Towards a Secure and Reliable Communication Network for Large-scale UAV Systems Deployed in Hostile Environments

Jiang Bian, Mengjun Xie and Remzi Seker

Unmanned Aerial Vehicles (UAVs) are used in hostile environments for various missions including surveillance and intelligence gathering. Rapid industry advancements in power and electric motor technologies, as well as dramatic improvements in artificial intelligence research will soon enable large numbers of small, cheap, and fully automated UAVs to carry out complex and long-term missions in hostile environments. However, to use hundreds even thousands of UAVs effectively at once introduces unique communication challenges. Traditional satellite-based UAV communication systems have well-known limitations, such as slow data transmission links, even with deployments involving only a small number of drones.

Imagine a large number of fully automated drones are deployed to collect intelligence in a hostile territory such a battle field. The available satellite bandwidth limits the number of drones that can communicate with the base station. It is challenging to be able to transmit the gathered information to the base station in real-time. A strategy is to store the information locally on each drone during its mission, and collect the intelligence when the drones are back. However, it is very likely that a number of drones can be destroyed during the mission either by accident or by the adversaries. Furthermore, the security of the information collected by the drones need to be assured such that when the drones are captured, the adversaries shall not be able to extract any sensitive information.

In this paper, we introduce the UAV Collaboration Wireless Network (UAV-CWN), a secure and reliable UAV mesh network for intelligence gathering. The proposed protocol is well-suited for deploying a large number of drones simultaneously to conduct surveillance missions in hostile environments. In a UAV-CWN system, the UAVs are wirelessly linked and working

cooperatively to achieve high fault-tolerance, while minimizing the risk of information exposure to the adversaries. In the UAV-CWN, each drone corresponds to a node in the collaboration network. When a piece of intelligence (e.g., images of the terrain, sound, motion detection data, etc.) is collected by a drone, the information will be split into n (i.e., based on the setting of the system) slices using an Information Dispersal Algorithm (IDA), and then delivered to n nearest neighbors. These data segments will be further propagated in the network by their receivers (other nodes in the network). In other words, the UAV-CWN exhibits mesh networking topology, where each node not only captures and disseminates its own data, but also serves as a relay for other nodes. The level of propagation shall be set based on the required level of redundancy and security. When the drones return the base station, an investigator can easily reconstruct the gathered data using the corresponding IDA decoder. Due to various reasons (e.g., some drones being destroyed, or a receiving node maybe facing a device failure during transmission, etc.), not all n data slices can be recovered. However, the property of IDA ensures that the complete gathered data can be easily restored as long as there are k (i.e., based on the setting of the IDA coder, and $k << n$) complete data slices.

Since wireless communications are conducted through radio waves in open air, it is relatively easier to be interfered by adversaries. If the data payload is not encrypted, an attacker can easily perform a man-in-the-middle attack and deduct sensitive information. To further ensure data privacy, we introduce the use of one-way hash key-chain. In UAV-CWN, a pair of private (x_i) and public (g^{x_i}) keys is generated and deployed onto each drone before the mission. The private key is known to that specific drone and the investigator, while the public key is public to all other nodes. Before applying the IDA, the drone shall compute a encryption key $h(x_i)$, where $h()$ is an one-way cryptographic hash function. When a piece of intelligence is gathered, the drone will first encrypt the data with $h(x_i)$, and then apply the IDA encoding to split the data into n slices. Before sending each data slice to a nearby node, the data packet is signed digitally with the drone's private key x_i to ensure integrity and authenticity. Moreover, the drone will send the next-level encryption key $h(h(x_i))$ to the relay nodes. The same process will be repeated upon propagation of the data slices by the receivers, except the receiver will use $h(h(x_i))$ obtained from the sender rather than its own private key for encryption. The properties of one-way cryptographic hash function ensures us that: 1) it is highly collision resilient, where no two piece of data

will have the same hash value; 2) it is irreversible, where it is impossible to deduce x_i from $h(x_i)$. Using one-way hash key-chain, we separate the data from its encryption key and ensure that only the originator will be able to decrypt the data stored in the mesh network formed by the drones.