Everything you Wanted to Know about Internet of Things (IoT)

IEEE Distinguished Lecture

CE Society Webinar, 16th Nov 2017 (Thu)

Dr. Saraju P. Mohanty, Professor
University of North Texas, USA.
Editor-in-Chief (EiC), IEEE Consumer Electronics Magazine
Conference Chair, ICCE 2018
Email: saraju.mohanty@unt.edu
More Info: http://www.smohanty.org
Talk - Outline

- Motivations for IoT
- Selected Components of IoT
- Selected Applications of IoT
- Driving Technologies of IoT
- Challenges and Research in IoT
- IoT Design Flow
- Tools and Solutions for IoT
- Related Buzzwords of IoT
- Conclusions and Future Directions
Human Migration Problem

- Uncontrolled growth of urban population
- Limited natural and man-made resources

70% of world population will be urban by 2050.

Source: https://humanitycollege.org
Urgent Push for Smart Cities

- **Smart Cities**: For effective management of limited resource to serve largest possible population to improve:
  - Livability
  - Workability
  - Sustainability
Smart Cities: 3 Is

Instrumentation

Smart Cities

Intelligence

Interconnection

The 3Is are provided by the Internet of Things (IoT).

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation

16 Nov 2017
IoT is the Backbone Smart Cities

Source: Mohanty 2016, CE Magazine July 2016
Internet of Things (IoT) - History

1969
The Internet Emerges
The first nodes of what would eventually become known as ARPANET, the precursor to today's Internet, are established at UCLA and Stanford universities.

1982
TCP/IP Takes Shape
Internet Protocol (TCP/IP) becomes a standard, ushering in a worldwide network of fully interconnected networks called the Internet.

1990
A Thing Is Born
John Romkey and Simon Hackett create the world's first connected device (other than a computer): a toaster powered through the Internet.

1999
The IoT Gets a Name
Kevin Ashton coins the term “Internet of things” and establishes MIT's Auto-ID Center, a global research network of academic laboratories focused on RFID and the IoT.

2005
Getting Global Attention
The United Nations first mentions IoT in an International Telecommunications Union report. Three years later, the first international IoT conference takes place in Zurich.

2008
Connections Count
The IPSO Alliance is formed to promote IP connections across networks of "smart objects." The alliance now boasts more than 50 member firms.

2011
IPV6 Launches
The protocol expands the number of objects that can connect to the Internet by introducing 340 undecillion IP addresses (2128).

2013
Google Raises the Glass
Google Glass, controlled through voice recognition software and a touchpad built into the device, is released to developers.

2014
Apple Takes a Bite
Apple announces HealthKit and HomeKit, two health and home automation developments. The firm's iBeacon advances context and geolocation services.

Components
Internet of Things (IoT) – Concept

**Things**
Sensors/actuators with IP address that can be connected to Internet

**Local Network**
Can be wired or wireless: LAN, Body Area Network (BAN), Personal Area Network (PAN), Controller Area Network (CAN)

**Cloud Services**
Data either sent to or received from cloud (e.g. machine activation, workflow, and analytics)

**Global Network**
Connecting bridge between the local network, cloud services and connected consumer devices

**Connected Consumer Electronics**
Smart phones, devices, cars, wearables which are connected to the Things

16 Nov 2017

IoT by Prof./Dr. Saraju P. Mohanty
**IoT – Definition - IoT European Research Cluster (IERC)**

A dynamic global network infrastructure

with self configuring capabilities

based on standard and interoperable communication protocols

where physical and virtual “things”

have identities, physical attributes, and virtual personalities and

use intelligent interfaces,

and are seamlessly integrated

into the information network.


IEEE also provides a formal, comprehensive definition of IoT.
IoT – Definition - International Telecommunication Union (ITU)

A network that is: “Available anywhere, anytime, by anything and anyone.”

IoT: Architecture

Overall architecture:
- A configurable dynamic global network of networks
- Systems-of-Systems

Four Main Components of IoT.

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation
IoT Architecture - 3 and 5 Level Model

Three Level Model

Five Level Model

Source: Nia 2017, IEEE TETC 2017
IoT Architecture - 7 Level Model

IoT: The Things

- EveryTHING is connected
- EveryTHING emits signals
- EveryTHING communicates

The “Things” refer to any physical object with a device that has its own IP address and can connect and send/receive data via network.
IoT - Communications

Selected IoT Communications Technology

- Bluetooth Low-Energy (BLE)
- Zigbee
- Z-Wave
- 6LowPAN
- Thread
- WiFi
- Cellular
- NFC
- Sigfox
- Neul
- LoRaWAN

Source: https://www.rs-online.com/designspark/eleven-internet-of-things-protocols-you-need-to-know-about

IoT - Applications
**IoT in Smart Healthcare**

- **Quality and sustainable healthcare with limited resources, anywhere, anytime.**
- **Source:** Mohanty 2016, CE Magazine July 2016

**IoT Role Includes:**
- Real-time monitoring
- Better emergency response
- Easy access of patient data
- Connectivity among stakeholders
- Remote access to healthcare

"$117 Billion Market For IoT in Healthcare By 2020."

