Blockchain-base structures for a secure and operate network of semi-autonomous Unmanned Aerial Vehicles

Alexander Kuzmin
(ITMO University)
St.-Petersburg, Russia
akouzmin@altirix.ru

Evgeny Znak
(Mikhailovskaya Academy)
St.-Petersburg, Russia
evgematem@mail.ru

Abstract—**Unmanned Aerial Vehicles — UAVs, or drones — are now being operated by several military forces and currently, to a more limited extent, by civilian organizations. These latter operations, however, may eventually expand to exceed, in number and diversity, those of the military. Further expected development in battery capacity, construction materials and software, especially regarding machine learning algorithms and drone integration, will definitely increase UAVs' autonomous. Unique risks associated with UAVs like risk of hackers' attacks to intercept the control are also increasing. More incidents likely will occur once regulations are finalized that encourage more use that is widespread. Such incidents could result in multi-million dollar claims against businesses, operators and manufacturers.**

Blockchain is the basis technology for cryptocurrencies. However, Blockchain can have far larger applications in the field of UAVs, because Blockchain is highly distributed and publically viewable system of sequentially linked cryptographically.

This paper presents a concept of application, where each UAV in the UAVNet is a Blockchain node, has on-board functionality for creating and reading transactions from the block, as well as communication tools for exchanging transactions with other UAVs.

***Keywords*—cyber security, drones, unmanned aerial vehicles, UAVNet, blockchain, integrity, consensus mechanisms**

I. Introduction

One of the challenges that comes with the increasing use of UAVs is integrating them into the air traffic control (ATC) system so that they do not conflict with other aircraft. Moreover, drones can replace manned aircraft for pipeline patrol, and they are already being used in law enforcement and border patrol.

If the one current rule that drones "must yield right of way to other aircraft" is maintained, current technology would allow any type of drone, for any type of use, to be integrated into the ATC system [1].

Over the last few years, we have seen a rapid development in the field of drone technology, with an ever-increasing degree of autonomy. While no approved autonomous drone systems are operational, as far as we know, the technology is being tested and developed. One of the greatest challenges for the development and approval of UAV with such technology is that it is extremely difficult to develop satisfactory validation systems, which would ensure that the technology is safe and acts like humans would. In practice, such sophisticated drones would involve programming for an incredible number of combinations of alternative courses of action, making it impossible to verify and test them to the level we are used to for manned aircraft.

Semi-autonomous UAV – meaning advanced UAVs' programmed with algorithms for countless human-defined courses of action to meet emerging challenges. We see testing of "swarms of drones" (drones which follow and take tasks from other drones) that, of course, are entirely dependent on autonomous processing [2].

In most cases, future UAV will require access to an interoperable, affordable, responsive, and sustainable-networked system of different systems capable of satisfying service, joint, interagency and real-time information exchanges. This system must be distributed, scalable and secure. It includes but is not limited to human interfaces, software applications and interfaces, network transport, network services, information services, and the hardware and interfaces necessary to form a complete system that delivers secured UAVs' operations. The network operates as independent, small sub-networks connected to each other and integrated with ATC system.

Current and near-term UAVs' data link protection capabilities through use of encryption require significant manual effort to implement and, once implemented, lack operational agility or transparency. In the future, enterprise-wide encryption capability must be simplified to make use some kind of Cryptography Infrastructure architecture resistance against the Man-In-The-Middle attack to distribute key data to desired operating locations. In addition, distribution methods must be able to deliver key information, operational changes to the route and validate users to minimize the burden to every UAV while protecting the network from intrusion or interception.

