Towards a Trusted Unmanned Aerial System Using Blockchain (BUAS) for the Protection of Critical Infrastructure

Ezedin Barka[1], Chaker Abdelaziz Kerrache[2], Hadjer Benkraouda[1], Khaled Shuaib[1],
Farhan Ahmad[3], Fatih Kurugollu[3]
[1]College of Information Technology, United Arab Emirates University, PO Box 15551, Al Ain, UAE
[2]Department of Mathematics and Computer Science, University of Ghardaia, Ghardaia, Algeria
[3]Cyber Security Research Group, College of Engineering and Technology, University of Derby, Derby, UK
[1]ebarka@uaeu.ac.ae; hb992@nyu.edu; k.shuaib@uaeu.ac.ae
[2]kr.abdelaziz@gmail.com; ch.kerrache@univ-ghardaia.dz
[3]{f.ahmad, f.kurugollu}@derby.ac.uk

***Abstract*— With the exponential growth in the number of vital infrastructures such as nuclear plants and transport and distribution networks, these systems have become more susceptible to coordinated cyber attacks. One of the effective approaches used to strengthen the security of these infrastructures is the use of Unmanned Aerial Vehicles (UAVs) for surveillance and data collection. However, UAVs themselves are prone to attacks on their collected sensor data. Recently, Blockchain (BC) has been proposed as a revolutionary technology which can be integrated within IoT to provide a desired level of security and privacy. However, the integration of BC within IoT networks, where UAV's sensors constitute a major component, is extremely challenging. The major contribution of this study is two-fold. (1) survey of the security issues for UAV's collected sensor data, define the security requirements for such systems, and identify ways to address them. (2) propose a novel Blockchain-based solution to ensure the security of, and the trust between the UAVs and their relevant ground control stations (GCS). Our implementation results and analysis show that using UAVs as means for protecting critical infrastructure is greatly enhanced through the utilization of trusted Blockchain-based Unmanned Aerial Systems (UASs).**

***Keywords*—UAV; UAS; FANET; Blockchain; Trust; Security**

I. Introduction

Flying Adhoc Networks (FANETs) are one of Self Organized Networks (SONs) in which mobile nodes are called Unmanned Aerial Vehicles (UAVs). In addition to the flying UAVs the overall system involves also ground control stations and sometimes satellites [1]. Various innovative applications in different domains have emerged with the development of FANETs including agriculture, crowd sensing, frontiers surveillance and search and rescue operations. [2], [3], to name a few.

To ensure this variety of applications, commercial drones (UAVs) are equipped with different sensors and cameras [4]. After gathering the sensed or captured data, a UAV; which can be sometimes remotely controlled; sends the data to the Ground Control Station (GCS) for further processing. At the same time, flying UAVs can also communicate with each other for data delivery purposes, positioning, accuracy purposes, or even for collision avoidance purposes.

Wireless communication devices, sensors and UAVs, are usually energy-restricted devices with low computational power systems and thus cannot run complex cryptography procedures to protect communicated data from possible malicious attacking entities. Thus, efficient security solutions should be developed to overcome this shortcoming, especially for the case of UAVs monitoring of critical infrastructures [5]. Several solutions have already been proposed in the literature based on both cryptography [6] and trust management [7]. However, ensuring the desired security and privacy level in the context of FANETs is still an open research problem with several unresolved challenges [8].

Recently, Blockchain has been proposed as a decentralized and auditable network where every participating node can add reliable data to the blockchain, thus, providing security-by-design architecture [9], [10]. Blockchain, originally designed for the financial industry, and it is currently revolutionizing the IoT industry including healthcare [11], supply chain [12] and logistics [13]. However, for a highly mobile network like FANETs, Blockchain is still in its early stage of research.

The literature demonstrates that combining peer-to-peer swarms of UAVs will revolutionize many industrial applications [14], [15], from targeted material delivery to precision farming, and ending with search and rescue. However, several of the heterogeneous characteristics of drones make them ideal for monitoring and detecting faults and malicious activities against critical infrastructure (i.e., dams, power grids, boarders, and even nuclear power sites.) [16], [17]. UAVs autonomy, decentralized control, collective emergent behavior, etc. can be of a great usage in protecting critical infrastructure facilities. However, the lack of secure communication and trust between drones make them more prone to possible attacks, especially when they operate in a swarm collaborating autonomously to monitor and provide near-real time data to a ground control station for timely decisions. Blockchain has demonstrated that by combining peer-to-peer networks with cryptographic algorithms, a group of agents can reach an agreement on a particular state of affairs and record that agreement without the need for a controlling authority. The combination of Blockchain with other distributed systems, such as a UAV swarm system, can provide the necessary capabilities to make UAVs operations more secure, autonomous, flexible and even profitable. Benefits from the security features provided by the blockchain technology, where there is a need for reliable and trustworthy systems is self-evident. Also, authentication of involved entities and integrity of exchanged data is very crucial.

In order to ensure trustworthiness of desired data for different FANET applications, we propose a novel blockchain-based trust management solution for Unmanned Aerial Systems (UASs) communication. Our proposal named Blockchain-based Unmanned Aerial System (BUAS). BUAS involves different communicating domains staring from the UAV embedded sensors to the Blockchain. In addition, BUAS is also based on the Bayesian Inference (BI) approach [18] which is known to offer high accuracy when estimating a given event credibility.

The rest of the paper is organized as follows: In Section II, we provide an overview about the Unmanned Aerial Systems, their security requirements, and we discuss existing solutions. Section III introduces our domain-based architecture (BUAS), and its performance is evaluated in Section IV. Lastly, we conclude the paper in Section V.

II. Background and Related work

In this section we present the components of the unmanned aerial systems, their adversary model, security requirements, and we discuss existing security solutions in the context of UASs

A. UASs Components

UAS refers to the system of unmanned aerial vehicle (UAV), their ground control station (GCS), and communication technologies linking the UAVs and their GCS. The literature describes many designs of UAVs and GCS, where every design depends on the applications of these systems. However, most UASs share the following main components [19].

