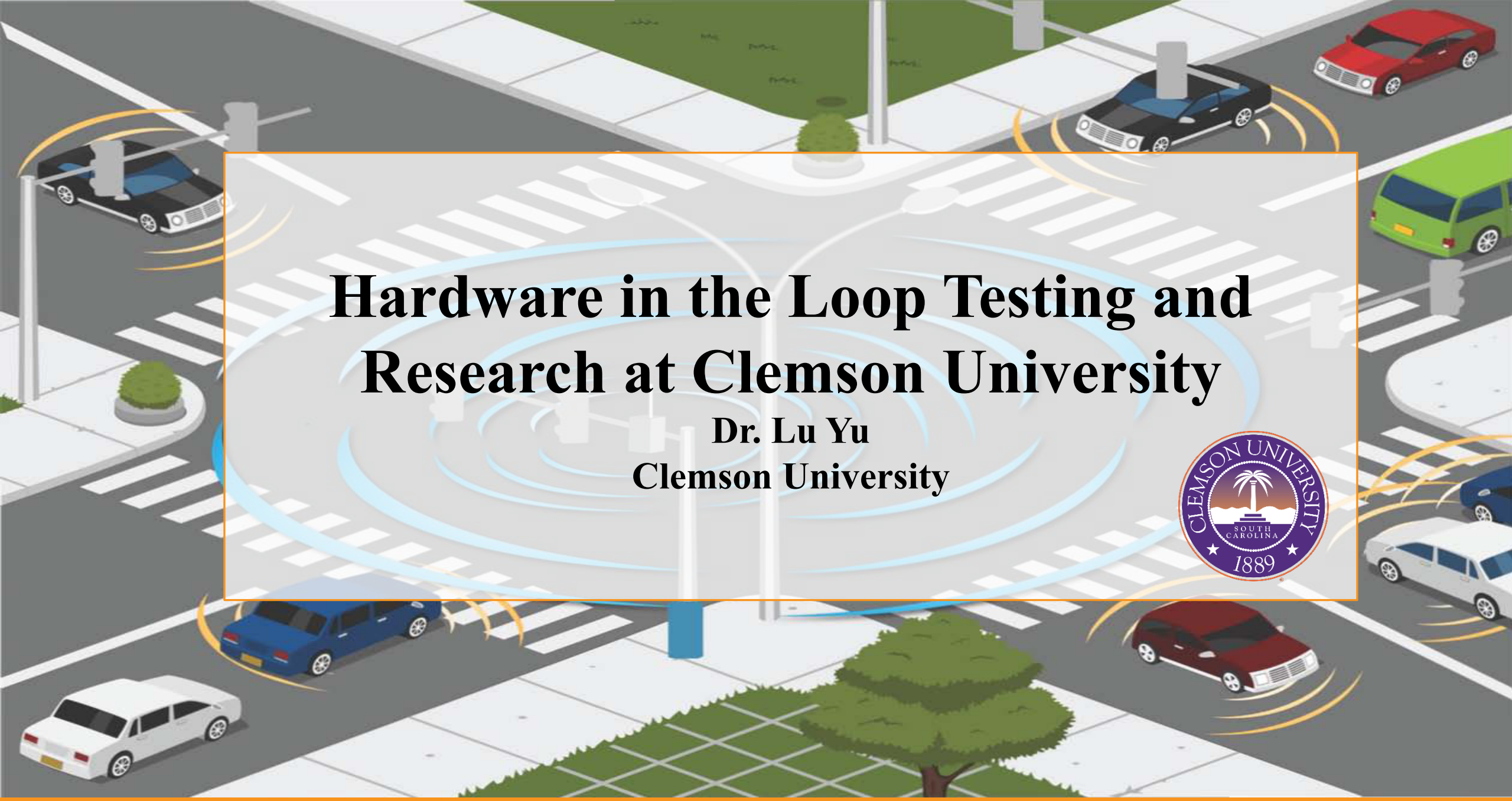


Hardware in the Loop Testing and Research at Clemson University

Dr. Lu Yu
Clemson University

Clemson Researchers (alphabetical order)

- **Dr. Richard Brooks**, Professor of Electrical and Computer Engineering

Network Security, information assurance, battlespace coordination, Behavior Pattern extraction/detection and game theory

- **Dr. Mashrur (Ronnie) Chowdhury**, Eugene Douglas Mays Professor of Transportation

Connected and Autonomous Vehicle Ecosystem, Cyber-Physical Systems for Smart Cities

- **Dr. Hongxin Hu**, Assistant Professor of School of Computing

Security in Software-Defined Networking (SDN), Network Function Virtualization (NFV), Internet of Things (IoT), Mobile Computing, Cloud Computing, and Big Data

- **Dr. Jim Martin**, Associate Professor of School of Computing

Delay-based Congestion control, Active Queue Management (AQM), and Internet video streaming based on HTTP-based Adaptive Streaming (HAS)

- **Dr. Pierluigi Pisu**, Associate Professor of Automotive Engineering, Leader of the Deep Orange 8 Project and Leader of the Connected Vehicle Technology Faculty Group

Diagnosis and Prognosis in Vehicle Electrical Systems, Batteries and Fuel Cells, Energy Management Control of Hybrid Electric Vehicles, Vehicle Systems Optimization, and Connected Vehicle Technologies

- **Dr. G Kumar Venayagamoorthy**, Duke Energy Distingusihed Professor of Power Engineering, and Professor of Electrical and Computer Engineering

Development and Implementation of advanced computational methods for smart grid applications, sensor networks and signal processing

- **Dr. Kuang-Ching Wang**, Associate Professor of Electrical and Computer Engineering

wireless networks and mobile computing, ad hoc and sensor networks, distributed protocols, and pervasive applications and embedded systems

Clemson Researchers (alphabetical order)

- **Dr. Richard Brooks**, Professor of Electrical and Computer Engineering

Network Security, information assurance, battlespace coordination, Behavior Pattern extraction/detection and game theory

- **Dr. Mashrur (Ronnie) Chowdhury**, Eugene Douglas Mays Professor of Transportation

Connected and Autonomous Vehicle Ecosystem, Cyber-Physical Systems for Smart Cities

- **Dr. Hongxin Hu**, Assistant Professor of School o

Security in Software-Defined Networ Internet of Things (IoT), Mobile Computing, Cloud Computing, an

- **Dr. Jim Martin**, Associate Pr

Delay-based Congestion control ing based on HTTP-based Adaptive Streaming (HAS)

- **Dr. Pierluigi Pisu**, Asso e 8 Project and Leader of the Connected Vehicle Techn

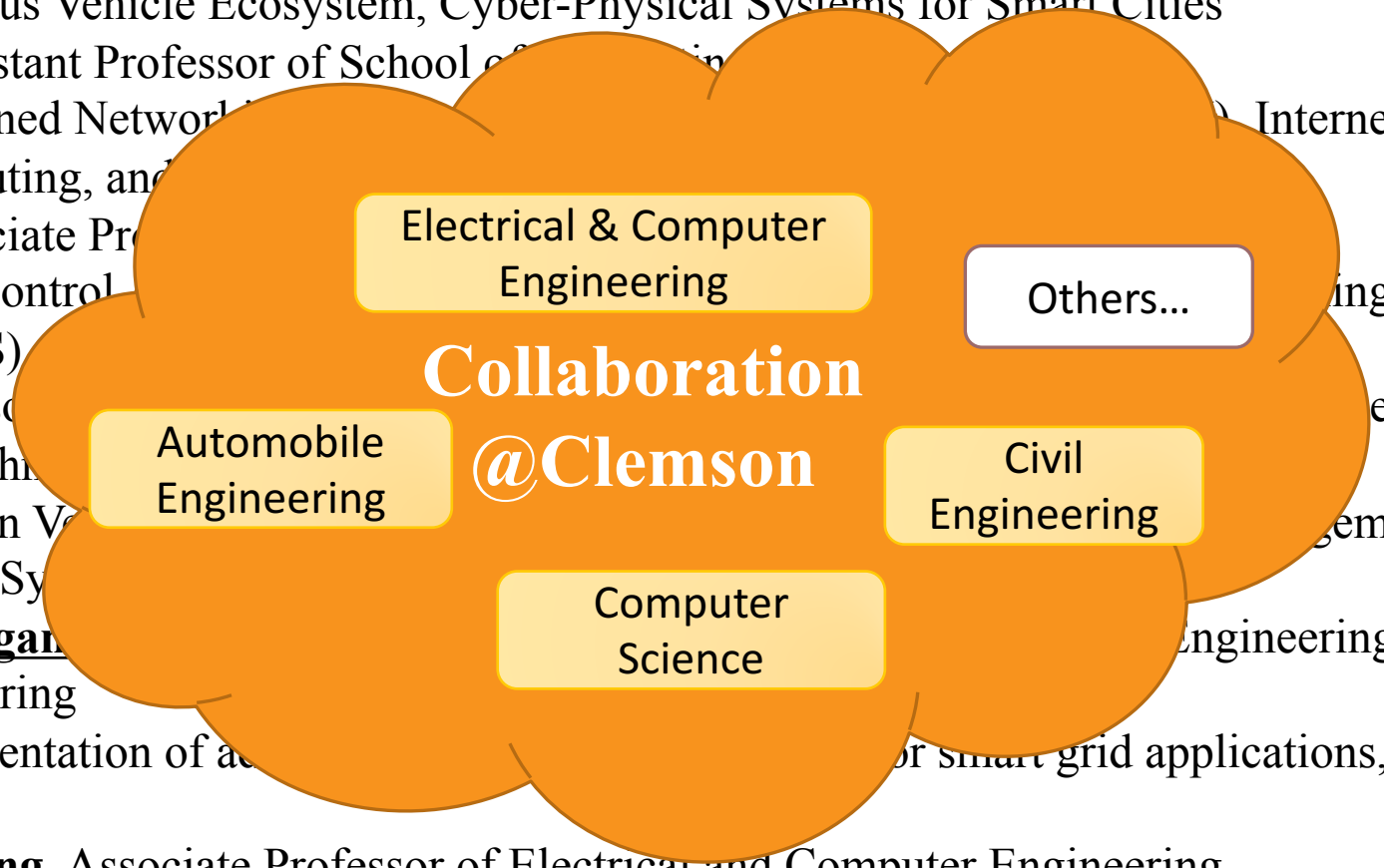
Diagnosis and Prognosis in Ve gement Control of Hybrid Electric Vehicles, Vehicle Sy

- **Dr. G Kumar Venayagan** ngineering, and Professor of Electrical and Computer Engineering

Development and Implementation of a r smart grid applications, sensor networks and signal processing

- **Dr. Kuang-Ching Wang**, Associate Professor of Electrical and Computer Engineering

wireless networks and mobile computing, ad hoc and sensor networks, distributed protocols, and pervasive applications and embedded systems



Connected Vehicle Research @Clemson

Clemson University International Center for Automotive Research (CU-ICAR)

- 250-acre campus located in Greenville.
- The nation's only graduate department of automotive engineering (over 200 master/PhD students).
- The U.S. Department of Energy made CU-ICAR one of the country's seven Graduate Automotive Technology Education (GATE) Centers of Excellence.

