Center for Embedded Systems

An NSF Industry/University Cooperative Research Center

Supporting Smart Machine Communication with Private LTE Network

Kang Chen and Gayan Aruma Baduge
Southern Illinois University

SIU Southern Illinois University CARBONDALE

National Science Foundation

ASU Ira A. Fulton Schools of Engineering ARIZONA STATE UNIVERSITY

Project Overview and Description

- Smart machine is an emerging domain
  - Sense and interact for collaborative and intelligent manufacturing and producing
  - Connected vehicle, automated mining, etc.
- Wireless communication is a key
  - Machine to machine & machine to infrastructure
  - Many technologies (e.g., WiFi) with different limitations
- How can private LTE contribute?
  - Capability: throughput, QoS, security, management, etc.
  - Any innovations needed?

Approach

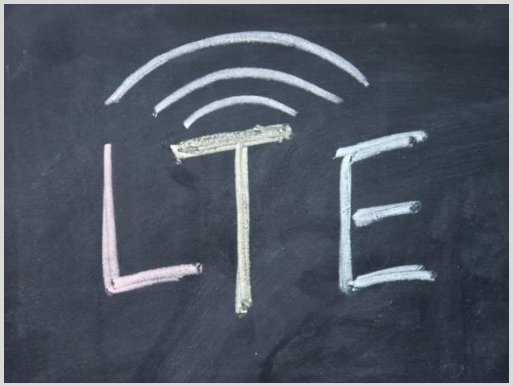
- Investigate the performance of private LTE network in supporting smart machines
  - Field measurement
    - Identify application scenarios
    - Varying various parameters, e.g., data rate and density
  - Theoretical analysis
    - Further validate measurement result
  - Performance enhancement
    - Algorithm design and network structure innovation
- Outcomes
  - Promoting the application domain of private LTE
  - Promoting the transition to smart machines

Project Tasks/ Deliverables

	Description	Date	Status
1	Identify representative application scenarios	Aug. 2016	
2	Design and build a testbed with private LTE equipment and client devices	Sep. 2016	
3	Design and conduct field measurement	Nov. 2016	
4	Conclude measurement results	Feb. 2017	
5	Validate measurement results through theoretical analysis	Mar 2017	
6	Performance enhancement with algorithm design and network structure innovation	April 2017	