1) Unmanned aerial vehicles modules: Fig. 1 represents the UAVs main components together with their interactions [19]:

- **Data acquisition:** This module is responsible for gathering sensor data.
- **Navigation system:** This module contains the UAVs mission. The accuracy of the mission's different points can be improved through the use of a GPS as an additional module.
- **Control module:** Once the data gathered, this module is then responsible for delivering the data to the ground control station.
- **Data logging module:** Same as any sensors-based system, a temporary cache is used to save the data until its delivery to the ground control station.

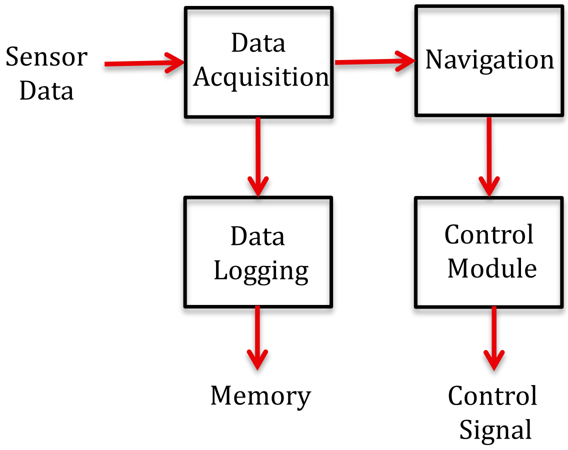

Fig. 1: Unmanned Aerial Vehicles modules

2) Ground control station modules:

- **Operator:** It represents the agent controlling the UAV during its mission. The operator can either be a person or a pre-loaded program.
- **Data storage:** Upon receiving the data collected by the UAVs, this module stores it before further processing.
- **Data analysis:** This is the most important module, it analyzes the data received from the GCS in order to make flight decisions.

B. UASs Adversary model

In UASs an attacker can target hardware devices, software applications or communications. These attackers can be classified into three categories:

1) Adversaries targeting software: The software component is a fundamental element that provides control of hardware and applications. The mobile operating system and applications installed on GCS or other smart devices are susceptible to some vulnerabilities such as buffer overflow or code injection after jailbreaking the operating system. An attacker can exploit these vulnerabilities to gain access to some services or in worst case scenarios control the UAV. For instance, a malicious entity can direct a UAVs weapon against defined targets, it can also corrupt data or inject falsified information. Security mechanisms must prevent unauthorized access and the execution of malicious code in the boot and the operation phases.

2) Adversaries targeting Hardware: Payloads on UAV such as camera, GPS, and storage devices are preferable targets for attackers. When an attacker becomes successful in controlling these devices, he/she can change the mission path or capture the UAV by falsifying the GPS positions. The attacker can then modify images captured by the camera, changes the angle of view (AOV) or destroys the UAV by disturbing the sensing devices and exhausting the power sources. These attacks can be achieved using malicious software or via hijacking the communication channels.

3) Adversaries targeting communications: The primary goal of such an adversary is to maliciously alter or damage the network functionality. In such cases, an attacker can eavesdrop, modifies or deletes data in-transit. The increased number of applications based on communication, broadens the attack surface. Thus, most of the attacks carried out in Wireless Sensor Network (WSN), Wireless Mesh Network (WMN) or Vehicular Ad-Hoc Network (VANET) can be launched against UAV communications. Even though, the data link represents an attractive choice for attackers, in UAVs, the control link between the GCS and the aircraft, is still the preferred target. Hence, by employing simple techniques such as jamming or spoofing, an adversary can be successful in interrupting the normal operations of UAVs.

C. UASs Security requirements

1) Confidentiality: Ensuring that communication information among UAVs cannot be retrieved by a man-in-the-middle is critical requirement of any security system. Encryption is usually used to prevent devastating consequences of information leakage. However, many challenges such as limited power and computing resources have to be considered especially in the case of UAVs.

2) Integrity and message authentication: In Non-Line of Sight (NLOS) scenarios, receiving messages from on-board UAV devices is not possible. Routing protocols can be used, in such cases, as an alternative solution. In this case, the message can be forwarded by means of another UAV or a ground nodes (sensor, vehicle, IoT device, etc.). However, man-in-the-middle attack cannot be avoided, and an attacker may change the content of the message. Therefore, detecting and preventing any alteration of message is an important requirements in any communication scenario in UASs.

3) Non-repudiation: Non-repudiation is the ability to prevent a sender from denying the generation of a messages or denying the content of a message. This requirement is important, especially, when a UAV oversteps boundaries for instance it can deny sending images or messages from a restricted area.

4) Authentication: The identity of an UAV should be verified in order to distinguish a legitimate UAV from an unauthorized one. Public key certificates can be used to authenticate the identity of the user. Moreover, in some applications such as in swarms, and traffic control, UAVs may use valid keys only for small intervals of time. Thus, for efficiency of security solutions, a set of valid keys must be pre-loaded before UAV release.

5) Access control: The variety of UAV applications requires communication mechanisms among different devices, that may have multiple identities (e.g. vehicles). Hence, ensuring that only authorized entities can connect to an UAV service or device is mandatory. As part of access control, access policies can be predefined, for each service, protocol or device, depending on the type of UAV (e.g. Police UAV, Ambulance, commercial).

6) Availability: Availability is ensuring the correct functionality of UAV modules, including communications, despite denial of service (DoS) attacks. In the case of UAVs, a DoS attack could be launched at any layer. Physical layer DoS attack targeting GPS services are the most cited in the literature [20]–[22]. But, media access control, networking (routing), or application layers represent an easy target to any adversary launching a DoS attack.

7) Trust and privacy: Finally, an evaluation and establishment of trustworthiness between the flying UAVs and their sensors must be available for both UAVs and their Ground Control Stations. Furthermore, the different kinds of privacy must be ensured for all UAS actors (UAVS, GSC, monitors ...) [23].

D. Existing UASs Security solutions

Although FANETs are among the hottest research topics, there still exists a lack of UAS-dedicated security solutions ensuring the aforementioned requirements.

