# Security in networks of unmanned aerial vehicles for surveillance

**Abstract**

Unmanned aerial vehicles (UAVs) can support surveillance even in areas without network infrastructure. UAV networks raise security challenges because of its dynamic topology. The current work proposes a technique for maintaining security in UAV networks in the context of surveillance, by corroborating information about events from different sources. In this way, UAV networks can conform peer-to-peer general knowledge inspired by the principles of blockchain, based on trust policies. This method uses a secure asymmetric encryption with a pre-shared list of official UAVs. This work addresses the misinformation detection when an official UAV is physically hijacked. The novel agent-based simulator called ABS-SecurityUAV shows the efficacy of the proposed approach.

*Keywords:* agent-based framework, agent-based simulator, agent-based social simulation, electric car, electric vehicle, multi-agent system

## 1. Introduction

Vehicular ad-hoc networks (VANETs) are difficult to maintain because of the rapidly and dynamic change of the network topology, the short connection durations, and the frequent disconnections [1]. Some of the challenges are the (a) trust and information verification, (b) the key distribution for maintaining secure channels, and (c) the forwarding algorithms for finding the best route. Some of the most common attacks are (1) identity and geographical position revealing, (2) Denial of Service (DoS), (3) Sybil attack creating the illusion of several cars with the same ID, (4) Spam to increase the latency of network transmissions, (5) Man in the Middle (MiM), in which a node listens and injects false information in the communication between two nodes, (6) black hole attack, by always declaring having the shortest path, (7) cheating with position info.

Unmanned aerial vehicles (UAVs) also usually use ad-hoc networks in the absence of network infrastructure. In particular, UAVs have been especially useful for supporting surveillance. In this context, UAVs normally cooperate for achieving an effective surveillance, like in the work of [2] that proposed a game-based approach with coordinated motion for optimal coverage, sensor observation, and cooperative information fusion. UAV have been used for different surveillance purposes such as the efficient control of a moving crowd [3] and the continuous inspection with UAVs that are dynamically charged with an algorithm for maintaining the structural inspection [4]

The communication of UAV networks varies as described in a recent review about classifications and architectures [5]. In VANETS and more concretely in UAV networks, it is necessary to detect the malicious behaviors. In particular, [6] proposed to use trust management as an alternative to cryptography to avoid excessive energy and processing consumption. Trust management is based in the assumption that malicious behaviour persist. However, malicious nodes can avoid this detection by by behaving intelligently. Their approach uses an UAV-assisted detection mechanism that was able to rapidly detect misbehaviors of network nodes. In addition, [7] proposed an authentication system for using and encrypted channel for protecting UAVs from cyber attacks. They tested their approach with commercial UAVs showing its utility. Agent-based simulators (ABSs) have been useful for testing security strategies in different kinds of networks, like ABS-TrustSDN [8], which allowed to manage trust on network nodes in software-defined networks.

Blockchain improves the security of distributed datasets by sharing and checking the information by the different implied parties [9]. In this context, blockchain is a defined as a collaborative security foundation to guarantee the veracity of information. The survey of [10] describes different kinds of security threats in blockchain systems and some security enhancement solutions for them.

In this context, the current work proposes to use a security approach based on the blockchain principles, for detecting suspicious event reports in surveillance. This is useful for conforming the distributed trust management about each UAVs. In this manner, the current work can discriminate UAVs that may have been compromised. The current approach is illustrated with a novel ABS.

The remainder of the paper is organized as follows. The next section presents work related to the current approach for introducing the context of the proposed contribution. Section 3 presents the novel security method for

surveillance from UAVs. It defends from official UAVs that may be officially compromised, and is illustrated with a novel ABS. Section 4 presents the experimentation of the current approach with the ABS for assessing the current approach. Concluding remarks are in section 5, including some possible future lines of research.

## 2. Related work

The connectivity in VANETs depends whether the vehicles are cooperative to obtain and end-to-end communication. In this line of work, [11] analyzed the effect of non-cooperative vehicles on path connectivity in VANETs, and proposed to use UAVs for assisting the connectivity of VANETs. One subtype of VANETs are the UAV networks. The survey of [12] analyzes the existing application of UAVs for civil applications from a communication viewpoint. UAVs can be used for civil applications such as natural disaster monitoring, border surveillance, emergency assistance, search and rescue missions, delivery of goods and construction. They conclude that communication security is essential for guaranteeing the proper communication among UAVs. All these works motivate the current work about improving the security of UAVs when using these for surveillance of controlled areas.

Several works focus on improving security in communications with UAVs. For instance, [13] presented a mechanism for guaranteeing secure communications. In particular, they used an iterative algorithm that guaranteed convergence. They applied a water-filling-based solution to make the algorithm computationally efficient. Their simulation results showed that their approach enhanced secrecy in comparison to an alternative static solution. In addition, [14] analyzed the intrusion detection focusing on the false positive rates. They applied a Bayesian game model for accurately detecting attacks with low false positive rates. Their simulation results corroborated that they achieved their goal of this reliable detection. Moreover, [15] studied the communication security in UAVs. More concretely, they presented low-cost implementation of the GPS spooling attack and the WiFi attack, which effectively compromised some UAVs. They also proposed some solutions for defending from these attacks. However, these works did not guarantee security in surveillance in case an official UAV was compromised.