978-1-5386-4522-2/18/$31.00 ©2018 IEEE

In addition, there are proposals to use LTE (pre-4G), 4G and 5G mobile networks for operate UAVs beyond visual line-of-sight (LOS) communications. Mobile networks offer wide area, high speed, and secure wireless connectivity, which can enhance control and safety [3], [4]. This scenario makes UAVs are part of the Internet of Things and preferred for commercial usage

UAVs' communication network (UAVNet) is tougher and different from other networks because of increased complexities and huge disparity in various properties. Channels of different type, range of communication, different power requirements for different devices, different types of data flows, integrity and confidentiality requirements. In addition, UAVNet consist of UAV-to-UAV (U2U) and UAV-to-Infrastructure (U2I) communication.

The Blockchain technology is being viewed as a powerful technology to decentralize and can be used in tracking billions of connected devices, enable the processing of transactions and coordination between devices; allow for significant savings to Internet of Things (IoT) industry manufacturers. This decentralized approach would eliminate single points of failure, creating a more resilient ecosystem for devices to run on. The cryptographic algorithms used by blockchains, would make consumer data more private. A lot of research is devoted to use the Blockchain technology for IoT protection.

Most researchers suggest using the blockchain as a stand-alone solution from the IoT network. Many proposals are reduced to the use blockchain as a decentralize database [5], [6], [7]. That does not use the full potential of technology and does not allow to significantly minimize the risks.

II. THREAT ANALYSIS AND MODELING

UAVs in their mass application for the delivery of goods, monitoring the urban environment, monitoring of implementing investment projects, combating illegal drug-trafficking, identifying evidence of corruption or supporting disaster management can become invisible killers. It is terrible to imagine what could happen with the seizure of control of the UAVs' network over the megapolis with millions people or over the hazardous plant.

Examples of interception of control or jamming on a UAV are already quite a lot, including with human victims. For example, suspected GPS jamming attack was executed on S-100 Camcopter, a UAV made by Schiebel, resulting in a crash into the ground control station and killing a Schiebel's engineer and injuring two remote operators during testing. An unknown actor performed the attack on 10th May 2012 during the UAV test, near the western port city of Incheon, South Korea. The attack was detected after the crash and is suspected that GPS jamming started on April 28th, also disrupting passenger flights at Kimpo and Incheon [8].

The modeling of security threats is an integral part of requirements and international standards, because it can actually lead to discovery of vulnerability in the system [10].

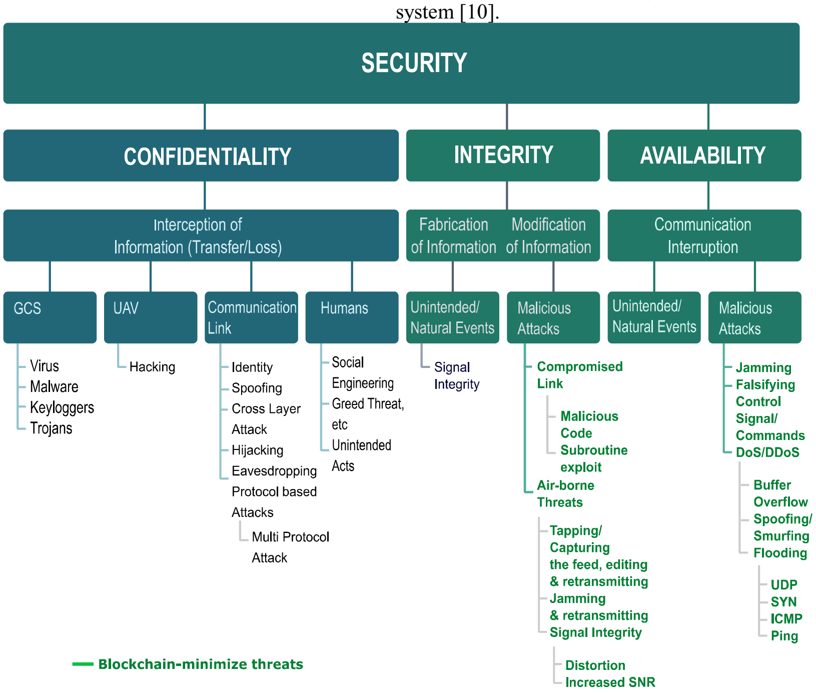


Figure 1. UAVNet cyber-security Threat model [9] and Blockchain-minimize threats.