Authors of [29] analyzed the UAV radio communication systems. They mainly studied the security of the data transferred between the SAMONIT (Polish UAV project Aircraft for monitoring) and other entities. However, this research focused on the cryptography aspects without taking into account the restrictions imposed on the resources of UAVs. On the other hand, the work in [30], [31] studied the adversary model of UAVs together with some proposed solutions. Both papers focus on providing a clear review of the security issues, adversaries and the possible solutions.

Since UAS is based on an open communication medium and a GPS-based positioning system, most of the research is focusing on mitigating GPS jamming and spoofing attacks [32]. The authors of [33] showed that UAVs relying on GPS systems during their missions are vulnerable to jamming attacks. In [34], authors revealed the viability of spoofing commercial GPS due to the lack of encryption. Both attacks can lead to the loss of critical UAVs.

Radu et al. designed a multi-path routing protocol (called MP-OLSR) to disseminate data packets among the nodes in FANETs during emergency scenarios [24]. Although, the proposed routing protocol performs well for emergency applications, the methodology of how this protocol reacts to malicious nodes is not discussed by the authors. Furthermore, Zhang et al. discussed the issues of eavesdropping in UAV-ground communication, where the potential eavesdropper can intercept the communication due to unknown channel-state information (CSI) [25]. To solve these issues, the authors proposed a physical layer-based solution which relies on adjusting UAV trajectory and transmitting power over a given flight time.

Recently, trust is studied as an alternative measure to secure UAVs. For instance, Singh et al. proposed a trust model to secure UAVs based on the genetic algorithm, which plays a vital role in calculating various involved parameters [26]. The authors further extended this trust model by using fuzzy-logic to classify nodes into three distinct level, i.e., good nodes, average nodes and bad nodes [27]. Simulation results of these trust models ensure promising results for detecting malicious UAVs in the presence of a high number of nodes. However,

TABLE I: Comparison of Trust Management Schemes in FANET

Study	Year	Details	Attacker Model	Drawback
Radu et al. [24]	2018	Multi-path routing for FANET	-	How it behave in presence of malicious nodes?
Zhang et al. [25]	2019	Physical layer security to deal eavesdrop between UAV-ground communication	Eavesdrop	How this solution will work in no-fly zones?
Singh et al. [26]	2018	Trust based on genetic algorithm	Selfish nodes	Poor performance for network with high malicious nodes
Singh et al. [27]	2018	Fuzz-logic based trust model	Selfish nodes	Poor performance for network with low legitimate nodes
Yuan et al. [28]	2017	Trust connectivity for overlaid UAV network	Selective forwarding	High number of nodes required to maintain communication link
Proposed	2019	Trust model based on blockchain and BI	Malicious fake reports	PoW computational and time complexity

this approach fails to detect malicious UAVs correctly when the network involves a low quantity of legitimate nodes. Yuan et al. further studied the issue of trust connectivity for overlaid UAV networks, where communication links between the nodes is established only if the achieved trust satisfies the minimum trust threshold [28]. This scheme requires high number of UAVs in order to establish trust. The main limitation of this proposal is building trust model in a network comprised of a limited number of UAVs.

In a nutshell, we can see that trust as a security measure is recently introduced in FANET to secure UAVs as depicted in Table I. It also depicts that the current trust management schemes for FANET have several issues in terms of security. In order to solve these issues, we proposed a novel trust management scheme based on blockchain, namely BUAS. In the next section, we provide details of our proposed trust model.

III. BUAS: A Trusted Unmanned Aerial System using Blockchain

In BUAS, we show how blockchain technology can be integrated with our UAV system to provide innovative solutions for trusted and secure communication in a collaborative decision-making, behavior differentiation when they are deployed in rural locations to protected critical infrastructure. This section describes the overall architecture of UAVs, its operations, and how UAVs trust is managed by using the recently emerged Blockhain technology.

A. Architecture of BUAS

BUAS is composed of three domains: i) UAV domain ii) Ground Control domain, and iii) Blockchain-enabled Infrastructure domain. In the following we explain the tasks of these three domains as shown in Fig. 2.

1) UAV domain: This domain includes the UAVs and their sensors which mostly transmit their data through wireless channel. For instance, drones are equipped with communication capabilities and continuously communicate with the back-end application center via wireless communication protocols. This domain is helpful in the generation of the useful information which needs to be disseminated across the network.

2) Ground Control domain: This domain acts as a communication middle-ware and is responsible for sharing the message generated from the UAVs with the back-end infrastructure. Further, Base Stations in this domain can act as cluster heads to transmit information towards back-end network in order to record data into the Blockchain.

3) Blockchain-enabled Infrastructure domain: This domain is the back-end domain of BUAS architecture which is equipped with BC. Miners are first elected in this domain based on their capability to solve the complex PoW puzzle. When the data from the UAVs is received at the miners via communication domain, the *Miners* first validates the information based on the consensus algorithm. Once, the PoW puzzle is solved by the miner, the data can be added within the BC. The block in BUAS has two major components, i.e., (1) Block header, and (2) Block data. *Block header* contains the Proof-of-Work Hash which includes control related information such as version number, Nonce value, previous block information, merkle trees and a timestamp. *Block data* contains the list of the transactions which are recorded by the miners after solving the PoW algorithm.

B. Operation of BUAS

BUAS takes advantage of blockchain to provide a secure and trusted connectivity between the UAVs and their final users. It operates in three parallel phases:

- First, the UAV sensor generates information which needs to be propagated to the ground control domain. This information contains highly sensitive data including accident warnings in smart transportation, or user's private information for some rescue scenarios.
- Afterwards, it comes the dissemination of the information over communication channel. To achieve this purpose, any available communication medium can be used. Similarly, for delay-tolerant information, the data and information can be aggregated at the Ground Controllers level, then transported to the third domain via Base Stations.
- Finally, the miners at the third domain can add, modify and record the information into the BC after solving the PoW algorithm. Miners are the only responsible nodes which can add the data into BC. However, the data is not added to the BC if miner is unable to solve PoW consensus algorithm.

