Herbert Wertheim College of Engineering
UNIVERSITY of FLORIDA

IEEE Internet of Things

Internet of Things (IoT) Summit at RWW2020
26-27 January 2020 // San Antonio, Texas, USA

Securing the Insecure

Developing Software-Defined Network Frameworks for Securing Wireless Sensing IoT Applications

Janise McNair
University of Florida
Wireless & Mobile Systems Lab
www.wam.ece.ufl.edu

POWERING THE NEW ENGINEER TO TRANSFORM THE FUTURE

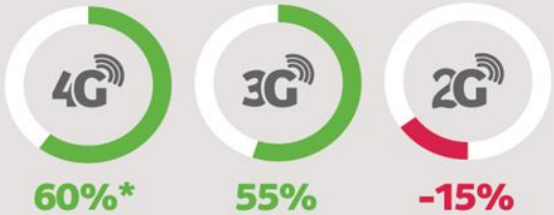
Internet of Things and Wireless Sensing

- **Internet of Things (IoT)**
  - A new communication system where the Internet is connected to the physical world via ubiquitous wireless sensor networks (WSNs).
- Internet everywhere!
- Physical world objects called “things”
- Near constant information exchange
- Evolving heterogeneous network traffic and user expectations

NOKIA

MBiT Index

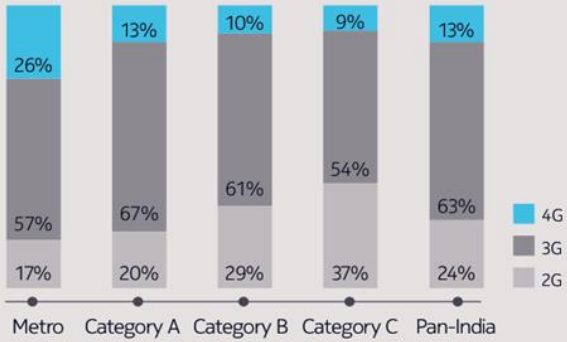
Share of incremental data payload: 2016 vs 2015



*(excluding Reliance Jio)

76% Total data traffic contributed by 3G+4G

Contribution of 2G, 3G and 4G

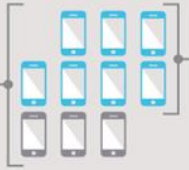


Data consumption/sub

4G 1400+ MB

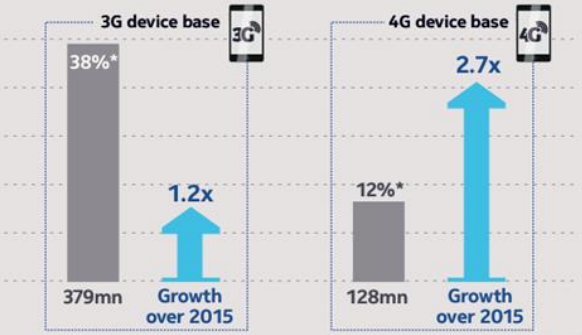
3G 850 MB

7 of 10 smartphones shipped are 4G and entry level phone priced at just **INR3,000**



4G smartphones are becoming mainstream

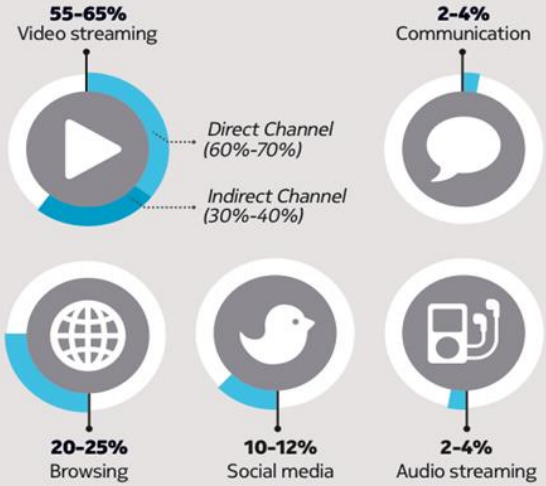
User base (mn)



*Device penetration

LTE device support by band (% of LTE devices)

Video drives data consumption, and social media and communication engage users



Operators are considering network deployment initiatives to support the data traffic surge and improve user experience

NOKIA

MBiT Index

Total data traffic growth

44x

2015 2019

Data traffic by technology

96% 4G

4% 3G

No. of 4G Data users

598 Million

Average usage/ month/ user

11.2 GB

CAGR of avg usage/ month/ user 2015-19

93%

Users with 4G devices

67% Device Penetration

4G

501 mn 4G capable unique devices

86% of 4G capable devices are VoLTE capable

LTE Device support by band

LTE 1800	99.6%
TDD 2300	96%
LTE 850	96%
LTE 2100	90%
LTE 900	71%
TDD 2500	59%
LTE 700	22%

Video consumption pattern

% of daily online video watching time

Others, 1.2%

Mobile Phone, 88%

OTT trends

70 mins/day
Average Time Spent on OTT Platforms

12.5 times/week
Average Frequency of Access

40 mins
Average Single Session Duration

Private LTE potential

adoption in....

Manufacturing

Logistics

Warehousing

Mining

application in....

