

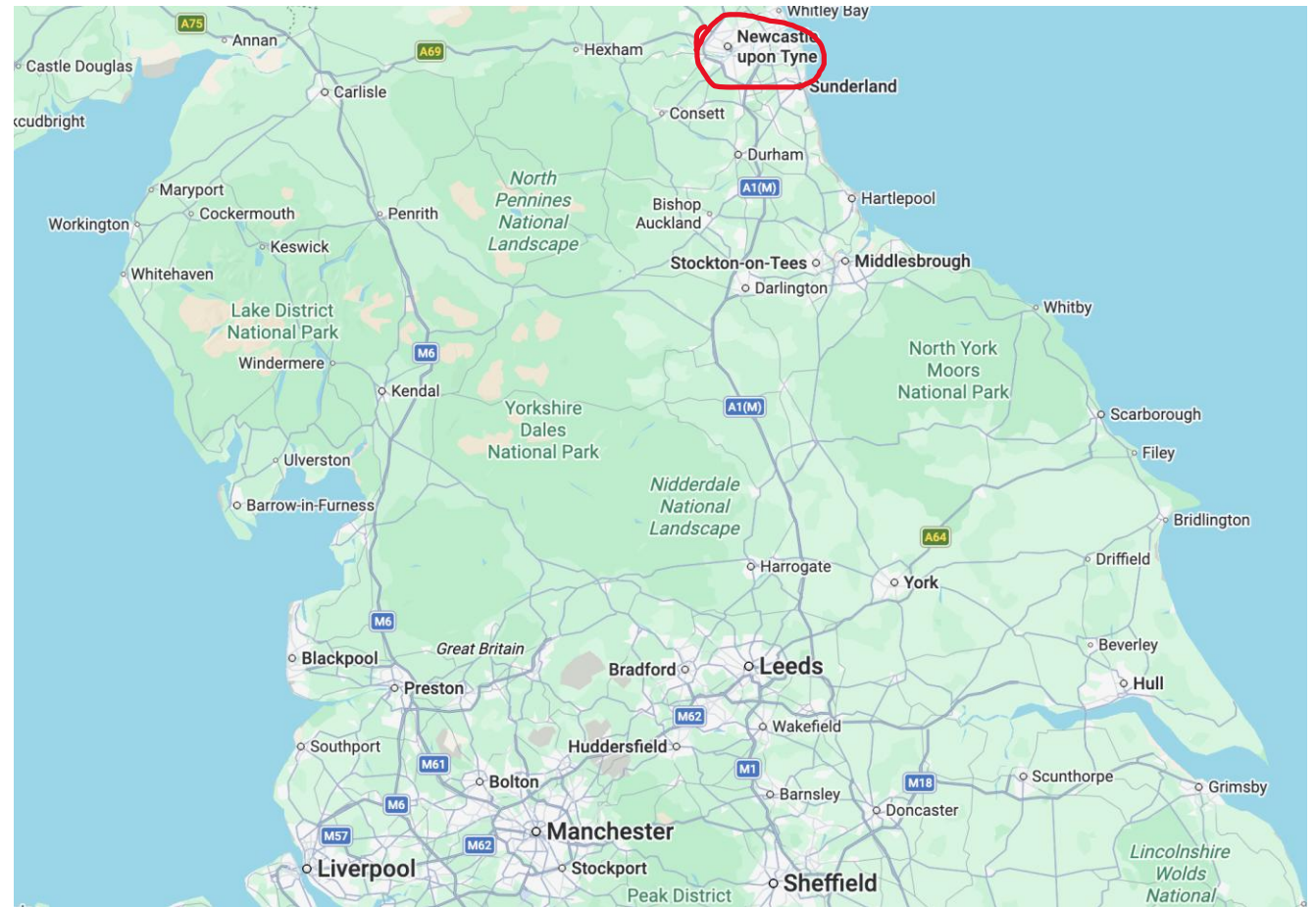
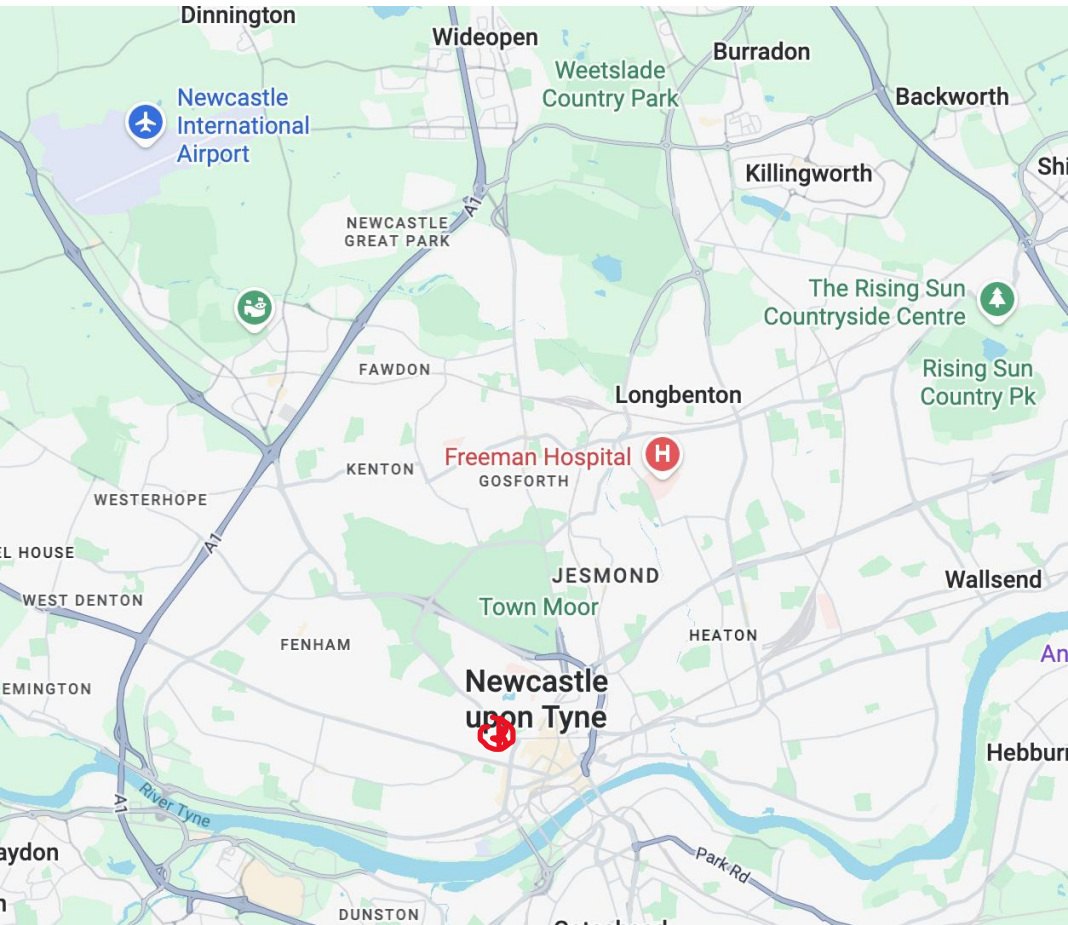
Towards Intelligent and Secure Edge AI Systems

