

ON THE SECURITY CHALLENGES OF 5G CONNECTED DRONE TRANSPORTATION SYSTEM

Aagii Mariam Thomas

School of Science Engineering and Environment

a.m.thomas1@edu.salford.ac.uk



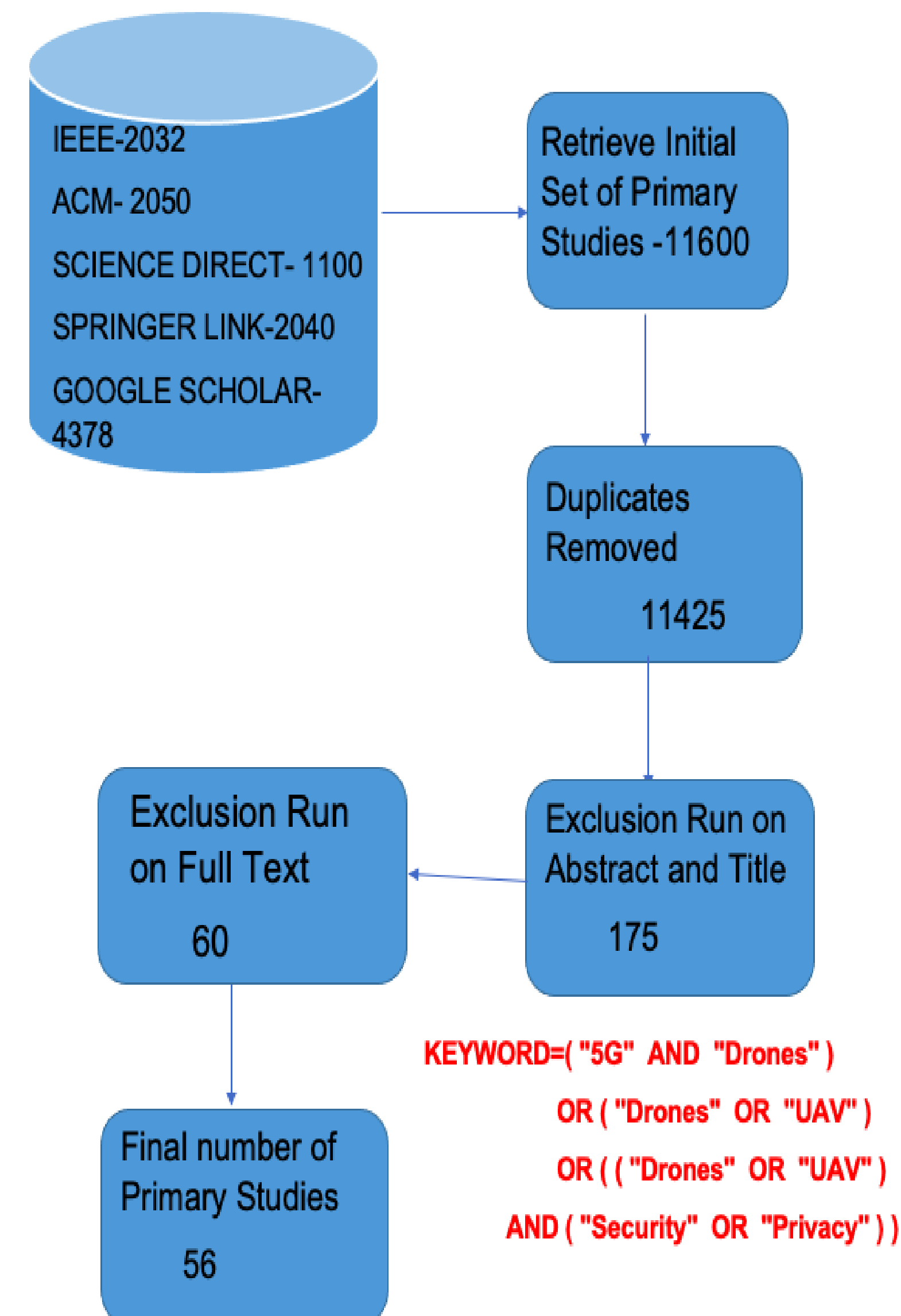
University of
Salford
MANCHESTER

1. INTRODUCTION

To explore

- ❑ The security issues of Unmanned Aerial Vehicle(UAV).
- ❑ The current security challenges in 5G connected UAV.
- ❑ The methods available to overcome the challenges and defend against possible attacks.