IoT in Smart Transportation

“The global market of IoT based connected cars is expected to reach $46 Billion by 2020.”

Source: Datta 2017, CE Magazine Oct 2017

IoT Role Includes:
- Traffic management
- Real-time vehicle tracking
- Vehicle-to-Vehicle communication
- Scheduling of train, aircraft
- Automatic payment/ticket system
- Automatic toll collection

IoT in Smart Energy

IoT Role Includes:
- Management of energy usage
- Power generation dispatch for solar, wind, etc.
- Better fault-tolerance of the grid
- Services for plug-in electric vehicles (PEV)
- Enhancing consumer relationships

Quality, sustainable, uninterrupted energy with minimal carbon footprint.

Source: Mohanty 2016, CE Magazine July 2016

16 Nov 2017


**IoT in Smart Agriculture**

**FUTURE FARMS** small and smart

**SURVEY DRONES**
Aerial drones survey the fields, mapping weeds, yield and soil variation. This enables precise application of inputs, mapping spread of pernicious weed blackgrass could increasing Wheat yields by 2-5%.

**FLEET OF AGRIBOTS**
A herd of specialised agribots tend to crops, weeding, fertilising and harvesting. Robots capable of microdol application of fertiliser reduce fertiliser cost by 99.9%.

**FARMING DATA**
The farm generates vast quantities of rich and varied data. This is stored in the cloud. Data can be used as digital evidence reducing time spent completing grant applications carrying out farm inspections saving on average £5,500 per farm per year.

**TEXTING COWS**
Sensors attached to livestock allowing monitoring of animal health and wellbeing. They can send texts to alert farmers when a cow goes into labour or develops infection increasing herd survival and increasing milk yields by 10%.

**SMART TRACTORS**
GPS controlled steering and optimised route planning reduces soil erosion, saving fuel costs by 10%.

**Climate-Smart Agriculture Objectives:**

- Increasing agricultural productivity
- Resilience to climate change
- Reducing greenhouse gas

Source: http://www.fao.org

16 Nov 2017

---

**Automatic Irrigation System**

Source: Maurya 2017, CE Magazine July 2017

Source: http://www.nesta.org.uk/blog/precision-agriculture-almost-20-increase-income-possible-smart-farming

---

IEEE Distinguished Lecture. IEEE CE Society Webinar.
Driving Technologies
Cheap and Compact Sensor Technology

- **Gas Sensor**
- **Temperature Sensor**
- **Air Quality Sensor**
- **Humidity and Temperature Sensor**
- **Light Sensor**
- **Barometer Sensor**
- **Water Sensor**
- **Dust Sensor**


Source: http://wiki.seeed.cc/Sensor/
Imaging Sensor Technology

Image Sensors

Charged Couple Device (CCD) Sensor

Complementary Metal Oxide Semiconductor (CMOS) Sensors

Passive Pixel Sensor (PPS)

Active Pixel Sensor (APS)

Digital Pixel Sensor (DPS)

Based on Sensing Element

Photodiode-Type APS

Photogate-Type APS

Based on Operation Mode

Linear-Mode APS

Logarithmic-Mode APS

“The global CMOS image sensor market is likely to be worth $10.17 billion by 2020.”

Visible Light Communications (VLC)

- LEDs can switch their light intensity at a rate that is imperceptible to human eye.
- This property can be used for the value added services based on Visible Light Communication (VLC).

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>LiFi</th>
<th>WiFi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Huge</td>
<td>Limited</td>
</tr>
<tr>
<td>Requires Line of Sight</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>EMI + Hazard Concerns</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Susceptibility to Eavesdropping</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Range</td>
<td>Short</td>
<td>Medium</td>
</tr>
<tr>
<td>Data Density</td>
<td>High</td>
<td>Limited</td>
</tr>
</tbody>
</table>

Source: Ribeiro 2017, CE Magazine October 2017

Source: VLCS-2014
Why BPG compression instead of JPEG?

Attributes that differentiate BPG from JPEG and make it an excellent choice include:

- Meeting modern display requirements: high quality and lower size.
- BPG compression is based on the High Efficiency Video Coding (HEVC), which is considered a major advance in compression techniques.
- Supported by most web browsers with a small Javascript decoder.