Dr Bo Wei

Senior Lecturer in Computing

Email: bo.wei@newcastle.ac.uk

The city: Newcastle upon Tyne



The city: Newcastle upon Tyne



Quayside



St James' Park for Newcastle United

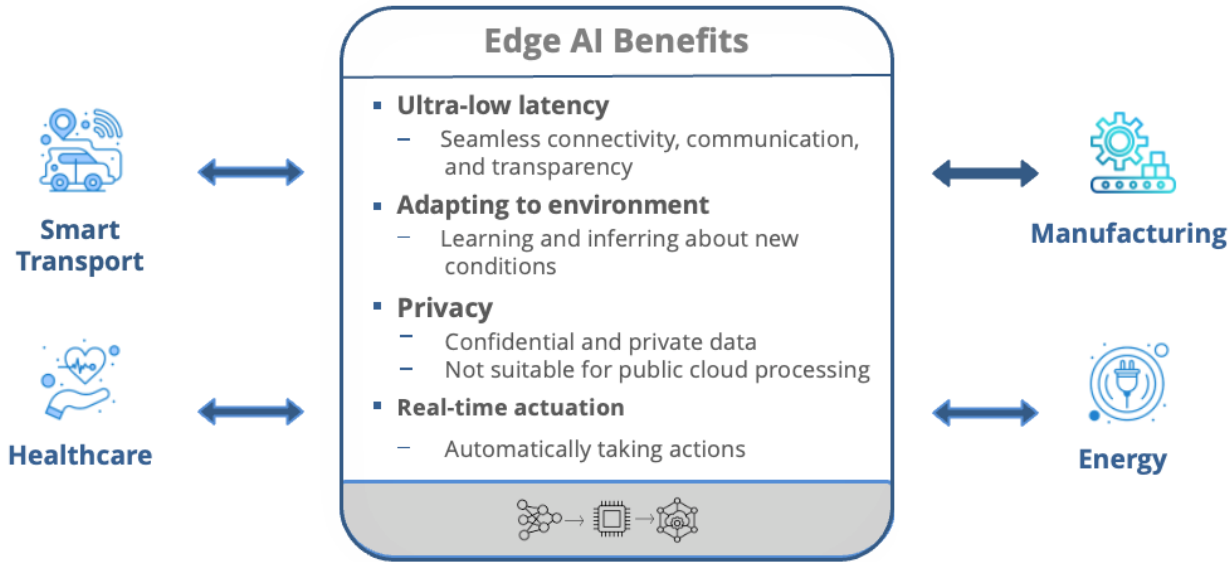
Photos from Wikipedia

School of Computing, Newcastle University

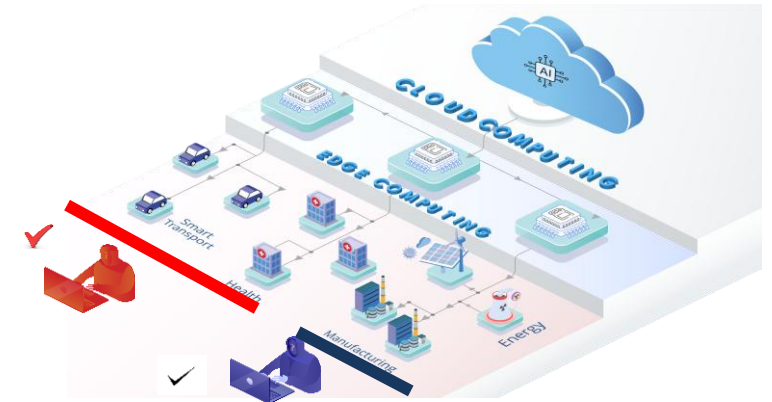


- Newcastle University: Russel Group University
- School of computing within Urban Science Building
- 70+ academic staff members

Problem motivation (Why edge AI?)



- Led by Newcastle University
- Funded by ESPRC, RC contribution £10M, 5 years from 2024



- RT1: Edge AI Hub Engagement and Impact
- RT2: Cyberdisturbance modelling for Edge Computing
- RT3: Edge Computing for AI
- RT4: AI Driven Edge Data and Model Guard
- RT5: Data Sensitive Application Use-Cases Driven Validation

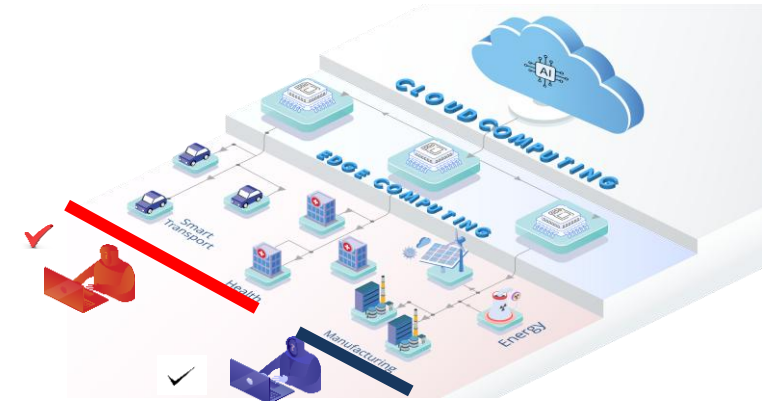
Our work is primarily focused on **smart transport**, **health**, **energy**, **manufacturing** and **smart cities**.