CUICAR
CLEMSON UNIVERSITY INTERNATIONAL CENTER FOR AUTOMOTIVE RESEARCH

Clemson University International Center for Automobile Research (CU-ICAR)

- CU-ICAR is UNIQUE:
  - ❑ A joint university (Clemson)-industry (BMW) research center.
  - ❑ Campus partners (20), parts partners (16), research partners (33), fellowship partners (13), pioneer/funding partner (9)
  - ❑ Professors and graduate students are routinely engaged in research that will benefit the automotive industry, which primarily sponsors the research projects.

Milestones

Year	Milestone
1992	BMW chooses a site along I-85 in Greer, South Carolina for its U.S. manufacturing plant.
1994	BMW opens its manufacturing plant.
2000	Clemson University's dean of engineering approaches BMW to explore the possibility of an industry-university partnership for constructing a commercial wind tunnel.
2003	BMW Information Technology Research Center launched.
2004	South Carolina General Assembly adopts the Research University Infrastructure Bond Act, allocating $217 million across three state research institutions, including $70 million to Clemson.
2006	CU-ICAR officially opens.
2007	Carroll A. Campbell Jr. Graduate Engineering Center building within CU-ICAR opens.
2008	BMW announces a second assembly plant, a $750 million investment that includes a 300,000-square-foot addition and a 1.2 million-square-foot flexible assembly second plant.
2010	Clemson University creates the Department of Automotive Engineering, diverging from the Department of Mechanical Engineering; program staff includes 11 professors as of 2012.
2011	CU-ICAR's newest building, the Center for Emerging Technologies, opens.
2011	BMW announces a $100 million investment in its Upstate assembly plant.

- Research
- Advanced Powertrain Systems
- Automotive Systems Integration
- Human Factors/HMI
- Manufacturing and Materials
- Vehicle Performance
- Vehicle-to-Vehicle and Vehicle-Infrastructure Integration
- Vehicular Electronics

Testing Services at CU-ICAR

- The world's most advanced, automotive equipment research and development technology available to Clemson students, including
  - ❑ a road simulation and climate test chamber,
  - ❑ drive-on vehicle coordinate measurements,
  - ❑ an engine performance facility, and
  - ❑ machine shop.
- The services provided by these facilities are offered at a deep discount to industry (partners have use of these facilities at no cost).

TESTING SERVICES

CARROLL A. CAMPBELL JR. GRADUATE ENGINEERING CENTER

The 90,000-square-foot graduate building houses the automotive engineering graduate program and is the center for systems integration research activities as well as faculty, student, staff offices and conference facilities. The industry-focused and interdisciplinary program utilizes facilities that include full vehicle and engine/powertrain testing. In addition, visiting industry partner offices and visiting faculty offices provide comfortable space for our partners.

Click here for a complete list of testing facilities and equipment.

Carroll A. Campbell Graduate Engineering Center

CU-ICAR Laboratory and Testing Brochure

CU-ICAR COMPONENT TESTING LABORATORY

Industrial-scale laboratories and testing facilities are accessible for commercial use to companies and professionals for applied R&D on n technology. Thanks to world-class partners, the campus houses more $12 million in state-of-the-art full-vehicle, component and material te facilities and equipment.

Click here to read more about the Component Testing Lab.

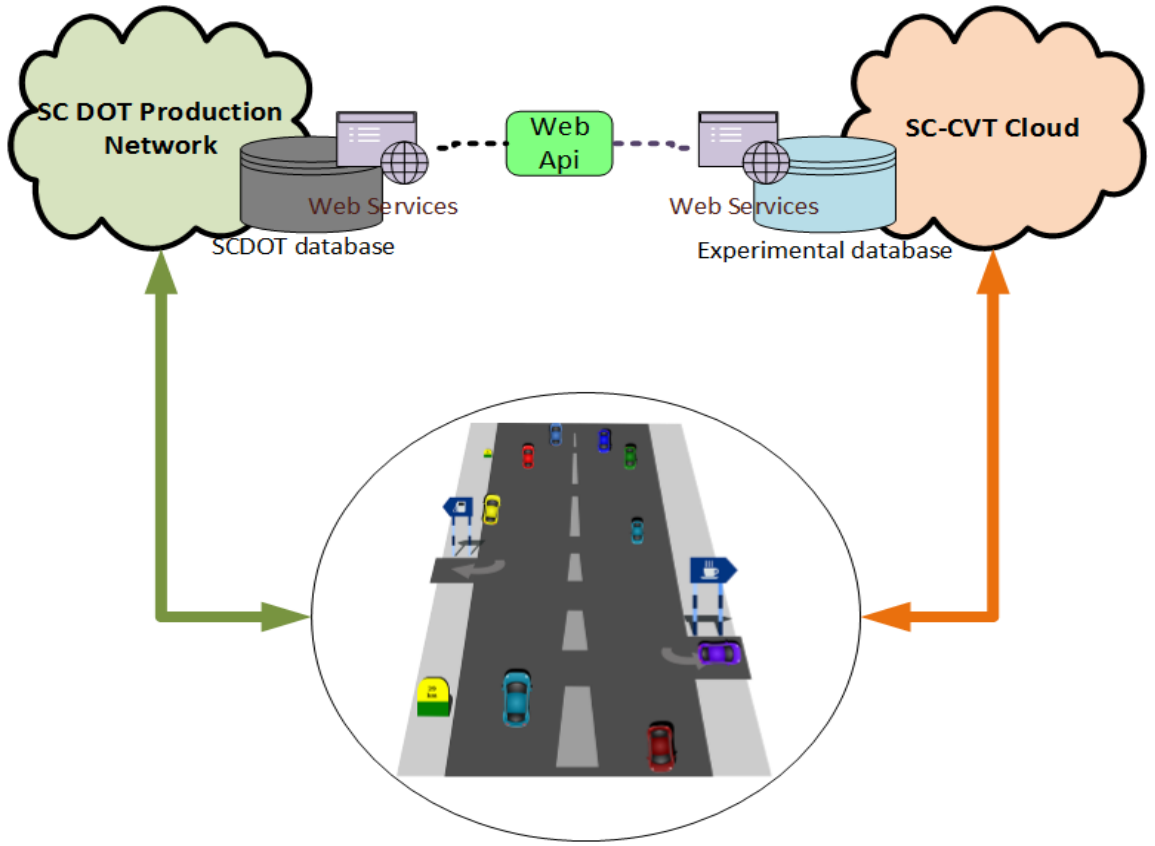
CU-ICAR Component Testing Laboratory

http://cuicar.com/

US Ignite

SC-CVT: South Carolina Connected Vehicle Testbed

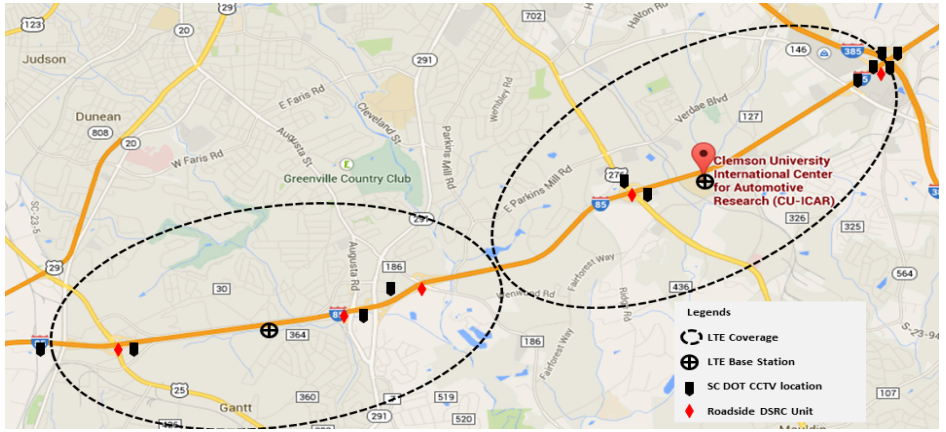
- Project will deploy DSRC/LTE/WiFi on a stretch of I-85 near Clemson
- SC DOT is involved, we can co-locate on their existing infrastructure and access their dark fiber
  - We can NOT connect to their network
  - We will make CV data available to SC DOT through a web interface



US Ignite

SC-CVT: South Carolina Connected Vehicle Testbed

- Advanced infrastructure: an SDN-enabled wireless infrastructure that includes DSRC, LTE, and Wifi
  - Cloud to the edge for IoT and M2M
  - Wireless hetnet architecture and service definition
- Specific Research Issues
  - Resource allocation strategy
  - Design and evaluation using SDN