Remote Monitoring

Robotics

Improving OEE

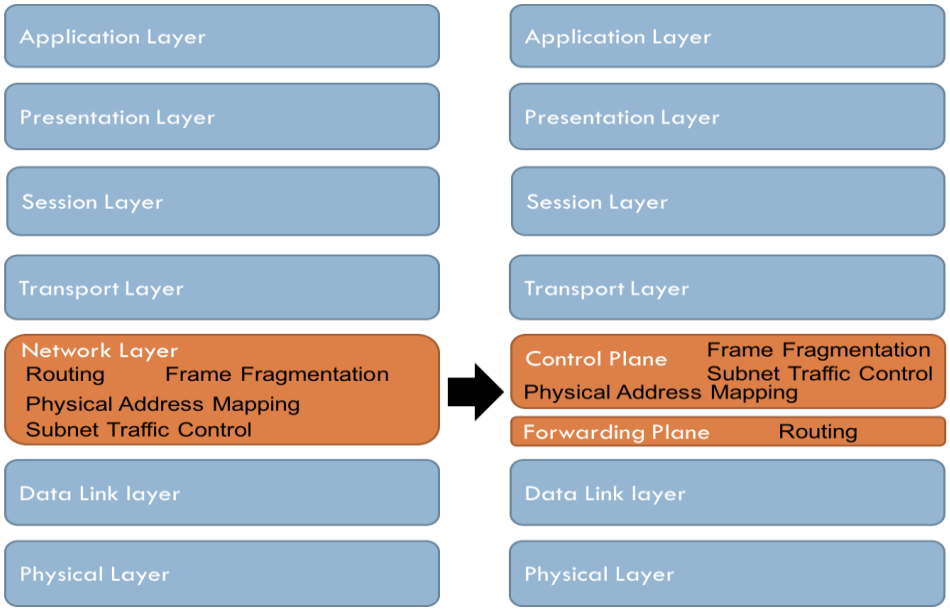
Material Handling

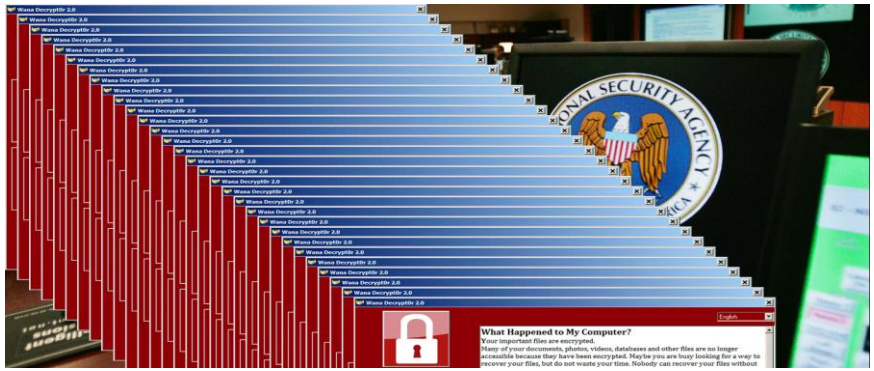
VR and Smart security

Networking Security Risks

Popular Cyber Attacks

- Malware
  - **WannaCry ransomware attack -** May 2017
  - 200,000 Microsoft devices infected
  - 100 million to billions worth of damage

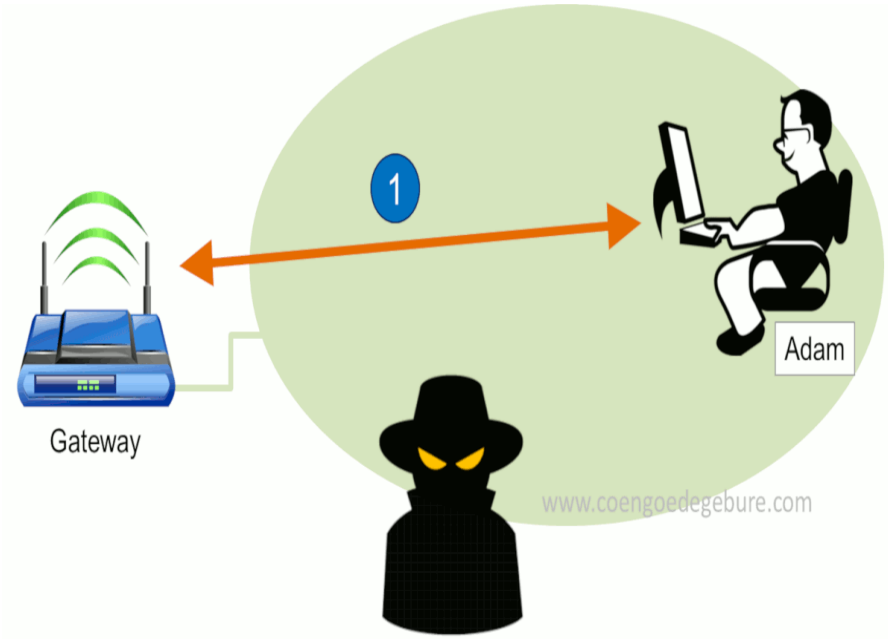


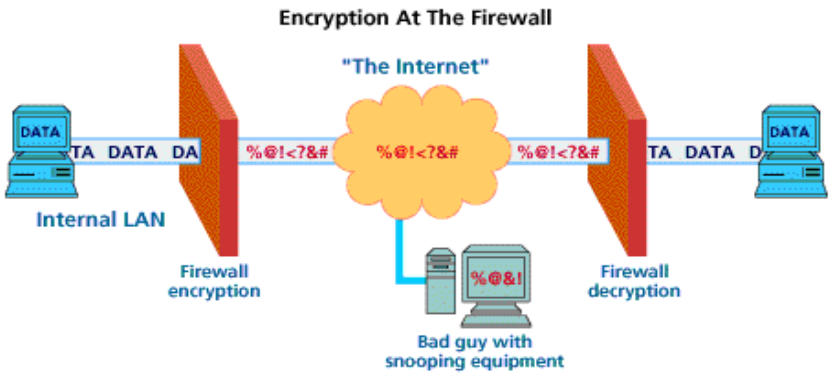


Networking Security Risks

Popular Cyber Attacks

- Malware
  - **WannaCry ransomware attack -** May 2017
  - 200,000 Microsoft devices infected
  - 100 million to billions worth of damage
- Man-in-the-Middle (MITM)
  - **The US National Security Agency posing as Google** – 2013

