Nextgen of Search and Rescue operations through trustworthy doped drones fleet

Antonello Calabrò and Eda Marchetti
Institute of Information Science and Technologies "A. Faedo" (ISTI)
National Research Council of Italy (CNR), Pisa, Italy
{antonello.calabro, eda.marchetti}@isti.cnr.it

***Abstract*—Search and rescue operations are critical and involve logistical and human infrastructures, requiring high technology trustworthiness. A multi-layer secure architecture on top of a drone mesh is presented to address these challenges. It is leveraged by security features such as blockchain and CIA-compliant communication paradigms.**

***Index Terms*—SAR, Drones, Trustworthiness, UAV, Cybersecurity**

I. Introduction

Systems dedicated to rescuing or protecting individuals in distress, known as Search and Rescue (SAR), involve logistical and human infrastructures in maritime and terrestrial environments. The European and Atlantic Pact signatories have agreements for search and rescue (SAR) operations, including Frontex and the EUR SAR Plan. Due to the vast number of entities and organizations involved in SAR Operations, their technical realization requires coordinating several heterogeneous techniques [1]. Indeed, most SAR systems are based on photographic analysis [2], either performed directly onboard the drone or by sending the data directly to a base station for sampling and analysis [3]. In [4] the authors focus on the possibility of using UAVs in catastrophic scenarios such as earthquakes or other natural disasters [5]; in [6] authors use LoRa technologies on drones for SAR operations. The system presented in [7] utilizes mobile networks for subject localization during SAR operations.

The criticality and complexity of SAR operations require high availability and trustworthiness. However, recent news and experiences still demonstrate a stringent need for innovative research and solutions to ensure trustworthy and successful results. In particular, the following criticalities of the SAR operations can be experienced: *Weather conditions* such as heavy rain, snow, or fog can make locating missing persons or stranded individuals difficult. *Terrain,* such as remote and rugged terrain like mountains, forests, or deserts, can pose challenges for rescue and communication between teams. *Time constraints* are also crucial, as the longer a person is missing or stranded, the greater the risk to their safety. *communication* is essential for rescue teams to coordinate with each other and other emergency responders, especially in remote or rugged terrain where radio signals may be weak or non-existent and different communication systems may be used. In addition, in the case of infrastructure-less technologies, ensuring the delivery, security, privacy, cryptography, dependability, and reliability of communication mechanisms can be fundamental. In all these cases, a single data packet's loss or delayed delivery can be the difference between life and death. The issues could be resolved by improving the supporting infrastructure, adopting reliable and robust communication devices, and increasing the number and expertise of personnel involved. However, all these solutions significantly increase the overall costs of SAR operations, which are already extremely high. Furthermore, the increasing number of cyber-attacks on drones or distributed infrastructure can impact the success of SAR operations due to communication violations or disruption.

To ensure the trustworthiness of SAR operations, we propose a secure architecture on top of a drone mesh, incorporating specific security features such as blockchain and CIA-compliant communication. The multi-layered architecture will facilitate the seamless transition between advanced technologies such as LoRa, NB-IoT, 4G, and 5G. This will enhance existing protocols by incorporating features such as ARQ on LoRa and data access through satellite connections, ensuring the reliable and privacy-preserving transmission of critical data among drones, base stations, and rescuers' devices.

II. Proposed Architecture

This section provides an overall of the features of the proposed multi-layer architecture and preliminary details of its implementation. In particular, as shown in Figure 1 it includes the following components:

a) Blockchain: The data captured by the onboard sensors, acquired images, and positioning information is managed through blockchain distributed over all the doped drones that compose the fleet to guarantee their non-repudiability.

b) GPS jamming/spoofing Avoidance: A certified positioning mechanism is deployed for the drone fleet to avoid GPS attacks that could corrupt legitimate positioning and navigation information, such as jamming and spoofing, potentially leading to tragedies or loss of drones. This mechanism operates over a distributed blockchain among the nodes participating in the mesh network.

c) Distributed data: A CIA-compliant communication paradigm is adopted among the fleet members. This is achieved by ensuring: *confidentiality* through data encryption and fingerprinting of the devices involved in the communication, *integrity* through file permissions and user access controls, and *availability* by providing adequate communication

