A Blockchain For The Collision Avoidance And The Recovery of Crashed UAVs

Michele Scarlato, Cristian Perra, *Mohamed Yaseen Jabarulla, *Giljun Jung, *Heung No Lee,
e-mail : michele.scarlato@diee.unica.it, cperra@ieee.org, yaseen@gist.ac.kr, jinpeg112@gist.ac.kr, heungno@gist.ac.kr,

Department of Electrical and Electronics Engineering Cagliari Univeristy,
****Gwangju Institute of Science and Technology.***

Abstract

The Unmanned Aerial Vehicles (UAVs) are a specific type of drones that have a large use nowadays, but which is subject to strict rules country specific. The sensors that equip the UAVs permit to perform several tasks, ranging from geolocalization to identification of objects or measurement of temperature. In several specific cases the UAVs are employed for the patrol of zones difficult or dangerous to reach, or simply far from where a human being is able to rescue a crashed one in case of an accident. It must be pointed out the possibility of crashes, due to several causes. In our work we are proposing the design of a blockchain for the collision avoidance and the recovery of crashed UAVs.

I. Introduction

The Unmanned Aerial Vehicles (UAV) can be employed for many purposes, ranging from first aid to people located in places hard to reach, to the monitoring of the environment to prevent fires or for package delivery directly to our houses.

There is no direct control from human beings and they need to be able to recognize autonomously obstacles along the path that they are following in order to avoid crashes. Many of them come equipped with 4G connections, able to give them access to the Internet via cellular network. The Internet access can be used in order to create a communication layer where the UAVs exchange information about the surrounding environment.

It is important to clarify the difference between UAV and drone. With the first term we refer to a flying vehicle where there is not a human being aboard controlling it, and, in some cases, can be self-driven by being programmed and instructed before the flight, or can be remotely controlled from the ground. The UAV is a kind of specific drone. Instead, with the term drone we refer to a vehicle that does not have a pilot inside, that can also be, for example, terrestrial or marine [1], including all kinds of vehicles that are self-manned.

To measure distances in remote sensing a technique called Lidar [2] is adopted. In particular, by using this method it is possible to retrieve the distance to an object by illuminating the target with a pulsed laser light, which can be near-infrared, ultraviolet or interferometric, and then measuring the reflected pulses with a sensor. The time elapsed by the laser to return and the wavelengths can be used for the creation of a 3D representation of the object. Lidar sensors are successfully used in agriculture for measuring the growth of crops. On the other hand, heat sensors can be used in critical situations, but also they can help in everyday tasks, such as, for example, to check the temperature of livestock or presence and temperature of a water well.

The blockchain technology has become object of study in several fields. Its application is really valid in those contexts where the confidentiality of the information needs to be preserved and guaranteed. The most widely adopted technology of this kind is for cryptocurrencies, where a permissionless access is allowed to every participant, without requiring any kind of identification of the new users. In order to maintain the usage of a certain cryptocurrency while adopting a permissioned blockchain, it is possible to use side chains.

In this work we are proposing the design of a permissioned side chain for the collision avoidance and the recovery of crashed UAVs, describing the use cases where it can be adopted and introducing the involved entities, their roles and their specific objectives.

The rest of the paper is organized as follows. In section II a blockchain for the geospatial identification of obstacles and UAVs recovery is presented. In section IV scenarios in which the blockchain can be adopted are described. Finally in section V conclusions and future directions are drawn.

II. A blockchain for the geospatial identification of obstacles and UAVs recovery

We chose to design a permissioned blockchain involving UAVs and human beings, in order to rescue the UAVs after their crash, by performing transactions where constantly the UAVs report their GPS coordinates and height flight. The adoption of one of the fastest consensus algorithms, such as Proof of Authority (PoA), will provide the high throughput required by the designed blockchain.

In most cases, the permissionless blockchains run a consensus algorithm which requires high computational power and, consequently, a large amount of electrical energy, in order to make the nodes solve puzzles that are useful to maintain the security of the whole blockchain. The most used consensus algorithm, also currently adopted in Bitcoin [3] and Ethereum [4], is the Proof of Work (PoW). A shift is actually going on towards more energy aware consensus algorithms, for example, the Proof of Stake (PoS) which, as requisite for the block mining, considers above all the interest of the participants in the blockchain. The permissionless blockchain is an approach that by nature requires a high effort in terms of resources, such as CPU and electricity, in order to maintain the whole blockchain safe, preventing it to be attacked by malevolent users. The main advantage that the blockchain technology brought is the creation of a peer to peer network, where nodes can perform transactions by using a cryptocurrency, adopting an open ledger that can be seen by all the participants and has the characteristic of immutability.