UAVs has assisted the communication of other networks. For example, the work of [16] analyzes the airborne network assisted applications based on the low-altitude UAVs combined with WLAN mesh networks (WMNs). Since

WMNs were prone to routing attacks according to their previous analyses, they proposed the position-aware, secure and efficient mesh routing approach (PASER). Their experimentations showed that this approach was secure from the corresponding routing attacks. Nevertheless, this work did not study the possible vulnerabilities raised by a physical hijacking of an UAV in the surveillance context.

Some works present mechanisms for achieving surveillance for UAVs. For example, [17] proposed a mechanism for achieving persistent surveillance with UAVs considering dynamic aspects of the environment. Their approach was designed for being tolerant to UAV failures. In addition, [4] proposed an algorithm for maintaining a permanent and continuous surveillance infrastructure of UAVs. In their approach, UAVs were coordinated for automatically charging and flying in a balanced way However, their approach did not consider security issues such as the fact that an UAV could be physically attacked and compromised for adopting a malicious behavior.

On the whole, UAVs have a great diversity of applications and in some cases they need to rely on their own network built upon vehicular-to-vehicular (V2V) instead of vehicular-to-infrastructure (V2I) ones. Surveillance is one of the most common applications, and the literature agrees on the importance of security in UAV networks. However, to the best of our knowledge, the literature lacks the appropriate methods for preventing from physical hijacking of one official UAV in the context of distributed surveillance of UAVs. The next section presents the current approach that covers this gap of the literature.

## 3. Method for detecting compromised UAVs in surveillance

### *3.1. Overview and assumptions*

In general, this approach is designed to be especially applied in borders with low transit of people (e.g. in natural borders such as mountains). Figure 1 shows an overview of the current method for detecting compromised UAVs in the surveillance context. This approach addresses the distributed management of an UAV network for detecting people in the surveillance of a particular wide area. This method is based on the assumption that normally each person crossing a controlled are is observed by several UAVs, although not necessarily. This method is inspired by blockchain principles. All the observations are propagated, and each UAV keeps track of the IDs of all the authenticated official UAV observers.

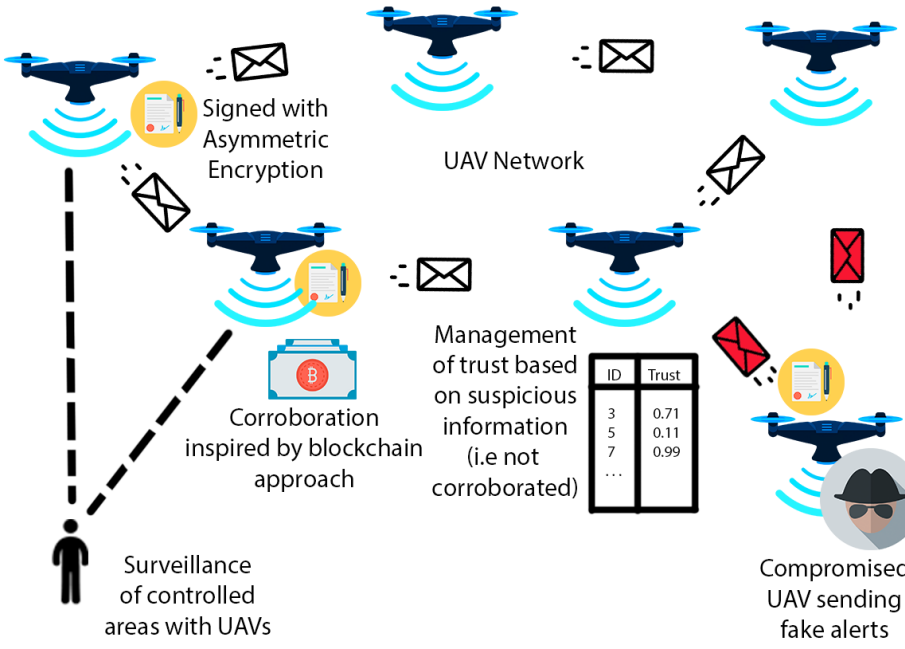



Figure 1: Overview of the detection of compromised UAVs in surveillance

In the current approach, all the UAVs should be officially registered before the UAV fleet starts surveillance. Each UAV has a list of the public keys of all the UAVs for signing each message and securely sending it to all UAVs avoiding MiM attacks by compromised UAVs. In this way, the UAVs can sign their messages with asymmetric encryption. The messages are forwarded over the UAV network, and each UAV can know a list of the observers of a particular person.

An official UAV could be physically captured and compromised. In this case, this UAV could send fake alerts properly signed in order to disturb the correct functioning of the UAV network. However, the compromised UAV cannot alter its identity for impersonating other agents, due to the required asymmetric encryption for authenticating senders.

Each UAV records the IDs of all the direct observers from the messages, and checks whether each intruder person is corroborated by at least several observers. However, UAVs can have a distributed management of trust in each UAV. This trust would consider the percentage of times a UAV was the only one in observing an intruder event, penalizing the trust on it. It also

considers the number of times it sent corroborated information. It would weight as more relevant the recent cases but it would also consider the whole history.

In very large areas, funds cannot usually cover an enough amount of UAVs to provide seamless communications. The current approach assumes that communications are usually disrupted, in the sense that an UAV may need to wait after generating a message until it can actually send the message. In particular, each UAV will wait until another UAV is enough close to actually communicate with it. Notice that this approach also assumes that UAVs cannot perform long-distance communications in order to save energy for having safe and relative long flights. In a similar way, when a UAV receives a message, it stores the received information for forwarding it to different UAVs for an established duration.