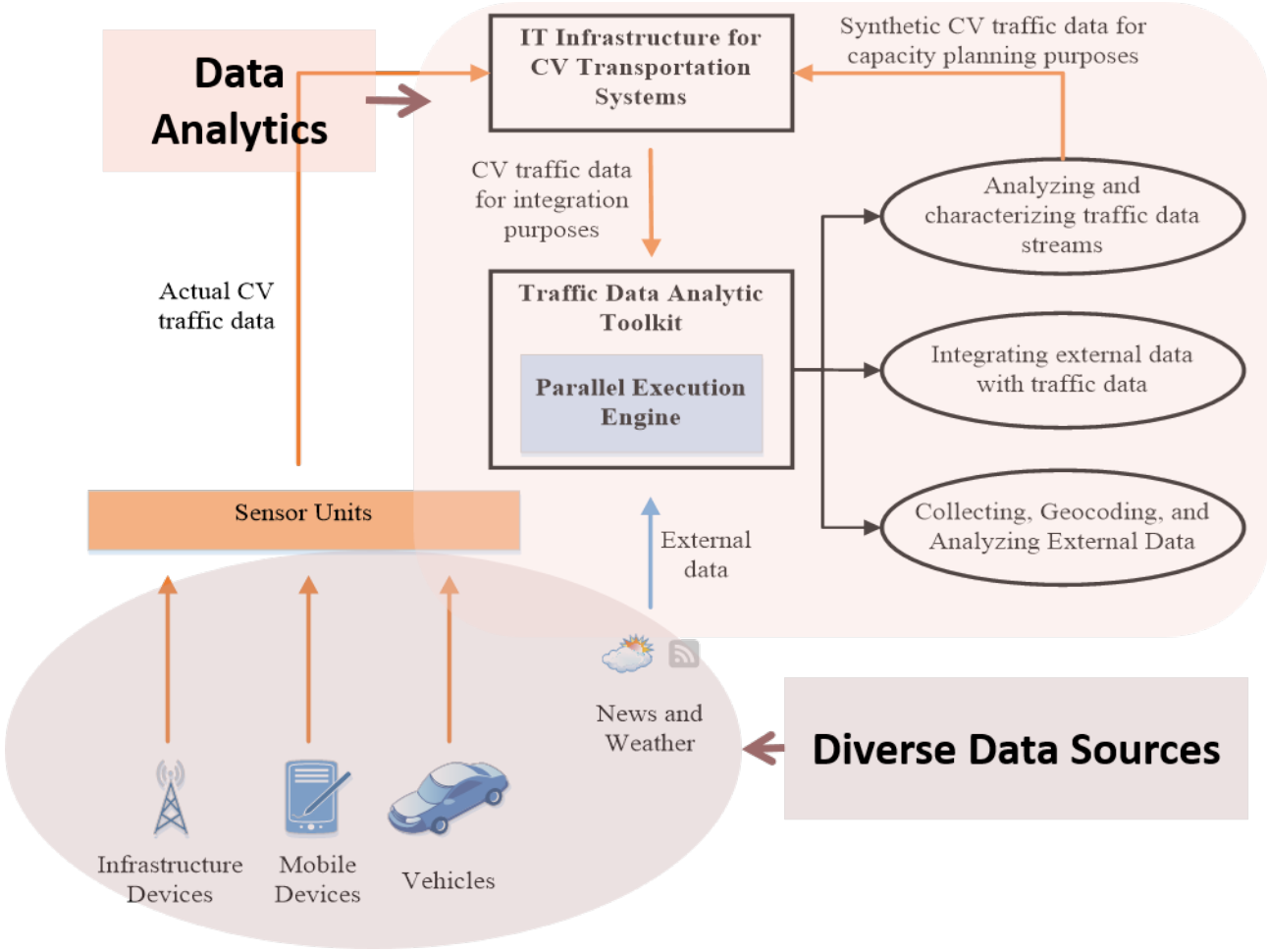
Tentative location for SC-CVT

Data Analytics in Connected Transportation

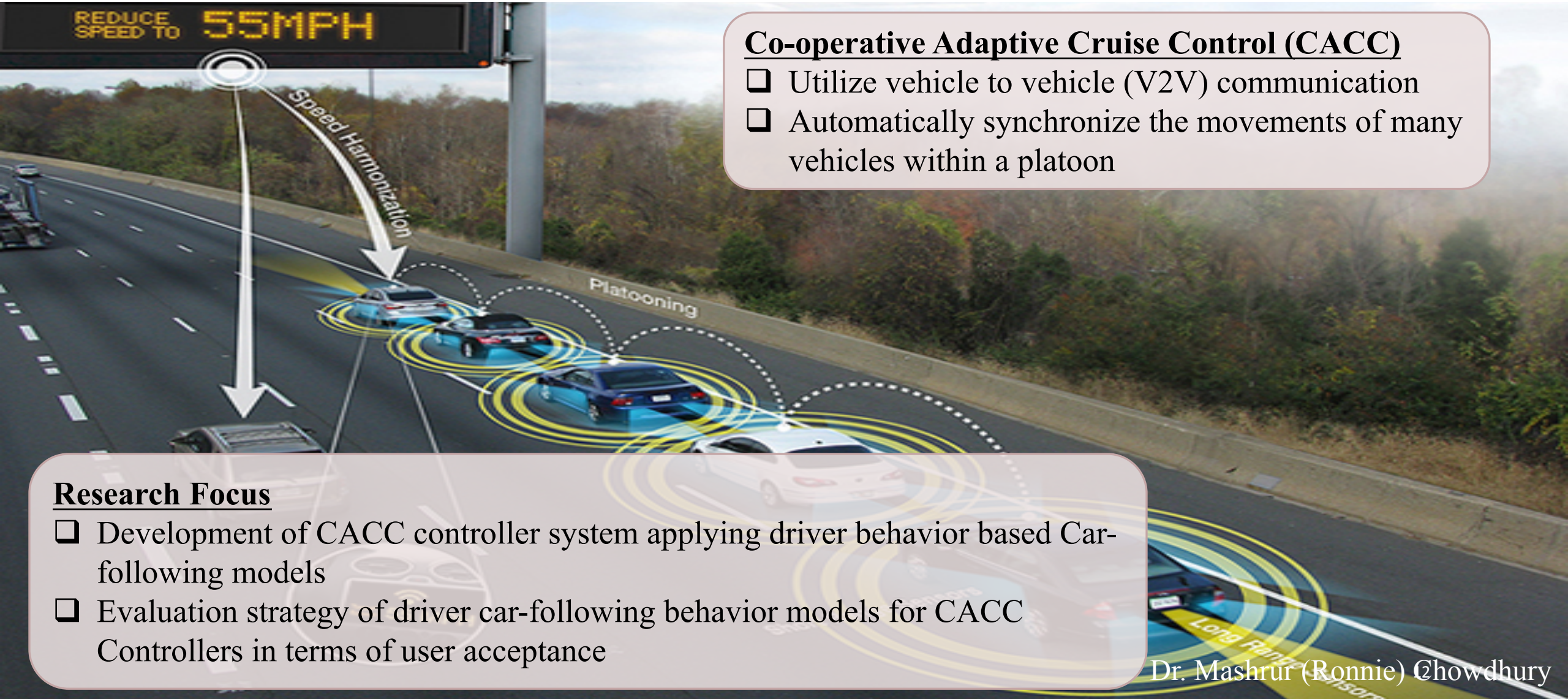
Data Analytics support the analysis of all collected connected transportation system data in combination with additional external data.

Research Focus

- ❑ Design of centralized and distributed data delivery infrastructure
- ❑ Evaluation of different data delivery Infrastructure



Co-operative Adaptive Cruise Control



Co-operative Adaptive Cruise Control (CACC)

- ❑ Utilize vehicle to vehicle (V2V) communication
- ❑ Automatically synchronize the movements of many vehicles within a platoon

Research Focus

- ❑ Development of CACC controller system applying driver behavior based Car-following models
- ❑ Evaluation strategy of driver car-following behavior models for CACC Controllers in terms of user acceptance

Feedback-based Network Optimization for Smart Cities

Research Focus

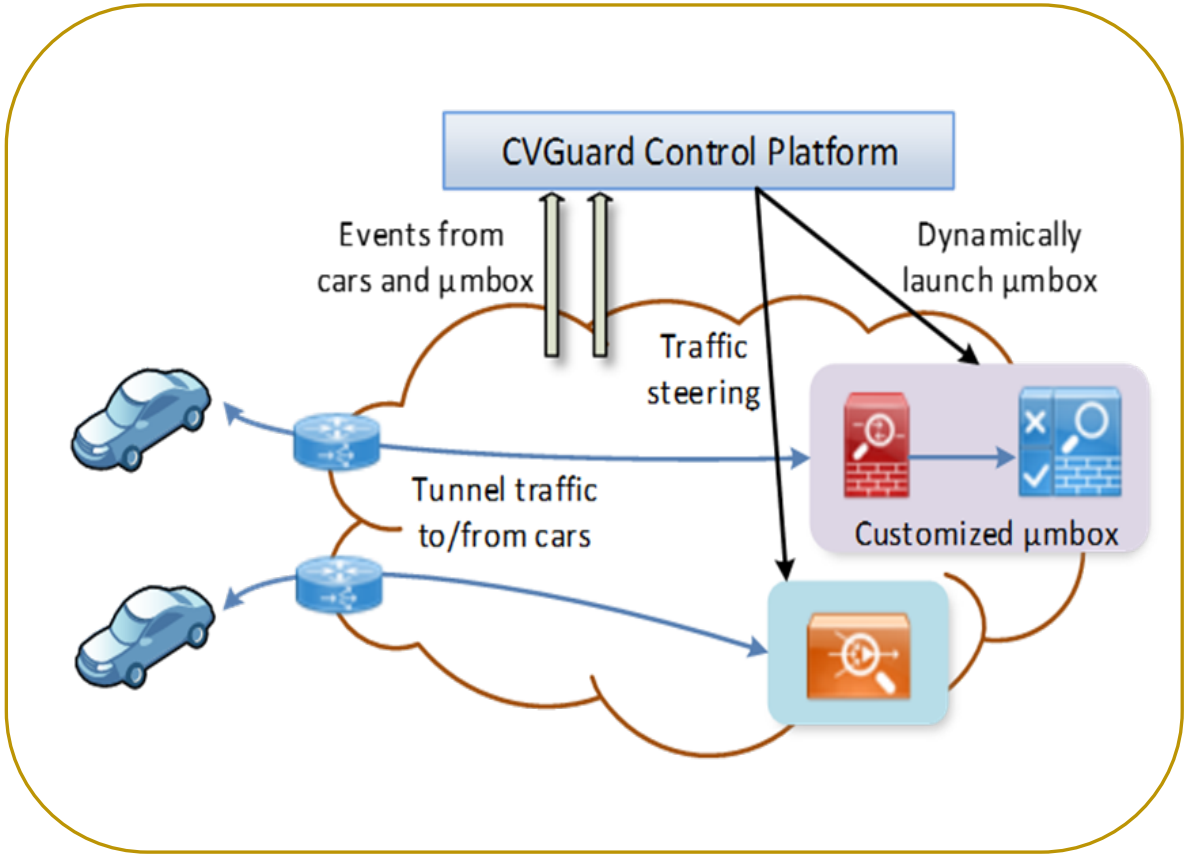
- Development of a human-concerned feedback mechanism to be integrated into an optimization framework of wireless charging infrastructure network
- Development of an efficient, multi-scale optimization algorithm for traffic system analysis, modeling, and management for transportation network in smart cities