Variety of Computer Memory

Based on Storage Capability

- Volatile
  - Static RAM (SRAM)
  - Dynamic RAM (DRAM)
  - Twin Transistor RAM (TTRAM)
  - Zero-Capacitor RAM (ZRAM)
  - Thyristor RAM (TRAM)

- Nonvolatile
  - Read-Only Memory (e.g., Programmable ROM (PROM), Erasable PROM (EPROM), Electrically Erasable PROM (EEPROM))
  - Magnetic Storage Hard Disk Drive (HDD)
  - Non-Volatile RAM (NVRAM) (e.g., Flash Memory)
  - Resistive RAM (RRAM or ReRAM)
  - Magnetic or Magnetoresistive RAM (MRAM)
  - Phase-Change RAM (PRAM, PCRAM)
  - Conductive Metal Oxide (CMOX) Memory

Based on Access

- Random-Access Memory (RAM)
- Serial Access Memory (e.g., Shift Registers, Queues)
- Content Addressable Memory (CAM)

The flash memory market is expected to be worth $37.6 worldwide by 2020.


Machine Learning Technology

Artificial Intelligence

Tensor Processing Unit (TPU)

IoT Use:
- Better decision
- Faster response

Source: http://transmitter.ieee.org/impact-aimachine-learning-iot-various-industries/

Source: https://fossbytes.com/googles-home-made-ai-processor-is-30x-faster-than-cpus-and-gpus/

April 2017
Vision Processing Unit

- High-Performance Machine Vision Processing
- Deep Neural Network-based Classification
- Pose Estimation
- 3D Depth Estimation
- Visual Inertial Odometry (Navigation)
- Gesture/Eye Tracking and Recognition

Video Processing Unit → Video encoding and decoding
Graphics Processing Unit (GPU) → Rasterization and Texture Mapping
Vision Processing Unit (VPU) → Machine vision algorithms (e.g. Convolutional Neural Network (CNN))

Vision Processing Unit (VPU)

Source: https://www.movidius.com/solutions/vision-processing-unit
Natural User Interface (NUI)

NUI: User interfaces where the interaction is direct and consistent with our “natural” behavior.

Source: https://www.interaction-design.org/literature/article/natural-user-interfaces-what-are-they-and-how-do-you-design-user-interfaces-that-feel-natural
Natural Language Processing (NLP)

- NLP is the computer method to analyze, understand, and derive meaning from human language.
- Enables user to address computers as if they are communicating with a person.

Selected NLP Applications

- Machine Translation
- Information Retrieval
- Text Categorization
- Big Data

Source: https://www.linkedin.com/pulse/natural-language-processing-2016-global-market-forecasts-rane

Source: http://blog.algorithmia.com/introduction-natural-language-processing-nlp/
Cognitive Computing: Not just “right” or “wrong” anymore but “probably”.

- Systems that learn at scale, reason with purpose and interact with humans naturally.
- Learn and reason from their interactions with humans and from their experiences with their environment; not programmed.

Neuromorphic Computing or Brain-Inspired Computing

Application 1: Integrate into assistive glasses for visually impaired people for navigating through complex environments, even without the need for a WiFi connection.


Application 2: Neuromorphic-based, solar-powered “sensor leaves” equipped with sensors for sight, smell or sound can help to monitor natural disasters.

“Currently, people interact with their devices by thumb-typing on their phones. A high-bandwidth interface to the brain would help achieve a symbiosis between human and machine intelligence and could make humans more useful in an AI-driven world.”

-- Neuralink - neurotechnology company - Elon Musk.

The Blockchain

- Think of it as cloud based peer to peer ledger.
- A Blockchain is a cloud based database shared by every participant in a system.
- The Blockchain contains the complete transaction or other record keeping.

Stay Tuned to: Mohanty 2018, CE Magazine March 2018
Challenges and Research
IoT – Multidiscipline Research

Source: Sethi 2017, JECE 2017

16 Nov 2017

IoT by Prof./Dr. Saraju P. Mohanty
IoT – Selected Challenges

- Robustness
- Massive Scaling
- Design and Operation Cost
- Energy Consumption
- Creating Knowledge and Big Data
- Security, Privacy, and IP Protection
- Architecture and Dependencies

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation
Massive Scaling

Eventually Trillions of Things

The Connected Life by 2020

- 2011: 9 Billion
- 2020: 24 Billion

Mobile Connected Devices

2011: 6 Billion

Revenue opportunity for connected devices in vertical sectors

- Health: $69 Billion
- Automotive: $202 Billion
- Consumer electronics: $445 Billion
- Utilities: $36 Billion

High Design and Operation Cost

- The **design cost** is a one-time cost.
- Design cost needs to be small to make a IoT realization possible.
- The **operations cost** is that required to maintain the IoT.
- A small operations cost will make it easier to operate in the long run with minimal burden on the budget of application in which IoT is deployed.

Communication Latency and Energy Consumption

- Connected cars require latency of ms to communicate and avoid impending crash.
  - Faster connection
  - Low latency
  - Lower power
- 5G for connected world: This enables all devices to be connected seamlessly.
- How about 5G, WiFi working together more effectively?