The current approach is illustrated with an ABS with several agent types. One agent type is the people for impersonating the intruders. Another agent type is the UAVs. In addition, UAVs have an internal flag that determines whether they are compromised.

### *3.2. Internal functioning of the security approach illustrated with an ABS model*

The current approach is illustrated with the novel ABS called ABS-SecurityUAV. This ABS was implemented with NetLogo for its support and utility for representing mobile ad hoc networks [18]. The model of this ABS was organized in three modules: the "Setup" methods (initially executed at the beginning of the simulation); the "Go" methods (periodically invoked in each frame of the simulation); and the "Measure" methods (used for updating the measures of the charts). This structure of modules was designed considering the common metrics for evaluating agent-oriented architectures [19] for reducing the coupling between modules and increasing the cohesion inside each of them. In addition, this ABS was developed considering the principles of PEABS (a process for developing efficient agent-based simulators) [20] for achieving efficient simulations.

In the Setup methods, UAVs are initialized considering the number entered by the user. One or several of these are compromised taking into account the number indicated by the user. These UAVs are initially located in a different place from the other UAVs, simulating that these are physically hijacked. Then, intruders are initialized if the user indicates so.

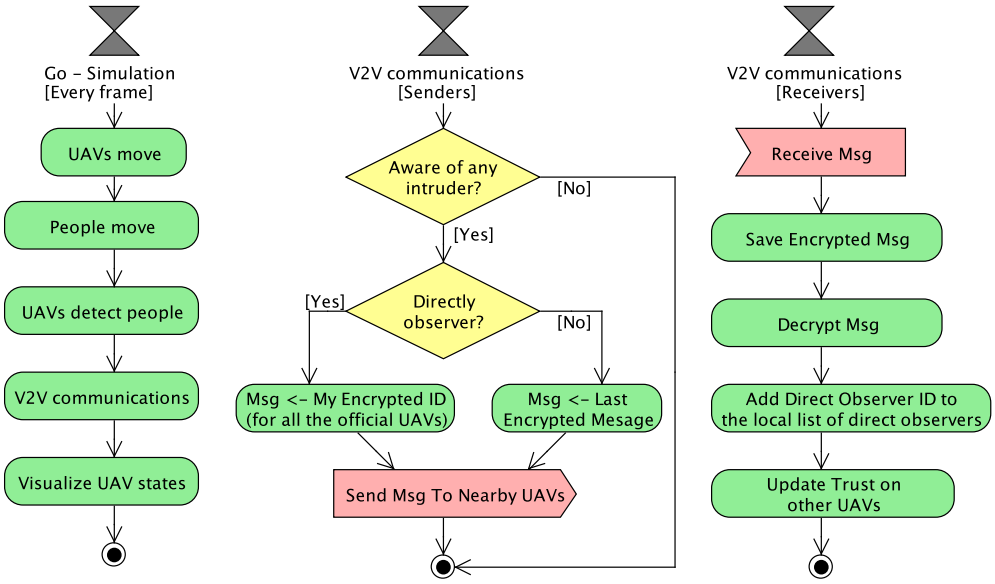



Figure 2: Block diagram of an excerpt of the Go methods of ABS-SecurityUAV

Regarding the Go methods, Figure 2 shows the block diagram of their most relevant part. The main method is shown in the left side. Firstly, both UAVs and people move. The former ones use a variable nondeterministic approach, while people mainly aim at crossing a controlled area following a specific direction with only slight variations. Then, UAVs detect whether any person is near. After this, V2V communications are simulated. Finally, the UAV states are visualized considering the color notation described in section 3.3 and showing some additional information in their labels. The block diagram also determines the V2V communications considering separately the perspectives of senders and receivers. UAVs communicate different messages regarding whether they have directly observed the intruder or they know it from other. They respectively encrypt a message for all the official UAVs or forward the received encrypted message. They only communicate with nearby UAVs given the energy restrictions. The receptor UAVs save the encrypted message for later forwarding it. They decrypt its content for updating their local list of direct UAV observers to update their trust on each UAV.

UAVs have a private key so they can authenticate their identity with

asymmetric encryption. Each time an UAV observes an event (e.g. a person crossing the frontier), it communicates to its neighbors. Then, the neighbors transmit this information to other neighbors recursively and so on. Each UAV continues moving and keep transmitting the message to new UAVs for a specific time period. The timeout of direct observers and the timeout of UAVs forwarding messages are established with two different input parameters. In order to simulate the timeouts, each UAV has two internal variables that determine the last times in which respectively it observed a person and it was alerted by another UAV.

In the trust management, if several UAV neighbors have observed the same intruder event, they can corroborate the information. The information that is observed by several UAVs is considered true. The information that is only observed by one UAV is considered true but suspicious. The UAV that reports suspicious information is penalized and the neighbors will gradually lose trust on this UAV. The neighbors of a compromised UAV might detect their malicious behavior of creating false information, when it continuously sends suspicious information. In order to keep track of the original UAV observers from which an UAV has received messages, the latter keeps an updated list of the IDs of these original observers. It is worth mentioning that the user can enter an input parameter indicating the minimum number of direct observers for trusting information. This input parameter is set to two by default, but the user could change this value.

