Safety and Security Challenges in RF-Based Wireless Power Transfer Networks

Kasım Sinan Yıldırım
Embedded Software Group, Delft University of Technology

November 8, 2016
IPA Fall Days on Communication, Safety & Privacy in the IoT
Battery-less Computers

Przemysław Pawełczak
Kasim Sinan Yildirim
Amjad Yousef Majid

Michel Jansen
Koen Schaper

Safety and Security Challenges in RF-Based Wireless Power Transfer Networks
IoT – Wireless Embedded Systems

Safety and Security Challenges in RF-Based Wireless Power Transfer Networks
Powering IoT

• Powering cyber-physical systems is a challenge
  – By 2025: >100 billion IoT devices
  – sustainable operation
  – large-scale deployment

• Batteries
  – increase weight, cost of the hardware
  – replenishment is generally impractical
  – ecological footprint

• Transfer of electromagnetic energy
  – from a power source to receiver devices over the air
  – wireless power transfer
Wireless Power Transfer (WPT) - I

- **Non-radiative techniques**
  - either inductive or magnetic resonant coupling
    - varying magnetic flux induces current
  - transfer power over short distances
Wireless Power Transfer (WPT) - II

• **Radiative** techniques
  – use the electric field of the electromagnetic waves
    • radio frequency (RF) waves as an energy delivery medium
  – transfer power over longer distances
  – provision of energy to many receivers simultaneously
    • broadcast nature
  – low complexity, size and cost for the energy receiver hardware
  – suitability for mobility
  – charge low-power embedded devices
    • RFID (Radio Frequency Identification) tags

[Diagram of an RFID tag with a chip and an antenna]
Outline

• RF-Powered Embedded Systems
  ─ Current Technologies
  ─ Communication Stack Requirements
  ─ Programming Platforms

• Wireless Power Transfer Networks (WPTNs)
  ─ Safety Issues in WPTNs
  ─ Security Issues in WPTNs
RF-Powered Embedded Systems
RF-Powered Computing

• A new class of low-power battery-less embedded systems
  – Intermittently Powered Devices (IPDs)
• CRFIDs (Computational RFIDs)
  – RFID technology as a foundation
  – Allow sensing, computation and communication without batteries
    • Charge a super capacitor using harvested rf energy
  – Equipped with a backscatter radio
    • simple circuitry for the receiver
    • allows communication to come almost for free

A CRFID platform: WISP - Wireless Identification and Sensing Platform
(University of Washington)

Ultimate goal: replacing existing battery-powered wireless sensor networks
Backscatter Communication

- Transmitting data requires too much energy for a battery-free device
- Modulate the reflections of an incident RF signal
  - use the signal sent by the reader to communicate data back
  - not by generating radio waves
WISP Hardware - Overview

RFID reader

Antenna

- Antenna gets RF signal
- Maximize power transfer to Power Harvester
- RF signal rectified into DC voltage
- Charge Supercapacitor
- Process incoming signal to detect 1s and 0s
- Transistor that changes antenna impedance for 'backscatter'


Safety and Security Challenges in RF-Based Wireless Power Transfer Networks
WISPCam: Battery-less Camera

- WISPCam - University of Washington

WISPCam captures a 160x120 low resolution image for face detection

Ambient Backscatter

- Traditional backscatter communication, (e.g. in RFID)
  - a device communicates by modulating its reflections of an incident RF signal - not by generating radio waves
- Ambient backscatter
  - Communicate using ambient RF signals as the only source of power
    - Ambient RF from TV and cellular communications

Vincent Liu et al. “Ambient Backscatter: Wireless Communication Out of Thin Air”, ISIGCOMM, August 2013
RF-Powered Networks vs Battery-Powered Networks
WISP tags vs WSN nodes - I

- Continuously **varying** voltage level
  - WSNs: stable voltage levels in the short term (battery-powered)
  - WISP: **fluctuating** input voltage\(^1\)

\[\text{Different voltage levels at different distances to the reader}\]

- Different side-effects
  - E.g. prevents short-term stability of the clock hardware\(^2\)

\(^1\text{Benjamin Ransford et al., ”Mementos: system support for long-running computation on RFID-scale devices.” Acm Sigplan Notices 47.4 (2012): 159-170.}\)


Safety and Security Challenges in RF-Based Wireless Power Transfer Networks
WISP tags vs WSN nodes - II

- Frequent loss of computation state
  - frequently ``die'' due to power loss
    - need to save the computation state into the non-volatile memory
    - recover when they harvested sufficient energy to start up
    - saving computational state to non-volatile memory is also energy consuming

---

WISP tags vs WSN nodes - III

• The classical motto of WSNs
  – "compute instead of communicate whenever possible"
  – No longer valid for the WISP platform
    • backscatter communication comes almost for free

• Intermittent power
  – lightweight methods in terms of computation are desirable
  – e.g. least-squares regression
    • Use all data and die or less data but inaccurate solutions
    • Store all data or a portion of it?
Communication Protocols
IPD – Communication Middleware

1. CRFID applications are developing
   - extremely small energy budgets to spare.
   - operate on short distances (less than 5 m)
   - very low throughput (in the order of kB/s).

2. Currently EPC Gen 2 Communication Standard
   - No multi-hop network
   - No Routing

3. Basic building blocks are missing
   - E.g. time synchronization in wireless sensor networks
Case Study – Synchronizing CRFIDs

Battery-less cameras (WISPCams) deployed to capture images of an object from different angles simultaneously.