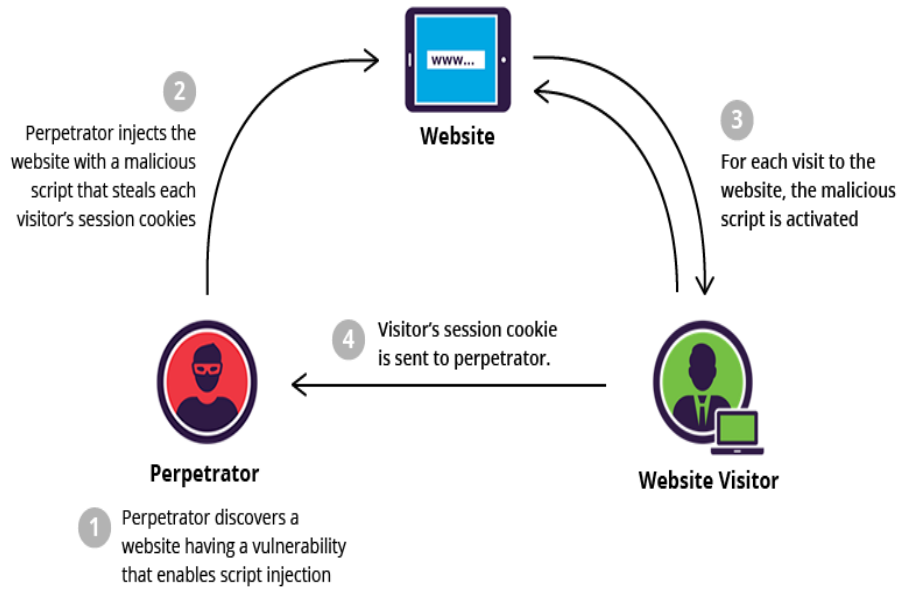


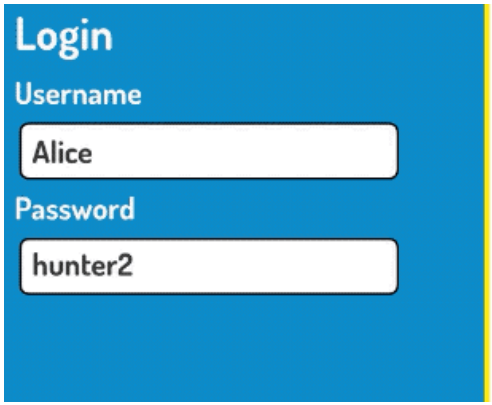


Networking Security Risks

Popular Cyber Attacks

- Malware
  - **WannaCry ransomware attack -** May 2017
  - 200,000 Microsoft devices infected
  - 100 million to billions worth of damage
- Man-in-the-Middle (MITM)
  - **The US National Security Agency posing as Google** – 2013
- SQL Injection
  - **Capital One data breach** – 2019
  - 100 million customers hacked



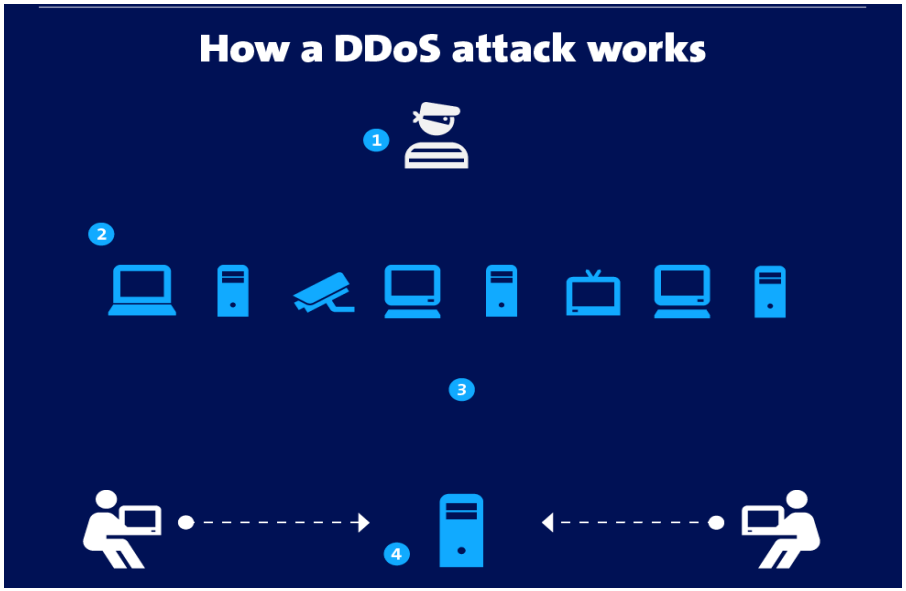


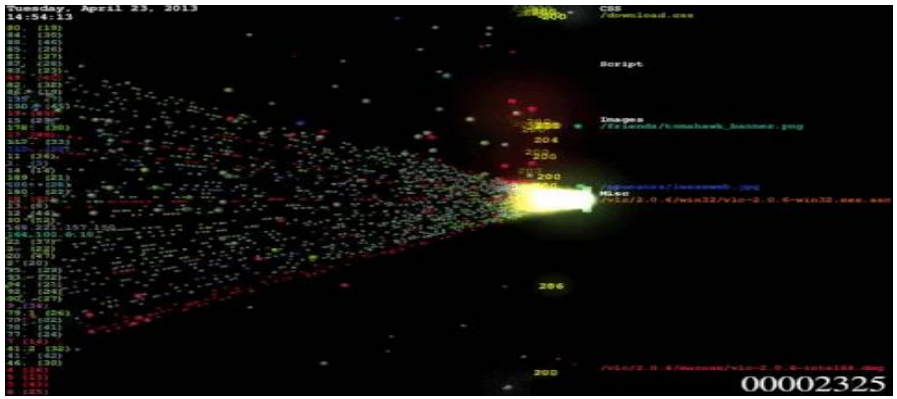

```
/* SQL */

SELECT COUNT(*)
FROM USERS
WHERE USERNAME = 'Alice'
AND PASSWORD = 'hunter2'
```