The studies [11] and news analysis show that sources of a very present threats of UAVNet are:

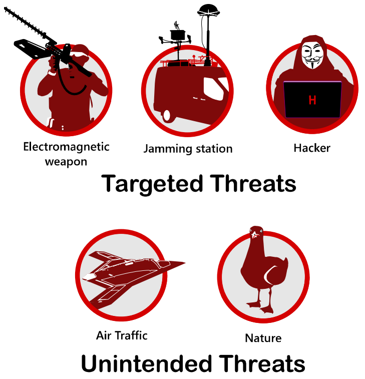


Figure 2. Sources of a very present threats of UAVNet.

Data types in UAVNet

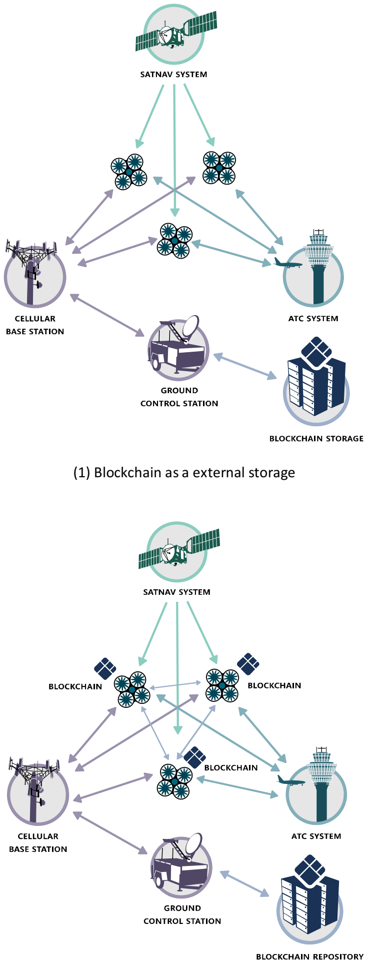
- UAVs' Identificator (UAV ID)
- Fly route control program with routing sheet and coordinates (route sheet)
- Sensors/LIDAR's data
- Flying schedule

Forgery of any of these data may cause significant negative consequences. Each of the Data types can be written and updated in the block of Blockchain for reading for decision purposes. For example, Fly route control and Flying schedule can be implement into smart-contract. The fulfillment of the conditions of the smart contact is an indicator of the completion of the UAVs' flight mission.

Blockchain and UAVNet cyber-security threats.

Sources of Targeted threats (Figure 5) set themselves the goal of breaking the UAVs' connections with UAVNet elements to destabilize control.

Blockchain minimizes threats to integrity of blocks' data or protect integrity of data in storage when write Hash (Checksum) of this data [12], [13]. In the case of UAVNet, it is not enough to ensure data integrity in external storage (Figure 3). As it was written above, there is a high probability of attack on the communication channels between UAV and GCS or the Satnav communication channel. When Blockchain deploy directly to the each UAV he can significantly hamper the implementation of threats to integrity and availability. Since each UAV has a copy of a Blockchain on its board will be able to autonomously complete its route, regardless of other elements of UAVNet. Knowing the route of the neighboring UAVs does not make a collision in the air. In the proposed scenario, there can also be an external storage - a Blockchain repository for long-term storage of flight parameters, like black box on a plane.



(1) Blockchain as a external storage

(2) Blockchain as a distributed control and security system

Figure 3. Scenarios of Blockchain implementation in UAVNet.

Blockchain as a distributed control and security system scenario can ensure the autonomy of the UAV when communication channels from other components of UAVNet are lost (Figure 4). To minimize the consequences of such a threat, the Blockchain must contain a Fly route control program (smart-contract) with the ability to operate without obtaining coordinates from the Satnav system. UAV taking into account only the readings of the sensors and Flying schedule of neighboring UAVs in the fully automatic mode until exiting the jamming zone. Electromagnetic rifle has such a principle of work as most jamming station, but directly.