C. Trust Management in BUAS

From the data acquisition to the blockchain registration several procedures are invoked. The overall process can be summarized in the following four phases: First, Rating generation and uploading; Second, Trust's offsets computation;

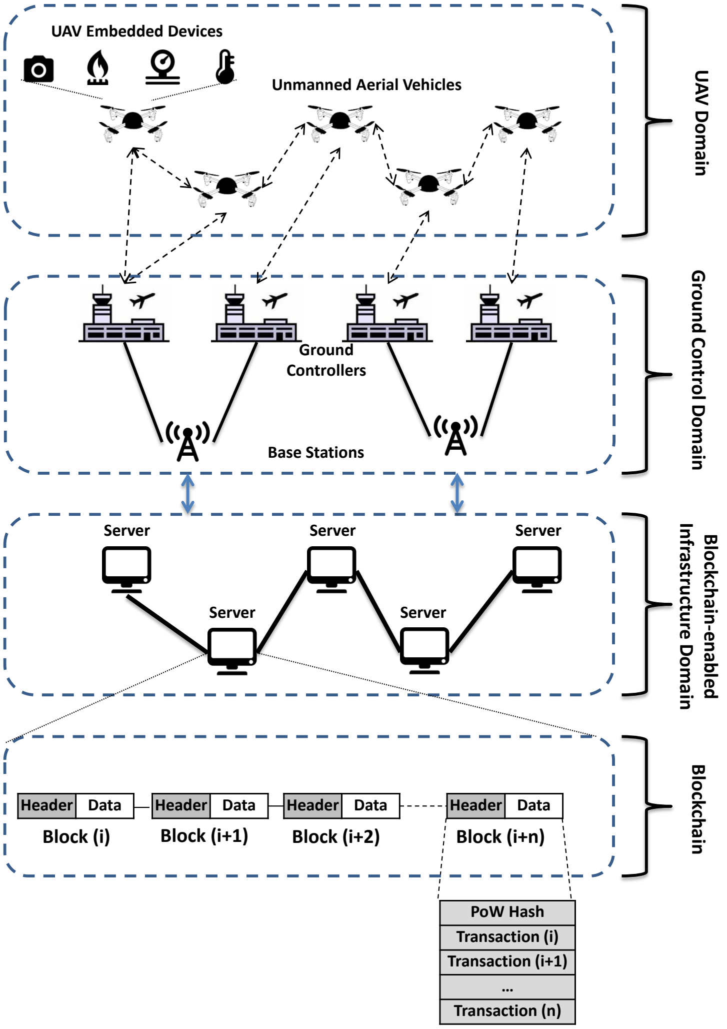

Fig. 2: Proposed Architecture for Blockchain in UAS

Third, Miners selection and generation of blocks; And fourth, the distributed consensus.

1) UAVs Trust Evaluation: The first phase is the Rating generation and uploading: Communicating UAVS have to evaluate the exchanged messages to evaluate their trustworthiness. Firstly, the UAV receiving message divides them into groups $\{M_1; M_2; ...M_j; ..\}$, in which M_j is the group of messages reporting a same event e_j such as "fire detected in position (x,y). However, messages within the same group may not have the same trustworthiness. The ones reported by UAVs close to the event are usually more trustworthy than the ones reported by remote UAVs. Hence, the trustworthiness of a message is given by the following equation [35]:

$$tr_k^j = \alpha + e^{-\beta \cdot Dist_k^j} \tag{1}$$

where tr_k^j is the trustworthiness of a given message belonging to M_j provided by a UAV k. $Dist_k^j$ is the distance separating the originator of the message (reporting UAV) and the position in which the event has occured. α and β represent two predefined weights controlling the lower bound and the update value of message trustworthiness.

Furthermore, tr_k^j= 0 if the UAV k did not generate and report about the event j. Through the use of the following equation, the trustworthiness set TR^j can be obtained by the receiving UAV for event e_j, where $TR^j = \{tr_1^j; tr_1^j...\}$. Based on the trustworthiness set T, afterwards, the UAV can estimate the overall trustworthiness/confidence about an event e following the Bayesian Inference theory [18].

$$P(e/TR) = \frac{P(e) \cdot \prod_{k=1}^{N} P(tr_k/e)}{P(e) \cdot \prod_{k=1}^{N} P(tr_k/e) + P(\bar{e}) \cdot \prod_{k=1}^{N} P(tr_k/\bar{e})} \tag{2}$$

where $\bar{e}$ represents the nonexistence of the event e. $P(trk/e) = trk \cdot P(tr_k/\bar{e}) = 1 - tr_k$. $P(e)$ is the previous probability of a given event e. With $P(e/TR) \in [0, 1]$.

Upon reaching a value of $P(e/TR)$ higher than a predefined threshold TH, the UAV receiving the messages regarding an event e can decide that this event has truly occurred, and hence, it generates positive ratings (+1) on messages reporting this event and vice versa for the events with $P(e/TR) < TH$ (-1).

Last but no least, UAVs periodically send their estimations (ratings) to the close ground control station. The format of these estimations is ($\#UAV_i$; $\#UAV_j$;m_k; rating), where

$\#UAV_i$ and $\#UAV_j$ are the number of UAVs receiving and reporting an event, respectively; m_k is the message's ID; and the evaluation (rating) takes -1 for trusted messages or +1 untrusted messages.

The second phase which consist of the Trust's offsets computation: After receiving the UAVs different ratings, the GCS may face conflicting ratings for a given message, for instance, 8 positive ratings and 5 negative ratings. For our case, weighted aggregation is used to obtain the trust's offset $\in [-1, +1]$ using the following equation:

$$\lambda_k^j = \frac{\varphi_1 \cdot pos - \varphi_2 \cdot neg}{pos + neg} \tag{3}$$

where λ_k^j is the trust's of UAV k based on message j and λ_k^j $\in$ [-1; 1]. pos and neg are the number of positive and negative ratings, whose weights are φ_1 and φ_2, respectively. φ_1 and φ_2 are calculated as follows.

$$\varphi_1 = \frac{K(pos)}{K(pos) + K(neg)}, \varphi_2 = \frac{K(neg)}{K(pos) + K(neg)} \tag{4}$$

Under the assumption that an attacker can only control a minority of the population (UAVs in our case), $K(.)$ is used to control the sensitivity to the minority group of ratings. Finally, the Ground Control Station regroup the different trust offsets in a set θ and tries to include it into the blockchain.