Networking Security Risks

Popular Cyber Attacks

- Malware
  - **WannaCry ransomware attack -** May 2017
  - 200,000 Microsoft devices infected
  - 100 million to billions worth of damage
- Man-in-the-Middle (MITM)
  - **The US National Security Agency posing as Google** – 2013
- SQL Injection
  - **Capital One data breach** – 2019
  - 100 million customers hacked
- Distributed Denial of Service (DDoS)
  - **Mirai botnet** – 2016
  - 600,000 devices infected
  - East coast left with no access to internet





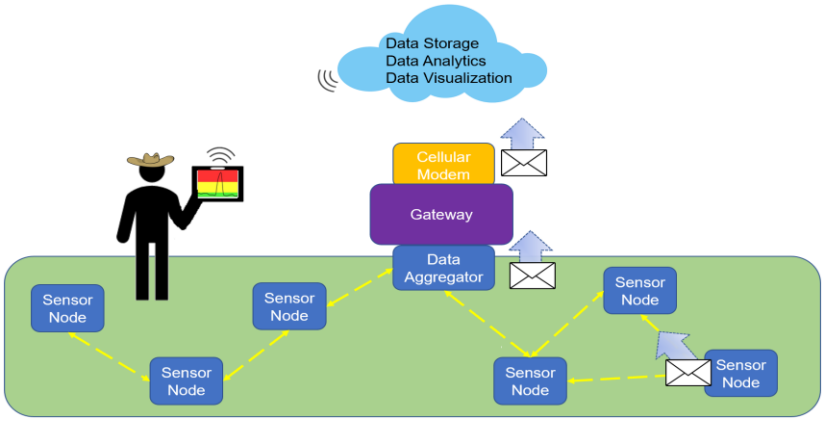
Challenge: The Expanse of IoT

- Virtually every physical thing in this world can also become a computer that is connected to the Internet.
- Decline of size, cost, energy consumption, hardware dimensions,…
- Expansion of memory, computing, wireless communications, cloud access
- Allow the manufacturing of extremely small and inexpensive low-end computers.
- Allow adoption into new and exciting areas, that are not prepared for the slate of IoT protocols and the network security challenges, e.g.,:
  - Agriculture
  - Construction
  - Smart Grid

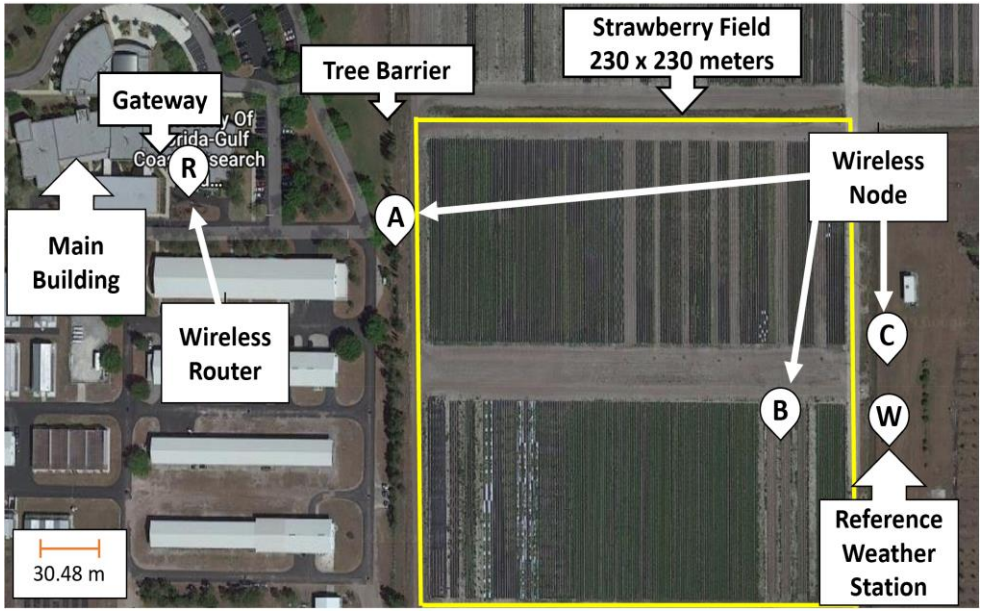
IoT Protocols

Function	IoT Protocols
Networking	6LowPAN (lightweight IPv6), RPL, LoRaWAN
Identification	EPC, uCode, IPv6, URIs
Communications	Xbee, Wifi, Bluetooth, LPWAN
Discovery	Physical Web, mDNS, DNS-SD
Data Protocols	MQTT, CoAP, AMQP, Websocket
Device Management	TR-069, OMA-DM
Semantic	JSON-LD, Web Thing Model
Multi-layer Frameworks	Alljoyn, IoTivity, Weave, Homekit

Case 1: Security and Data: IoT in Agriculture



Collect data
Manage and control processes
Disseminate data
Interact with non-technical customers



Recent security challenges

T&A recalls whole heads of romaine lettuce for E. coli contamination

By News Desk on November 9, 2020

A public notice sent out today by the FDA announces a romaine lettuce recall three days after Tanimura & Antle initiated the action because of tests in Michigan that showed E. coli O157:H7 contamination.

The notice from the Food and Drug Administration, dated Nov. 6, reports that the California company is recalling certain whole heads of romaine. Tanimura & Antle officials said the implicated romaine was packed on Oct. 15 and 16 and therefore no longer available to consumers.

The recall affects single packaged whole heads of romaine lettuce produced under the brand name Tanimura & Antle, according to a press release posted to the Food and Drug Administration (FDA) website. Only those with packaging dates of October 15 or October 16, 2020, are included. In all, the recall includes 3,396 cartons of romaine lettuce that were distributed to 20 states.

