Mitigating IoT Device Based DDoS Attacks Using Blockchain

Uzair Javaid, Ang Kiang Siang, Muhammad Naveed Aman, Biplab Sikdar

by **Uzair Javaid**
National University of Singapore, Singapore
Cryblock, **MobiSys** '18, Munich, Germany
Dated: **June 15, 2018**

Outline

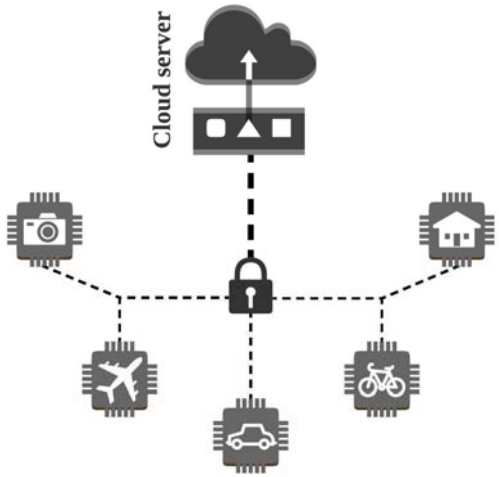
- **Introduction**
  - Internet of Things **IoT**
  - Denial of Service **DoS**/Distributed **DoS** Attacks
  - Blockchain
- **Mitigation of DoS/DDoS Attacks**
  - Common Approach
  - The **IoT-Ethereum** Model
- **Evaluation**
  - Central v/s Decentralized
  - Trusted Devices List
  - Defense against DDoS Attacks
- **Conclusion**

Introduction

- Internet of Things **IoT**

  ✓Devices interacting with each other through Internet

  ✓Resource constrained and easy to attack due to cheap security architecture



continued…

- Denial of Service **DoS**/Distributed **DoS** Attacks
  - ✓Device uploading extremely large quantity of data to crash server(s) **DoS**
  - ✓Devices uploading extremely large quantity of data to crash server(s) **DDoS**
  - ✓Enabled primarily through IoT devices because of weak security protocols

continued…

- Blockchain
  - ✓A digital ledger with chronological blocks
  - ✓Decentralized architecture
  - ✓Common consensus agreements
  - ✓Smart contracts

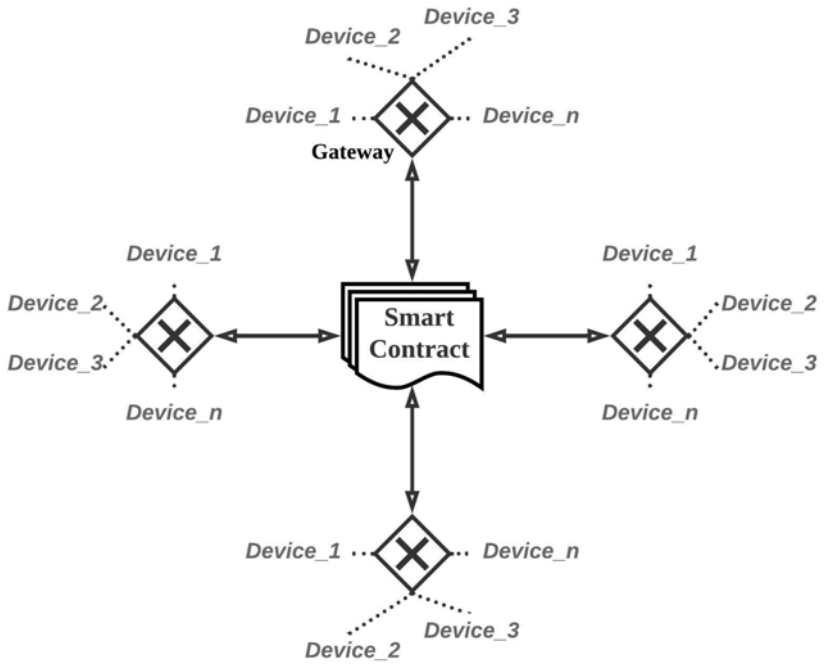
Mitigation of DoS/DDoS Attacks

- Common approach
  - ✓No trusted list of IoT devices
  - ✓Bandwidth limit of each device is usually not limited
  - ✓Reactive measures rather than proactive

