Secure Communications in Unmanned Aerial Vehicle Network

*Dr. Reza Tourani, Dr. Srikanth Gururajan Saint Louis University*

# ABSTRACT

Recently, Unmanned Autonomous Vehicles (UAVs) have gained extensive attention from both academia and industry. UAVs are a complex system composed of many subsystems, making them a typical target for attackers. In, the intent to secure these UAV’s we propose “Cipher-text Policy Attribute-Based Encryption (CP-ABE)” a promising cryptographic mechanism for fine-grained access control to shared data between UAVs and sub-systems. In our scenario, each UAV system is associated with a list of attributes that reflect his/her role in the system. A special entity called Attribute Authority (AA) generates a public key PK which is shared with all system entities, and generates also users’ private keys SK from their lists of attributes. An entity that wishes to encrypt a message will specify an access policy in the form of an access tree. Attributes list of a UAV that wants to decrypt a cipher-text must satisfy the access policy to be able to decrypt the message. An access tree is used to describe access policy of an encrypted message. For instance, access policy shown in Figure 1 can be expressed differently as follows: (("Student" OR "Ph. d Student" OR "researcher") AND ("Physics" OR "Biology")). By employing this mechanism, we achieve hierarchical identity-based broadcast encryption and pseudonym mechanism, all the devices in this system can broadcast encrypted messages anonymously and decrypt the legal cipher-text. our proposed scheme satisfies two important security properties of confidentiality and authentication.

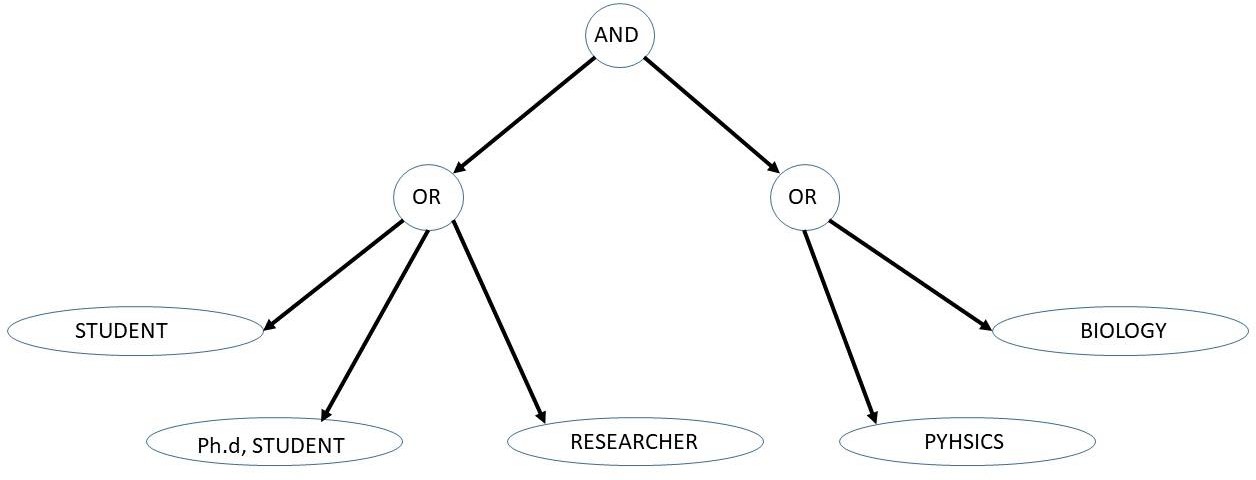


Figure 1: Example of an Access Tree

# MOTIVATION

SkyGrabber is an offline satellite internet downloader. SkyGrabber is a simple enough concept: grab the signals that spill from a satellite broadcast (or even narrowcast), aimed from a satellite towards a specific location, and turn them into TV feeds you can look at. Or in simple terms: "You don't need an online internet connection. Just customize your satellite dish to a selected satellite provider and start grabbing."

The US military drones would send their video up to a US military satellite (the "uplink") that cannot be intercepted. The signal would then be beamed by that satellite or a linked one down to the controllers – who might be behind enemy lines. Because that signal was unencrypted, anyone who can tune their satellite dish to the correct frequency and location in the sky could pick up the signal, and decode it. And because any satellite downlink signal spreads a little, the area where it can be picked up is potentially huge.

# IMPLEMENTATION

We applied and tested a software encryption policy named “Cipher text- Policy Attribute-Based Encryption (CP-ABE)” that yields excellent access control to share data between UAV and its sub-systems. From our approach, each UAS is associated with a list of attributes that reflects its role in the overall system. For instance, key attributes that identify a specific drone could be a drone with an infrared camera, long rage communication link, extra battery, or other unique/distinguishing features.

Implementing a centralized compute node (similar in function to an Air Traffic Control tower) that features an authentication server, named Attribute Authority (AA) to generate a Public Key (PK) on instantiation which is then shared with all members of the system; this server will also generate a drone’s Secret Key (SK) from lists of attributes that the drone’s shares with server respectively. Note that master key (MK) is a secrete key generated by Attribute authority (AA) on instantiation and is one time process or might change if (MK) is compromised. Similarly, Public key(PK) is also a one-time instantiation.

Functionally, when an ATC generates secret key specific to drone it share the same along with public key over a secure channel. So, any entity (UAV) that wishes to decrypt the cipher-text must satisfy the access policy to be able to decrypt the message. And, in addition the drones or UAV entity should have successfully learnt the public key and it’s secrete key which is required at the time of decoding messages.