Source: https://www.linkedin.com/pulse/key-technologies-connected-world-cloud-computing-ione-balakrishnan
Energy Consumption of Sensors, Components, and Systems

Sources: Mohanty 2015, McGraw-Hill 2015

During GSM Communications

During WiFi Communications
Battery less operations can lead to reduction of size and weight of the edge devices.

Battery-Less IoT

Source: https://www.technologyreview.com/s/529206/a-batteryless-sensor-chip-for-the-internet-of-things/

Batter-Less SoC


Energy Harvesting and Power Management

Source: http://rlpvlsi.ece.virginia.edu/node/368
Safety of Electronics

Smartphone Battery

1. Heating starts.
2. Protective layer breaks down.
3. Electrolyte breaks down into flammable gases.
4. Separator melts, possibly causing a short circuit.
5. Cathode breaks down, generating oxygen.

Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithium-ion-battery
Energy Storage - High Capacity and Safer Needed

(Silicon Anode)

(Lithium Nickel Cobalt Aluminum Oxide - NCA) Cathode

Fuel oxidizing enzymes:
Glucose Oxidase
Glucose Dehydrogenases

Anode current collector
Cathode current collector
Separator (Ceramic)

Oxygen from air

Fuel Cell Car

3D Silicon Lithium-ion Rechargeable Battery

Solid Polymer Lithium Metal Battery

Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithiumion-battery

Microbial Fuel Cell (MFC)

Enzymatic Biofuel Cell


Source: https://www.nytimes.com/2016/12/11/technology/designing-a-safer-battery-for-smartphones-that-wont-catch-fire.html
Huge Amount of Data

Estimated Data Generated per Day:
2.5 quintillion bytes
Bigdata in IoT and Smart Cities

## IoT Security - Attacks and Countermeasures

<table>
<thead>
<tr>
<th>Threat</th>
<th>Against</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Trojans</td>
<td>All</td>
<td>Side-channel signal analysis</td>
</tr>
<tr>
<td>Side-channel attacks</td>
<td>C,AU,NR,P</td>
<td>Trojan activation methods</td>
</tr>
<tr>
<td>Denial of Service (DoS)</td>
<td>A,AC,AU,NR,P</td>
<td>Intrusion Detection Systems (IDSs)</td>
</tr>
<tr>
<td>Physical attacks</td>
<td>All</td>
<td>Securing firmware update</td>
</tr>
<tr>
<td>Node replication attacks</td>
<td>All</td>
<td>Kill/sleep command</td>
</tr>
<tr>
<td>Camouflage</td>
<td>All</td>
<td>Isolation</td>
</tr>
<tr>
<td>Corrupted node</td>
<td>All</td>
<td>Blocking</td>
</tr>
<tr>
<td>Tracking</td>
<td>P, NR</td>
<td>Anonymous tag</td>
</tr>
<tr>
<td>Inventorying</td>
<td>P, NR</td>
<td>Distance estimation</td>
</tr>
<tr>
<td>Tag cloning</td>
<td>All</td>
<td>Personal firewall</td>
</tr>
<tr>
<td>Counterfeiting</td>
<td>All</td>
<td>Cryptographic schemes</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>C,NR,P</td>
<td>Reliable routing</td>
</tr>
<tr>
<td>Injecting fraudulent packets</td>
<td>P,I,AU,TW,NR</td>
<td>De-patterning and Decentralization</td>
</tr>
<tr>
<td>Routing attacks</td>
<td>C,I,AC,NR,P</td>
<td>Role-based authorization</td>
</tr>
<tr>
<td>Unauthorized conversation</td>
<td>All</td>
<td>Information Flooding</td>
</tr>
<tr>
<td>Malicious injection</td>
<td>All</td>
<td>Pre-testing</td>
</tr>
<tr>
<td>Integrity attacks against learning</td>
<td>C,I</td>
<td>Outlier detection</td>
</tr>
<tr>
<td>Non-standard frameworks and inadequate testing</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Insufficient/Inessential logging</td>
<td>C,AC,NR,P</td>
<td></td>
</tr>
</tbody>
</table>

C - Confidentiality, I - Integrity, A - Availability, AC - Accountability, AU - Auditability, TW - Trustworthiness, NR - Non-repudiation, P - Privacy

Source: Nia 2017, IEEE TETC 2017
Security, Privacy, and Copyright
Security - Information, System ... 

Cybercrime: Top 20 Countries

- Cybercrime damage costs to hit $6 trillion annually by 2021
- Cybersecurity spending to exceed $1 trillion from 2017 to 2021

Source: https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

Security in Communications Technology

- NFC
- Bluetooth
- 4G LTE 2600mhz
- 4G

Routing Attacks
Denial-of-Service (DoS) Attacks
Malicious Injection

16 Nov 2017
Security - Systems ...

Power Grid Attack


Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/
Different Attacks on a Typical CE System

Malicious Design Modifications Issue

Information may bypass giving a non-watermarked or non-encrypted output.