continued…

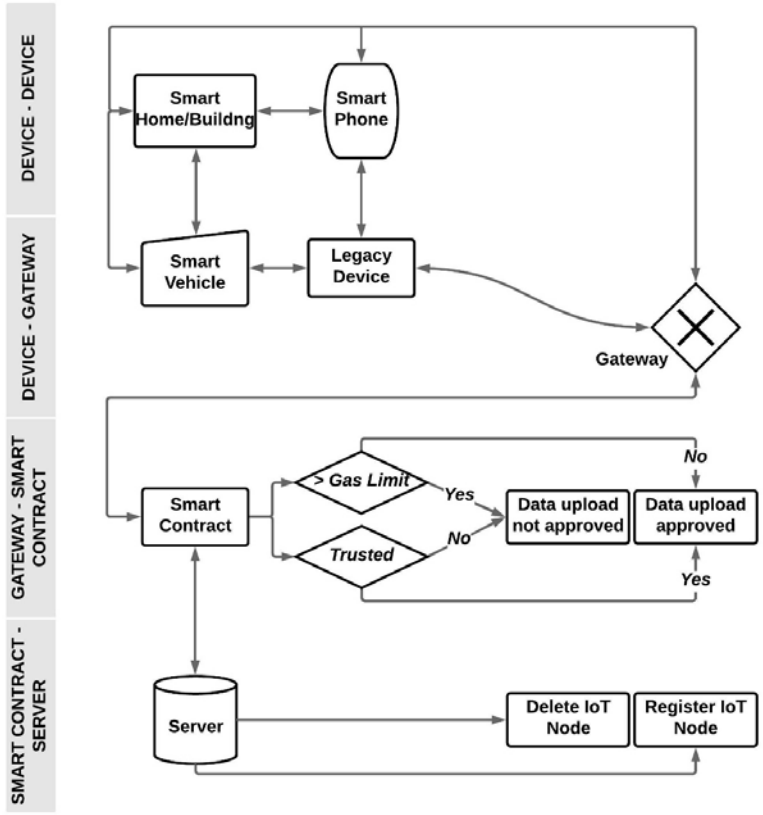
- **IoT-Ethereum** Model
  - ✓Trusted list of IoT devices
  - ✓Bandwidth constrained (static)
  - ✓Proactive protocol rather than reactive

continued…



- **IoT-Ethereum** architecture

continued…



- System Operation

Evaluation

- Centralized v/s Decentralized

  - ✓Single point of failure
  - ✓Distributed control (consensus)
  - ✓Shared resources

continued…

- Trusted Devices List
  - ✓Registering a device first before it can upload data
  - ✓Blocking rogue devices from interacting with the system

continued…

- Defense against DDoS Attacks
  - ✓Authenticating devices when uploading data
  - ✓Keep devices within good bandwidth limit

Algorithm 1: Smart contract algorithm for validation

```
1  function access(device_i)
   Input  : message(device_i)
   Output : trusted, untrusted
2  if (message(device_i) exists and message(device_i) is valid) then
       // Check device_i is trusted/untrusted
3      if (device_i is registered in the trusted list) then
           // Check device_i has good gas limit
4          if (device_i.gas.used ≤ gas.limit) then
5              return trusted
6          else
7              return untrusted
8          end
9      else
10         return untrusted
11     end
12 else
13     return untrusted
14 end
15 end function
```

Conclusion

- IoT and Blockchain Platform
  - ✓Decentralized
  - ✓Trust-free system operation
  - ✓Defense against DDoS attacks and blocking rogue deivces

Discussion

- ✓Scalability issues
- ✓Advance performance evaluation and security analyses
- ✓Protection for IoT devices from inter-DDoS attacks
- ✓Dynamic resource allocation
- ✓Geo-tagging IoT devices

Q u e s t i o n s ***?***