Cybersecurity in Connected Vehicle Environment

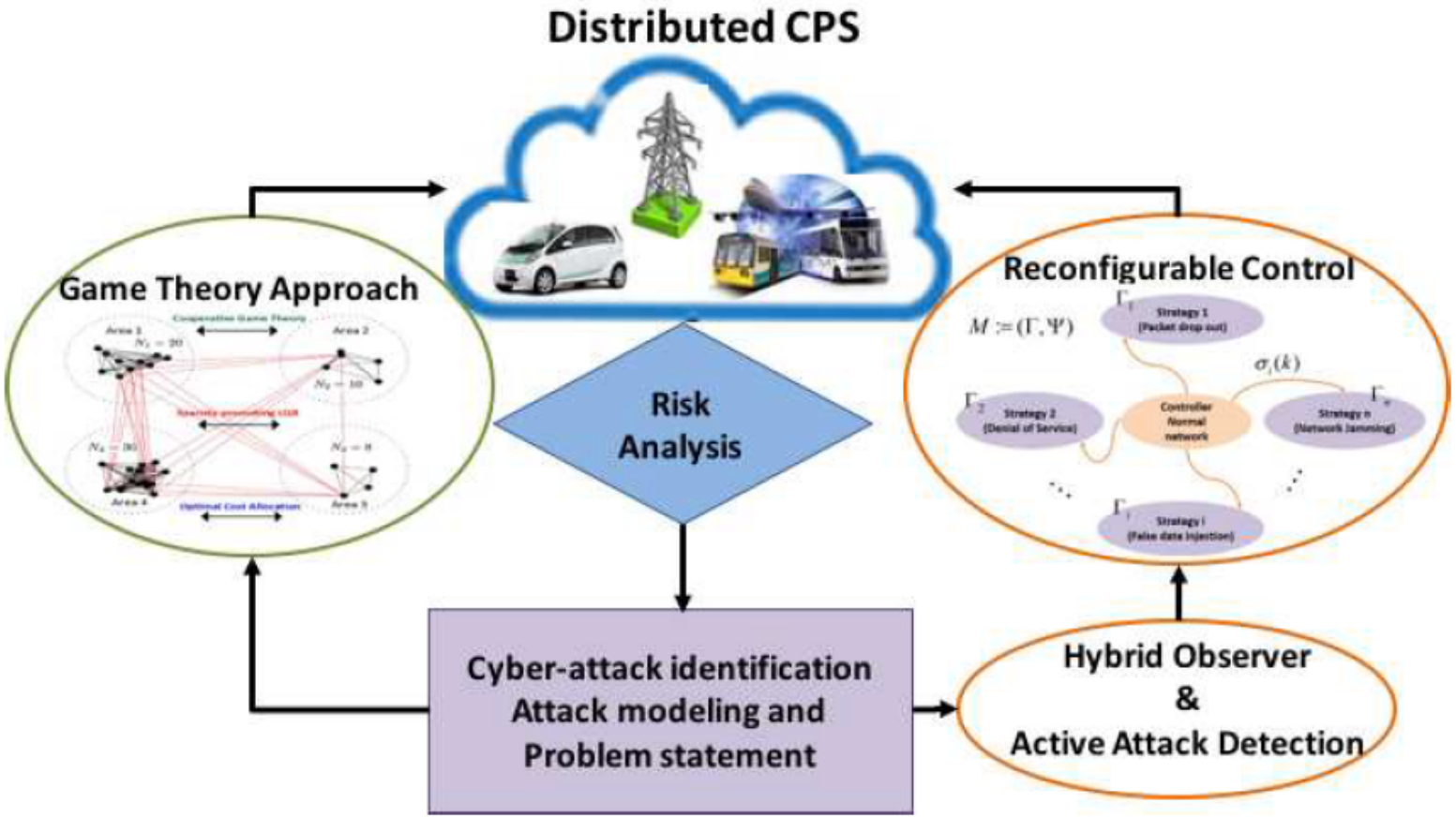
CVGuard is a security protection mechanism for a CV ecosystem, leveraging emerging network techniques like SDN, and NFV etc.

Research Focus

- ❑ Develop a security platform(CVGuard) against cyber-attack in CV environment
- ❑ Evaluate and Test the performance of the platform using simulated and real field use case scenarios



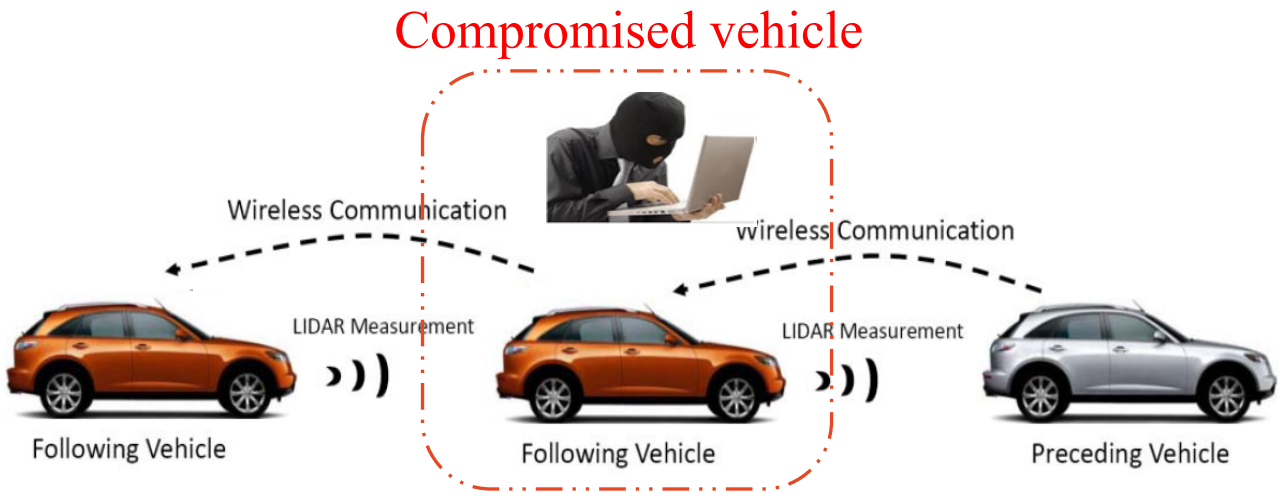
Security of Distributed Cyber-Physical Systems with Connected Vehicle Applications



Security of Distributed Cyber-Physical Systems with Connected Vehicle Applications

Game Theory: Attack Resilient Countermeasure

- One or more subsystems in distributed CPS are malicious
- Byzantine Generals
- Malicious components try to maximize the global cost function
- The rest of the group want to minimize the cost function
- Control countermeasure uses game theory



Computer Network Research @ Clemson

geni
Exploring Networks of the Future

OpenFlow

Google's OpenFlow WAN

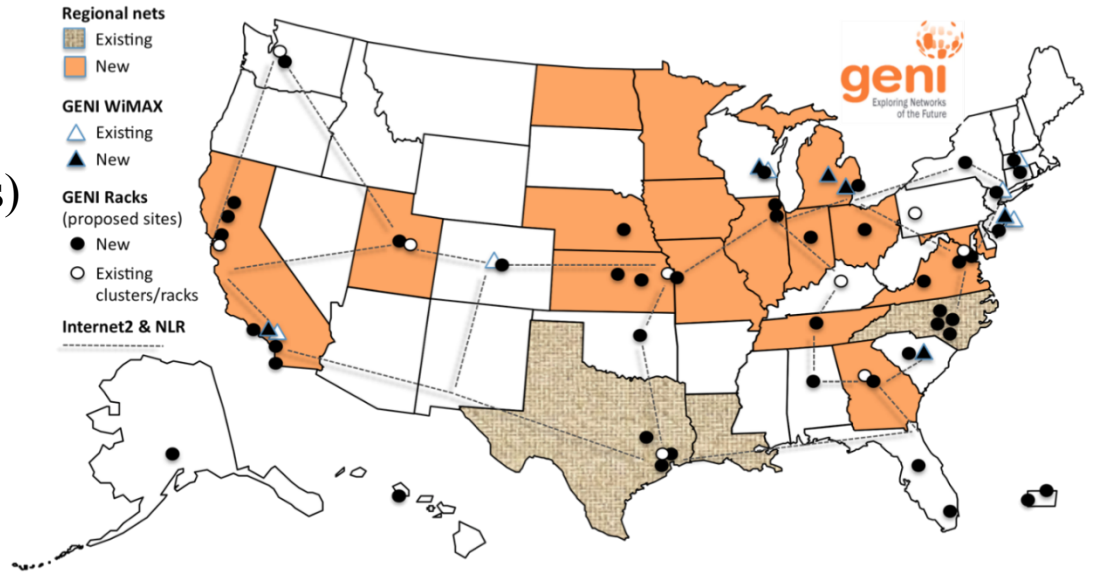
Google

What is GENI?

