Problem Statement

Disaster Scenario

Every year, disasters and crises devastate people, communities, and entire societies worldwide. Worryingly, they are predicted to become more common in the future. Disasters can occur naturally (e.g., tornadoes, hurricanes, earthquakes, floods, wildfires, mudslides, or drought) or be human-caused (e.g., mass shootings, chemical spills, or terrorist attacks). Preparing for, responding to, and recovering from disasters and traumatic events is essential to individuals' and communities' behavioral health.

When people experience a disaster, they may experience a variety of reactions, many of which are natural responses to challenging situations. Most people show resilience after a disaster. Resilience is the ability to bounce back, cope with adversity, and endure demanding conditions. Thankfully, resilience in disaster recovery is ordinary, not extraordinary, and people regularly demonstrate this ability. Supportive resources to address stress and other hardships are critical to resilience.

Like war, disasters are also very unstructured in scope. No one can predict the exact time and how a disaster will strike. Sometimes, the local infrastructure is devasted, and no telecommunication resources are available to provide essential communication necessities, such as means for the affected communities to ask for help. Usually, this type of situation requires a complete telecommunication infrastructure to provide Command and Control to support the operations.

Figure 1 - Flooding west of Pittsburgh in the Oakdale area.

We use a flooding scenario to support the course in the project development. Because the changes to our climate and environment are already contributing to the increased frequency, intensity, and unpredictability of severe weather events, what makes this type of disaster usually in different countries, generating many victims and causing fatalities and incalculable losses (financial and social) for the population.

The Federal Emergency Management Agency stated, quoting NOAA data, that flooding caused more damage in the United States than any other severe weather-related event, an average of $5-$8.2 billion a year. States such as Texas, New Jersey, and Florida dominated the top 10 on the list created by NOAA and had the most flooding risk. Louisiana joined those states to monopolize the top 25, while Pennsylvania, Oregon, South Carolina, and Virginia made brief appearances. The Gulf Coast states comprise almost half of the top 100 most-at-risk counties[1].

For example, in November of 2008, Santa Catarina, a state in the south of Brazil, had a period of heavy rainfall (20-23 November). The state had suffered constant rains for over two months, which turned the soil wet enough to cause a landslide during the storm that hit the state in late November. Around 60 towns and over 1.5 million people were affected. At least 128 people have been killed, with over 78,700 forced to evacuate their homes. A further 150,000 have been left without electricity, while water rationing is being carried out in at least one town due to purification problems. Several regions' cities have become cut off due to floodwater and landslide debris. Water levels in the Vale do Itajaí have risen to eleven meters above normal. Because of the electrical blackout, many communities were left without communication, which made it difficult for people to call for help and inform where they were.

Solution Description – Argus Crisis

The problem to be answered is providing an efficient and secure environment to send a distress message when a natural disaster occurs (in our case, the flood disaster situation). In the scenario, there are no telecommunication links to provide essential communication (voice and data) to the rescue teams. Consequently, innovation is required. It uses the means existent in the community and by volunteers, for example, drones, to provide communication resources and support the identification of hazards.

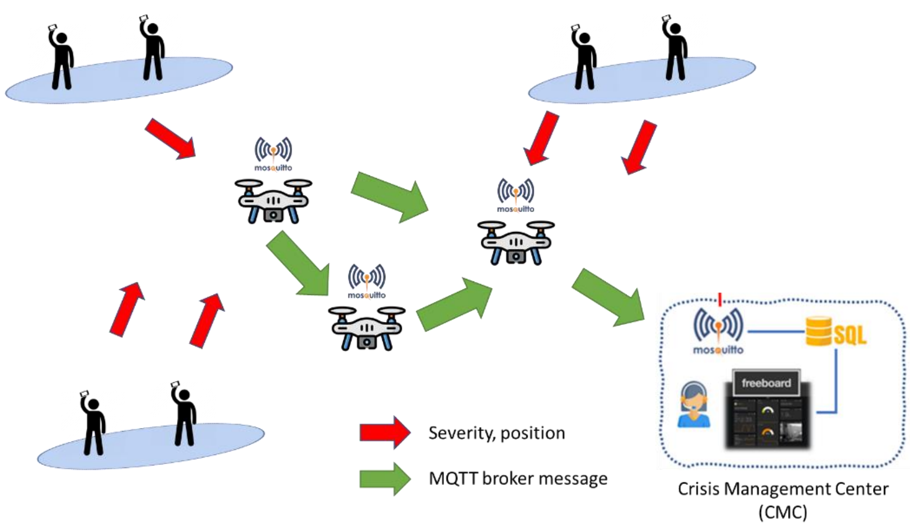

Figure 2 - Argus Crisis Architecture.