Hardware Trojans


Input

Watermarking and/or Cryptography Processor

Unprotected/Unsecure Information

Protected/Secure Information

Select

Trojan

Output

Chip fails to work during critical needs.


16 Nov 2017
Trojans Secure Digital Hardware Synthesis

Design-For-Security (DFS) flow against Trojan resulting into functional change

Source: Sengupta and Mohanty 2017, TCAD April 2017
Memory Attacks

- **Snooping Attacks**: Read confidential information in memory.
- **Spoofing Attacks**: Replace a block with fake.
- **Splicing Attacks**: Replace a block with a block from another location.
- **Cold Boot Attacks**: Attacker remembers the value of a block at a given address at one time, and writes that value at exactly the same address at a different times; Hardest attack.
- **Replay Attacks**: A side channel attack, an attacker has physical access memory to retrieve encryption keys, has to be in seconds-to-minute of power OFF.

Source: Mohanty 2013, Springer CSSP Dec 2013
Memory Security and Protection

Nonvolatile Storage
Source: http://datalocker.com

On-Chip/On-Board Memory Protection
Source: Mohanty 2013, Springer CSSP Dec 2013

16 Nov 2017
IoT by Prof./Dr. Saraju P. Mohanty
RFID Security - Attacks

Selected RFID Attacks

Physical RFID Threats
- Disabling Tags
- Tag Modification
- Cloning Tags
- Reverse Engineering and Physical Exploration

RFID Channel Threats
- Eavesdropping
- Snooping
- Skimming
- Replay Attack
- Relay Attacks
- Electromagnetic Interference

System Threats
- Counterfeiting and Spoofing Attacks
- Tracing and Tracking
- Password Decoding
- Denial of Service (DoS) Attacks

Numerous Applications

Source: Khattab 2017: Springer 2017 RFID Security

16 Nov 2017

IoT by Prof./Dr. Saraju P. Mohanty
RFID Security - Solutions

Selected RFID Security Methods

- Killing Tags
- Sleeping Tags
- Faraday Cage
- Blocker Tags
- Tag Relabeling
- Minimalist Cryptography
- Proxy Privacy Devices

Faraday Cage

Source: Khattab 2017, Springer 2017 RFID Security
NFC Security - Attacks

- Selected NFC Attacks
  - Eavesdropping
  - Data Modification
  - Relay Attacks
  - Data Corruption
  - Spoofing
  - Interception Attacks
  - Theft

### Eavesdropping

### Relay Attack
Source: [https://www.slideshare.net/cgvwzq/on-relaying-nfc-payment-transactions-using-android-devices](https://www.slideshare.net/cgvwzq/on-relaying-nfc-payment-transactions-using-android-devices)

---

16 Nov 2017

IoT by Prof./Dr. Saraju P. Mohanty

154
NFC Security - Solutions

CryptoTag

8-bit Microcontroller

Program ROM

MC Patterns

AMBA Bus

Advanced Microcontroller

Bus Architecture (AMBA) Bus

Framing Logic

Digital Part

Cryptographic Unit

Memory Unit

EEPROM

RAM

ROM

Source: Mohanty 2017, CE Magazine Jan 2017

Source: Plos 2013, TVLSI Nov 2013

Swing-Pay

Source: Mohanty 2017, CE Magazine Jan 2017

Source: Plos 2013, TVLSI Nov 2013
Autonomous Car – Security Vulnerability

Selected Attacks on Autonomous Cars

- Replay
- Relay
- Jamming
- Spoofing
- Tracking

Light Detection and Ranging (LiDAR)

Camera

Cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors – Massive security issues.


Source: Petit 2015: IEEE-TITS Apr 2015
Autonomous Car Security – Cryptographic Hardware

Cryptographic Services Engine (CSE) Block

Qorivva MPC564xB/C Family from NXP/Freescale

Microcontroller Unit (MCU)


16 Nov 2017

IoT by Prof./Dr. Saraju P. Mohanty
Smart Healthcare - Security and Privacy Issue

Selected Smart Healthcare Security/Privacy Challenges

- Data Eavesdropping
- Data Confidentiality
- Data Privacy
- Location Privacy
- Identity Threats
- Access Control
- Unique Identification
- Data Integrity
Smart Healthcare Security

Insulin Delivery System

Rolling Code Encoder in Remote Control

- Remote Control’s Sequence Counter
- Information Bits (i.e., control command)

Key Encryption

Transmitted Data

Rolling Code Decoder in Insulin Pump

- Insulin Pump’s Sequence Counter
- Received Counter Value

Key Decryption

Received Information (i.e., control command)

Security Attacks

- Active Attacks: Impersonation
- Passive Interception

Insulin Pump

- Universal Software Radio Peripheral

PDA

- Universal Software Radio Peripheral

- Remote Control

- Glucose Meter

Continuous Glucose Sensor

Glucose Level

Report Data/Control

Insulin Pump

Insulin Delivery System

Source: Li 2011, e-Health 2011
Side Channel Attacks – Differential and Correlation Power Analysis (DPA/CDA)