With the Ethereum platform, which is considered to be the first implementation of the second generation of blockchain, it is also possible to write source codes in a high level programming language called Solidity, whose syntax is based on Javascript, but also borrows concepts from Python and C++. Pieces of a program can be executed through the Smart Contract, where they are contained, when a particular transaction occurs. A well known problem for most of the permissionless blockchains is the quantity of transactions supported per second.

The Ethereum platform is close to release an important update of its consensus algorithm, in which a hybrid PoW and PoS is implemented, in order to reduce the amount of electricity used and try to speed up the transaction throughput. On the other hand, the PoA consensus algorithm is faster, thanks to the adoption of validators which perform the block mining.

A mining leader, who is in charge of proposing new blocks, is elected by the validators. Consequently, the quantity of messages exchanged is much less, hence improving the performances [5]. Furthermore, for the block mining, no resolution of a puzzle is required.

In order to tackle the problem of the obstacle recognition and avoidance, widely addressed in literature, by using several techniques, as crucial point we considered the need of a collaboration among people and UAVs.

We highlighted the blockchain as the technology able to create this communication layer, and the use of smart contracts to reward the entities involved in the rescue and repair activities. In the designed blockchain the transaction included in each block contains information regarding the exact position revealed by the GPS of each drone and its flight height, sent out every 3 seconds. According to the Small Unmanned Aircraft Regulations, the FAA established that a drone for commercial use cannot reach more than 100 mph, meaning that in 3 seconds, at maximum velocity, it is able to travel 150 meters at the utmost. Combining the flight height with the coordinate it can be quite easy to detect where the collision has occurred, considering that to reach the maximum velocity a drone needs to fly in a quite free space, namely not among buildings in a city, but most probably in open country. Considering another possibility, the crash of a UAV in the city, it has to be taken into account that, due to the lower velocity, the impact may not damage any of the components that the drone uses to communicate with the blockchain, namely the 4G modem and the motherboard, hence it can be able to communicate its last correct position even after the crash, making it easier to locate its position. The system proposed should be used in a cooperative scenario where other UAVs are participating. The collective participation permits the communication of obstacles that are not signaled in their maps and that are needed to be avoided.

The human beings interacting with the blockchain can be owners, rescuers and UAV repairers. The owners are those individuals whose interest is to preserve the safety of their drones and are the ones who will give a compensation to the rescuers or repairers. The rescuers are those people that will receive a notification about a crashed drone close to their fixed location. The repairers are recognized shops able to fix crashed components of the damaged drones.

No limit is imposed to the participants to impersonate more than one role. For example, a rescuer can also be an owner, or a repairer, or vice versa a repairer may also perform the role of owner or repairer.

The calculation of the reward will occur by using smart contracts, through which three main use cases will be considered. The first is the restitution, by delivering the crashed UAV directly to the owner. Another use case taken into account is the custody waiting for the collection, while the third use case is the delivery to a UAV repairer.

In figure 1 a simple use case is described. A private blockchain is deployed, three human actors and three UAVs are involved in the communication. The three humans are performing the role of owners, but two of them are also performing the role of rescuer or repairer. The three UAVs are constantly sending their position and their flight height.

Our PoA algorithm is based on a set of trusted nodes, called authorities. At least N/2 + 1 authority nodes is assumed to be honest.

In our design, only humans can be elected as authorities. We considered that UAVs need to apply policies of energy saving, preventing them to be involved in the mining process. In order to fairly distribute the responsibility of block creation, a mining rotation schema is adopted by the PoA algorithm.

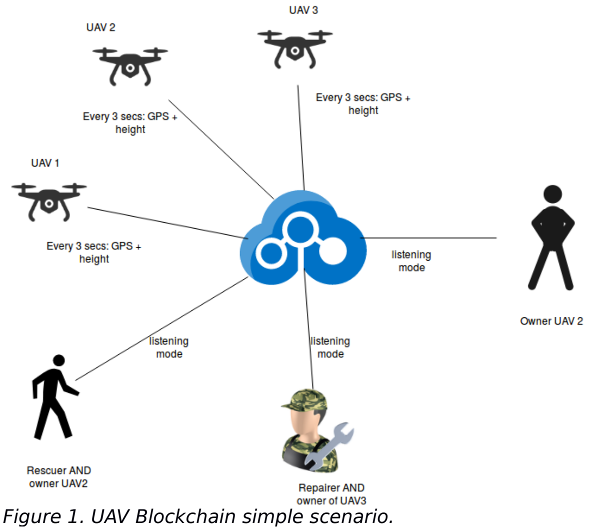
UAV 3
UAV 2
Every 3 secs: GPS + height
Every 3 secs: GPS + height
UAV 1
Every 3 secs: GPS + height
listening mode
Owner UAV 2
listening mode
listening mode
Rescuer AND owner UAV2
Repairer AND owner of UAV3

Figure 1. UAV Blockchain simple scenario.

The transactions made by clients are ordered by the elected authority, which performs the role of mining leader.

