Security and Reliability of Internet of Things (IoT) : Part II

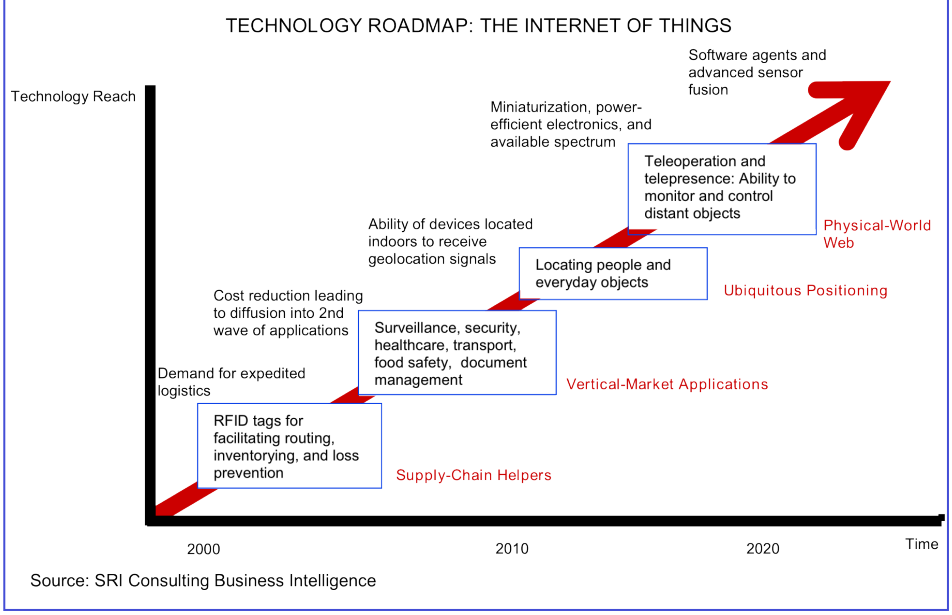
Presented by Paul Wood

PURDUE UNIVERSITY

What is the Internet of Things?

- There is no exact definition, only general ideas
  - Traditional internet relies on human-generated inputs
    - Pictures, Video, Audio, Text, etc
  - IoT relies on "thing"-generated inputs
    - Temperature, Time, Location, etc. (Sensors in general)
- "Things" have physical attributes
  - Primary driver of IoT was initially supply-chain based (Position)
  - Evolved into additional surveillance, healthcare, and other applications (Expanded Sensors)
  - Future things will have more control integration (Expanded Actuation)

PURDUE UNIVERSITY



Implications for Dependable Computing

- Replication has a physical implication
  - Since sensors are responsible for a majority of IoT inputs, the sensors themselves would require replication
    - Alternatives involve sensor fusion-building a state or context based on multiple sensors
      - Example: A room has an IR based motion detector/camera and an ambient air sensor. Both can be used to detect fire in a room.
  - Software-only replication and offloading will exist as in today's smartphones, etc.
- The IoT is about physical world integration, and thus dependable computing will focus on operating in harsh environments

Implications for Security

- National Intelligence Council (NIC) listed IoT as a top-6 security risk to the US by 2025.
  - Disruptive Technologies Global Trends 2025. National Intelligence Council (NIC), April 2008, P. 27.
  - Risk to 4th amendment rights
  - Risks associated with today's internet hacking will extend and distribute more widely as even mundane devices become remotely controllable
    - Hacking into your refrigerator and spoiling your food, locking your doors, watching you, etc.
- "Just as the Internet aggravated the risks of cyberwarfare, spam, identity theft, and denial-of-service attacks, connected everyday objects become targets for malicious software that causes everyday devices to fail or spy."