The third phase consisting of Miners selection and generation of blocks: One of the main advantages and challenges at the same time of blockchain is the fully distributed architecture. Hence, miners should be periodically selected so they can generate new blocks of offset. Usually, the selection is based on proof-of-work algorithm. Hence, all peers keep changing the nonce and compute the blocks' new hash values with the newly changed nonce. Afterward, all peers generated hash values are compared with a threshold, the one getting the hash value lower than a threshold is selected as the miner and is able to publish its block. All nodes have the same threshold, which makes nodes with more powerful computation capacity easier to get the right nonce and win the election. On the other hand, to ensure certain fairness the miners selection, the proof-of-stake is also used so that different peers have different hash thresholds, and by consequence different time requirements to generate blocks.

An alternative solution is to use both proof-of-work and proof-of-stake miner selection at the same time as proposed in [35], they propose to take as a stake the sum of the absolute compensations and that the difficulty of completing the proof of work depends on the stake. GCS with more stakes can easily find the nonce and thus be selected and publish its blocks quickly, which guarantees the fast update of the data stored in the blockchain. The following part summarize the proof-of-work and proof-of-stake hybridization:

$$Hash(ID_{RSU}, time, PreHash, nonce) \leqslant S_i \tag{5}$$

where S_i is the hash threshold for GCS_i. And as mentioned above all GCS continuously change their nonce. Thus, once a CS gets the nonce that satisfies the above condition it gets selected. S_i increases while increasing F_i, it is defined as the sum of the absolute values of the trust compensations (offsets):

$$Q_i = Minimum(\sum_{o_k^j \in \theta_i} \left| o_k^j \right|, Q_{max}) \tag{6}$$

θ_i represent the current offset set of the GCS i. Hence, the GCS with higher value of Q_i is likely to be selected and then publish its block. Using this strategy, a huger number of trust evaluations guarantees the fast update blockchain. Q_{max} is the upper bound of Q_i used to ensure the fair miner selection and prevent GCS with high value of Q_i from continuously wining the selection. After publishing its blocks, the GCS selected as a miner clears the elements in θ_i.

Same as all blockchain-based systems, the construction of S_i: S_i is series of binary bits starting by a number of zeros. Here, the relationship between S_i and Q_i is given by the following equation [35]:

$$N_z = int(e^{-(\eta \cdot Q_i + v)}), S_i = 2^{N_m - N_z} - 1 \tag{7}$$

$int(.)$ is a function returning the integer part of the introduced value as a parameter; N_z is the number of zeros with which S_i starts; and N_m is generated hash value depending on the considered hashing function.

The fourth and final phase is the distributed consensus: Upon receiving a miner's block, the server in the blockchain-enable infrastructure domain checks the nonce's validity then add it to the blockchain. However, a given server may receive a large number of blocks simultaneously. Thus, the blockchain may start to fork. To face this problem, a distributed consensus strategy should be used. Servers will chose to fork one block and continue adding new blocks. Afterwards, the fork recognized by the largest number of servers is growing faster than others. In the end, the longest one becomes the distributed consensus of the network and the remaining ones will be removed. Furthermore, the servers will gather their generated blocks in the removed forks and try adding them to the blockchain later. Using this strategy all servers are holding the same copy of the blockchain.

2) Malicious UAVs revocation: In our proposal, Ground Control Station notifies the UAVs with low trust evaluations, therefor they can adjust their behavior accordingly before getting dismissed from all network operations. To this end, two thresholds ($TH_{warning}$ and $TH_{revocation}$) are used such that to punish the UAVs with unwanted behavior, where $TH_{warning} > TH_{revocation}$. UAVs having trust evaluation higher than $TH_{revocation}$ and lower than $TH_{warning}$ are added the a grey list and will be later notified to push them to operate honestly. As for the UAVs with trust evaluation lower than $TH_{revocation}$, they are blacklisted and revoked from all network operations.

IV. Performance Evaluation

To evaluate performance of BUAS, we have implemented its different modules in the NS-3 simulator. The theoretical communication range of UAVs is assumed to be $300m$ radius of the sphere created around their positions. In addition, UAVs are moving following the 3D random Waypoint Mobility Model with roughly $30m$ altitude. Simulated area is considered to be 16 km^2 with 4 Ground Control Stations. Furthermore, we assume that 10 events occur in the 5 randomly distributed critical infrastructures. On the other hand, 10% then 20% of the UAVs are considered malicious reporting fake events. The total simulation duration is 600 sec for each of the 10 runs. We first created a local blockchain on our system, where all the nodes are containers and these containers are created on the same system. Afterwards, to run our simulations we connected every node with each other in NS3 simulation. Another way which we did not use is the "Bitcoin-Simulator" which is developed in NS3 and freely available through: "https://github.com/arthurgervais/Bitcoin-Simulator" We did not use this last solution mainly because we needed more flexibility in managing the different domains of our proposal, something that we could not achieve using Bitcoin-Simulator.

The rest simulation parameters are summarized in Table II:

TABLE II: Simulation parameters.

Parameters	Value
Simulated region (km×km)	4×4
Simulation duration (s)	600
Number of UAVs	[10,100]
UAVs communication range (m)	300
UAVs speed (km/h)	[0,40]
Dishonest UAVs ratio (%)	[10, 20]
α	0.5
β	0.02
TH	0.5
η	0.01
υ	-3
Message size (bytes)	500
Block size (bytes)	5000

In the following we discuss BUAS performance in terms of detection ratio, trust's variation, generated falses when monitoring critical infrastructures, Blockchain generated overhead, and finally UAVs energy consumption with and without our proposal.