UF Experiments

- Installed/tested in a drip-irrigated strawberry field from Oct 20, 2017 to March 27, 2018.
- UF Gulf Coast Research & Education Center (UF-GCREC), Balm, Florida
- 2,500 m^2 (0.62 acres) field
- Installed current weather station used by SAS (Metos v3.3)

- Installed SAS-WSNs in 3 different locations
  - Node A just outside of the strawberry field, on the grass and near a tree barrier.
  - Node # inside of the strawberry field, on bare soil.
  - Node C just outside of the cropped area, next to the Reference Weather Station

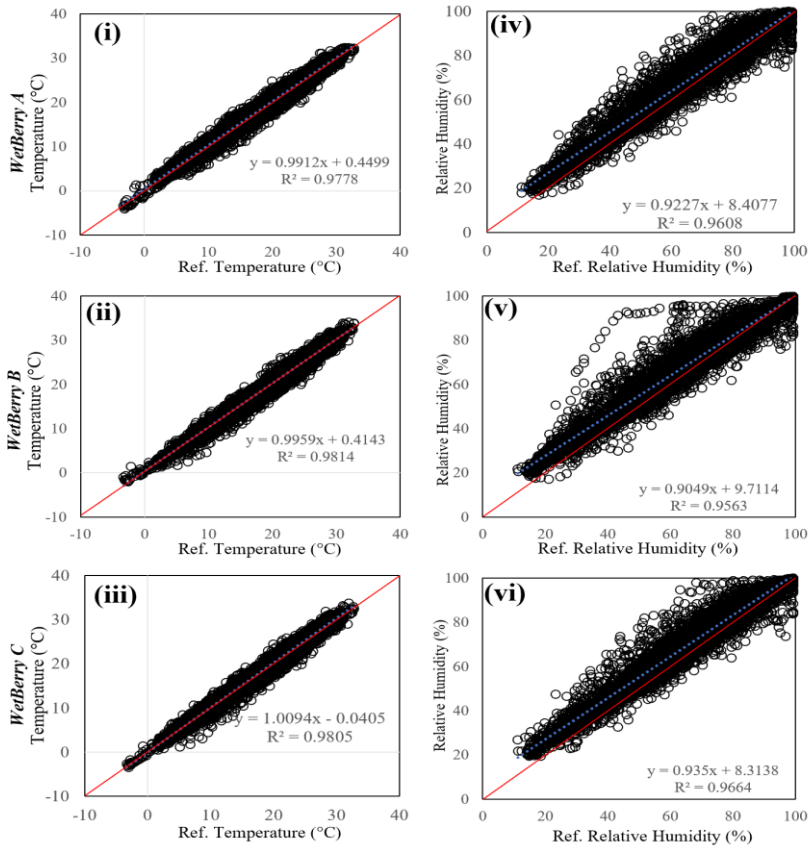
PhD

Air Temperature and Relative Humidity

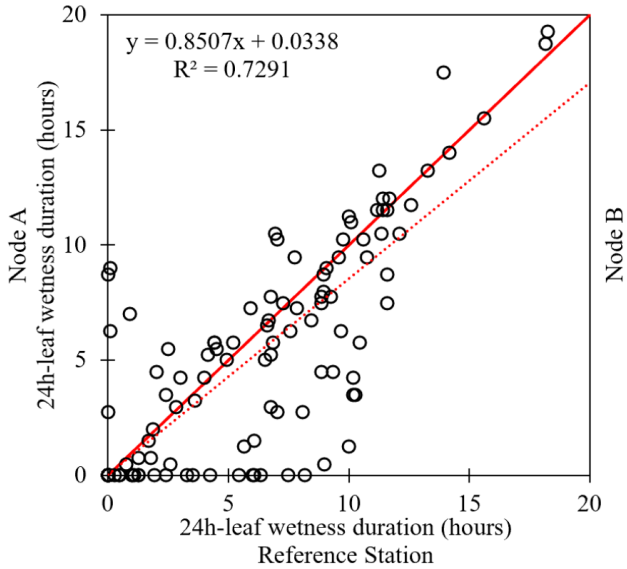
Node A

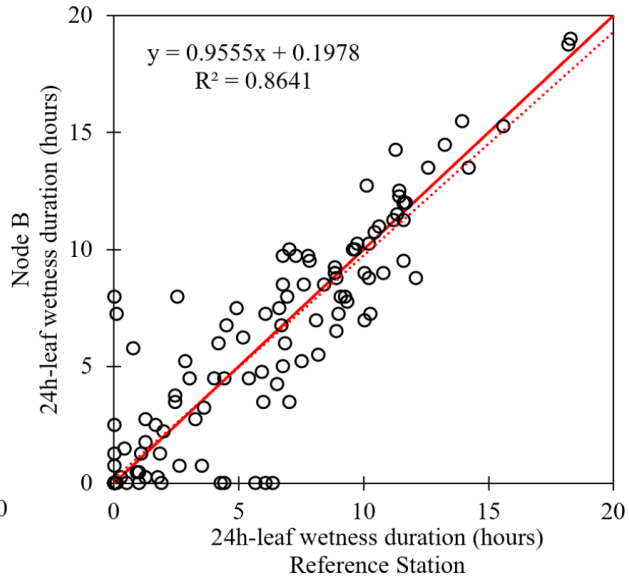
Node B

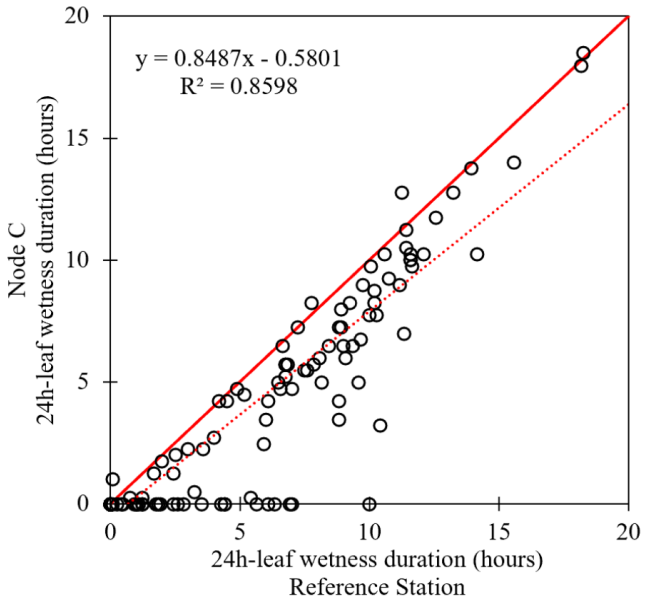
Node C



Leaf Wetness Duration







Risk Recommendation – Fungal Disease

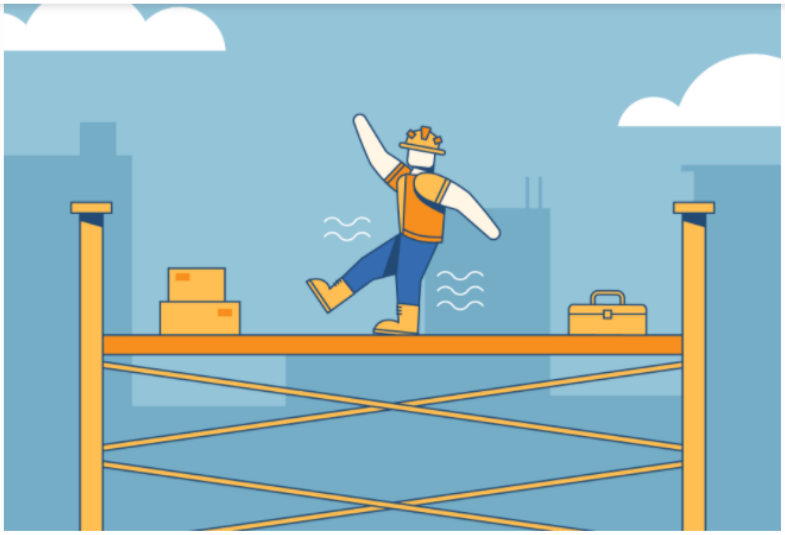
(a)	Node A		Node B		Node C	
INFa	Risk	No Risk	Risk	No Risk	Risk	No Risk