Security Challenges

- Low power, inexpensive devices
  - The budget of IoT devices may be paramount to security, leaving breakable cryptography in place
  - "Common Sense" Management – "This cereal box doesn't need to be secure!"
- Interoperable, Mandated Standards
  - Legal requirements and forced standard usage will be necessary for fluid integration and security in devices
  - Micro-USB vs Apple's Proprietary ports
  - I.E. All hardware can support communication using AES-128
- Privacy Regulation
  - Preventing "By purchasing this cereal you agree to be tracked"

Unique Attack Opportunities

- IoT relies more heavily on peer to peer routing
  - DoS attacks can originate anywhere in the network
  - Tree topology no longer the norm for local networks
- Devices have a power constraint
  - DoS can take the form of power consumption rather than network or processing, though they are related
- Sensor Interference
  - Disabling or reducing the function of an IoT can involve attacks on sensors, falsifying information and creating new challenges for detection

Today's IoT

- The fundamental building block of IoT is the Sensor Network
  - Significant research related to IoT is occurring in this field
- Other Cyber-Physical systems are being included under the IoT umbrella
  - Vehicle to vehicle communications
    - Position, coordination
  - Mobile Phones
    - Near Field Communications, QR codes, etc.
  - Smart Grid

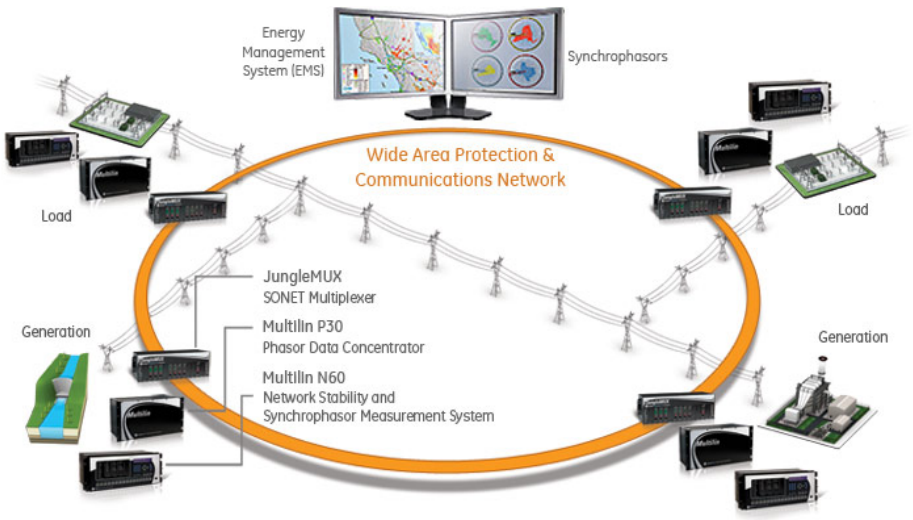
Security Survey

- Example of Sensor Interference
  - **"Combating time synchronization attack: a cross layer defense mechanism"**
    - **Zhenghao Zhang** **University of Tennessee, Knoxville, TN**
    - **Matthew Trinkle** **University of Adelaide, Australia**
    - **Husheng Li** **University of Tennessee, Knoxville, TN**
    - **Aleksandar D. Dimitrovski** **Oak Ridge National Lab, Oak, Ridge, TN**
  - Paper appeared in ICCPS 2013
    - International Conference on Cyber-Physical Systems
- Example of DoS Attacks
  - "**Denial of service in sensor networks**"
    - **Wood, A. ; Virginia Univ., Charlottesville, VA, USA ; Stankovic, J.A.**
  - **Appeared in Computer Magazine,** vol.35 Oct 2002