Fig. 3 represents the achieved detection ratio when varying the UAVs density in the simulated area for both 10% and 20% malicious UAVs ratio. It depicts that, except for very sparse cases when UAVs cannot monitor each other, BUAS can offer high detection ratios exceeding the 95%. This is mainly due to the efficient majority-based Bayesian Inference trust management technique.

On the other hand, Fig. 4 shows the relation between trust offsets and the ratio of negative ratings for four different K(.) functions ($K(x) = x$, $K(x) = x^2$, $K(x) = x^3$, and $K(x) = e^x$). It depicts that the offsets decrease with the increase of negative ratings ranging between -1 and +1. It is clear that different $K(x)$ may have different effects on trust's offsets. For instance, the cases of $K(x) = x^3$ and $K(x) = e^x$ are less vulnerable compared to $K(x) = x$ and $K(x) = x^2$ when the negative ratings ratio is less than 40%.

To show the importance of BUAS for securing critical infrastructures we concentrated all event withing the 5 critical infrastructures, and measured the generated positive and negative false of BUAS compared to UNION [36] and RPM [37] when detecting fake events. The results show that the blockchain-based strategy of BUAS have clearly reduced the generated errors compared to the classical solutions (without blockchain) with less than 3% false negative and less than 1.5 % false positive in the worst cases. Whereas, both UNION and RPM generate higher errors that cannot be accepted for critical infrastructures cases (see Fig. 5 and Fig. 6).

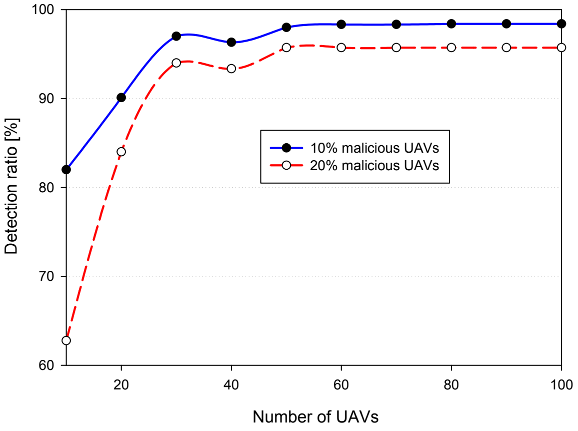

Fig. 3: Detection ratios of BUAS for different dishonesty ratios

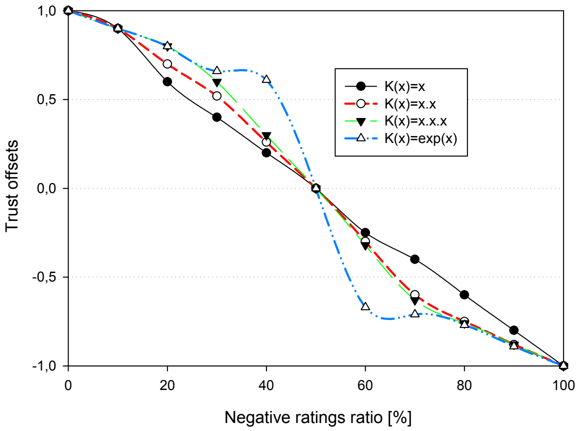

Fig. 4: Trust's offsets in respect of the ration of negative ratings.

The use of blockchain in BUAS involves more exchanged messages betwwen the different domains. Fig. 7 shows the generated overhead for different UAVs densities. It shows that even for the very dense scenario (100 UAVs), generated overhead did not exceeded the 5Kb, which does not affect the network operation because of the very small exchanged packets.

In addition, when pushing the inter-UAV trust evaluation towards Blockchain, this will not affect the UAVs energy consumption compared to the in-UAV complex computations. Fig. 8 shows that the energy consumption is almost the same with and without BUAS, and this is one of the most important advantages of BUAS lightweight trust establishment solution, especially for the case of energy-restricted devices like UAVs.

To evaluate the scalability of BUAS at the level of the

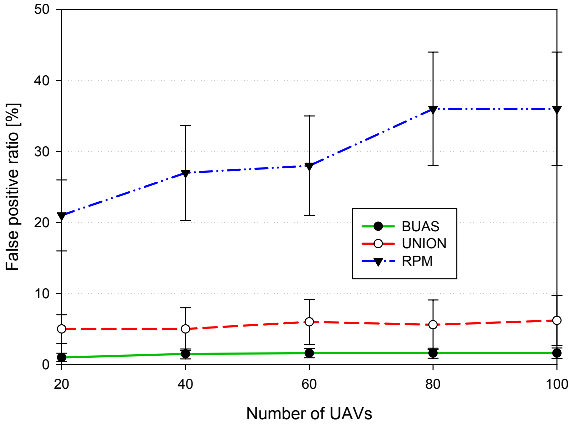

Fig. 5: Generated false positive of BUAS compared to both UNION and RPM.

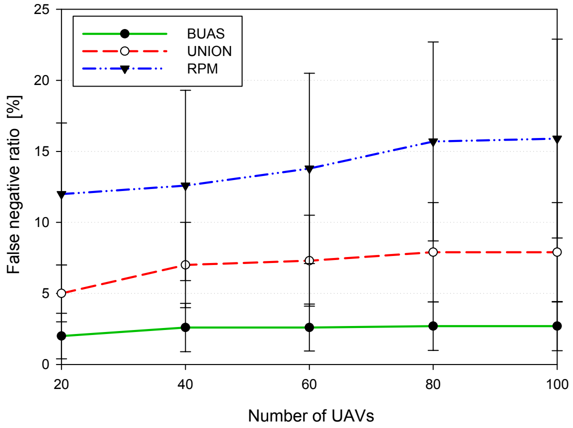

Fig. 6: Generated false negative of BUAS compared to both UNION and RPM.