- The Global Environment for Network Innovations (GENI)

A federated testbed for network experiments (50 sites in more than 30 countries).

- GENI provides
  - ❑ Computing resources (VMs and bare machines)
  - ❑ Network resources (links, switches and WiMAX base stations)
- GENI allows experimenters to
  - ❑ Obtain compute resources from locations around the United States;
  - ❑ Connect compute resources using L2 networks in topologies best suited to their experiments;
  - ❑ Install custom software or even custom operating systems on these compute resources;
  - ❑ Control how network switches in their experiment handle traffic flows;
  - ❑ Run you own L3 and above protocols by installing protocol software in your compute resources and by providing flow controllers for their switches.



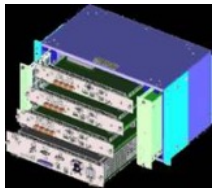
Clemson has been engaged in the NSF GENI project since its early phases.

GENI/OpenFlow@Clemson

GENI/OpenFlow Technology R&D

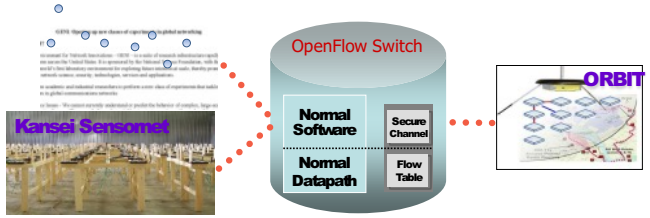
Mobile, Mesh, and Directional Vehicle Networks

WiMAX QoS and Security

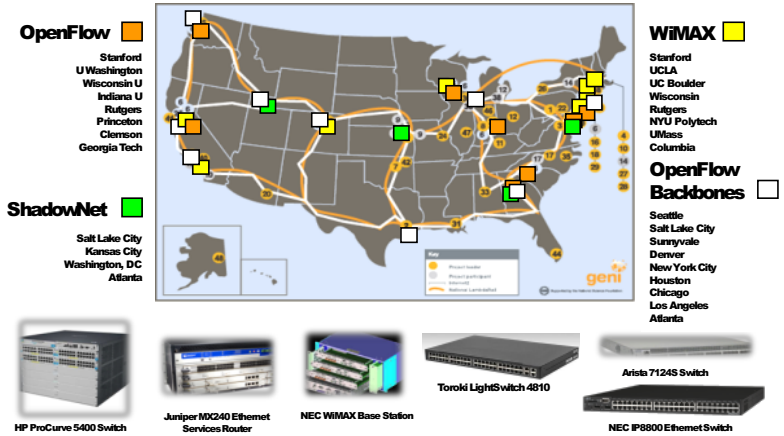


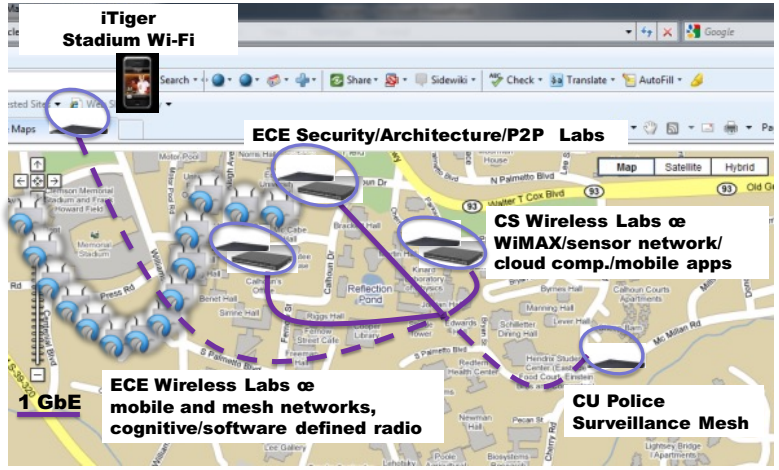
Software Defined Radio for Any-layer Experiment

P2P across Core, MANET, and Sensor Networks



Campus Deployment & Integration

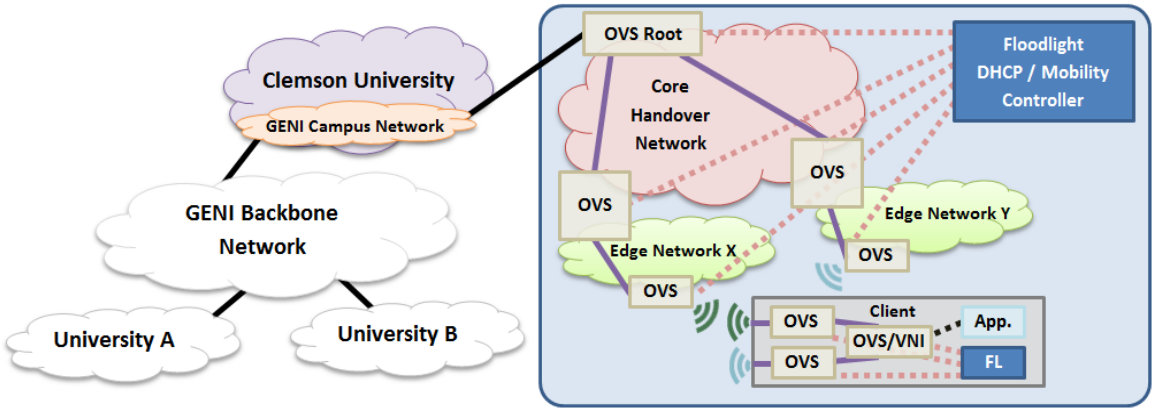




Including a campus OpenFlow Wi-Fi corridor for vehicle networking research

An OpenFlow Testbed for the Evaluation of Vertical Handover Decision Algorithms

- The Open-Access Research Testbed for the Next-Generation Wireless Network (ORBIT)
  - ❑ First funded in 2003 under the Network Research Testbeds (NRT) program and subsequently under a number of follow-on grants.
  - ❑ Support wireless aspects of the GENI.
  - ❑ the ORBIT Management Framework (OMF) is one of the core control frameworks in GENI.
- Clemson is a partner of ORBIT.
- Clemson is one of the GENI WiMAX campuses with ORBIT nodes.



System Framework

DoS Detection

- Entropy features are common in recent DDoS detection publications. Are entropy-based detections really effective in the really world?
  - Simple answer is No…
- A **mirrored copy** of Clemson University campus network traffic was used as background traffic during the tests (see Figure).
- A entropy-spoofing attack is presented.

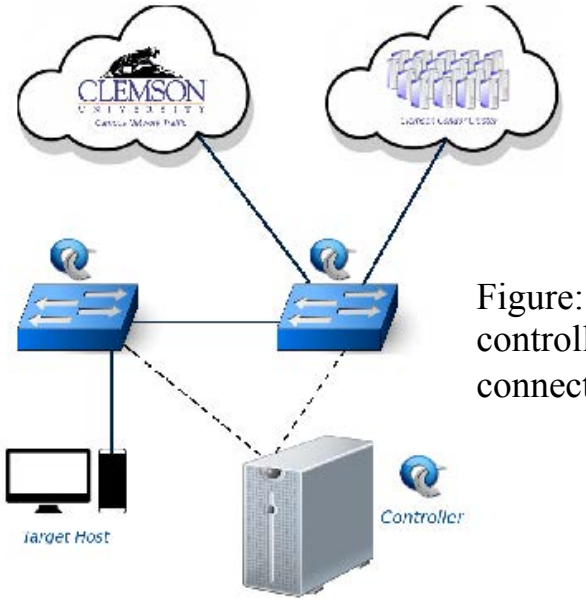
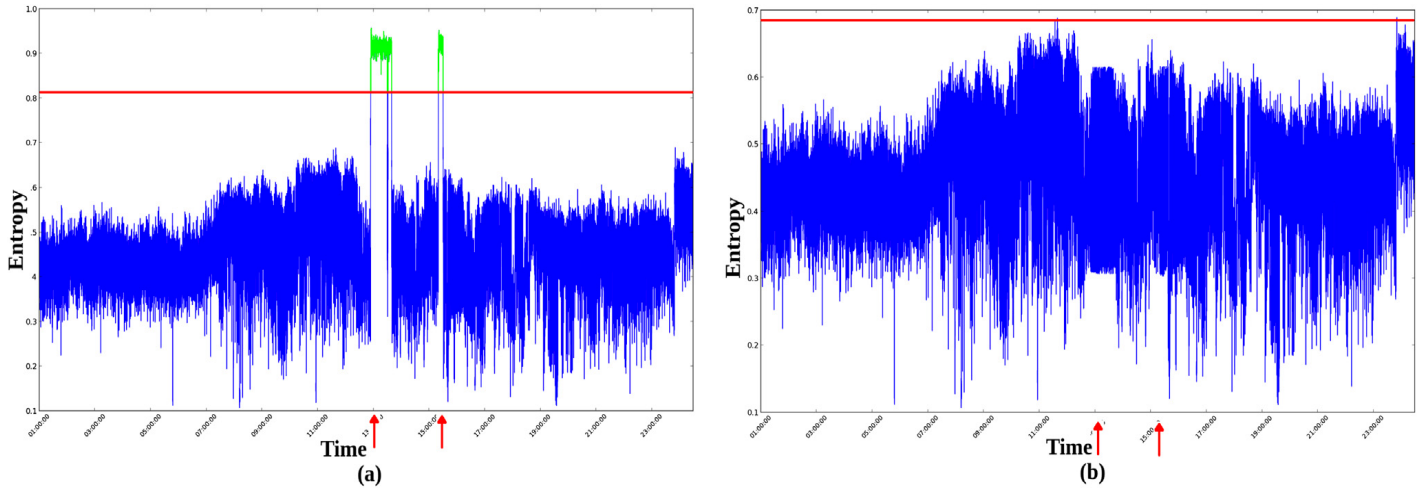
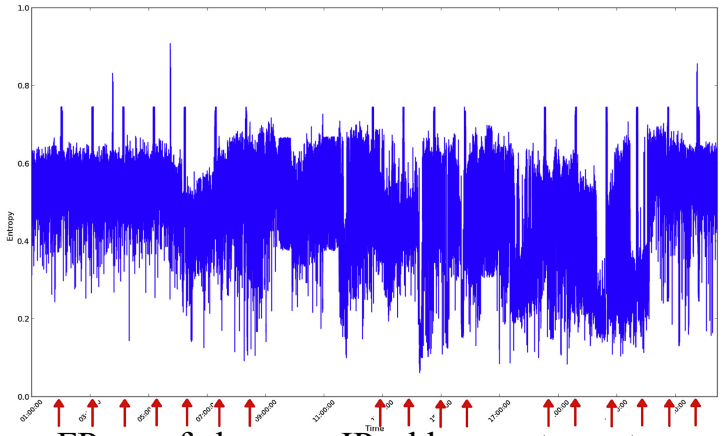