Sensor Interference

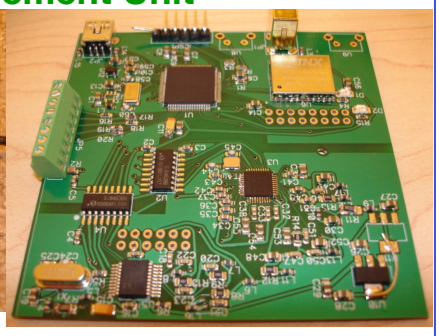
- Attacker's Goal
  - Identify vulnerable sensors and disrupt the sensor network's operation by attacking the sensor
- In this paper, the target is a phasor measurement unit (PMU)
  - PMU's rely on a high precision global timing reference (GPS)
  - PMU's are generally not premise level devices, but are placed at key locations throughout the power grid (Generators, Transformers, etc.)
  - The precise timing information is used to generate a reference for measuring phase angle of voltage (or current) in the grid

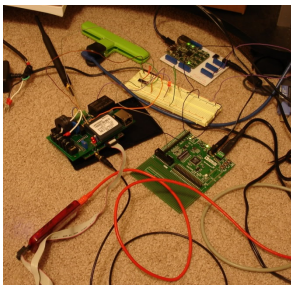
Phasor Measurement Units



PURDUE UNIVERSITY

Phasor Measurement Unit

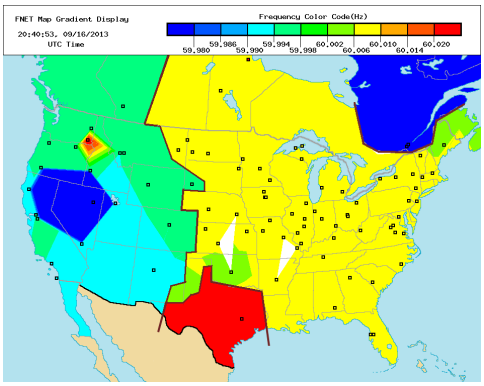




PURDUE UNIVERSITY

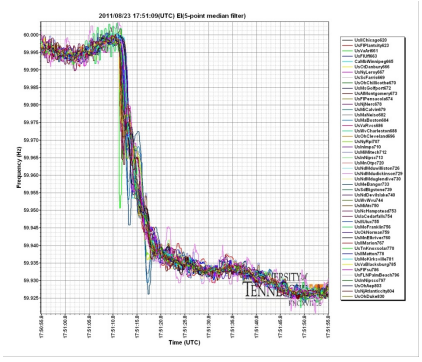
Example Event

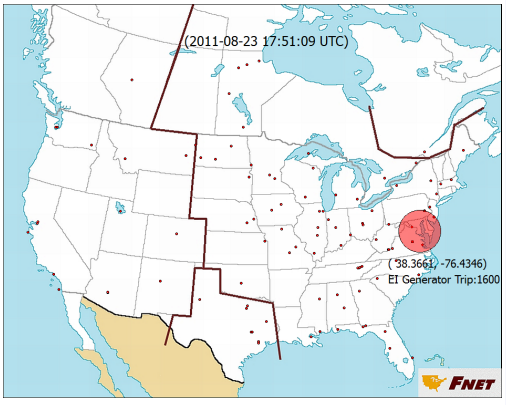
- Virginia Tech and UTK partner in a program called FNET
- A network of PMU's were developed and deployed across the US