Given the assumption that there is not enough UAVs to cover all the area, we have decided to use a strategy that is difficult to be predicted by intruders. If UAVs moved deterministically, then the intruder could plan a route that avoids all the UAVs observation areas. Hence, we decided that in this approach UAVs move in a nondeterministic way, avoiding to be predicted by intruders. This UAV motion also has the advantage that each UAV has contact with many other UAVs. In this way, when a UAV starts having a malicious behavior for being hijacked, many other UAVs would notice conforming a distributed corroborated detection of the hijacked UAV, in order to exclude its information and alert the official services about it. The nondeterministic decisions were implemented following TABSAOND (a Technique for developing ABS Apps and Online tools with Nondeterministic Decisions) [21]. In this way, a probability was assigned to the decision of changing the direction, and then this decision was simulated by comparing a random number with the threshold obtained from this probability. In addition, the rotation angle was calculated nondeterministically with certain

limits, as Equation 1 shows:

$$\alpha = \begin{cases} r_f(\beta) - (\beta/2), & \text{if } r \leq p_r \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

where $\alpha$ is the angle of rotation (being zero going straight, a positive number turning right, and a negative turning left), $\beta$ is the maximum angle of rotation, $r_f(x)$ is a random function that returns a real number between zero and the $x$ parameter, $r$ is a random real number in the [0, 1] interval, and $p_r$ is the probability of changing the direction of the UAV.

The speed of UAVs was constant. The same formula was used for simulating the movement and direction changes of each person, but its maximum angle of rotation was much lower, so their path was almost straight. The speed of the person was also indicated by a different variable from the one for UAVs.

The methods of the Measure module allows the simulator to present the evolution of respectively (a) the percentage of indirectly alerted UAVs considering all the UAVs (referred as $a_p$ in equation 2), (b) the percentage of alerted UAVs that trust the messages considering only the alerted UAVs (denoted as $t$ in equation 3), (c) the percentage of UAVs that directly observed an intruder ($d_p$ in equation 4), and (d) the average number of direct observer UAV IDs stored locally in each alerted UAV ($ids$ in equation 5). Equations 2-5 respectively define these metrics:

$$a_p = a/n \tag{2}$$

$$t = a_t/a \tag{3}$$

$$d_p = d/n \tag{4}$$

$$ids = \frac{\sum_{x \in A} |l_x|}{a} \tag{5}$$

where $a$ is the number of UAVs alerted by other UAVs, $n$ is the total number of UAVs, $a_t$ is the number of UAVs that trust the information received by other UAVs about an intruder, $d$ is the number of UAVs that directly observed and reported an intruder, $A$ is the set of all the alerted UAVs, and $l_x$ is the list of direct UAV observer IDs stored locally in the UAV $x$.

The hijacked UAVs move as any other UAVs. The only difference is that they continuously report fake alerts of intruders. Their goal is to make the fleet of UAVs report false alarms, so that the system loses credibility and users may start ignoring it. In this way, a real intruder could go through the controlled area when UAV alarms are ignored.

### *3.3. User interface of the novel ABS-SecurityUAV*

Figure 3 shows the user interface (UI) of ABS-SecurityUAV. In the left side, user can enter certain numeric input parameters in the corresponding input fields. The user can indicate the number of UAVs in the simulation. They can also indicate the number of compromised UAVs and the number of people crossing the controlled area, to test different scenarios. They can also indicate the time-out duration for forwarding alert messages through V2V communications in the "duration-v2v" parameter. In addition, the "duration-alert" determines the time-out duration while a direct observer transmit its message to the nearby UAVs. Further, the "trust-threshold" parameter indicates the number of direct UAV observer IDs necessary for trusting the information. For example, two would indicate that at least two IDs are necessary for corroborating the information.

The UI has two buttons respectively labeled as "setup" and "go". The former one allows users to establish the initial state of the simulation using the parameters indicated in the input number fields. The latter button allows both running and pausing the simulation evolution.

UI shows a graphical representation of the locations and information of the UAVs in a wide square area, as shown in the right side of Figure 3. UAVs are represented with an airplane icon. The colors of UAVs represent different states. Blue represents the default state of flying without detecting any person. A red UAV means that it has directly observed a person. A green UAV represents that it has received a message of alert from another UAV regardless this was a direct observer or was indirectly alerted. In addition, each UAV shows a list of the direct UAV observer IDs from which it has received an alert. This distributed information was inspired by blockchain principles for corroborating information.

In addition, ABS-SecurityUAV shows some charts in the UI for representing the evolution of some global measurements in the simulation evolution. Figure 4 shows these charts for a simulation execution example. The upper chart shows the evolution of the percentage of direct observers reporting a