- Cryptographic device (e.g., smart card and reader)
- Input data
- Device under attack (DUA)
- Statistical Analysis
- Input, keyguesses
- Abstract model of the DUA

Decision on key guess

- Oscilloscope
- Computer
- Control, Waveform data
- Control, Cyphertexts
- Physical side-channel leakage
- Predicted side-channel leakage
DPA Resilience Hardware - Synthesis Flow

Cryptography Algorithm

Hamming code based concurrent error detection and correction in Galois Field

Uniform switching cell Library

Physical-Attack Tolerant Cryptography Hardware

Proposed Design Approach

Cryptography Hardware Architecture Description

Module DUT
AND U1 ....
XOR U2 R ...
Adder U3 ....
Reg U4 ....
endmodule

Uniform SWitching-Activity Logic Cell Library

Gate Level Synthesis

Synthesized Netlist with Error Correction in Sequential Elements with Uniformly Switching Cell Library

Source: Mohanty 2013, Elsevier CEE 2013
Multimedia Piracy – Movie/Video

“Film piracy cost the US economy $20.5 billion annually.”

Source: http://www.ipi.org/ipi_issues/detail/illegal-streaming-is-dominating-online-piracy
A DRM Hardware Integrated CE System – Secure Digital Camera (SDC) Example

Copyright Protection Hardwares –

DCT Domain Watermarking

**Datapath Architecture**

**Hardware Layout**

Physical Design Data
Total Area: 16.2 sq mm
No. of Transistors: 1.4 million
Power Consumption: 0.3 mW

Source: Mohanty 2006, TCASII May 2006

16 Nov 2017
Copyright Protection Hardware – MPEG-4 Video Watermarking

Video Watermarking Architecture: Simulink Model

Video Watermarking Architecture Datapath

FPGA Prototyping
Throughput: 44 frames/sec
Logic Elements in FPGA Prototyping: 28322

Source: Mohanty 2011, JSS May 2011
DRM Hardware - Secure Better Portable Graphics (SBPG)

Idea of Secure BPG (SBPG)  High-Efficiency Video Coding Architecture

Simulink Prototyping
Throughput: 44 frames/sec
Power Dissipation: 8 nW

Hardware IP Right Infringement

- False Ownership Claim
- Sub-licensing
- Piracy (Reverse Engineering)


Hardware Reverse Engineering

CE System disassembly
Subsystem identification, modification

Chip-Level Modification


Source: https://www.slideshare.net/SOURCEConference/slicing-into-apple-iphone-reverse-engineering


Source: http://pic-microcontroller.com/counting-bits-hardware-reverse-engineering-silicon-arm1-processor/
Counterfeit Hardware

2014 Analog Hardware Market (Total Shipment Revenue US $)

- **Wireless Market**: $18.9 billion (34.8%)
- **Consumer Electronics**: $9.0 billion (16.6%)
- **Industrial Electronics**: $8.9 billion (16.5%)
- **Automotive**: $8.5 billion (15.7%)
- **Data Processing**: $6.0 billion (11%)
- **Wired Communications**: $2.9 billion (5.4%)

Source: https://www.slideshare.net/rorykingihs/ihs-electronics-conference-rory-king-october

Top counterfeits could have impact of $300B on the semiconductor market.

Source: https://www.slideshare.net/rorykingihs/ihs-electronics-conference-rory-king-october
Cloned/Fake Electronics Hardware – Example - 1

Typical Consumer Electronics

Source: https://petapixel.com/2015/08/14/i-bought-a-fake-nikon-dslr-my-experience-with-gray-market-imports/

Source: http://www.manoramaonline.com/

Source: http://www.cbs.cc/fake-capacity-usb-drives/
Cloned/Fake Electronics Hardware – Example - 2

A plug-in for car-engine computers.

Digital Hardware - Watermark

Source: Mohanty 2017: CE Magazine October 2017
Digital Hardware – Obfuscation

Obfuscation – Intentional modification of the description or the structure of electronic hardware to conceal its functionality for making reverse-engineering difficult.

Source: Sengupta, Mohanty 2017, TCE November 2017
Physical Unclonable Function (PUF)

- Physical Unclonable Functions are simple primitives for security.
- PUFs are easy to build and impossible to duplicate (Theoretically).
- Input and Output are called Challenge Response Pair (CRP).

Only an authentic hardware can produce a correct Response for a Challenge.

Source: Mohanty 2017, Springer ALOG Dec 2017
**PUF - Principle**

PUFs don’t store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.