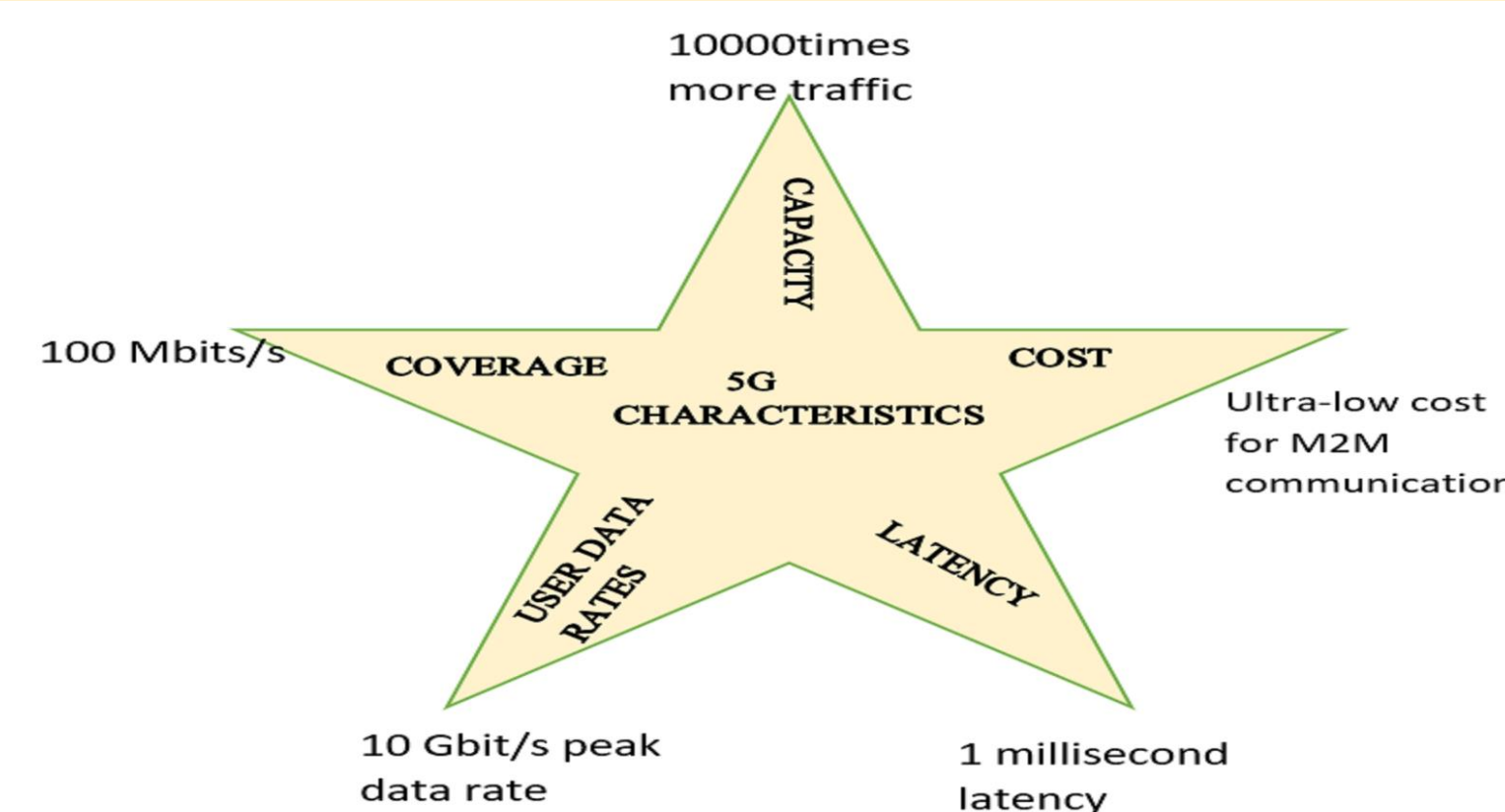
2. METHODOLOGY



3. BACKGROUND

5G NETWORK

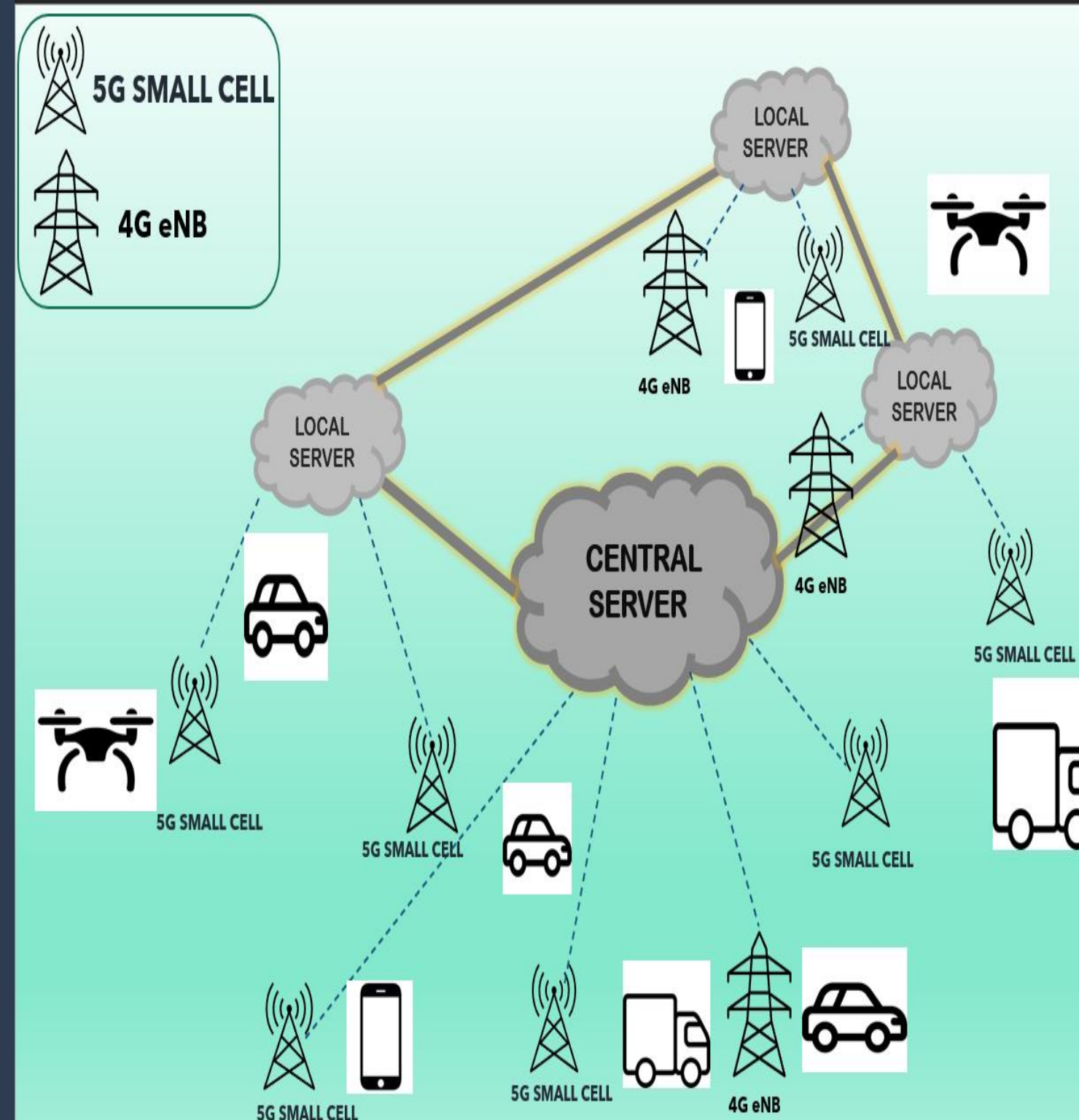
- 5G known as fifth generation offers higher speed than the previous generations.
- Consists of 2 logical network layers:
 - A radio network (RN) with a minimum set of L1/L2 functionalities.
 - A network cloud with all higher layer functionalities.
- Main characteristics are low latency, reliability, enhanced mobile broadband, massive machine type communication.