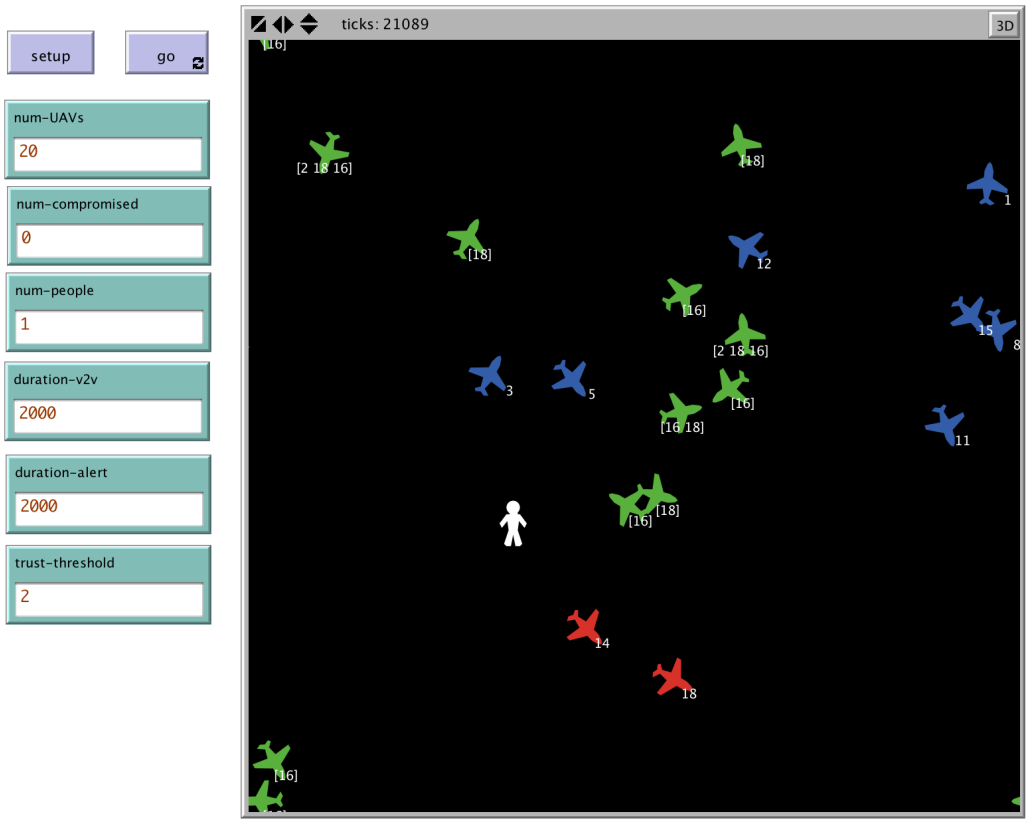
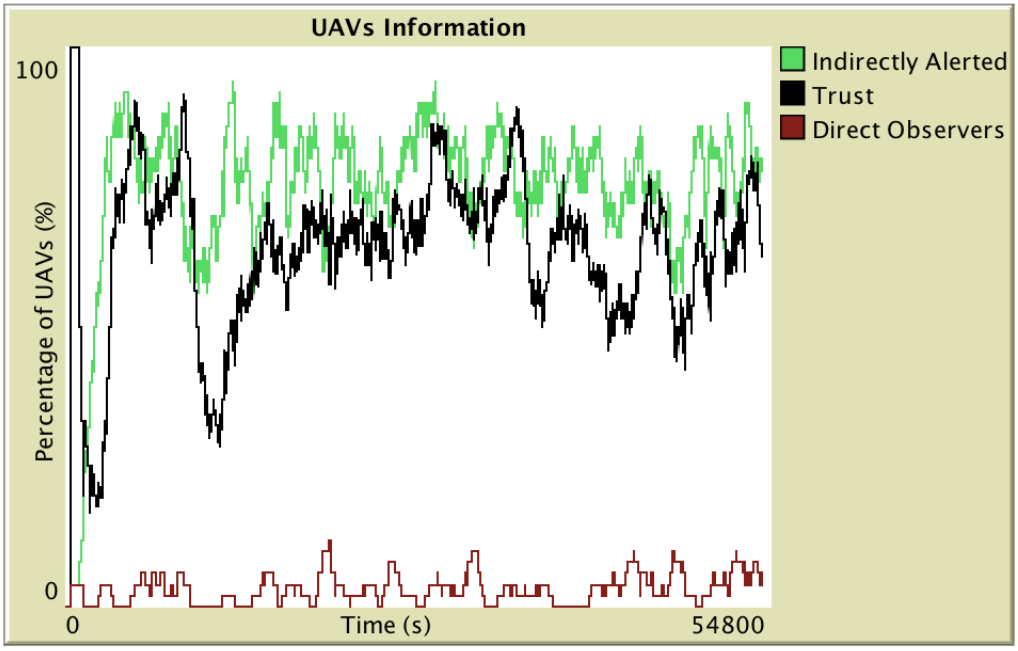