Figure: Test setup and controller logical connection.

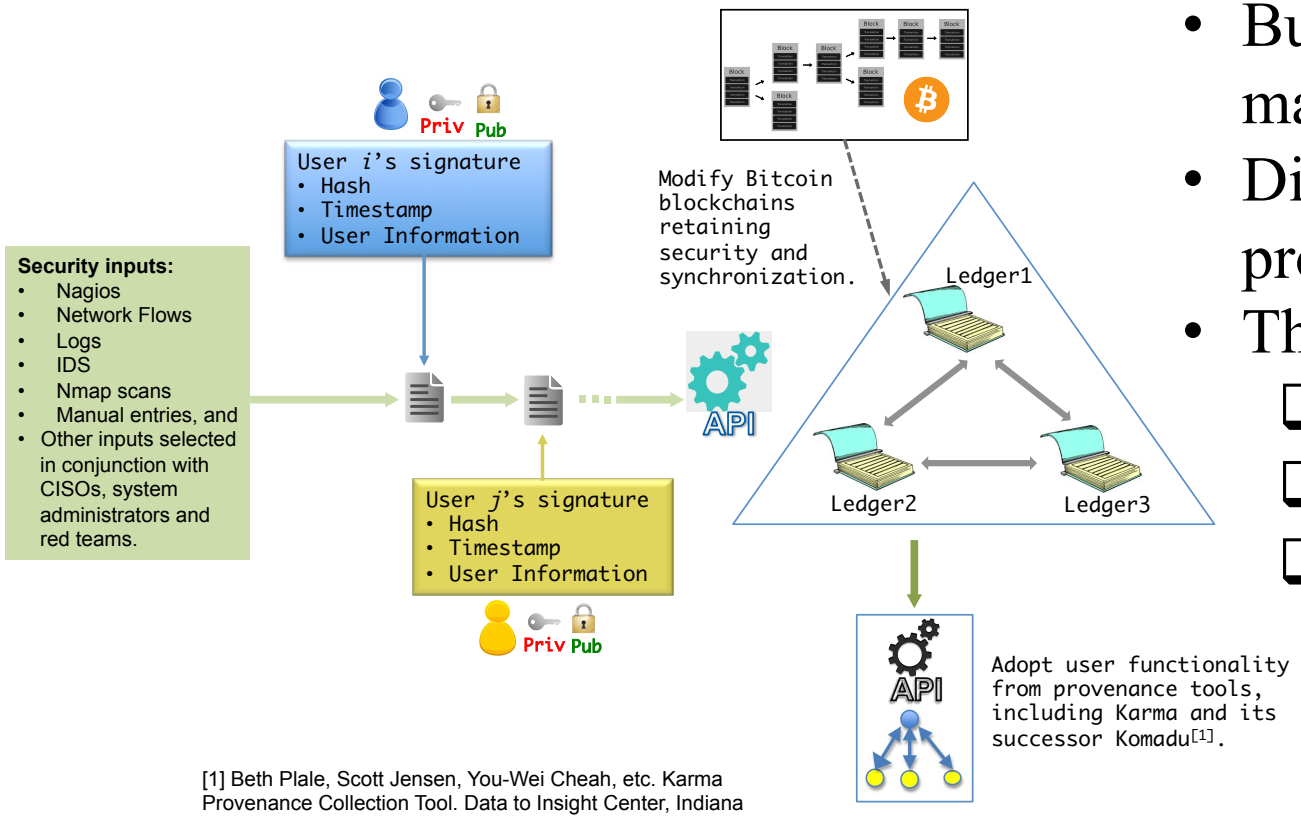


(a) Source IP address entropy trace with 2 DDoS attacks (b) Spoofed source IP address entropy trace with 2 DDoS attacks. Attacks are shown using arrows.



FP spoofed source IP address entropy trace.

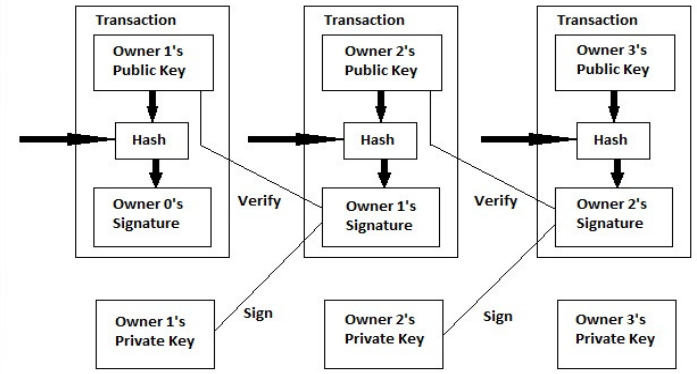
Provenance Assurance Using Currency Primitives



[1] Beth Plale, Scott Jensen, You-Wei Cheah, etc. Karma Provenance Collection Tool. Data to Insight Center, Indiana University Pervasive Technology Center. Available: http://d2i.indiana.edu/tools

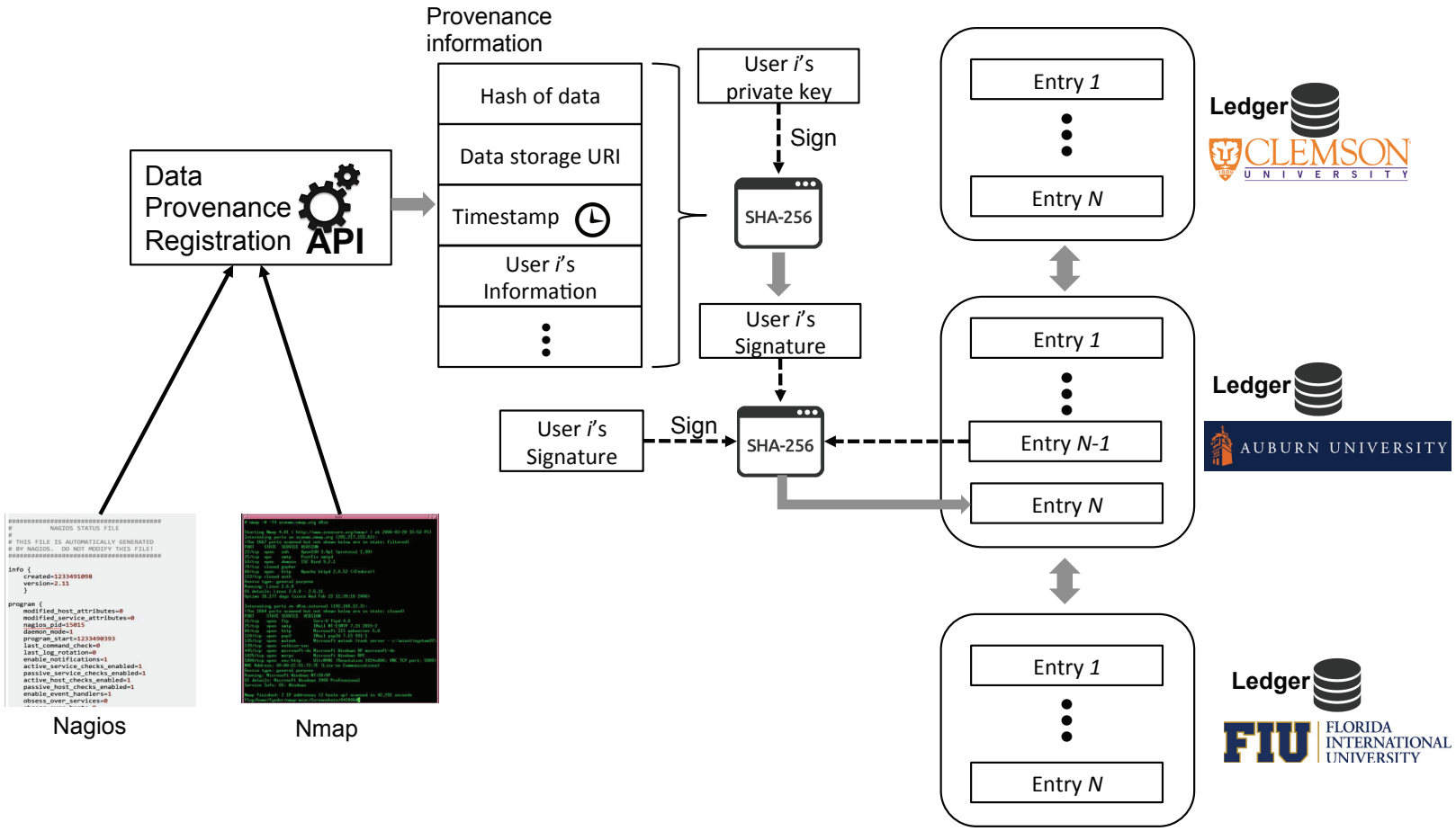
System Overview.