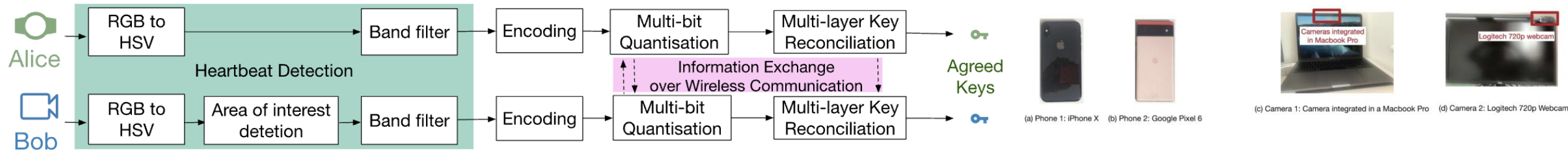
15 academic partners
>20 industry partners

Importance of Edge AI

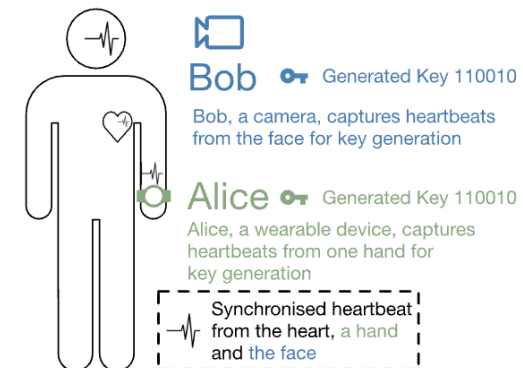
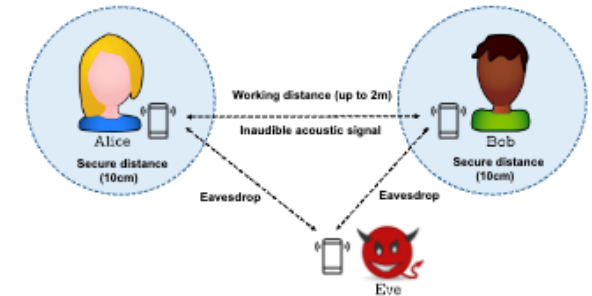
- Over the next 10 years, Edge AI will be the nucleus of AI Innovation (Gartner 2023)
- The global Edge AI market is experiencing explosive growth
 - exhibiting a Compound annual growth rate (CAGR) of 33.3% during the forecast period.
 - The global edge AI market size was valued at USD 20.45 billion in 2023.
 - The market is projected to grow from USD 27.01 billion in 2024 to USD 269.82 billion by 2032 (Fortune Business Insights)



Research topic 1: Next-generation IoT device pairing using sensor measurements



- Device pairing: Fundamental research question for authentication and wireless communication.
- Motivations:
 - Existing: Encryption methods like public key and symmetric key rely on a certificate authority (CA) for key management.
 - The existing key sharing protocols suffer from man-in-the-middle attacks.
 - Attackers could eavesdrop on messages over wireless communication and obtain keys.
 - The mutually trusted third-party certificate authority does not always exist.
 - Certificates are offered to legal users for authentication.
- Novelties:
 - We have designed sensor based symmetric key generation methods for mobile devices.
 - Evaluation in real environments: the key match rate can be achieved up to 100%, and the energy consumption is also tested.