Figure 3: Main part of the user interface of ABS-SecurityUAV



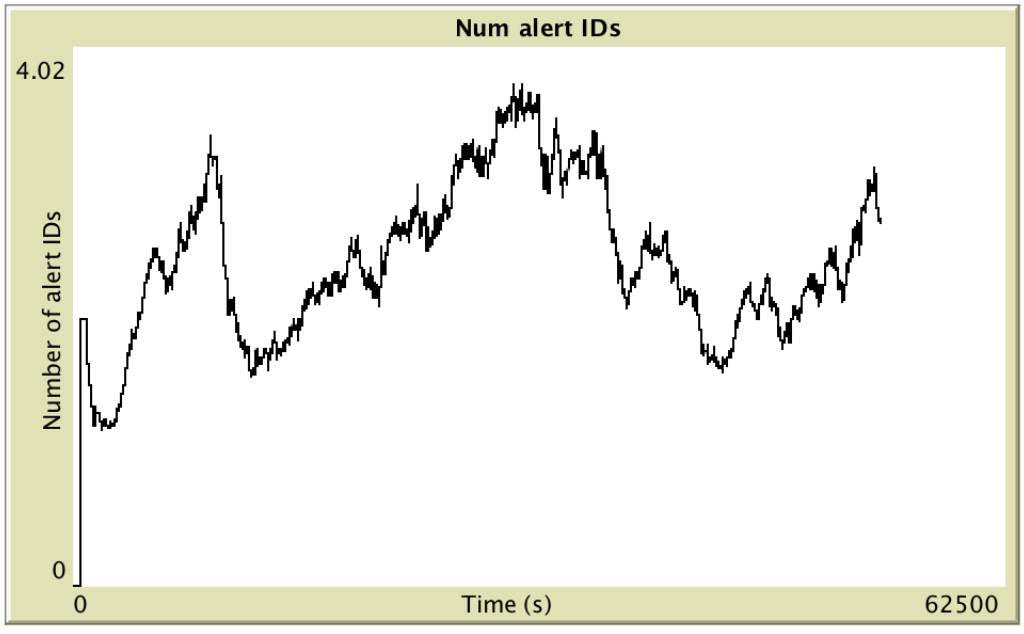




Figure 4: Charts of the user interface of ABS-SecurityUAV

person detection. It also presents the evolution of the percentage of UAVs indirectly alerted in the simulation. This chart also represents the evolution of average trust on a given person detection based on the local corroborations in each UAVs. The lower chart represents the number of alert IDs considering only the UAVs that have been alerted.

## 4. Experimentation

In order to assess the current approach, we performed several simulations with 100 UAVs. We set a time out duration of 1000 s for both V2V communications and for transmitting direct observations. The trust threshold was two indicating that at least two UAVs were necessary for corroborating the information. Firstly, we run simulations for an scenario in which we assumed that a real-person was crossing the controlled area. This scenario had one simulated person and zero compromised UAVs. In a second scenario, we simulated the existence of one compromised UAV sending false alerts without any person crossing the controlled area.

Figure 5 shows the results in the scenario in which a real person was crossing the controlled area. This chart shows the percentage of UAVs that were aware of this human intruder under the label "indirectly alerted". These UAVs did not directly observed the intruder, but they received the information. One can observe that this amount gradually increased for the occurring event, and reaches high values in the interval 90-100%. Thus, the information spread worked properly in true positives (i.e. when an intruder entered the controller area) according to the results. The percentage of alerted UAVs that trust this information reaches initial values in the interval 40-80%, when there were several direct observers. The variability of initial period was probably due to the small sample of alerted UAVs, which reflected big changes with each change in an UAVs. When the simulation continues, one con observe that trust increased and became stable around 90%. The chart also presents the percentage of UAVs that directly observed the intruder. One can observe that even with a relative small percentage (i.e. in the 0-8% interval), the distributed trust properly coincided the reality with high values (around 90%).

Figure 6 shows the same information as in the previous chart, but in the scenario without any real intruder. An UAV simulated to be compromised, alerting about a false intruder detection. This false information was spread to the UAVs reaching the interval 90-100% of indirectly alerted UAVs at the

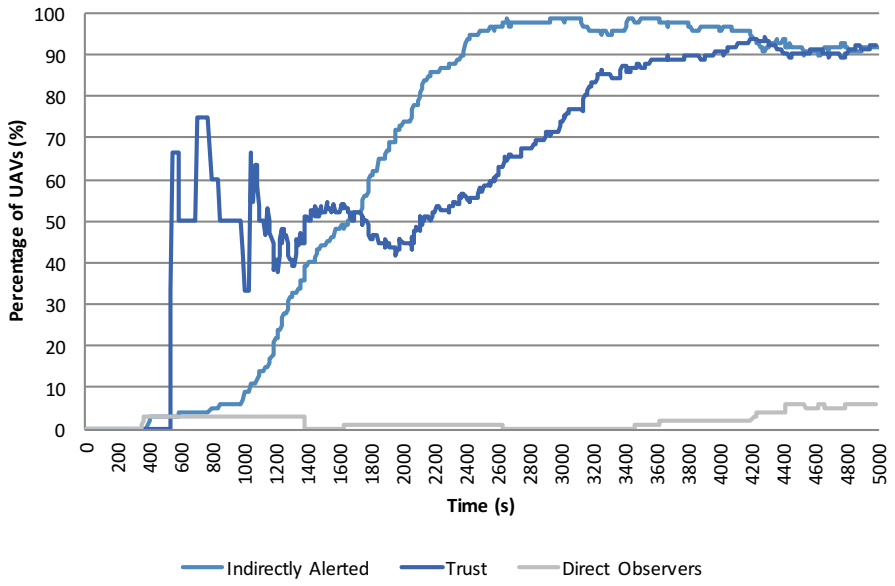



Figure 5: Results when a person was crossing the controlled area

end of the simulation. However, this chart shows that the trust remained as zero in the whole evolution. This information was never completely trusted, as it was never corroborated by any other direct observer. In fact, the chart also reveals that there was only one direct observer (the UAV with malicious behavior) along all the simulation. Therefore, the current approach properly detected the misbehavior of the compromised UAVs when alerting about a false event.