[1] https://www.foxweather.com/extreme-weather/counties-most-risk-flooding-2024

In this scenario, victims in the flood area will have a smartphone with a rescue app, which enables the citizens to send their position continuously and when they are in danger (severity level message: high, medium, or low) as a simple text message (description of their situation), as it is presented in Figure 3. To provide communication support (enabling victims' messages to flow to the Crisis Management Center - CMC), drones flying in the crisis area intercept the message and forward it to other drones until the message arrives at the CMC. The CMC data is processed and aggregated, and a dashboard is provided for the operators to plan the rescue operation efficiently.

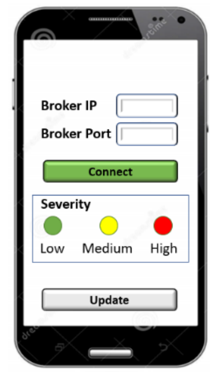

Figure 3 - GUI Argus Crisis.

The approach used to implement the solution is through an Internet of Things (IoT) architecture. IoT is an advanced automation and analytics system that deals with artificial intelligence, sensors, networking, electronics, cloud messaging, etc., to deliver complete systems for the product or services. A logical view of the technical architecture of the solution is presented in Figure 2. There, you can see drones with phone devices, which periodically send MQTT messages to the Crisis Management Center through bridge brokers existent in drones, informing the severity and position of the user.

An essential entity in this environment is the MQTT broker, implemented using Eclipse Mosquito (embedded in drones). Eclipse Mosquito is an open-source (EPL/EDL licensed) message broker that implements the MQTT. Mosquito is lightweight and suitable for all devices, from low-power single-board computers to full servers. The drone runs in bridge mode, which means it receives the messages from the user nodes and forwards them to the primary Broker at the Crisis Management Center (see Figure 4).

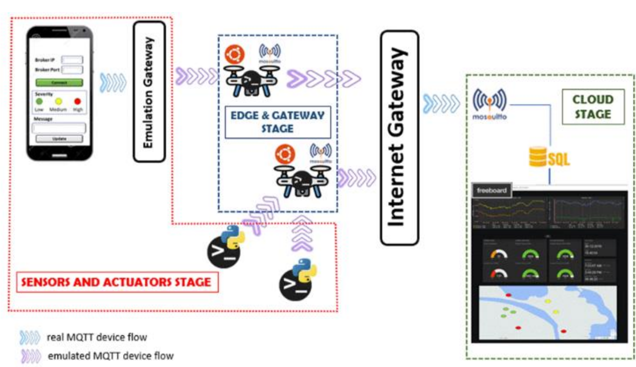

Figure 4 - Argus Crise Message Flow (Brokers).

The Crisis Management Center provides users with Command-and-Control (C2) features. It is a node that runs on a server box (Linux or Windows). This server has a Mosquito broker, which receives all messages from the bridge ones and persists them in an SQL database. Also, it has a dashboard that organizes the data in a helpful format, presents the information in a map visualization, and calculates the Risk KPI (explained in the text).

As we cited, the dashboard must present helpful information, including geo-information about the user nodes as the classification (KPI), calculated based on the severity sent. The formula to calculate the KPI is shown, and the color code is presented in the dashboard, which you can see in the following Figure.

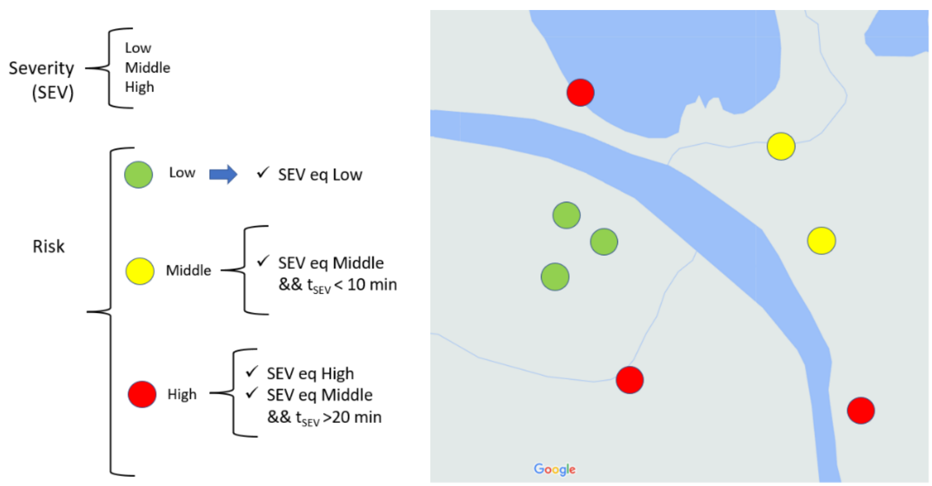

Figure 5 - Argus Crisis C2 Dashboard.

As you commented, each node sends its state using MQTT to the bridge broker. The conditions can be low, middle, or high; where high, the individual is in danger, and low, he is safe. The dashboard needs to compile this data and, using the formula presented in the previous figure, define the risk situation and colorize the node representation in the map.