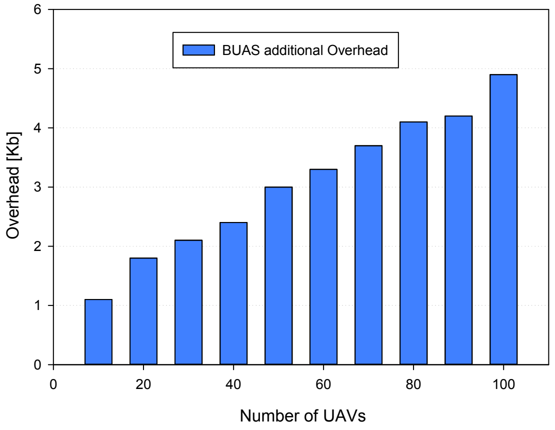

Fig. 7: Generated overhead due to Blockchain usage.

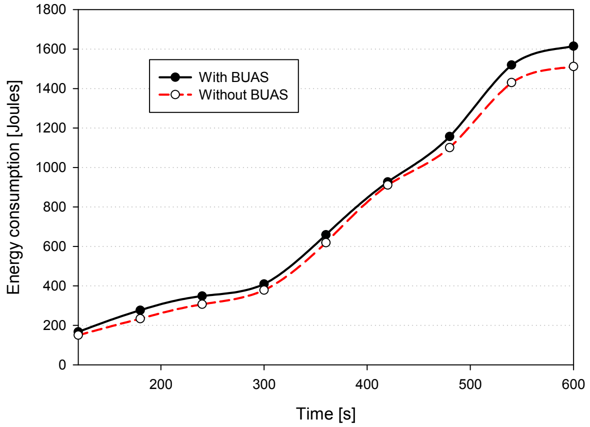

Fig. 8: UAVs average consumed energy with and without BUAS.

'Blockchain-enabled Infrastructure Domain', we performed two tasks: First, we fixed the GCSs messaging rate at 50 messages per second, and second, we increased both the number of GCSs and the number of servers. Fig. 9 represents the communication throughput in respect of the number GCSs. It shows that the number of validated transactions increased with the increase of the GCSs (miners) until reaching a stability with more than 15 miners which are enough to timely validate all coming transactions. This is explained by the fact that more than 15 GCSs are required to cover all the simulated area. Hence, all transactions are received by GCSs in a timely manner without any UAVs mobility-related delay.

On the other hand, Fig. 10 represents the network latency while changing the number of GCSs. It shows that with the increase in number of GCSs, the latency in the network increases as well. Overall, we can say that the use of PoW affected negatively the system scalability due to its high time and computation complexity.

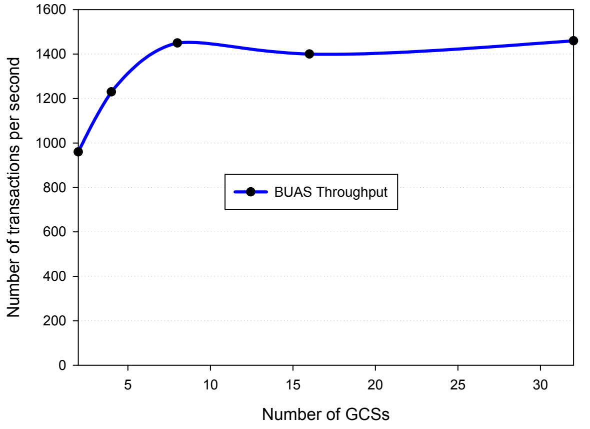

Fig. 9: Throughput-related performance of BUAS.

V. Conclusions

Critical infrastructures such as nuclear plants, transmission, and distribution grids, are widely deployed nowadays. In addition, these systems have become more prone to coordinated cyber-physical attacks. This work proposes "BUAS"

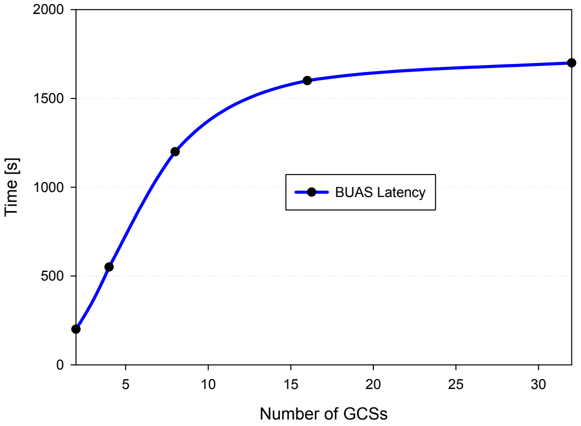

Fig. 10: Latency-related performance of BUAS.

a blockchain-based inter-UAV trust evaluation solution for securing critical infrastructures. Our proposal is a domain-based architecture involving all the Unmanned Aerial Systems components together with the blockchain-enabled servers to ensure the lightest and most efficient possible solution securing critical infrastructures. Simulation results show that with high detection ratios, low energy consumption, and reduced overhead, BUAS can offer very accurate decisions which is a requirement especially for the critical infrastructures case.

As a future work, we plan to extend BUAS with more modules ensuring other needs such as Geofencing and privacy protection in UASs. In addition, another lightweight consensus algorithm would clearly enhance the overall performance and this will also be our future work.

References

[1] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3949–3963, 2016.

[2] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (fanets): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, 2013.

[3] G. Pajares, "Overview and current status of remote sensing applications based on unmanned aerial vehicles (uavs)," *Photogrammetric Engineering & Remote Sensing*, vol. 81, no. 4, pp. 281–330, 2015.

[4] D. Floreano and R. J. Wood, "Science, technology and the future of small autonomous drones," *Nature*, vol. 521, no. 7553, p. 460, 2015.

[5] D. Avola, G. L. Foresti, N. Martinel, C. Micheloni, D. Pannone, and C. Piciarelli, "Aerial video surveillance system for small-scale uav environment monitoring," in *Advanced Video and Signal Based Surveillance (AVSS), 2017 14th IEEE International Conference on*. IEEE, 2017, pp. 1–6.

[6] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson, "Security authentication system using encrypted channel on uav network," in *Robotic Computing (IRC), IEEE International Conference on*. IEEE, 2017, pp. 393–398.