PURDUE UNIVERSITY

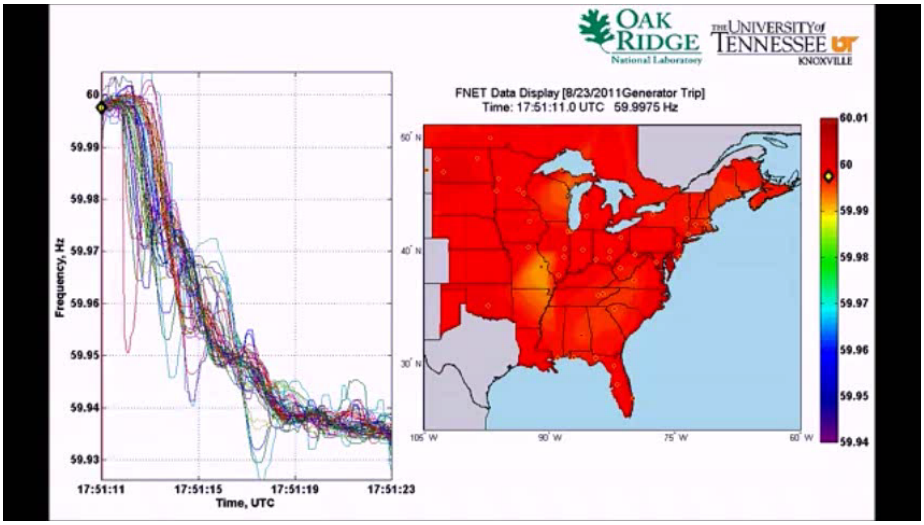
Example Event





PURDUE UNIVERSITY

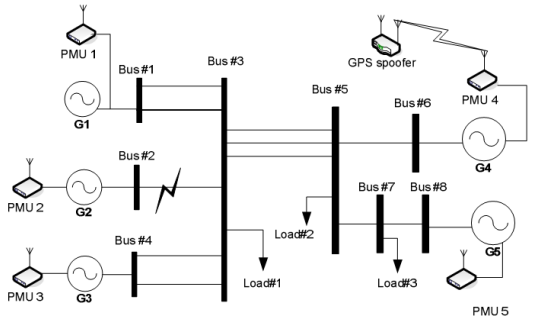
Example Event



PURDUE UNIVERSITY

Time Synchronization Attack (TSA)

- TSA in the context of PMU can result in
  - Incorrect fault localization
  - Invalid load-flow analysis
  - Generator or Transformer Trip (taken offline due to suspected over/under-loading)



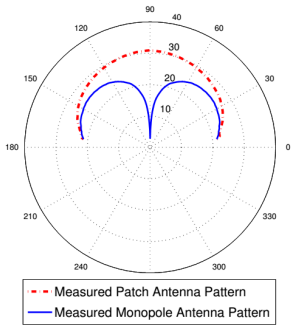
PURDUE UNIVERSITY

TSA

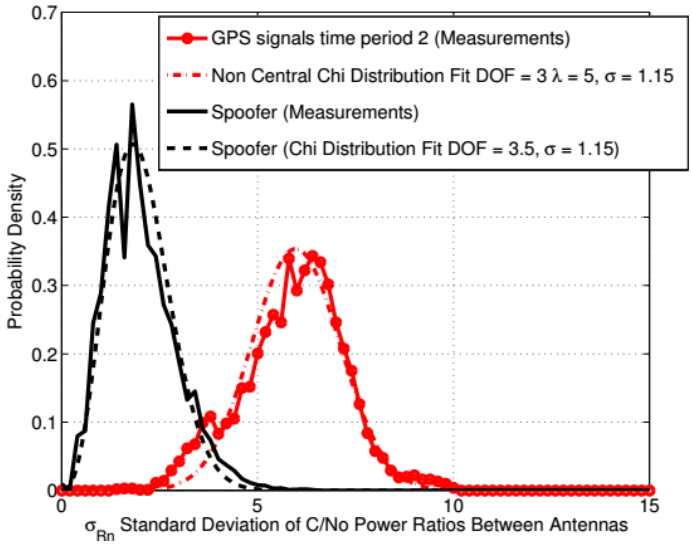
- The PMU relies on a GPS receiver to provide timing information
  - Location accuracy is directly related to timing accuracy
    - 300 m of accuracy requires 1 us of timing accuracy
- Attack relies on spoofing the GPS signal to create a false time in one or more of the PMU's
  - GPS Spoofing Attack
    1. Jam the existing locked GPS signal
    2. Broadcast a replacement GPS signal with a higher SNR than satellite signals
       - Receiver selects the highest SNR carrier