Some studies have concluded that data integrity for IoT is a priority requirement. In the security triad CIA (Confidentiality, Integrity, Availability), integrity comes to the forefront, in an era of comprehensive access to secrets [14]. However, it would be criminal to think that unlawful access to the UAVs' flight routes has no security implications.

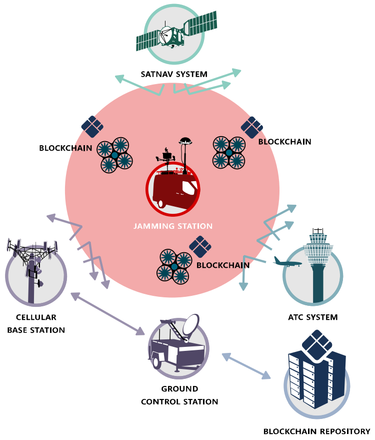


Figure 4. Jamming station and UAVNet.

Standard privacy mechanisms can be discredited by hackers. By nature, Blockchain cannot solve the problem of confidentiality. Data masking mechanisms can help minimize the consequences of obtaining unauthorized access. More information in the Section III of the article.

III. Stochastic Blocks

In the proposed scenario, N of numbered computing devices (UAVs) are randomly divided into m equivalent groups at random times t_k:

$$T_k \text{ and } F_{k1}\,,\ F_{k2}\,,\ \ldots\,,\ F_{k\,,m-1}$$
$$\left(\ N = mn\,,\ \ |T_k| = n = |F_{kj}|\ \ \right).$$

Here$t_{j+1} = t_j + \tau_j$ and a random operational period τ_j is evenly distributed between fixed values $s_1$and s_2 (see below for the optimal choice of boundaries $s_1,\ s_2$).

During a time period τ_k, computing devices of the group T_k are used to simultaneously store copies of information broadcast from unmanned vehicles, i.e., during a period τ_k, the T_k group devices become actual Blockchain participants. During the next time period τ_{k+1}, this role is transferred to other computing devices (devices of the group T_{k+1}) and so on. In parallel, during the period τ_k, computing devices of the groups $F_{k1}\,,\ F_{k2}\,,\ \ldots\,,\ F_{k\,,m-1}$ simulate *the most plausible but **false*** variants of routing and current information from unmanned devices (a specific version for each individual group F_{ki}).

From the general description we now turn to a more detailed algorithm:

1) at the time t_k, the duration of the next operation period τ_k is generated;

2) in parallel, at the time t_k, the set of numbers $1,\ 2,\ \ldots\ ,\ N$ is *randomly* divided into m groups of n numbers in each, that is, forming a two-dimensional random array

$$\begin{pmatrix} T_k^1 & T_k^2 & \ldots & T_k^n \\ F_{k1}^1 & F_{k1}^2 & \ldots & F_{k1}^n \\ . & . & & . \\ F_{k,m-1}^1 & F_{k,m-1}^2 & \ldots & F_{k,m-1}^n \end{pmatrix}$$

(the first row contains the device numbers of the group T_k, the jth row contains the device numbers of the group $F_{k,j-1}$ ($j \geq 2$));

3) all current information (specified routes plus operational information appearing on the move) is almost instantly transferred from the device with the number T_{k-1}^j to the device with the number T_k^j and from the device with the number $F_{k-1,i}^j$ to the device with the number F_{ki}^j, respectively;

4) all the information at the carriers T_{k-1} and $F_{k-1,1}\,,\ F_{k-1,2}\,,\ \ldots\,,\ F_{k-1,m-1}$ is deleted after being transferred and, in addition, the previous matrix of numbers is erased

$$\begin{pmatrix} T_{k-1}^1 & T_{k-1}^2 & \ldots & T_{k-1}^n \\ F_{k-1,1}^1 & F_{k-1,1}^2 & \ldots & F_{k-1,1}^n \\ . & . & & . \\ F_{k-1,m-1}^1 & F_{k-1,m-1}^2 & \ldots & F_{k-1,m-1}^n \end{pmatrix}$$

5) during the operation period τ_k (i.e., until the moment t_{k+1}), unmanned devices systematically receive route confirmation (and, in general, control the integrity of all operational information), relying on the carriers of the group T_k.