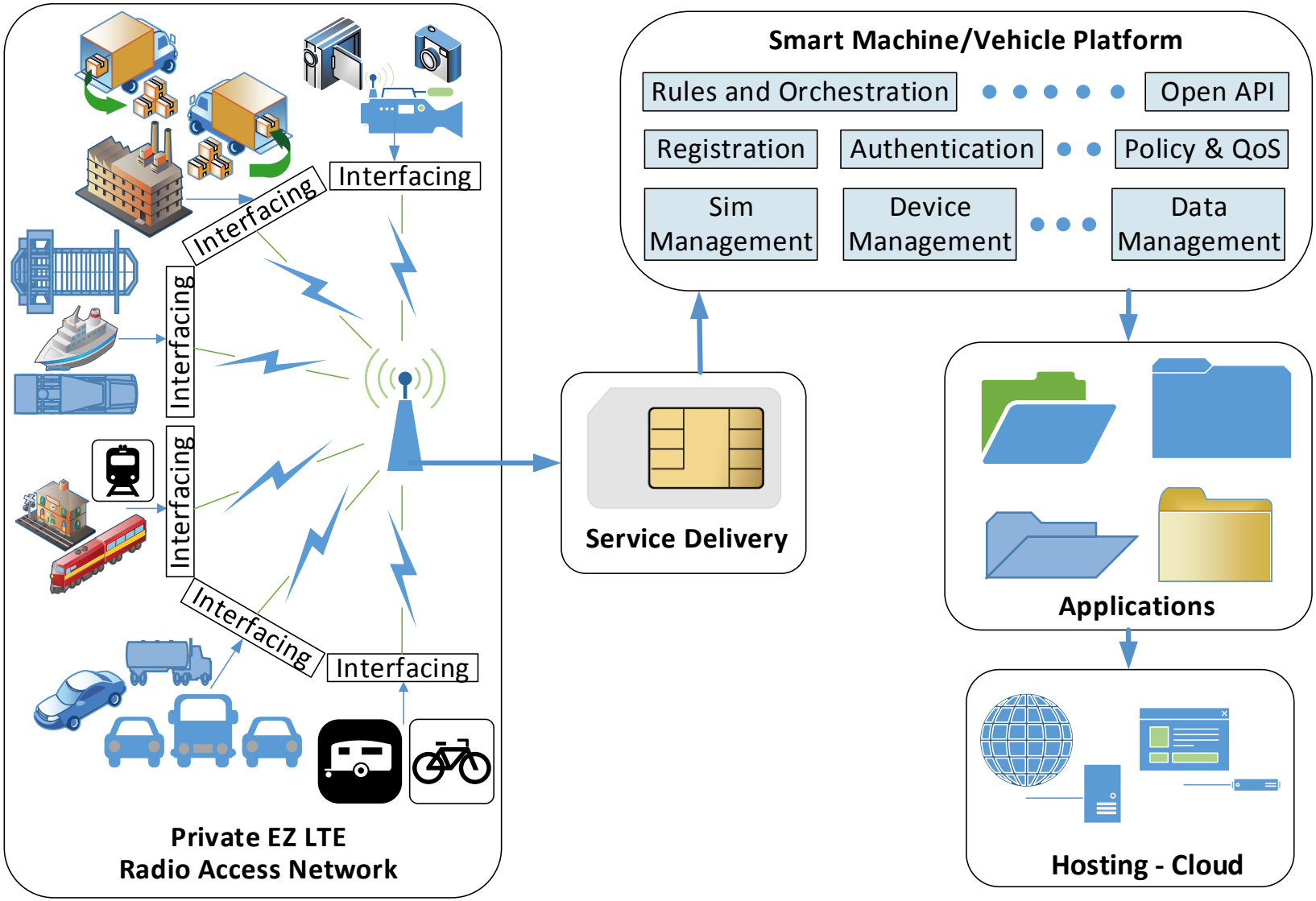
Executive Summary

- **Smart machine is promising**
  - Automated X (driving, manufacture, mining)
  - Smart X (city, industry, grid)
- **Private LTE**
  - As powerful as commercial LTE network
  - As flexible and agile as a private network



Technical Detail

- **System Architecture: Smart machine & Vehicle framework over private LTE**



Technical Detail

- **Smart machine**
  - Vast amount of application scenarios: utilities, logistic, mining, manufacturing, healthcare, etc.
  - Diverse requirements on the underlying wireless networks including security, mobility, bandwidth, reliability, and QoS
  - Raise an important question about how to design a suitable wireless network for smart machines

Technical Detail

- **Wireless communication techniques**
  - WiFi: limited coverage, limited QoS, limited security
  - Zigbee: limited coverage, limited bandwidth
  - WiMAX: wide area mobile broadband service but a mainstream standard.
  - LTE: wide area mobile broadband service, major standard today and on the evolution map of 5G

Technical Detail

- **Private LTE**
  - LTE is good but needs dedicated spectrum, which often is owned by major carriers
  - Carrier owned LTE network is not flexible to use in industry scenarios
  - Opening up of 3.65 GHz CBS band removes this barrier

Technical Detail

- **Field Measurement**
  - Delay: the distribution of packet delays in both crowd and sparse scenarios.
  - Throughput: the throughput a machine can achieve in both crowd and sparse scenarios.
  - QoS support: measure the delay of and throughput of nodes under different QoS configurations. This measurement tries to answer what guarantee can the private LTE network offer?
  - Handoff under mobility: measure the delay, throughput, and packet loss probability when a machine moves from one base station to another base station.

Technical Detail

- **Theoretical analysis**
  - Learn the techniques used in LTE
  - Modeling the measurement scenario
  - Deducing the theoretical performance under the measurement scenario
  - Check the validity of the measurement results

Technical Detail

- **Performance enhancement**
  - Compare application needs and measurement results
  - Identify challenges
  - Design new algorithms to solve the gap
  - Example:
    - Guarantee the packet delivery probability under the handoff scenario