Combating TSA

- At a high level, the PMU needs to know additional information about the GPS signal
  - Develop a trustworthiness factor
  - Detect hijacking signal
- Solution uses two antennas with different gain patterns for comparing SNR's
- Angle of Attack (AoA) for the real satellite and the spoofing transmitter will be different
  - Spoofing transmitter is low on the horizon



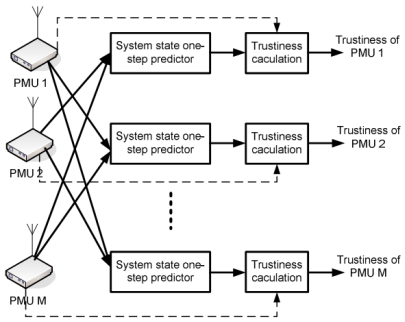
Combating TSA



PURDUE UNIVERSITY

Combating TSA

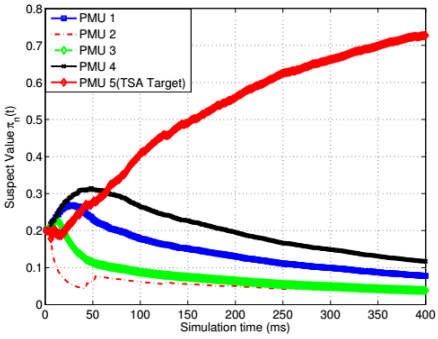
- Second defense involves a Kalman Filter (State Estimation)
  - System state is established
  - As the attack begins, the system state deviates from expectation
  - Amount of deviation goes into a trustworthiness calculation

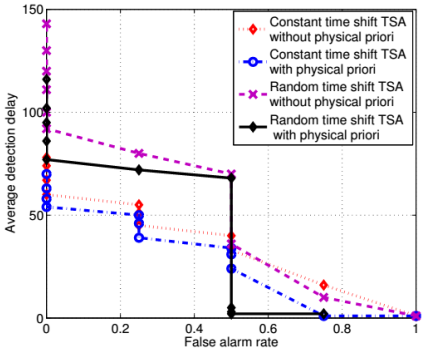


PURDUE UNIVERSITY

Combating TSA

- Author combines two methods into a single cross-layer TSA detection method





PURDUE UNIVERSITY

Conclusions

- The author presented a workable TSA combat method
- The method was shown to find attacks without unreasonable false alarm rates
- Criticisms
  - Method is expensive (Requires Kalman Filtering and a second GPS receiver)
  - Detection latency may not be usable in many situations
    - Decisions may be made with sub-second measurement periods
    - PMU example used only a 15 second window to determine fault location
  - Solution will work for any GPS-timing based application
    - General IoT may not rely heavily on this, however the solution is at odds with the low power, low cost goals

PURDUE UNIVERSITY

DoS in Sensor Networks

- As sensor networks and IoT grows in usage, DoS attacks will gain additional impact factors
  - False alarms in public safety networks will result in disregard
  - Resource reliance during a disaster or military attack
- Sensor nodes are also routers
  - DoS attack under a compromised router
    - May drop packets, invert priorities, etc
  - Attacks may result in disjoint networks
    - Adaptability is a new defense

Jamming Attack

- Physical layer radio interference
  - Defenses include spread spectrum technologies
    - Low cost devices will likely not be able to afford this
- Conservation of energy may allow nodes to outlive an attack

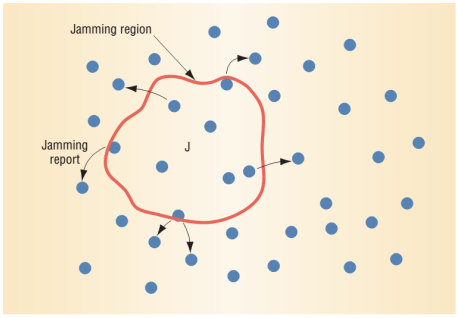


Figure 1. Defense against a jamming attack, phase one. Nodes along the edge of a jammed region report the attack to their neighbors.