Figures 7 and 8 show the average number of the direct UAV observer IDs known by each alerted UAV. Since only the alerted UAVs were considered for this average, the least positive value was one because each UAVs was alerted at least by one. In case, there is not any alert, then the simulator presents the zero value. The difference between both charts is that Figure 7 presents the results of a simulation with a real intruder, while Figure 8 shows the results of a simulation without any real intruder and a compromised UAV faking alerts. One can observe that the real person was initially detected with an evolving average within [1.5, 2.0] interval. Then, when most UAVs were alerted, the propagation of the real observer alerts was spread, gradually increasing the number of UAV IDs. By contrast, in the case of fake alerts by

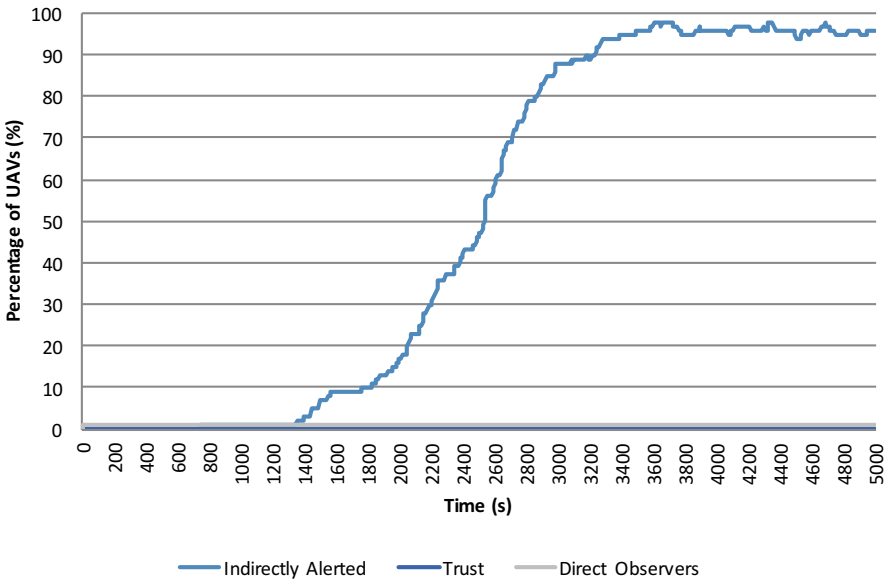



Figure 6: Results when an UAV was compromised

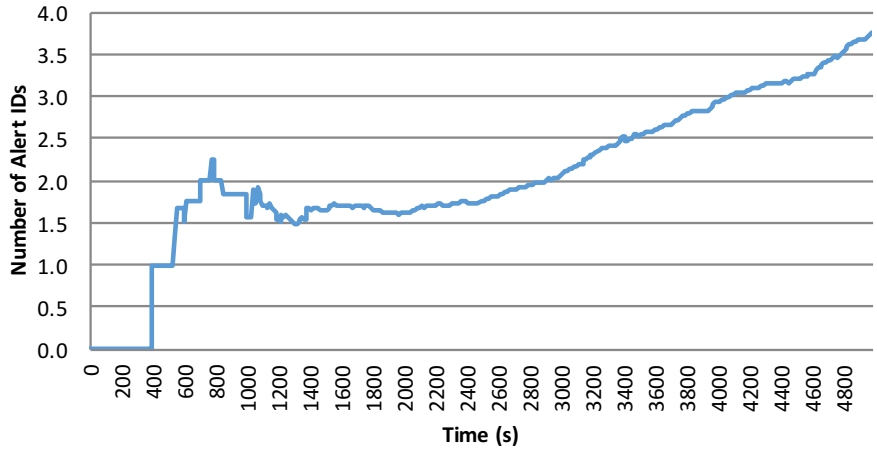



Figure 7: Average number of alert IDs when a person was crossing the controlled area

a compromised UAVs, the number of alert IDs remains as one from the first alert. This allows the distributed system to detect the suspicious behavior over the time and confirm its malicious behavior.

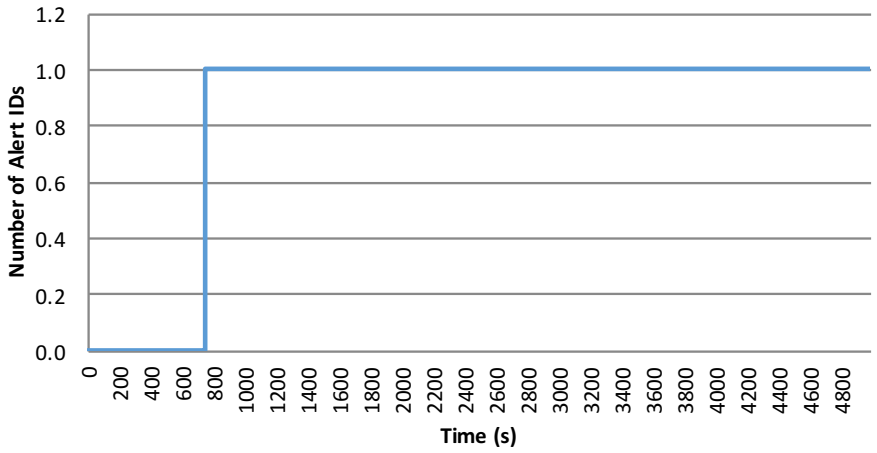



Figure 8: Average number of alert IDs when an UAV was compromised

## 5. Conclusions and future work

This work has presented a security mechanism for detecting compromised UAVs in UAV networks for supporting surveillance. It is based on the assumption that people will be usually observed by more than one UAV. Hence, if a UAV repeatedly report people that any other UAV does, each UAV will detect this fact following an information diffusion approach inspired in the blockchain principles. We developed the novel simulator called ABS-SecurityUAV to illustrate this approach. The experimentation results show its efficacy.

The current work is planned to be extended by testing this approach in real-world UAVs. In particular, we plan to apply this approach in the surveillance of schools for detecting bullying activities and reporting these to the school authorities. This work may also be tested for assisting military operations in detecting possible threats in critical areas and the surveillance of the surroundings of military bases that are far from cities.