Basic technical principles

An idle (unoccupied) unmanned vehicle of the reserve fleet falling into a certain period (t_j ; t_{j+1}) receives its 'route sheet' from the carriers of the group T_j at the time of starting its operation. A qualifying operator adds the corresponding 'route sheet' data to the Blockchain prior to this moment.

An unmanned vehicle fully fulfilling the 'route sheet' sends a signal to the Blockchain and goes idle automatically. After that, the information directly related to this device is deleted at the current carriers (if necessary, you can provide for the transferring of the routing history to a permanent secure archive storage - Blockchain repository, before deleting).

In addition to N commercially available computing devices, there is a small and stable *assisting device group T*. The number of devices in the assisting group T is relatively small and all of these devices are guaranteed to be on around the clock. The assisting group T is automatically used to duplicate some of the group T_j devices in a situation (supposedly unlikely), when at a moment t_j, it turns out that more than two-thirds of the group T_j devices are off-line.

Reliability evaluation and choice of boundary values

If an attacker has active access to l computing devices and gets to know the true version (at least the beginning of the scenario) with probability $p = \frac{1}{m}$, then the probability of his success in the short-term analysis can be minorized at a first approximation by a linear function of the product $(1-(1-p)^{l}) \cdot p$, where the first factor is equal to the probability of having a true version at one of the l carriers. If the average operation time of a unmanned vehicle is equal τ, then the number of interchanged number groups can be approximately estimated as $\tau : \frac{s_1 + s_2}{2}$, and the probability of success of the attacker in the continuous analysis can be minorized at a first approximation by a linear function of the formal probability $(1-(1-p)^{d}) \cdot p$, where $d = l \cdot \frac{2\tau}{s_1 + s_2}$.

Thus, there is a natural boundary.

$$(1-(1-p)^{d}) \cdot p < \gamma$$

It can be amplified or weakened, giving the threshold probability γ a correspondingly smaller or larger value.

	20	**100**	**200**	**500**	**1500**
0.1	8000	40,000	80,000	200,000	600,000
0.5	1600	8000	16,000	40,000	120,000
2	400	2000	4000	10,000	30,000
5	160	800	1600	4000	12,000
10	80	400	800	2000	6000
25	32	160	320	800	2400

For the estimated average operation time of a unmanned vehicle of $\tau = 40$ *minutes* (Amazon promises get packages to customers in 30 minutes or less using unmanned aerial vehicles [15], add 10 minutes for greater objectivity) and the assumed range $10^3 < N < 5 \cdot 10^6$ (scale of cities, from small to large), we provide tables that give some idea of the values d (the upper table) and $(1-(1-p)^{d}) \cdot p$ (the lower table).

The values of $\frac{s_1+s_2}{2}$ vary in the rows (in minutes), the possible values of l vary in the columns.

	10	**50**	**100**	**500**	**1000**
2	0.4995	0.4999	0.5	0.5	0.5
5	0.1785	0.1999	0.2	0.2	0.2
10	0.0651	0.0994	0.0999	0.1	0.1
20	0.02	0.0461	0.0497	0.0499	0.05
50	0.0036	0.0127	0.0173	0.0199	0.02
100	0.0009	0.0039	0.0063	0.0099	0.01
200	0.0002	0.0011	0.0019	0.0045	0.0049
500	0	0.0002	0.0004	0.0013	0.0017
1000	0	0	0.0001	0.0004	0.0006

The values of m vary in the rows (in minutes), the possible values of d vary in the columns.

