Blockchain-Based Multi-UAV Surveillance System

Mario Santos de Campos, Caroline Chanel, Corentin Chauffaut, Jérôme Lacan

Groupe BLEND : BLockchains for aEronautical aND Space systems
https://websites.isae-supaero.fr/blockchain/blockchains-at-isae-supaero

Séminaire STORE – 01/12/2021
Context and objective

- Starting point: Bitcoin is one of the most resilient system in the world
- Objective: show that this resiliency can be applied in other contexts: network of autonomous drones
- Application to a scenario of a surveillance system based of a fleet of drones

<table>
<thead>
<tr>
<th>1 - Hardware/Infrastructure</th>
<th>Hardware, Operating System and Internet infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 - P2P</td>
<td>Management of the P2P overlay network</td>
</tr>
<tr>
<td>3 - Consensus</td>
<td>Modification and validation of the blockchain</td>
</tr>
<tr>
<td>4 - Smart Contracts / Applications</td>
<td>Distributed applications deployed over the blockchain</td>
</tr>
</tbody>
</table>
Blockchain

- Shared
- Distributed
- Immutable

Common Ledger

Block Chain

Consensus Mechanism

Transaction

Internal Data

Ledger

Public

Private

Consortium
Smart Contract

Irreversible Program

Smart Contract

Block Chain
Deterministic

Smart Contract

Block Chain

Transaction
Internal Data
Ledger
Multi-UAVs Context

- Surveillance (Portugal and Rocha, 2016, 2013)
- Inspection Mission (Liu and Kroll, 2012)
- Search and Rescue (Murphy et al., 2008; Ubaldino de Souza, 2017)
- Exploration (Benavides et al., 2019)

more...
Surveillance Problem

- **Autonomous UAV**: The UAV must operate autonomously and independently.
- **Independent POIs**: Points-of-interest are the targets to be visited by the UAVs.
- **Unpredictability & Efficiency**: Drone movements must not be predictable. The time between POI visits should be minimized.
Blockchain Integration

Synchronize Data Between Nodes
(Doriya et al., 2015; Benavides et al., 2019)

Resistance to Single-Point Failure
(Benavides et al., 2019; de Souza et al., 2016)

Transparency

Anonymity
Decision-Making Algorithm

**Classic Optimization**
- Too complex to be implemented on a Smart Contract
- Resource intensive
- Consists in minimizing an utility function
  Takes as input POI locations, UAVs locations and idleness of each POI

**Game Theory**
- High efficiency
- Low complexity
- Easy to implement on a Smart Contract
POV & POL

**Smart POIs**
It must be an electronic device

**Simple Locations**
The POI can be a tree in a forest

**Proof-of-Visit**
**Proof-of-Location**

**POI Signature**
Both the POI and the UAV sign the transaction

**POL blockchain service**
- FOAM (Foamspace Corp., 2018)
- XYO (Trouw et al., 2018)
- Platin (Wolberger et al., 2018)
Smart Contracts

- Defines the POIs and UAVs participating in the system
- Collects the subscriptions (tokens) of the POIs to the system in an escrow account
- After a UAV stores a POV, it defines the next POI to visit by computing the one minimizing the utility function
- After a POV, it rewards the UAV and the system administrator

User Manager

Subscription

Decision

Reward
Smart Contracts

POI 1

POI 2

POI 3

POI 4

POI 5
Smart Contracts

POI 1

POI 2

POI 3

POI 4

POI 5

which POI next?
Smart Contracts

POI 1

POI 2

POI 3

DECISION smart contract

go to POI 4

POI 4

POI 5
Smart Contracts

POI 1

POI 2

POI 3

sending POV

POI 4

POI 5
Decision algorithm

- The choice of the next POI is done by minimizing a utility function based on:
  - the **path cost** (e.g. distance) for the UAV to move from its current position to a given POI;
  - the **weighted sum of all other UAVs inverted distance**.
  - the **negative of the expected reward** to reach a POI (idleness of the POI).

- It was shown that minimizing each utility function individually is the best choice for the group.
Embedded UAV System

Communication handled by the Blockchain

Each UAV runs a blockchain node
Blockchain Choice

- dApp
  - Bitcoin
  - Ethereum
  - IOTA
Choices

- Blockchain Ethereum: client Besu
- Smart contracts: written in solidity
  - SUBSCRIPTION: collects the subscriptions (in tokens) of the POIs to the system in an escrow account;
  - DECISION: defines the next POI – based on game theory
  - REWARD: rewards the UAVs

- First evaluation on simulation
- Implementation and demonstration
Simulations

- Management in python
- Besu clients and smart contracts written in Solidity
- Objectives: Validate the algorithms and tune the parameters
Simulations (2)

Individual drone heatmaps

Failing condition path illustration
Platform

[Image of a heatmap and an indoor setting with drones flying]

[Image showing a wall with colored markers and a drone flying nearby]
Conclusions and future work

- Definition of a surveillance system based on autonomous drones embedding a blockchain - Managed by smart contracts
- Validated by simulations and implementations on real drones
- Publications:
  - A Mission-Level Resilient Blockchain-based Robotic System, to be (re-) submitted
- Future work:
  - Extensions to other drone missions: package delivery, ...
  - Extensions to small satellite swarms
  - 2 PhD starting october 2021 on IA and cryptography for embedded blockchains
Questions ?