices discovery:**
- Replay honeypot traffic in IoT network
- Identify vulnerable devices from responses
- Discover new vulnerable IoT devices (not in honeypot)