On the other hand, there is a basic limitation $n_0 < n = \frac{N}{m}$, where n_0 is a critical number of the blockchain participants at which the integrity of the information can not be guaranteed sufficiently (say, with a probability not less than 0,995). In this case, the principle of information integrity control 'by most coincidences' (the true value is that, which has the maximum number of confirmations) naturally implies the fulfillment of the inequality $l \leq \frac{n-1}{2}$ for the number l of compromised computing devices (see above). These three requirements should be considered together for a quasi-optimal choice of the parameters N, m and s_2. Regarding s_1, the choice of this time boundary is:

1. Essentially tied to the speed of the entire system that performs the proposed algorithm;
2. Conditioned by fact that ***too frequent*** *change of groups* is beneficial to the attacker (this is confirmed, in addition to all other considerations, by the last probability table).

This last consideration affects, in the end, the choice of the boundary value s_2.

IV. Proof-Of-Graph (PoG) consensus mechanism

The existing consensus mechanisms have a number of limitations. On the other hand, the tasks of moving and logistics have specific data capable of assuming the role of validators.

For the validate new transaction, Blockchain of UAVNet can use confirmation from chain, consisting of UAVs and GCS formed from the graph nodes on the optimal path from the request node (UAV) to the GCS. The formation of a Complete Graph confirmation system, when the computing devices of any two UAVs interact with each other, is limited by the problem of insufficient UAVs' computing power.

For this reason, it is proposed to use the dynamic partitioning of the aggregated of UAVs, involved into a number of conditional groups - independent information exchange circuits. The number of autonomous circuits can vary depending on the day time and some other factors. A conditional model of partitioning into chains is the collection of Complete Graphs $Y_1(t), \dots, Y_m(t)$ depending on the current time t. The vertices of the Complete Graph $Y_k(t)$ are interpreted as the numbers of UAVs and GCS, used at the time t in the autonomous circuit with the number k. Information exchange inside $Y_k(t)$ can be organized on the principle of a chain of transaction blocks.

Well-known algorithms can be used to find the optimal path. Dijkstra's Algorithm is good in finding the shortest path, but he spends time exploring all directions, even hopeless ones. A Greedy Algorithm explores perspective directions, but may not find the shortest path. Algorithm A* uses both the actual distance from the beginning, and the estimated distance to the target (Figure 5). SMA* or Simplified Memory Bounded A* is a shortest path algorithm based on the A* algorithm. The main advantage of SMA* is that it uses a bounded memory, while the A* algorithm might need exponential memory. All other characteristics of SMA* are inherited from A* [16].

SMA has the following properties:*

- It works with a heuristic, just as A*.
- It is complete if the allowed memory is high enough to store the shallowest solution.
- It is optimal if the allowed memory is high enough to store the shallowest optimal solution, otherwise it will return the best solution that fits in the allowed memory.
- It avoids repeated states as long as the memory bound allows it.
- It will use all memory available.
- Enlarging the memory bound of the algorithm will only speed up the calculation.
- When enough memory is available to contain the entire search tree, then calculation has an optimal speed.

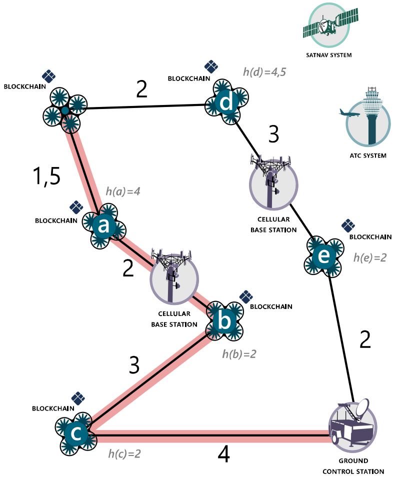


Figure 5. Example of SMA* algorithm for PoG.