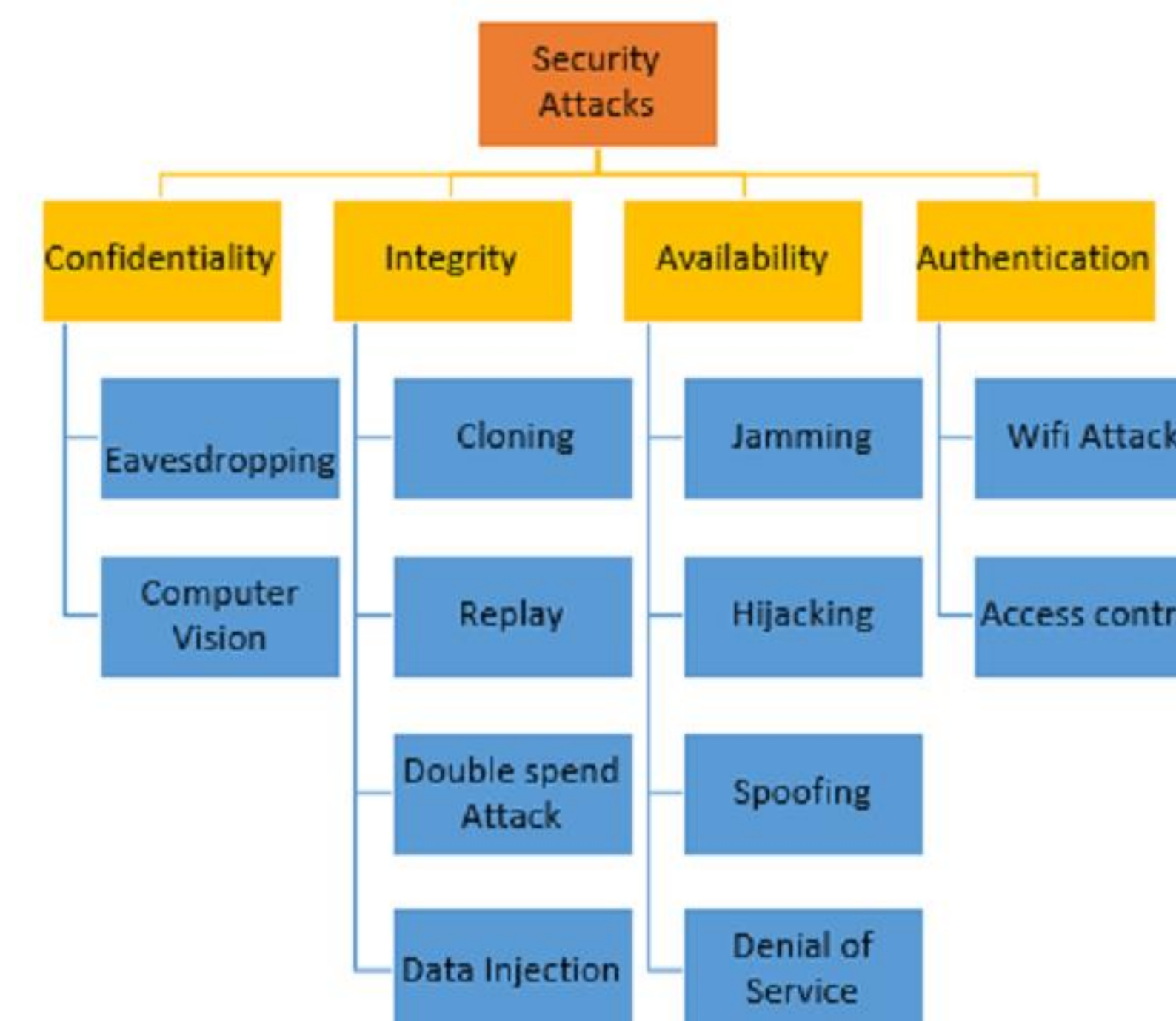
DRONES

- Drones are aircrafts without any human pilot, crew or passengers on board.
- Mainly used by military, aviation and civil sectors, now used for delivering packages, food, medicines, or other goods.
- Three types of UAV communication are there:
 - a) UAV-to-UAV communication
 - b) UAV-to-base station communication
 - c) UAV-to-satellite communication.

5G Based Drone Architecture



4.TAXONOMY OF SECURITY ATTACKS AGAINST DRONES



5. RESEARCH DIRECTION

There are several ways to prevent the communication between the Drones and the network:

- 1. Secure Data Aggregation:** Using the homomorphic encryption method, it aggregates all the encrypted texts into a single encrypted text without the need of decryption.
- 2. Intrusion Detection and Prevention:** Drones are subjected to intrusions, thus designing an energy-efficient and effective intrusion detection and prevention system to identify malicious cyber activities is crucial.
- 3. Secure UAV-to-UAV communication :** The security of UAV-to-UAV systems is more complicated as opposed to UAV-to-ground system, since the receivers or eavesdroppers operate in all directions of 3D space.

6. CONCLUSION

- ❑ Drones can benefit from using a 5G connection.
- ❑ UAVs are prone to attacks and there are several possible solutions like encryption method which will be subjected to future research.

7. REFERENCE

- Parimal Mehta, Rajesh Gupta, and Sudeep Tanwar. Blockchain envisioned uav networks: Challenges, solutions, and comparisons. Computer Communications, 151:518–538, 2020.
- Yulei Wu, Hong-Ning Dai, Hao Wang, and Kim-Kwang Raymond Choo. Blockchain-based privacy preservation for 5g-enabled drone communications. IEEE Network, 35(1):50–56, 2021.
- Aparna Kumari, Rajesh Gupta, Sudeep Tanwar, and Neeraj Kumar. A taxonomy of blockchain-enabled softwarization for secure uav network. Computer Communications, 161:304–323, 2020.