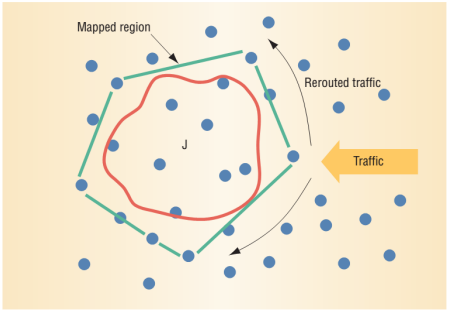


Figure 2. Defense against a jamming attack, phase two. Neighboring nodes collaborate to map the jamming reports, then reroute traffic around the jammed region.

Physical Tampering

- DoS can take place by brute force destruction of sensor nodes
- Physical tampering can allow extraction of cryptographic keys
- Defenses
  - Tamper detection resulting in fail-completely
    - Entry detection results in erasure of keys, etc.
  - Well placed sensors and other physical security considerations

Link Layer

- Media Access Control (MAC) level exchanges
- Collision
  - An attacker can transmit during only part of a communication and cause a collision and thus a dropped packet
    - Error Correcting Codes can be a defense
    - Attacker has power exhaustion advantage
- Exhaustion
  - An attacker can repeatedly request to send information, resulting in starvation
    - MAC rate limiting that ignores too many RTS can combat this
- Unfairness
  - Abusing MAC-priority schemes to perform a weak DoS attack
    - Using small frames can mitigate this problem

Network and Routing Layer

- All nodes (including compromised) are potentially routers
- Neglect and Greed
  - The node refuses to route some packets
    - Redundant routes may mitigate this problem at the expense of power
- Homing
  - Some nodes perform critical functions and can be identified
    - Attackers are more interested in these nodes as they may manage keys or perform other critical functions
    - Can be defended against by encryption of communications making it less obvious which node is performing critical functions
- Misdirection and Smurfing
  - A node publishes false routes to direct traffic to victims
    - Source address verification can defend in this attack
- Black holes
  - Nodes advertise zero-cost routes, disrupting traffic

Network and Routing Layer (continued)

- Authorization
  - Some routers sign route publications to prevent black hole / etc attacks
    - High cost for the nodes to perform this function
- Monitoring
  - Watchdogs can exist on the network to identify problems and perform flow analysis
- Probing
  - In the case of centralized route control, probing can be used to identify problem routes in the network
- Redundancy
  - Diversity coding or message duplication can mitigate some black hole attacks

Transport Layer

- End-to-end connections
  - Involves state/memory at transmit and receive nodes
- Flooding
  - Resource exhaustion through false creation of connections
    - Can be prevented with cryptographic puzzles for proof of resource utilization by the client
      - If an attack is another sensor node, then it will at most be able to starve one victim node
- Desynchronization
  - Disrupting an existing end-to-end connection by forging control flag messages
    - Message authentication can prevent such tampering but comes at a high cost

DoS in Sensor Networks

Table 1. Sensor network layers and denial-of-service defenses.

Network layer	Attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proofing, hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network and routing	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization, monitoring
	Black holes	Authorization, monitoring, redundancy
Transport	Flooding	Client puzzles
	Desynchronization	Authentication

DoS Summary

- Each layer of communication is susceptible to some form of attack
- Defense at each layer involves increased cost, in power consumption or additional hardware requirements
- Authentication, encryption, and digital-signatures are all foundations for DoS defense, but are all difficult to establish in the context of IoT
  - Ongoing research in low cost, low power cryptographic schemes

Conclusion

- IoT presents many challenges for security
  - Large scale key management
  - Increased impact of privacy
  - Huge resource constraints
- Both papers on IoT related topics were fairly well written
  - The GPS TSA was math heavy but tolerable
  - The Computer Magazine article provided a nice overview of DoS attacks in general, though somewhat specific to sensor networks/IoT