- Build on the block-chain infrastructure to maintain provenance metadata securely.
- Distributed ledgers that maintain distributed provenance data outside of user control.
- Three use cases:
  - ❑ Academic integrity (scientific workflows)
  - ❑ Digital forensics
  - ❑ Log security



The blockchain of Bitcoin.

Provenance Assurance Using Currency Primitives



The use case of system log security.

A collaborative research effort between Clemson, Auburn and FIU.

SCIGUARD: A Security Architecture for Science DMZ based on SDN and NFV

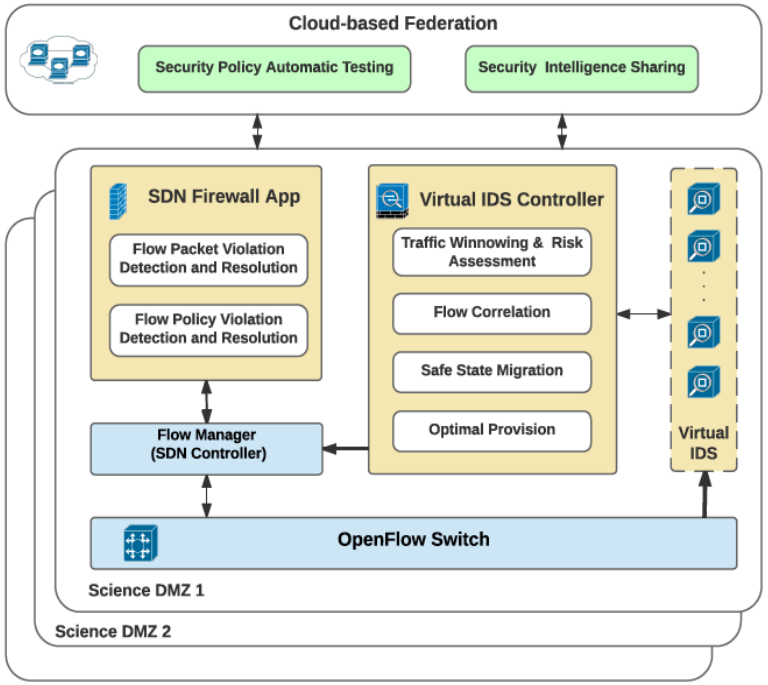


Figure: SCIGUARD architecture overview.

- ❑ Task 1: SDN firewall application for securing science DMZ
- ❑ Task 2: NFV-based virtual IDS for securing science DMZ
- ❑ Task 3: Cloud-based Federation for the science DMZ

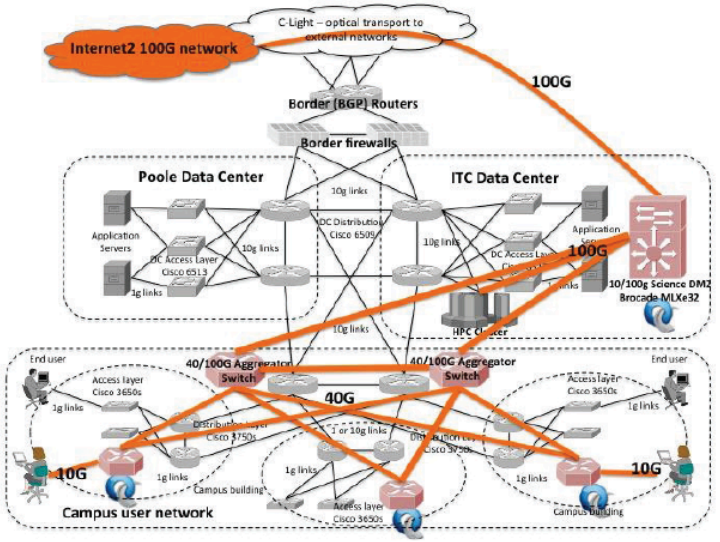


Figure: Clemson Science DMZ.

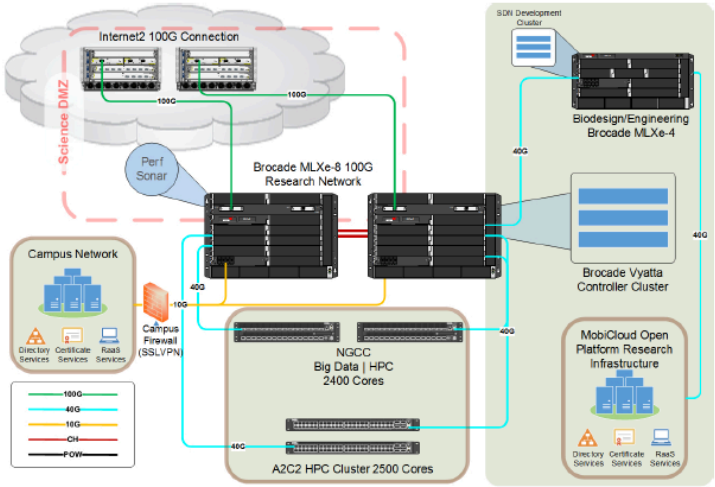


Figure: ASU Science DMZ.

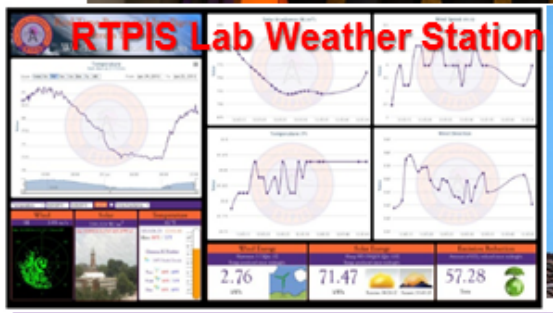
- ❖ A collaborative research between Clemson and ASU.

Smart Grid Research @ Clemson

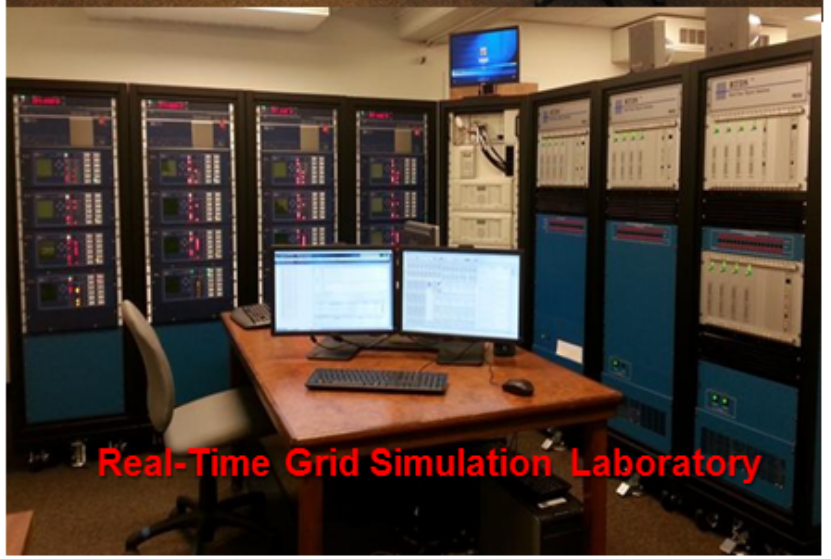
CLEMSON UNIVERSITY

Real-Time Power and Intelligent Systems (RTPIS) Laboratory

Emphasis: Research, Education and Innovation-Ecosystem Laboratory for Smart Grid Technologies

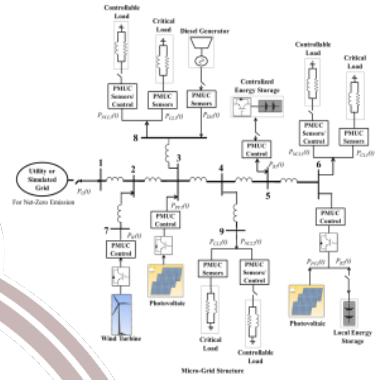


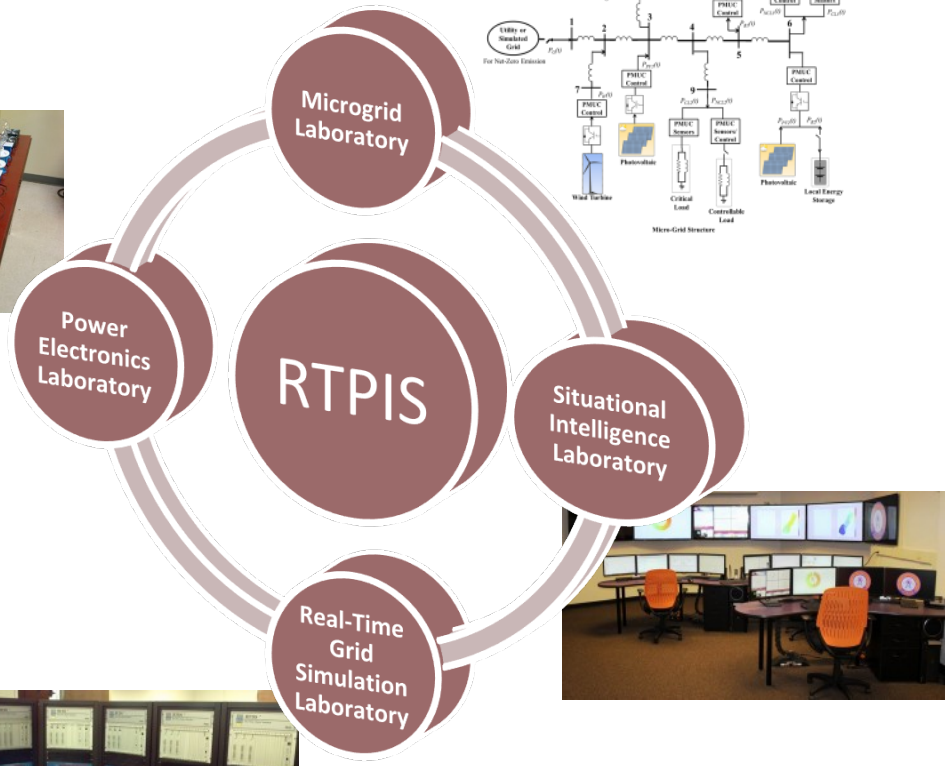
Director: Dr. Kumar Venayagamoorthy
gvenaya@clemson.edu; http://rtpis.org