[7] K. Singh and A. K. Verma, "A fuzzy-based trust model for flying ad hoc networks (fanets)," *International Journal of Communication Systems*, vol. 31, no. 6, p. e3517, 2018.

[8] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial wifi-based uavs from common security attacks," in *Military Communications Conference, MILCOM 2016-2016 IEEE*. IEEE, 2016, pp. 1213–1218.

[9] M. Pilkington, "11 blockchain technology: principles and applications," *Research handbook on digital transformations*, p. 225, 2016.

[10] F. Ahmad, C. A. Kerrache, F. Kurugollu, and R. Hussain, "Realization of Blockchain in Named Data Networking-based Internet-of-Vehicles," *IT Professional*, 2019, doi:10.1109/MITP.2019.2912142 [In Press].

[11] H. Wu and C. Tsai, "Toward Blockchains for Health-Care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy in Data Sharing," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 65–71, July 2018.

[12] D. Miller, "Blockchain and the Internet of Things in the Industrial Sector," *IEEE IT Professional*, vol. 20, no. 3, pp. 15–18, May 2018.

[13] G. Perboli, S. Musso, and M. Rosano, "Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases," *IEEE Access*, vol. 6, pp. 62 018–62 028, 2018.

[14] M. Campion, P. Ranganathan, and S. Faruque, "Uav swarm communication and control architectures: a review," *Journal of Unmanned Vehicle Systems*, no. 0, pp. 1–14, 2018.

[15] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "Uav-enabled intelligent transportation systems for the smart city: Applications and challenges," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 22–28, 2017.

[16] F. Flammini, C. Pragliola, and G. Smarra, "Railway infrastructure monitoring by drones," in *2016 International Conference on Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles & International Transportation Electrification Conference (ESARS-ITEC)*. IEEE, 2016, pp. 1–6.

[17] P. Samczynski, M. Malanowski, G. Krawczyk, J. Kulpa, and M. Żywek, "Passive radar as a part of critical infrastructure protection system," in *2018 International Conference on Radar (RADAR)*. IEEE, 2018, pp. 1–5.

[18] G. E. Box and G. C. Tiao, *Bayesian inference in statistical analysis*. John Wiley & Sons, 2011, vol. 40.

[19] K. P. Valavanis, *Advances in unmanned aerial vehicles: state of the art and the road to autonomy*. Springer Science & Business Media, 2008, vol. 33.

[20] H. Zhang, Y. Qi, J. Wu, L. Fu, and L. He, "Dos attack energy management against remote state estimation," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 383–394, 2018.

[21] J. Chen, Z. Feng, J.-Y. Wen, B. Liu, and L. Sha, "A container-based dos attack-resilient control framework for real-time uav systems," *arXiv preprint arXiv:1812.02834*, 2018.

[22] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Transactions on Automatic Control*, vol. 60, no. 10, pp. 2831–2836, 2015.

[23] İ. Bekmezci, E. Şentürk, and T. Türker, "Security issues in flying ad-hoc networks (fanets)," *Journal of Aeronautics and Space Technologies*, vol. 9, no. 2, pp. 13–21, 2016.

[24] D. Radu, A. Cretu, B. Parrein, J. Yi, C. Avram, and A. Aştilean, "Flying ad hoc network for emergency applications connected to a fog system," in *Advances in Internet, Data & Web Technologies*, L. Barolli, F. Xhafa, N. Javaid, E. Spaho, and V. Kolici, Eds. Cham: Springer International Publishing, 2018, pp. 675–686.

[25] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing uav communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1376–1389, Feb 2019.

[26] K. Singh and A. K. Verma, "A trust model for effective cooperation in flying ad hoc networks using genetic algorithm," in *International Conference on Communication and Signal Processing (ICCSP)*, April 2018, pp. 0491–0495.

[27] K. Singh and A. K. Verma, "FCTM: A novel fuzzy classification trust model for enhancing reliability in flying ad hoc networks (fanets)," *Ad Hoc Sensor Wireless Networks*, vol. 40, pp. 23–47, 2018.

[28] X. Yuan, Z. Wei, Z. Feng, and W. Xu, "Trust connectivity analysis in overlaid unmanned aerial vehicle networks," in *17th International Symposium on Communications and Information Technologies (ISCIT)*, Sep. 2017, pp. 1–6.

[29] D. Rudinskas, Z. Goraj, and J. Stankūnas, "Security analysis of uav radio communication system," *Aviation*, vol. 13, no. 4, pp. 116–121, 2009.

[30] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*. IEEE, 2012, pp. 585–590.

[31] V. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defences," in *Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on*. IEEE, 2016, pp. 164–170.

[32] C. L. Krishna and R. R. Murphy, “A review on cybersecurity vulnerabilities for unmanned aerial vehicles,” in *Safety, Security and Rescue Robotics (SSRR), 2017 IEEE International Symposium on*. IEEE, 2017, pp. 194–199.

[33] K. Wesson and T. Humphreys, “Hacking drones,” *Scientific American*, vol. 309, no. 5, pp. 54–59, 2013.

[34] A. Y. Javaid, F. Jahan, and W. Sun, “Analysis of global positioning system-based attacks and a novel global positioning system spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation,” *Simulation*, vol. 93, no. 5, pp. 427–441, 2017.

[35] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, “Blockchain-based decentralized trust management in vehicular networks,” *IEEE Internet of Things Journal*, 2018.

[36] E. Barka, C. A. Kerrache, N. Lagraa, A. Lakas, C. T. Calafate, and J.-C. Cano, “Union: a trust model distinguishing intentional and unintentional misbehavior in inter-uav communication,” *Journal of Advanced Transportation*, vol. 2018, 2018.

[37] C. A. Kerrache, E. Barka, N. Lagraa, and A. Lakas, “Reputation-aware energy-efficient solution for fanet monitoring,” in *Wireless and Mobile Networking Conference (WMNC), 2017 10th IFIP*. IEEE, 2017, pp. 1–6.