Reference station Risk	27	7	26	8	30	4
Reference No Risk	5	19	8	16	1	23

(b)	Node A		Node B		Node C	
INFb	Risk	No Risk	Risk	No Risk	Risk	No Risk
Reference Risk	27	7	26	8	30	4
Reference No Risk	5	19	8	16	1	23

(c)	Θ1- INFa	Θ1- INFb	k - INFa	k - INFb
Node A	0.79	0.77	0.58	0.55
Node B	0.72	0.65	0.43	0.31
Node C	0.91	0.91	0.83	0.83

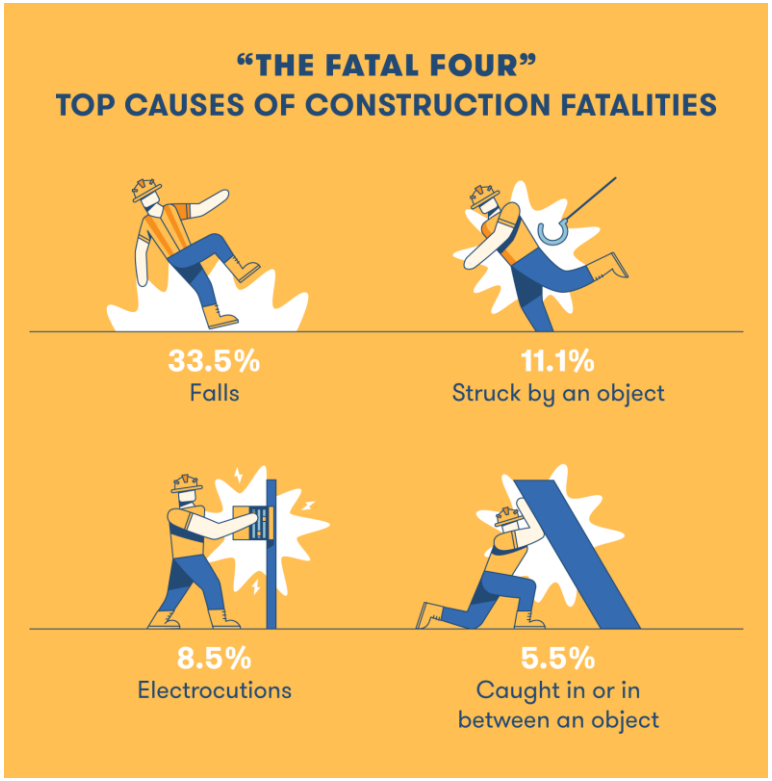
Case 2: Security and Human Safety: IoT in Construction

BIG RENTZ Equipment Solutions Resources Company Blog



The construction industry is known for being one of the most dangerous fields to work in. Out of every 5,000 private-industry worker fatalities, 20 percent are in construction. That means one out of every five worker deaths is construction-related!

Construction also results in many non-fatal injuries that cost companies millions of dollars per year. This makes safety paramount in the industry. While safety measures and precautions, like those outlined by OSHA, can be costly upfront,