Design Flow
IoT – Design Flow

1. Concept
2. High Level Design
3. Component Level Design
4. Design Analysis
5. Prototyping
6. To Next Step

IoT – Design Flow

6. Field Testing
7. Release of Beta Version
8. Production
9. Release and Documentation


16 Nov 2017
IoT Design – Case Study – Indoor Air Quality Monitoring

Source: UNT ETECH Senior Project 2017
## IoT Hardware Domains

### Embedded Systems and Boards (e.g. Arduino Yun, Raspberry Pi, BeagleBone, Samsung ARTIK)

<table>
<thead>
<tr>
<th>Features</th>
<th>Processor/Microcontroller</th>
<th>Graphics Processing Unit</th>
<th>Clock Speed</th>
<th>Size</th>
<th>Memory</th>
<th>RAM</th>
<th>Supply Voltage</th>
<th>Listed Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>SparkFun Blynk Board</td>
<td>Tensilica L106 32-b</td>
<td>No</td>
<td>26 MHz</td>
<td>51 mm x 42 mm</td>
<td>4 MB</td>
<td>128 KB</td>
<td>5 V via micro-USB/ Li-Po connector and charging circuit</td>
<td>US$29.95</td>
</tr>
<tr>
<td>Arduino Yun</td>
<td>ATmega32u4 and Atheros AR9331 (for Linux)</td>
<td>No</td>
<td>16 MHz and 400 MHz</td>
<td>73 mm x 53 mm</td>
<td>32 KB and 16 MB + micro-SD</td>
<td>64 MB DDR2</td>
<td>5 V via micro-USB</td>
<td>US$58</td>
</tr>
<tr>
<td>Raspberry Pi 3</td>
<td>Broadcom BCM2837 and ARM Cortex-A53 64-b Quad Core</td>
<td>VideoCore IV @ 300/400 MHz</td>
<td>1.2 GHz</td>
<td>85 mm x 56 mm</td>
<td>Micro-SD</td>
<td>1 G E LPDDR2</td>
<td>5 V via micro-USB</td>
<td>US$35</td>
</tr>
<tr>
<td>cloudBit</td>
<td>Freescale i.MX233 (ARM926EJ-S core)</td>
<td>No</td>
<td>454 MHz</td>
<td>55 mm x 19 mm</td>
<td>Micro-SD slot with 4-GB micro-SD</td>
<td>64 MB</td>
<td>5 V via micro-USB</td>
<td>US$59.95</td>
</tr>
<tr>
<td>Photon</td>
<td>STM32F205 120MHz ARM Cortex M3</td>
<td>No</td>
<td>120 MHz</td>
<td>36.5 mm x 20.3 mm</td>
<td>1 MB</td>
<td>128 KB</td>
<td>5 V via micro-USB</td>
<td>US$19</td>
</tr>
<tr>
<td>BeagleBone Black</td>
<td>AM335x ARM Cortex A8</td>
<td>PowerVR SGX530</td>
<td>1 GHz</td>
<td>86 mm x 56 mm</td>
<td>4 GB 8-b eMMC, micro-SD</td>
<td>512 MB DDR3</td>
<td>5 V via mini-USB</td>
<td>US$49</td>
</tr>
<tr>
<td>Pinoccio</td>
<td>ATmega256RF2</td>
<td>No</td>
<td>16 MHz</td>
<td>70 mm x 25 mm</td>
<td>256 KB</td>
<td>32 KB</td>
<td>5 V via micro-USB/ Li-Po connector and charging circuit</td>
<td>US$109</td>
</tr>
<tr>
<td>UDOO</td>
<td>Freescale i.MX 6 ARM Cortex-A9 and Atmel SAM3X8E ARM Cortex-M3</td>
<td>Vivante GC2000 for 3-D + GC 355 for 2-D (vector graphics) + GC 320 for 2-D</td>
<td>1 GHz</td>
<td>110 mm x 85 mm</td>
<td>Micro-SD</td>
<td>1 G E DDR3</td>
<td>12 V</td>
<td>US$135</td>
</tr>
<tr>
<td>Samsung Artik 10</td>
<td>ARM A15x4 and A7x4</td>
<td>Mali-T628 MP6 core</td>
<td>1.3 GHz and 1.0 GHz</td>
<td>39 mm x 29 mm</td>
<td>16 GB</td>
<td>2 G E LPDDR3</td>
<td>3.4-5 V</td>
<td>US$100</td>
</tr>
</tbody>
</table>

### Wearable Devices and Gadgets (e.g. Samsung Gear 2, FitBit Flex, FLORA, iWallet)

Source: Singh 2017, CE Magazine, April 2017
Software for IoT

Platforms
- Temboo
- Kaa
- Carriots
- Ubidots
- ThingSpeak
- Artik Cloud
- Pinoccio
- Smartliving
- Samsung ARTIK

Languages
- C/C++
- Java
- HTML5
- Javascript
- Python

Source: Singh 2017, CE Magazine, April 2017
Tools and Solutions
IoT: Design and Simulation Challenges