Node (vertex) weights and edge weights can be random variables or selected in such a way as to shorten the validation time.

The solution of the following tasks is required:

1) online selection of an autonomous circuit, which will include the next (starting) UAV;

2) the implementation of algorithms for the regular reset of archival information in a Blockchain Repository for the purpose of clearing the operational memory of UAVs in the autonomous circuit;

3) automatic control of the number of autonomous circuits and, in particular, prevention of degeneration of individual circuits;

4) automatic maintenance of the minimum number of autonomous circuits in the active state.

V. Conclusion and Future work

The proposed Blockchain technology usage scenario needs mathematical modeling. The PoG consensus algorithm requires the research of the dynamic partitioning of UAV groups - autonomous information exchange circuits. Successful research will help to improve functional and information security of UAVNet and prevent air traffic incidents.

References

[1] Randall G. Holcombe, Integrating Drones into the US Air Traffic Control System, Mercatus Center at George Mason University, Arlington, VA, October 2016.

[2] Autonomous military drones: no longer science fiction, NATO Review, July 2017 (available at: https://www.nato.int/docu/Review/2017/Also-in-2017/autonomous-military-drones-no-longer-science-fiction/EN/index.htm).

[3] Richard Wiren, 5G and UAV use cases, IEEE 5G-IOT SUMMIT HELSINKI, Ericsson, September 2017.

[4] Xingqin Lin, Vijaya Yajnanarayana, Siva D. Muruganathan, Shiwei Gao, Henrik Asplund, Helka-Liina Maattanen, Mattias Bergström A, Sebastian Euler, Y.-P. Eric Wang, The Sky Is Not the Limit: LTE for Unmanned Aerial Vehicles, Ericsson, Jule 2017.

[5] Ali Dorri, Salil S. Kanhere, Raja Jurdak and Praveen Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home", The 2nd IEEE Percom workshop on security privacy and trust in the. Internet of things, 2017.

[6] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future to Internet of Things security: A position paper, Digital Communications and Networks, 2017, doi: 10.1016/j.dcan.2017.10.006.

[7] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems, 2017, https://doi.org/10.1016/j.future.2017.11.022

[8] Y. S. Lee, Y.-J. Kang, S.-G. Lee, H. Lee, and Y. Ryu, "An overview of unmanned aerial vehicle: Cyber security perspective," Korea, vol. 12, p. 13, 2012.

[9] A. Y. Javaid, W. Sun, V. K. Devabhaktuni and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, 2012, pp. 585-590. doi: 10.1109/THS.2012.64599145656565.

[10] R. Crook, D. Ince, L. Lin, and B. Nuseibeh, "Security requirements engineering: When anti-requirements hit the fan", Proceedings of International IEEE Requirements Engineering Conference, RE-2002.

[11] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), Shanghai, 2017, pp. 194-199. doi: 10.1109/SSRR.2017.8088163.

[12] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev and L. Yalansky, "Ensuring data integrity using blockchain technology," 2017 20th Conference of Open Innovations Association (FRUCT), St. Petersburg, 2017, pp. 534-539. doi: 10.23919/FRUCT.2017.8071359.

[13] B. Liu, X. L. Yu, S. Chen, X. Xu and L. Zhu, "Blockchain Based Data Integrity Service Framework for IoT Data," 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, 2017, pp. 468-475. doi: 10.1109/ICWS.2017.54.

[14] Robert K. Ackerman, Data Integrity Is the Biggest Threat in Cyberspace, SIGNAL Magazine, 2013 (available at: http://www.afcea.org/content/? q=node/11438).

[15] Amazon Prime Air, Amazon.com, Inc. (available at: https://www.amazon.com/Amazon-Prime-Air/b?node=8037720011).

[16] Stuart Russell, Efficient memory-bounded search methods, ECAI '92 Proceedings of the 10th European conference on Artificial intelligence, John Wiley & Sons, Inc. New York, NY, USA, 1992, pp. 1-5.