NSF Project

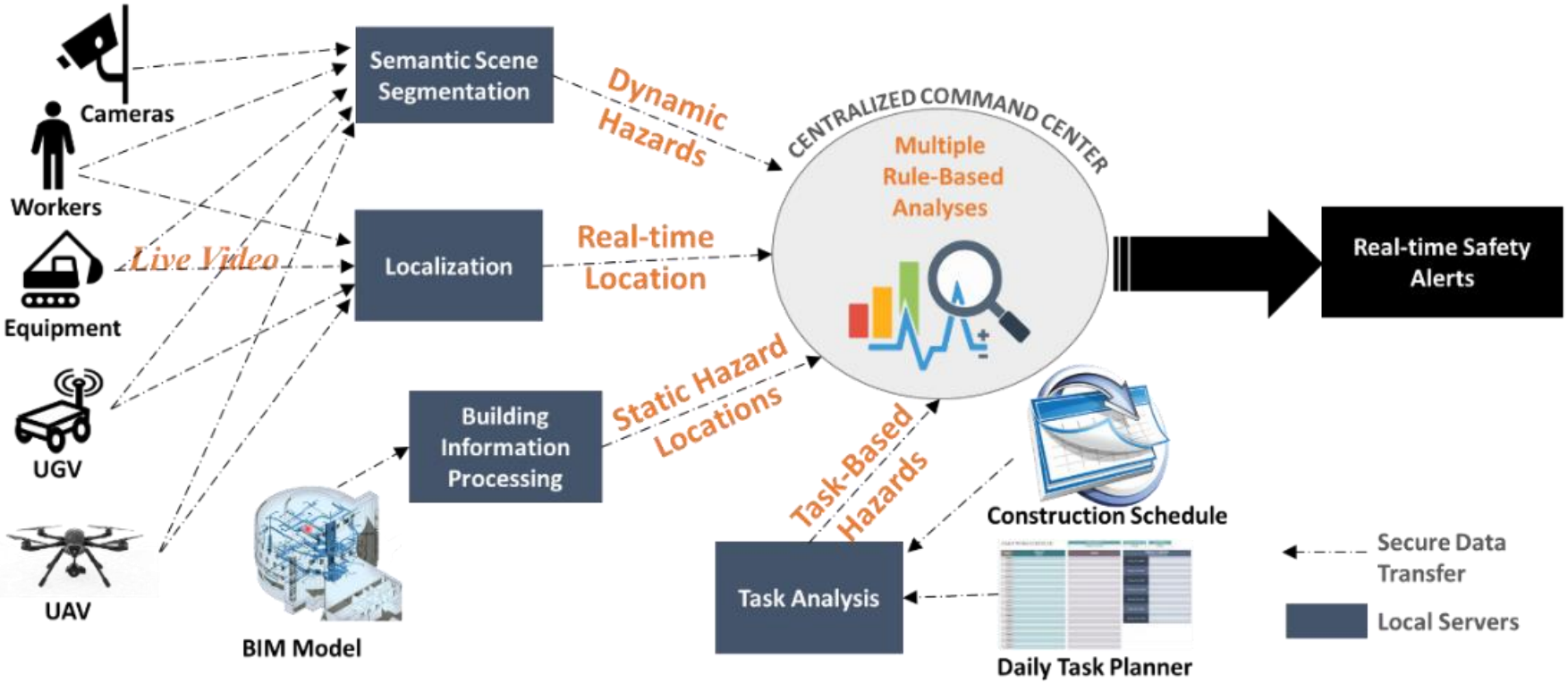
- ELEMENTS: CYBERINFRASTRUCTURE SERVICE FOR IOT-BASED CONSTRUCTION RESEARCH AND APPLICATIONS

PIs: Aaron Costin(Construction)
Janise McNair (Networks and Systems)
Sanjeev Koppal (Imaging)
Idris Jeelani (Construction)