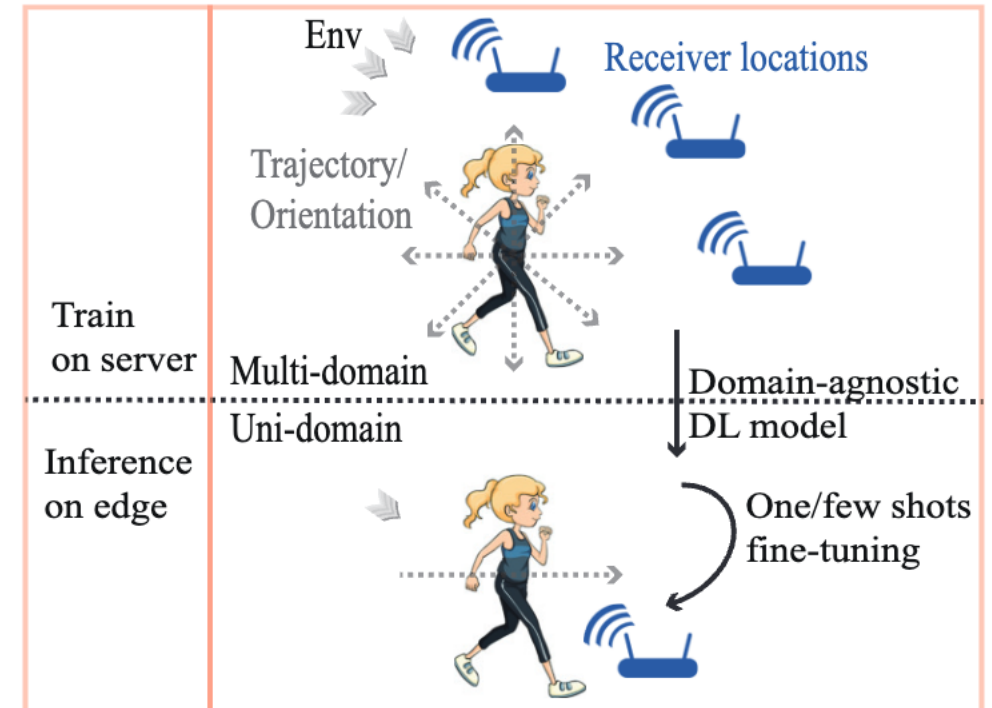
Research topic 2: Large Language Model (LLM)for robot control

- The global robotics market is expected to grow to \$73 billion by 2029. (Source: Statista Market Insights, 2024).
- the increasing adoption of LLM-controlled robots:
 - manufacturing, healthcare, and autonomous systems, etc.
- Vision Language Navigation (VLN)
- Vision Language Action (VLA)
- Solution:
 - Edge AI for VLA and VLN: Efficient and effective LLM mechanism and machine learning model
 - Tailored for resource-constrained robots
 - Using robots and edge architecture
 - Both physical robots and digital twin: data collection, fast deployment and evaluation
 - Sim-to-Real