# TEST BED SETUP

Hardware: The UAV platform that we have chosen to conduct the experiments for this effort is the QAV 250 quadcopter from Luminier Labs. The QAV 250 is a reliable airframe and as configured has adequate payload capacity and sustain flight for approximately 6 minutes. The fully integrated platform is shown in Figure 2, and some of its specifications are listed in Table 1.

Table 1: Specifications of the UAV platform to be used in this effort

|  |  |  |
| --- | --- | --- |
| Figure 2: QAV 250 UAV | Parameter | Description |
| Airframe | Lumenier QAV 250 |
| Motors & Prop. | 4x Lumenier RX1806-14 2300kv, Gemfan 5x3 |
| Onboard Computing | Raspberry Pi 4 SBC or equivalent |
| ESC | Lumenier Mini 20A ESC with SimonK AutoShot, 5V/1A BEC (2-4s) |
| Battery | 1300mAh, @11.1v (3S LiPo) |
| Endurance | Minimum: ~3 min, Max: ~8 min |
| All up Weight | ~620g |

Flight Test Facility: The flights will be conducted in the Parks College indoor UAV test cage, shown below in Figure 3. The cage is situated within a motion capture volume and has dimensions of approximately 10′×10′×8′ and has soccer netting on all sides to ensure the UAV stays within the confines of the cage.

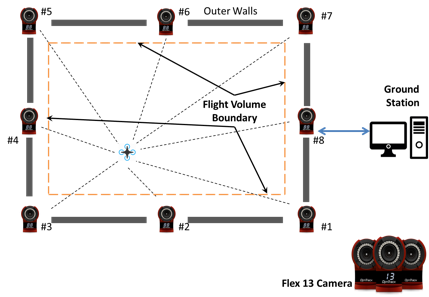
 

Figure 3: Saint Louis University indoor UAV Flight Test cage Figure 4: Illustration of Motion Capture setup

# TEST CASE AND EXECUTION

To validate our experiment, we grouped the UAV’s in two groups of BLUE and RED team which by themselves acts as an access policy attribute. Where our goal was to encrypt message from voice commands (i.e.) voice commands turned into text command are read into attributes and corresponding text is encrypted and broadcasted over the network. And our attempt was to make sure the entities or UAV that satisfies the attributes only can decrypt the message. This was successfully achieved using test case scenarios as shown below in table 2.

Table 2: Test scenarios highlighting words of speech that acts as access policy attributes.

|  |  |  |
| --- | --- | --- |
| SL.No | Test Description (Input speech) | Results Outcome |
| 1. | Blue team and unit one and camera takeoff | Only Drone that belongs to blue team and is unit one and has camera enabled is subjected to takeoff. |
| 2. | Red team and unit one and audio takeoff | Only Drone that belongs to Red team and is unit one and has audio enabled is subjected to takeoff |
| 3. | Blue or Red team and region one takeoff | Both blue Or red team drones can takeoff if they belong to zone called region1 |

From the above test scenarios, we provide the clear information about the attribute list corresponding to respective drone from our experiment as shown in below table 3.

Table 3: Drone Access policy used in above experimental test cases

|  |  |
| --- | --- |
| Drone-1 | [[‘BLUE’, ‘UNIT-1’, ‘CAMERA’, ‘REGION-1’]] |
| Drone-2 | [[‘RED’, ‘UNIT-1’, ‘AUDIO’, ‘REGION-1’]] |

# CONCLUSION

# This work is an approach for using CP-ABE scheme in resource-constrained nodes like UAV’s (drone). Our solution takes advantage from the heterogeneity of the network to distribute the overhead due to CP-ABE encryption primitive. Furthermore, our approach validates each drone maintains and manages an area in which the authorized devices can obtain and broadcast key from centralized client server approach. Our work also provides partial privacy-preservation and resistance to denial of service attacks. Along these lines our current approach doesn’t include a secure communication channel to exchange secretes between client (UAV’s) and Attribute Authority server (AA) which is proposed for future extension of the paper.

# REFERENCES

# Arthur, C.: SkyGrabber: the $26 software used by insurgents to hack into US drones (2009). <https://www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked>

# Asadpour, M., Giustiniano, D., Hummel, K.A., Egli, S.: UAV networks in rescue missions. In: Proceedings of the 8th ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization, pp. 91–92. ACM (2013)[Google Scholar](https://scholar.google.com/scholar?q=Asadpour%2C%20M.%2C%20Giustiniano%2C%20D.%2C%20Hummel%2C%20K.A.%2C%20Egli%2C%20S.%3A%20UAV%20networks%20in%20rescue%20missions.%20In%3A%20Proceedings%20of%20the%208th%20ACM%20International%20Workshop%20on%20Wireless%20Network%20Testbeds%2C%20Experimental%20Evaluation%20and%20Characterization%2C%20pp.%2091%E2%80%9392.%20ACM%20%282013%29)

# Barreto, P.S.L.M., Libert, B., McCullagh, N., Quisquater, J.-J.: Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 515–532. Springer, Heidelberg (2005).  [https://doi.org/10.1007/11593447\_28CrossRef](https://doi.org/10.1007/11593447_28)[Google Scholar](http://scholar.google.com/scholar_lookup?title=Efficient%20and%20provably-secure%20identity-based%20signatures%20and%20signcryption%20from%20bilinear%20maps&author=PSLM.%20Barreto&author=B.%20Libert&author=N.%20McCullagh&author=J-J.%20Quisquater&pages=515-532&publication_year=2005)