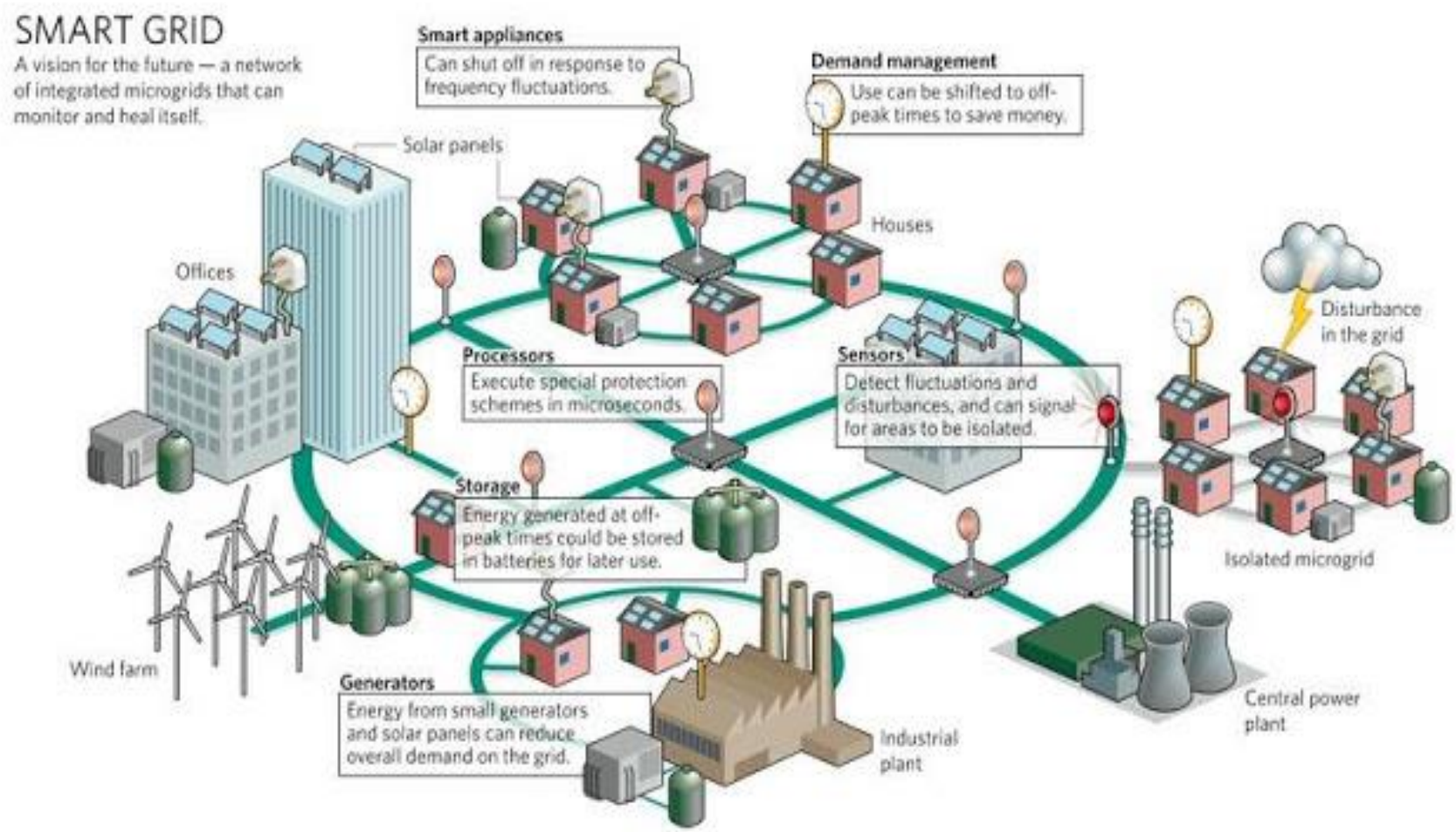
NSF Project – OAC and CNS

IoT-ACRES

Applied Construction Research and Education Services



Security in Public Facing Services: Smart Grid



Recent Attacks – June 2019

WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE SIGN IN SUBSCRIBE

ANDY GREENBERG SECURITY 06.14.2019 07:00 AM

The Highly Dangerous 'Triton' Hackers Have Probed the US Grid

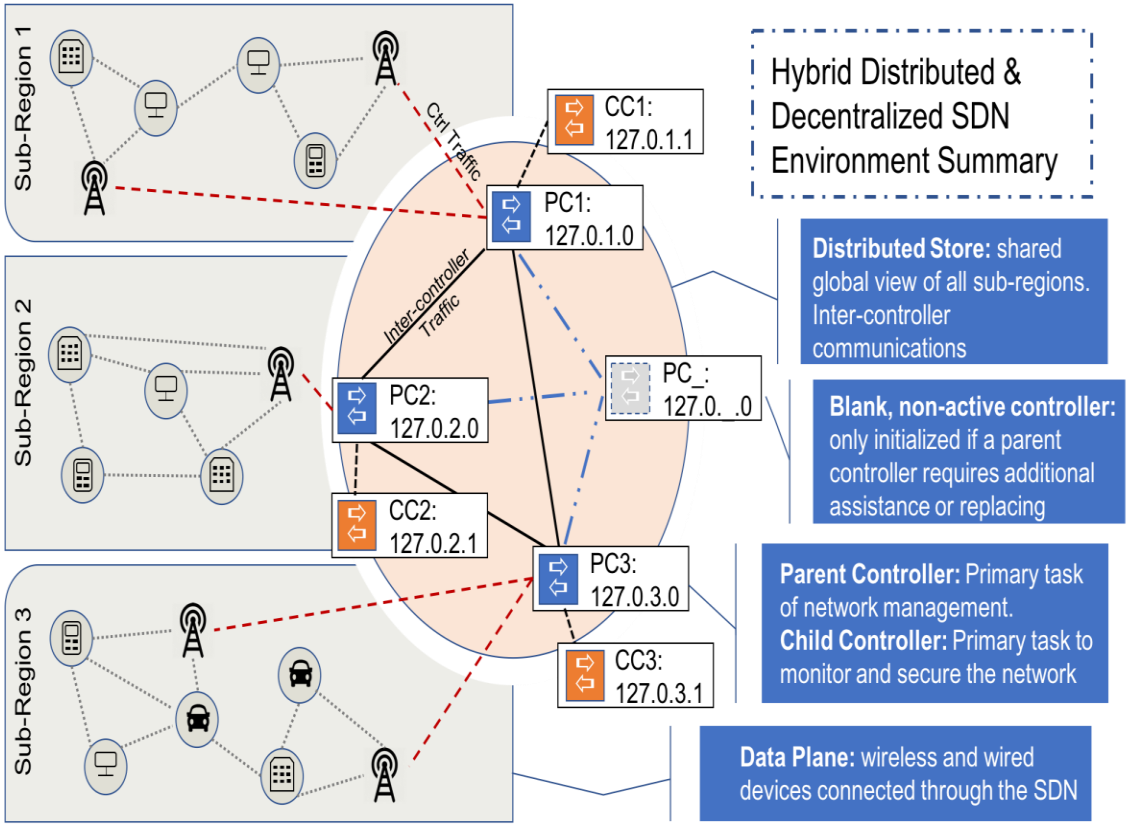
The same hackers behind a potentially lethal 2017 oil refinery cyberattack are now sniffing at US electrical utility targets.

Concerns for Interconnection and Dependence

- Dependence on power system monitoring and control raises concerns with respect to cyber-threats.
  - **False data injection (FDI) attack**, where a subset of measurement values are modified by an adversarial attacker aiming to disrupt the power grid.
  - **Bad data analysis**, Gross Errors detected via Chi Squared Test, largest normalized residual [3] or innovation-based [4] approaches.
    - May be assisted by machine learning techniques
    - May fail in the presence of Cyber-attacks

Goal: Software-Defined Network Management

- Goal:
  - Design smart networks with the ability to autonomously protect and reconfigure themselves in the presence of threats
  - Leverage the adaptive reconfigurable features of SDN for this purpose



Summary

- Great, new applications for IoT.
- The wide range of customers in various application areas are unprepared for the security concerns and network management required.
- Not everyone has to become a network expert!
- New cyber physical system methods are needed to address problems in the supply chain as well as in the distribution of services.

IEEE
Internet of Things

Internet of Things (IoT) Summit at RWW2020
26-27 January 2020 // San Antonio, Texas, USA

THANK YOU!

Janise McNair
Associate Professor,
Electrical & Computer Engineering
Director, Wireless And Mobile (WAM) Systems Lab

Email: mcnair@ece.ufl.edu
URL: http://wam.ece.ufl.edu