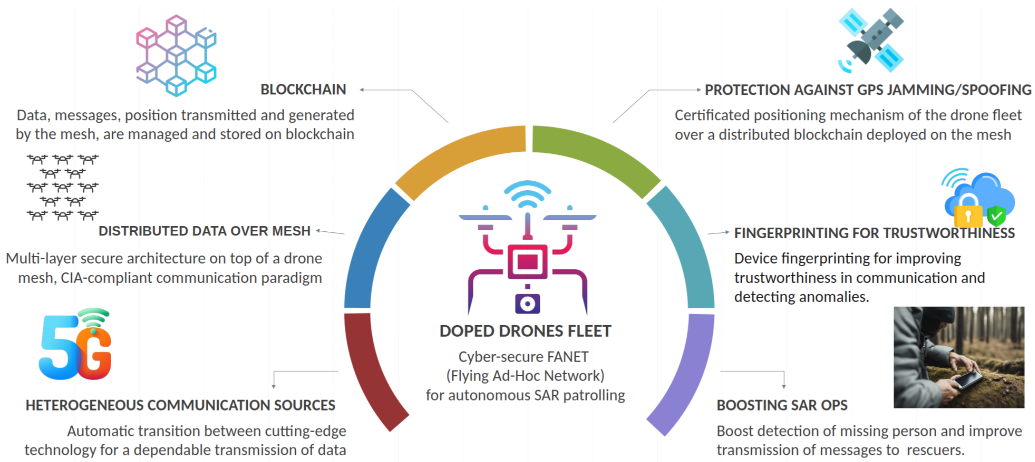

Fig. 1. Proposed approach overview

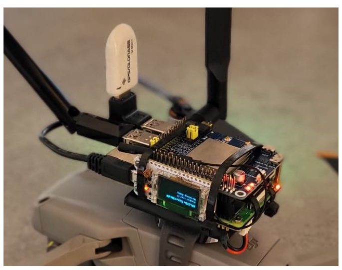

Fig. 2. The preliminary prototype

bandwidth, transparent switching among available transmission technologies preventing transmission bottlenecks.

d) Fingerprinting: Devices' fingerprinting is utilized to enhance trust in communication and identify unusual deviations in the device's CFO (Carrier Frequency Offset) behavior, potentially caused by adversaries.

e) Heterogeneous Communication Sources: The drones must manage multiple and diverse communication technologies such as NB-IoT, 4G/5G, LoRa, Wi-Fi, and satellite communications. This will speed up and enhance the transmission of messages to the rescuers, ensure reliable communication, and enable the use of the most reliable and available method as needed.

f) Boosting SAR ops: The necessary functionalities and techniques for managing self-flying capabilities and implementing a collaborative fleet will be included. These ensure convergence on the objective by utilizing captured data, such as images, device beacons detected, and thermoscanning.

A preliminary prototype running the above-described multi-layer architecture is shown in Figure 2. It is a 250gm device including a Raspberry-Pi model 4B 8GB; a High-gain 2.4/5 GHz Wi-Fi module; a USB GPS; a Waveshare SIM7600G-H 4G HAT; Battery pack; LoRa device SX1275 ESP32. All the communication hardware is managed by native libraries available on the Raspberry OS[1]. The blockchain relies on Hyperledger Fabric [8]. The *Dependable Delivery Switcher* is the core component responsible for monitoring the correct delivery of messages sent and received among each node (drone). It also selects the best communication method according to the lower energy consumption or operational cost (e.g., the SAT communication).

[1]https://www.raspbian.org/

For future work, we will continue refining and validating the prototype in a real environment.

References

[1] N. Nomikos, P. K. Gkonis, P. S. Bithas, and P. Trakadas, "A survey on uav-aided maritime communications: Deployment considerations, applications, and future challenges," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 56–78, 2023.

[2] C. Liu and T. Szirányi, "Real-time human detection and gesture recognition for on-board UAV rescue," *Sensors*, vol. 21, no. 6, p. 2180, 2021. [Online]. Available: https://doi.org/10.3390/s21062180

[3] D. Bozic-Stulic, Z. Marusic, and S. Gotovac, "Deep learning approach in aerial imagery for supporting land search and rescue missions," *Int. J. Comput. Vis.*, vol. 127, no. 9, pp. 1256–1278, 2019. [Online]. Available: https://doi.org/10.1007/s11263-019-01177-1

[4] M. H. Khyavi, "Rescue network: Using uavs (drones) in earthquake crisis management," 2021.

[5] C. Tabasso, N. Mimmo, V. Cichella, and L. Marconi, "Optimal motion planning for localization of avalanche victims by multiple uavs," *IEEE Control. Syst. Lett.*, vol. 5, no. 6, pp. 2054–2059, 2021. [Online]. Available: https://doi.org/10.1109/LCSYS.2021.3049314

[6] A. Calabrò and E. Marchetti, "Improving sar ops using wi-fi and lora on uav," in *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. IEEE, 2022, pp. 82–84.

[7] A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "SARDO: an automated search-and-rescue drone-based solution for victims localization," *CoRR*, vol. abs/2003.05819, 2020. [Online]. Available: https://arxiv.org/abs/2003.05819

[8] S. Upahm Abas, F. Duran, and A. Tekerek, "A raspberry pi based blockchain application on iot security," *Expert Systems with Applications*, vol. 229, p. 120486, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417423009880

Acknowledgment

This work was partially supported by the project RESTART (PE00000001) and project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NextGenerationEU.