- Traditional controllers and processors do not meet IoT requirements, such as multiple sensor, communication protocol, and security requirements.
- Existing tools are not enough to meet challenges such as time-to-market, complexity, cost of IoT.
- Can a framework be developed for simulation, verification, and optimization:
  - of individual (multidiscipline) “Things”
  - of IoT Components
  - of IoT Architecture
IoT by Prof./Dr. Saraju P. Mohanty

16 Nov 2017

IoT Simulators

Selected IoT Simulators

- Bevywise IoT Simulator
- CUPCARBON
- IoTIFY
- Meshify
- Node-RED
- NetSim
- SimpleIoTTSimulator
IoT Simulator - CUPCARBON

About
- CUPCARBON is a smart city and Internet of Things Wireless sensor network simulator (SCI-WSN)

Objective
- Design, Visualize, Debug
- Validate distributed algorithms
- Create environmental scenarios

Environments
- Design of mobility scenarios and the generation of natural events such as fires and gas as well as the simulation of mobiles such as vehicles and flying objects (e.g. UAVs, insects, etc.).
- A discrete event simulation of WSNs which takes into account the scenario designed on the basis of the first environment.

Source: http://www.cupcarbon.com/
IoT Simulators - Node-RED

About:
- Node-RED is a flow-based IoT Simulator.
- It is a programming tool for wiring together hardware devices, APIs and online services in new ways.
- The light-weight runtime is built on Node.js, taking full advantage of its event-driven, non-blocking model.

Editor:
- Browser-based editor.
- The flows created in Node-RED are stored using JSON which can be easily imported and exported for sharing with others.

Advantages:
- Available for smaller computing devices such as Raspberry Pi.
- It takes moments to create cloud applications that combine services from across the platform.
Related Buzzwords
Some related Buzzwords

- Internet of Everything (IoE)
- Internet of Things (IoT)
- Cyber Physical Systems (CPS)
- Smarter Planet
- Machine to Machine (M2M)
- The Fog
- Industry 4.0 (Automation and Data Exchange in Manufacturing Technology)
- Industrial Internet of Things (IIoT)
- Trillion Sensors (Tsensors)

Source: Sangiovanni-Vincentelli 2016, ISC2 2016
IoT Vs Sensor Networks

Wireless Sensor Networks (WSN)

- WSN is like the eyes and ears of the IoT.
- A network of small wireless electronic nodes which consists of different sensors.
- The purpose is to collect data from the environment.

IoT

- IoT in a broad sense is like a brain.
- Store both real world data and can also be used to monitor the real world parameters and give meaningful interpretation.

IoT adds value to data!

Source: Nia 2017, IEEE TETC 2017
Fog vs Edge vs Cloud Computing

Fog computing and edge computing involve pushing intelligence and processing capabilities closer to where the data originates from "Things" to reduce communication traffic and improve IoT response.

**Fog Computing**
- Intelligence - LAN, Processing - fog node or IoT gateway.
- Real-Time Control
- Real-Time Analysis
- Data Ownership Protection
- Secure Multi-Cloud interworking

**Edge Computing**
- Dedicated App Hosting
- Embedded OS
- Device management
- Data Service
- Communication

**Cloud Computing**
- Scalability
- Big Data Analytics
- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Resource Pooling
- Elastic Compute
- Secure Access

**Edge**: Intelligence, Processing, and Communication - Devices like Programmable Automation Controllers (PACs)

Source: https://www.automationworld.com/fog-computing-vs-edge-computing-whats-difference

IoT by Prof./Dr. Saraju P. Mohanty
IoT Vs Cyber Physical Systems (CPS)

Source: Mohanty 2016, CE Magazine July 2016
Internet of Every Things (IoE)

People
Connecting people in more relevant, valuable ways

Data
Converting data into intelligence to make better decisions

Process
Delivering the right information to the right person (or machine) at the right time

Things
Physical devices and objects connected to the Internet and each other for intelligent decision making; often called Internet of Things (IoT)

Conclusions
Conclusions

- IoT has following components: Things, LAN, Cloud, Internet.
- IoT is backbone of smart cities.
- Scalability, Cost, Energy-consumption, Security are some important challenges of IoT.
- Security, Privacy, and Ownership Rights are critical for trustworthy IoT design.
- Physical Unclonable Functions (PUF) emerging as a good security solution.
- Coordination among the various researchers and design engineers is a challenge as IoT is multidisciplinary.
Future Directions

- Energy-Efficient “Thing” design is needed.
- Security and Privacy of Information need more research.
- Security of the CE systems (e.g. UAV, Smart Cars) needs research.
- Safer and efficient battery need research.
- IoT automatic design tool needs research.
- Some IoT simulators exist, but more needed for efficient, accurate, scalable, multi-discipline simulations.
Hardwares are the drivers of the civilization, even softwares need them.

Thank You !!!

Slides Available at:
http://www.smohanty.org