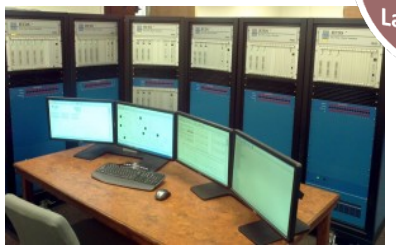


Real-Time Power and Intelligent Systems (RTPIS) Laboratory

- RTPIS Laboratory is a premier world class research, education and innovation-ecosystem laboratory for smart grid technologies.
- Smart Grid Research areas include, but not limited to,
  - adaptive devices and intelligent circuits and systems,
  - big data analytics and visualization,
  - computational methods and high performance computing platforms,
  - cyber-physical systems and cyber-security,
  - hardware/software-in-the-loop simulation,
  - micro-grids and nano-grids,
  - plug-in electric and hybrid vehicles, power electronics,
  - power system computation, control, modeling, operation and stability,
  - renewable energy systems,
  - real-time/faster than real-time large scale power system simulation and operational intelligence,
  - sensor networks and synchrophasor technology,
  - signal processing and wide area systems.







http://rtpis.org/

Real-Time Power and Intelligent Systems (RTPIS) Laboratory

Projects

All-Electric Ship Power System

Brain-Like Intelligence for Complex Systems

Clemson University's Synchrophasor Engineering Education Program (CU ShEEP)

Dynamic Energy Management System for a Smart Microgrid

Dynamic Stochastic Optimal Control of Power Systems

Frequency Stability and Control of a Power Plant with Large PV Plants Using PMU Information

Intelligent Cyber Physical Power and Energy System

Real-Time Predictive Modeling and State Estimation for Power Systems

Real-Time Small Coherency Analysis and Visualization for Multi-machine Power Systems

Real-Time Small Signal Stability Analysis for Power Systems

Grants

EFRI-COPN: Neuroscience and Neural Networks for Engineering the Future Intelligent Electric Power Grid

GOALI: Neural Networks and Adaptive Critic Designs For Energy Security and Sustainability

Scalable Intelligent Power Monitoring and Optimal Control of Distributed Energy Systems Using Adaptive Critics

RAPID: Impact of Earthquakes on the Electricity Infrastructure

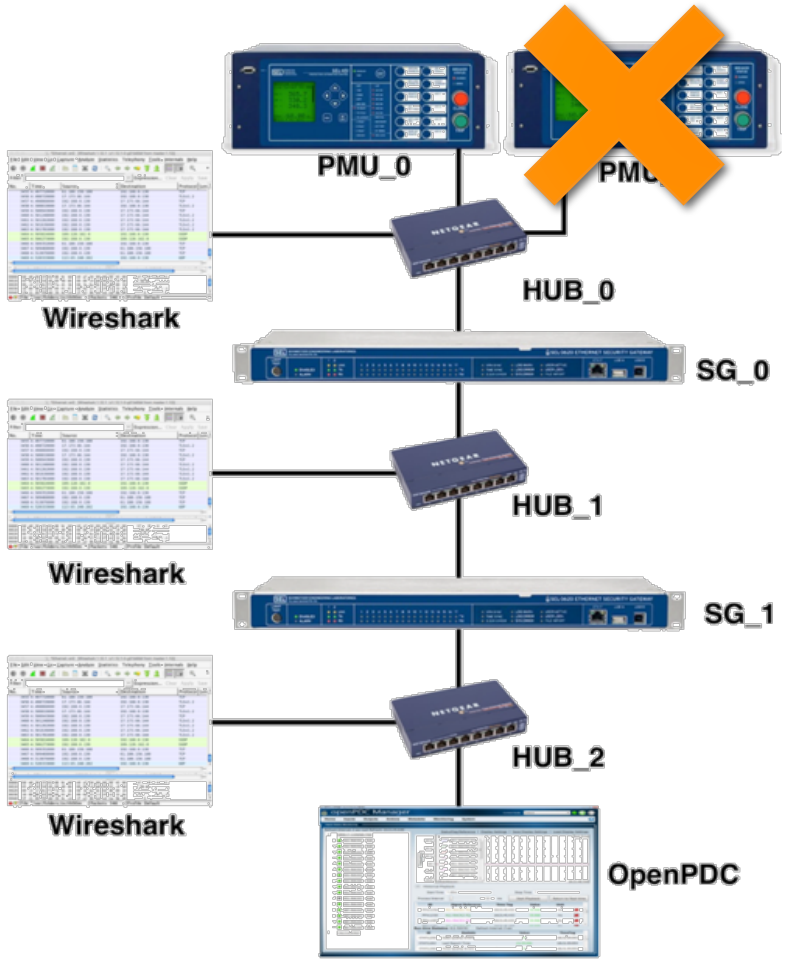
AIR Option 2: Research Alliance Situational Intelligence for Smart Grid Optimization and Intelligent Control

Collaborative Research: Computational Intelligence Methods for Dynamic Stochastic Optimization of Smart Grid Operation with High Penetration of Renewable Energy

Side-channel Attacks against Smart Grid

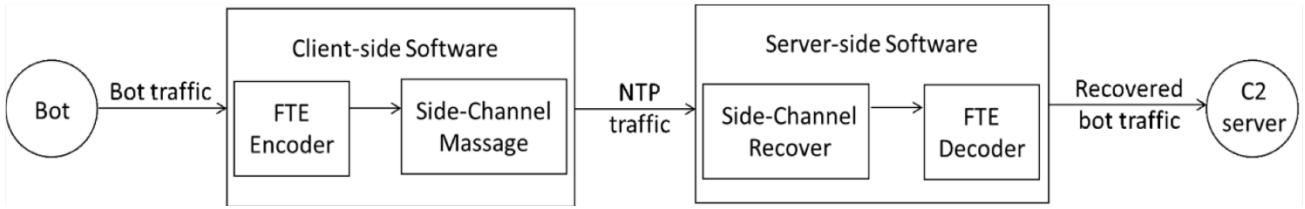
- **Side-Channel Attacks** extract *useful information* by observing implementation artifacts.

- Hidden Markov Models (HMM) can be used to map packets to PMUs.
- VPN tunnel (Hard to detect).
- The ability to differentiate packets sources in near real-time make it possible to **identify**, **redirect** and **drop** a target network communication application without infect other network communication instances within the same



Smart Grid Traffic Camouflage

- **Traffic Camouflage** counters traffic analysis by camouflaging PMU traffic as another protocol.
- Method:
  - ❑ Format-transforming encryption (FTE) translates protocol syntax to mimic another innocuous protocol
  - ❑ while side-channel massage (SCM) obscures traffic side-channels.
- Results:
  - ❑ The syntax of the counterfeit PMU packet is consistent with real PMU traffic.
  - ❑ False PMU packets are accepted by OpenPDC without any errors.



Filter: tcp.srcport == 4712 Expression... Clear Apply Save

No.	Delta time displayed	Framesize	Protocol	Info
4	0.000000000		TCP	4712→62849 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
8	0.001280000		TCP	4712→62849 [ACK] Seq=1 Ack=19 Win=408256 Len=0 TS
10	0.000083000		TCP	4712→62849 [ACK] Seq=1 Ack=37 Win=408256 Len=0 TS
11	0.001065000	954	SYNCHROPHASOR	Configuration Frame 2
14	0.000244000		TCP	4712→62849 [ACK] Seq=955 Ack=55 Win=408224 Len=0
15	0.026628000	284	SYNCHROPHASOR	Data Frame
17	0.048858000	284	SYNCHROPHASOR	Data Frame
19	0.026190000	284	SYNCHROPHASOR	Data Frame
21	0.051151000	284	SYNCHROPHASOR	Data Frame
23	0.025759000	284	SYNCHROPHASOR	Data Frame
25	0.051969000	284	SYNCHROPHASOR	Data Frame
27	0.025822000	284	SYNCHROPHASOR	Data Frame

(a) Screen-shot of false PMU traffic (part)

Filter: ip.src==192.168.65.9 Expression... Clear Apply Save

No.	Delta time displayed	Framesize	Protocol	Info
78	0.000000000		TCP	4712→62665 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0
86	0.002932000		TCP	4712→62665 [ACK] Seq=1 Ack=19 Win=8742 Len=0
89	1.000115000		TCP	4712→62665 [ACK] Seq=1 Ack=37 Win=8724 Len=0
93	0.001743000	954	SYNCHROPHASOR	Configuration Frame 2
96	0.002656000		TCP	4712→62665 [ACK] Seq=955 Ack=55 Win=8706 Len=0
98	0.040361000	284	SYNCHROPHASOR	Data Frame
101	0.025043000	284	SYNCHROPHASOR	Data Frame
103	0.024950000	284	SYNCHROPHASOR	Data Frame
107	0.050074000	284	SYNCHROPHASOR	Data Frame
110	0.024846000	284	SYNCHROPHASOR	Data Frame
111	0.025111000	284	SYNCHROPHASOR	Data Frame
116	0.050022000	284	SYNCHROPHASOR	Data Frame

(b) Screen-shot of real PMU to PDC traffic (part)

THANK YOU FOR YOUR ATTENTION!
ANY QUESTIONS?
memegenerator.net