In case of crash, a function defined in the smart contract will notify every rescuer, in this specific case only the owner of UAV 1, informing about the position of the crashed UAV.

Ⅲ.Scenarios in which the blockchain can be adopted

In [6], Paneque-Galvez et al. carried on a study above the usage of drones for the enhancement of the community-based forest monitoring (CBFM) programs, where data gathering is achieved with lower costs, with respect to those gathered by professional scientists. Among the principal tasks carried on in CBFM programs, we found conventional ground surveys to gather forest data inventories. These inventories can be performed by measuring variables in permanent plots, such as tree height, diameter at breast height (DBH), number of trees, tree species and canopy cover. These kinds of surveys cannot be easily extended to large areas, and even covering small areas, they result to be time-consuming, costly, tedious and affected by logistical difficulties. In fact, in the tropical forests environment, difficulties rise, related, for example, to safety of the worker for the access to remote sampling sites. In their work they discussed the key advantages and disadvantages that can be expected by using small UAVs for CBFM.

The adoption of UAVs in surveillance tasks can extend the role of cameras from a higher perspective and they are able to scour zones that are not easily reachable. For example, the companies can employ them to control pipelines and buildings. Another important usage is to perform dangerous control instead of the human beings, like the inspection of tall structures such as chimneys and roofs, or power lines.

Among the first enterprises which started to do research on how to deliver packages by delivery drones there is Amazon, DHL, Google and Fedex. The real adoption of their delivery system is still undermined, among the others, by local laws and risk for public safety.

In particular, Amazon in the patent [7] says that attackers can be able to hack the communication signal towards their UAVs and take its control, but they developed a system able to put the UAV in safety mode, which will be able to perform one or more actions in order to reestablish the communication with the controller, or bring the UAV in a safe location, in case of an event such as a hostile takeover.

It is possible that a certain UAVs network can be attacked by hackers who want to take the control of one or more UAVs. As described in [8], Sedjelmaci et al. report several kinds of attacks that can affect UAVs networks, among them we can find the ones classified as Integrity Attacks, such as GPS spoofing attacks and false information dissemination attacks.

The first ones consist into leading the UAV to estimate a false GPS position of itself, causing, for example, the capture of the latter by driving it to a false home base.

The second ones can be related, for example, to the broadcast of a different physical phenomenon, such as forest fires, to its neighbor UAVs or false environmental conditions. This kind of attacks may put at risk the health of the UAVs leading them in dangerous situations, where crashes may occur.

The designed blockchain can be also used directly for UAV to UAV communication, in order to rescue UAVs that crashed while they were working in team, such as, for example, in the environmental monitoring use cases. In fact, in this latter case, probably no human beings will be close to a crashed UAV, thus making it impossible to be rescued by an occasional passer-by, neither someone that is living close to the crash. In this specific case, other AUVs can go close to the crashed one and take pictures, in order to organize some rescue equipment able to bring the AUV in a safe place, or to the closest repairer.

Ⅳ. Conclusions and future directions

In this paper we presented the design of a permissioned blockchain for the collision avoidance and the recovery of crashed UAVs.

The next step of our research is to provide a proof-of-concept simulation of the system to give some additional understanding of its feasibility (e.g., in terms of scalability of the performance of the blockchain with increasing number of UAVs).

The further step will be the implementation of the proposed solution in testbed scenario.

Acknowledgements

This work was supported by the PhD scholarship from Region Sardinia (P.O.R. Sardegna, European Social Fund 2007- 2013 - Axis IV Human Resources, Line of Activity l.3.1.).This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2019-0-00465, Scalable Decentralized Secure (DeSecure) ECCPoW Blockchain) and This work was partly supported by the "Practical Research and Development support program supervised by the GTI (GIST Technology Institute)" grant funded by GIST in 2019 (Development of Error Correction Codes PoW and Bitcoin/Ethereum Hardfork 1.0)

References

[1]Chmaj, Grzegorz, and Henry Selvaraj. "Distributed processing applications for UAV/drones: a survey." *Progress in Systems Engineering*. Springer, Cham, 2015. 449-454.

[2]Schwarz, Brent. "LIDAR: Mapping the world in 3D." *Nature Photonics* 4.7 (2010): 429.

[3]Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[4]Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum project yellow paper* 151 (2014): 1-32.

[5]De Angelis, Stefano, et al. "Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain." (2018).

[6]Paneque-Gálvez, Jaime, et al. "Small drones for community-based forest monitoring: An assessment of their feasibility and potential in tropical areas." *Forests* 5.6 (2014): 1481-1507.

[7]Larsen, Glen C. "Hostile takeover avoidance of unmanned vehicles." U.S. Patent Application No. 15/239,570.

[8]Sedjelmaci, Hichem, Sidi Mohammed Senouci, and Nirwan Ansari. "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 48.9 (2017): 1594-1606.