*Acknowledgments*

This work acknowledges the research project "Construcción de un framework para agilizar el desarrollo de aplicaciones móviles en el ámbito de la salud" funded by University of Zaragoza and Foundation Ibercaja with grant

reference JIUZ-2017-TEC-03. This work has been supported by the program "Estancias de movilidad en el extranjero José Castillejo para jóvenes doctores" funded by the Spanish Ministry of Education, Culture and Sport with reference CAS17/00005. We also acknowledge support from "Universidad de Zaragoza", "Fundación Bancaria Ibercaja" and "Fundación CAI" in the "Programa Ibercaja-CAI de Estancias de Investigación" with reference IT1/18. We acknowledge the research project "Desarrollo Colaborativo de Soluciones AAL" with reference TIN2014-57028-R funded by the Spanish Ministry of Economy and Competitiveness. It has also been supported by "Organismo Autónomo Programas Educativos Europeos" with reference 2013-1-CZ1-GRU06-14277.

## References

[1] H. Hasrouny, A. E. Samhat, C. Bassil, A. Laouiti, VANet security challenges and solutions: A survey, Vehicular Communications 7 (2017) 7–20.

[2] P. Li, H. Duan, A potential game approach to multiple uav cooperative search and surveillance, Aerospace Science and Technology 68 (2017) 403–415.

[3] A. M. Khaleghi, D. Xu, Z. Wang, M. Li, A. Lobos, J. Liu, Y.-J. Son, A DDDAMS-based planning and control framework for surveillance and crowd control via UAVs and UGVs, Expert Systems with Applications 40 (18) (2013) 7168–7183.

[4] M. Erdelj, O. Saif, E. Natalizio, I. Fantoni, UAVs that fly forever: Uninterrupted structural inspection through automatic UAV replacement, Ad Hoc Networks (2017) https://doi.org/10.1016/j.adhoc.2017.11.012.

[5] I. Jawhar, N. Mohamed, J. Al-Jaroodi, D. P. Agrawal, S. Zhang, Communication and networking of UAV-based systems: Classification and associated architectures, Journal of Network and Computer Applications 84 (2017) 93–108.

[6] C. A. Kerrache, A. Lakas, N. Lagraa, E. Barka, UAV-assisted technique for the detection of malicious and selfish nodes in VANETs, Vehicular Communications 11 (2018) 1–11.

[7] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, M. Robinson, Security Authentication System Using Encrypted Channel on UAV Network, in: Robotic Computing (IRC), IEEE International Conference on, IEEE, 2017, pp. 393–398.

[8] I. García-Magariño, R. Lacuesta, ABS-TrustSDN: An agent-based simulator of trust strategies in software-defined networks, Security and Communication Networks 2017 (2017) Article ID 8575842, 9 pages, https://doi.org/10.1155/2017/8575842.

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

[10] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems (2017) https://doi.org/10.1016/j.future.2017.08.020.

[11] W. Fawaz, Effect of non-cooperative vehicles on path connectivity in vehicular networks: A theoretical analysis and UAV-based remedy, Vehicular Communications (2018) https://doi.org/10.1016/j.vehcom.2018.01.005.

[12] S. Hayat, E. Yanmaz, R. Muzaffar, Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint, IEEE Communications Surveys & Tutorials 18 (4) (2016) 2624–2661.

[13] Q. Wang, Z. Chen, W. Mei, J. Fang, Improving physical layer security using UAV-enabled mobile relaying, IEEE Wireless Communications Letters 6 (3) (2017) 310–313.

[14] H. Sedjelmaci, S. M. Senouci, N. Ansari, Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology, IEEE Transactions on Intelligent Transportation Systems 18 (5) (2017) 1143–1153.

[15] D. He, S. Chan, M. Guizani, Communication security of unmanned aerial vehicles, IEEE Wireless Communications 24 (4) (2017) 134–139.

[16] M. Sbeiti, N. Goddemeier, D. Behnke, C. Wietfeld, PASER: secure and efficient routing approach for airborne mesh networks, IEEE Transactions on Wireless Communications 15 (3) (2016) 1950–1964.

[17] N. Nigam, S. Bieniawski, I. Kroo, J. Vian, Control of multiple UAVs for persistent surveillance: algorithm and flight test results, IEEE Transactions on Control Systems Technology 20 (5) (2012) 1236–1251.

[18] M. Babiš, P. Magula, NetLogo - An alternative way of simulating mobile ad hoc networks, in: Wireless and Mobile Networking Conference (WMNC), 2012 5th Joint IFIP, IEEE, 2012, pp. 122–125.

[19] I. García-Magariño, M. Cossentino, V. Seidita, A metrics suite for evaluating agent-oriented architectures, in: Proceedings of the 2010 ACM Symposium on Applied Computing, ACM, 2010, pp. 912–919.

[20] I. García-Magariño, A. Gómez-Rodríguez, J. C. González-Moreno, G. Palacios-Navarro, PEABS: a process for developing efficient agent-based simulators, Engineering Applications of Artificial Intelligence 46 (2015) 104–112.

[21] I. García-Magariño, G. Palacios-Navarro, R. Lacuesta, TABSAOND: A technique for developing agent-based simulation apps and online tools with nondeterministic decisions, Simulation Modelling Practice and Theory 77 (2017) 84–107.