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
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
Share of incremental data payload: 2016 vs 2015

- 4G: 60%*
- 3G: 55%
- 2G: -15%

*(excluding Reliance Jio)

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)

- 3G device base: 38%
- 4G device base: 12%

Growth over 2015:
- 3G: 1.2x
- 4G: 2.7x

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

- 55-65% Video streaming
- 20-25% Browsing
- 10-12% Social media
- 2-4% Audio streaming

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

LTE device support by band (% of LTE devices)

- 1800MHz: 97%
- 2300MHz: 90%
- 800MHz: 72%
- 900MHz: 61%

Contribution of 2G, 3G and 4G

- 2G: 26%
- 3G: 13%
- 4G: 54%

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

Metro Category A Category B Category C Pan-India

- 4G: 57%
- 3G: 67%
- 2G: 61%
Total data traffic growth:
- 44x increase from 2015 to 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:
- 93% (2015-19)

Users with 4G devices:
- 67% Device Penetration
- 501 mn 4G capable unique devices
- 86% of 4G capable devices are VoLTE capable

Video consumption pattern:
- % of daily online video watching time

Private LTE potential:
- Adoption in:
  - Manufacturing
  - Logistics
  - Warehousing
  - Mining

Application in:
- Remote Monitoring
- Improving OEE
- Material Handling
- VR and Smart security

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%

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
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
Networking
Identification
Communications
Discovery
Data Protocols
Device Management
Semantic
Multi-layer Frameworks

IoT Protocols
6LoWPAN (lightweight IPv6), RPL, LoRaWAN
EPC, uCode, IPv6, URIs
Xbee, Wifi, Bluetooth, LPWAN
Physical Web, mDNS, DNS-SD
MQTT, CoAP, AMQP, Websocket
TR-069, OMA-DM
JSON-LD, Web Thing Model
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 m² (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
Air Temperature and Relative Humidity

Node A

(i) y = 0.9912x + 0.4499
R² = 0.9778

(iv) y = 0.9227x + 8.4077
R² = 0.9608

Node B

(ii) y = 0.9959x + 0.4143
R² = 0.9814

(v) y = 0.9949x + 9.7114
R² = 0.9563

Node C

(iii) y = 1.0094x - 0.0405
R² = 0.9805

(vi) y = 0.935x + 8.3138
R² = 0.9664
Leaf Wetness Duration

Node A:
\[
y = 0.8507x + 0.0338 \\
R^2 = 0.7291
\]

Node B:
\[
y = 0.9555x + 0.1978 \\
R^2 = 0.8641
\]

Node C:
\[
y = 0.8487x - 0.5801 \\
R^2 = 0.8598
\]
### Risk Recommendation – Fungal Disease

<table>
<thead>
<tr>
<th>(a)</th>
<th>Node A</th>
<th>Node B</th>
<th>Node C</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFa</td>
<td>Risk</td>
<td>No Risk</td>
<td>Risk</td>
</tr>
<tr>
<td>Reference station Risk</td>
<td>27</td>
<td>7</td>
<td>26</td>
</tr>
<tr>
<td>Reference No Risk</td>
<td>5</td>
<td>19</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(b)</th>
<th>Node A</th>
<th>Node B</th>
<th>Node C</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFb</td>
<td>Risk</td>
<td>No Risk</td>
<td>Risk</td>
</tr>
<tr>
<td>Reference Risk</td>
<td>27</td>
<td>7</td>
<td>26</td>
</tr>
<tr>
<td>Reference No Risk</td>
<td>5</td>
<td>19</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(c)</th>
<th>O1- INFa</th>
<th>O1- INFb</th>
<th>k - INFa</th>
<th>k - INFb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node A</td>
<td>0.79</td>
<td>0.77</td>
<td>0.58</td>
<td>0.55</td>
</tr>
<tr>
<td>Node B</td>
<td>0.72</td>
<td>0.65</td>
<td>0.43</td>
<td>0.31</td>
</tr>
<tr>
<td>Node C</td>
<td>0.91</td>
<td>0.91</td>
<td>0.83</td>
<td>0.83</td>
</tr>
</tbody>
</table>
Case 2: Security and Human Safety: IoT in Construction

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

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.
  - 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.
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