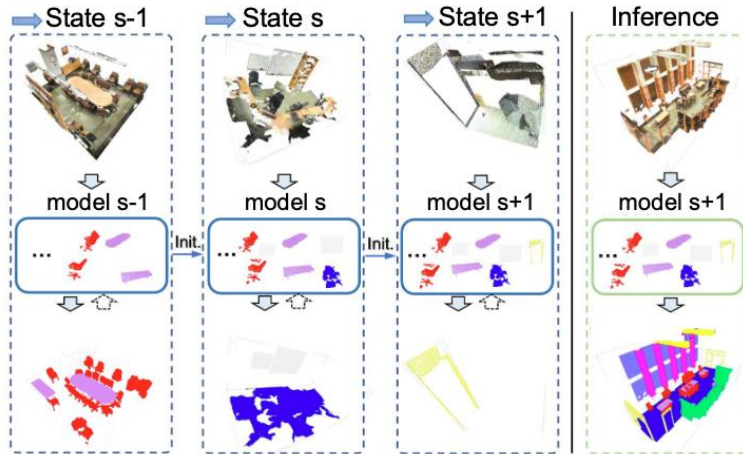


Research topic 3: Wireless Sensing

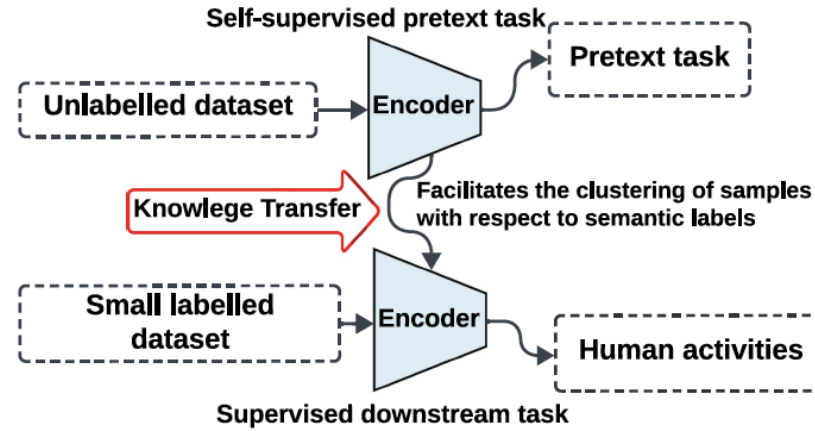
- Wireless sensing: using wireless signal around the environment, the monitored people do not need to carry any devices:
 - Wireless signal: WiFi, mmWave radar
 - Application: Localisation, activity recognition, identity recognition
 - Principle behind:
 - Received Signal Strength (RSS) or Channel State Information (CSI) can be inferred by human being between the transmitter and the receiver
 - Due to multiple path effect
 - Challenges we solved:
 - Robust to various people, locations, etc.
 - One/few shot model training



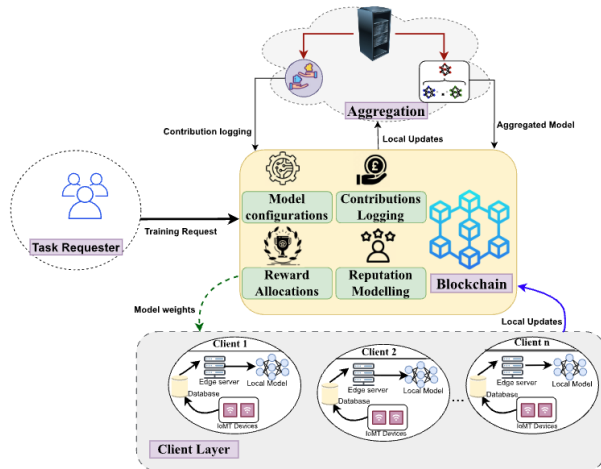
Research topic 4: Edge AI



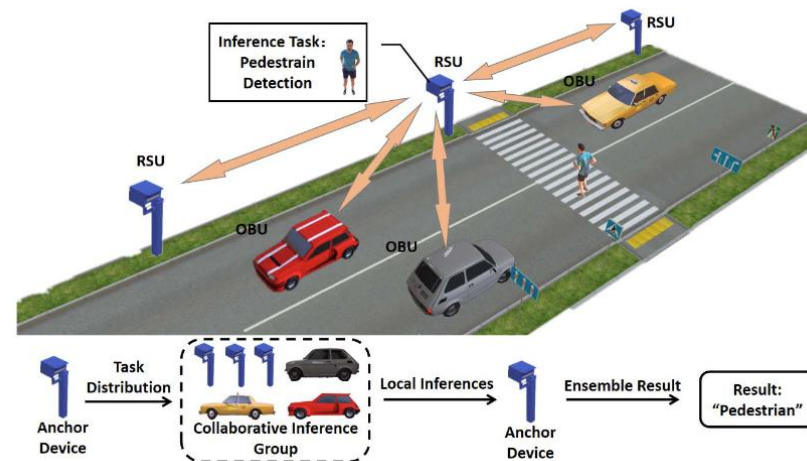
Catastrophic forgetting in 3D segmentation (AAAI'25)



Self-supervised learning for imbalanced datasets (IEEE TETCI'25)



Federated learning (IEEE TCE'25)



Intelligent Transportation (IEEE TITS'22)

- Thanks for your time.
- I am happy to take any questions.
- Email: bo.wei@newcastle.ac.uk