Each battery-less camera has its own built-in clock whose oscillator generate pulses at slightly different speeds.

How to obtain a common time notion for such collaborative and coordinated actions?
Challenges - I

- Continuously **varying** voltage level in **short-term**
  - The **prominent factor** affecting the frequency of the crystal oscillator
  - Prevents short-term stability and introduces **significant drift**.

- Frequent **loss** of **synchronization state**
  - WISP tags frequently “die”
  - Need to save synchronization state
    - Saving computational state is also an **energy consuming task**
Challenges - II

- **Computation** and **memory** overhead sensitivity
  - computationally **lightweight methods**
- **Communication** is free
  - backscatter communication
- **Single-hop** architecture
  - RFID reader itself is the **natural reference**
- Limitations of EPC Gen 2 standard
  - does not assign **timestamps** to the radio packets
    - a fundamental requirement
  - **communication delays** between the reader and tag
    - RFID reader dependent
WISPSync - I

- RFID reader
  - generates events at regular intervals.
- WISP tag
  - predicts the occurrence of the next event

\[ u(t) = -k_P e(t) - k_I \int e(t) dt \]

Event period is not deterministic due to jitter.


Safety and Security Challenges in RF-Based Wireless Power Transfer Networks
WISPSync - II

- Inspired from PI controllers
  - performs only a few computation steps
    - runs efficiently under limited harvested energy
  - keeps a few variables to hold the synchronization state
    - recovers from power interruptions with minimum overhead
  - adaptive to react to short-term clock instabilities
    - fast (depending on the integral gain).

---

Safety and Security Challenges in RF-Based Wireless Power Transfer Networks

---

Programming Challenges
IPD – Programming Platforms

• How to **design** programs under power interruptions?
  – How to ensure
    • **Consistency** of the non-volatile memory?
    • **Correctness** of the program?

• How to determine **when and what** to save in non-volatile memory
  – Energy consuming

---

1 Safety and Security Challenges in RF-Based Wireless Power Transfer Networks
   Alexei Colin, Brandon Lucia, OOPSLA 2016
Future...

<table>
<thead>
<tr>
<th>Power Source</th>
<th>Active</th>
<th>Passive</th>
<th>Ideal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Battery-powered</td>
<td>RF-powered (battery-free)</td>
<td>RF-powered (battery-free)</td>
</tr>
<tr>
<td>Physical Operating</td>
<td>Unlimited</td>
<td>Requires proximity to RF power</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Range</td>
<td></td>
<td>source</td>
<td></td>
</tr>
<tr>
<td>Lifespan</td>
<td>Months to years</td>
<td>No fundamental limitation</td>
<td>No fundamental limitation</td>
</tr>
</tbody>
</table>

Safety and Security Challenges in RF-Based Wireless Power Transfer Networks

Not Yet
Wireless Power Transfer Networks
Provision of Energy to IPDs

- Wireless power transfer networks (WPTNs)
  - Energy transmitters (ETs)
    - charge different types of energy receivers (ERs)
    - controlling their transmit power and time/frequency of the waveforms
  - Each ER is equipped with a harvester circuit
    - converts the received RF signal to a DC signal
    - charges built-in capacitor/energy storage
Safety and Security Issues in WPTNs

• Power transfer channels are open to attacks
  – wirelessly transmitted energy can be neither encrypted nor authenticated
  – cannot ensure charging a specific harvester

• Radiated power from commercial WPTNs
  – radiation safety thresholds are more likely to be exceeded

• Conventional security mechanisms
  – demand non-negligible computational resources.
  – challenging under limited harvested energy

Safety Issues
Safe power transfer in WPTNs - I

• Several ETs can be active *simultaneously*
  – aimed at charging ERs collaboratively
    • charge *as fast as* possible (reduce charging delay)
    • optimize the transferred energy

• A safe-charging WPTN
  – *electromagnetic radiation (EMR)* under a safety threshold
  – a power transfer *schedule*
    • maximize total transmitted power and ensure EMR safety
    • an *NP-hard* problem\(^1\)
  – quite challenging
    • end-users are allowed to deploy *new ETs* and *modify the locations*
    • as more ETs are deployed, users might be exposed to *more radiation*

Safe power transfer in WPTNs - II

• A **dynamic system** should
  – guarantee the **safety**
    • considering run-time influence of unpredictable end-user actions.
  – maximize **total transmitted power**
    • Received power is inversely proportional with the distance
  – ensure **EMR safety** at each point
    • EMR is linearly proportional with the received power

---

Wireless power density
Hard to estimate and control due to reflection and refraction of the signals.

Centralized/Distributed Control of ETs
Security Attacks
Charging Deadlocks

- Suppose that an ER 1 is being charged by ET 1.
- Let ER 2 with an almost depleted battery sends a charge request to ET 2.
  - ET 2 is turned on and starts transmitting energy
    - RF exposure *exceeds* the safety threshold for ER 1.
  - ET 2 remains turned off
    - ER 2 might *stop* operating.
Safety Attacks

• Safety regulations can be **abused** - **denial of service**
  – to degrade charging performance of ETs
  – even to force them to stop working

• A **malicious ER** can report that the RF exposure is over the safety limit.
  – ETs should
    • either **turn-off** their transceivers
    • **reduce** their transmission power.

• The more safety attacks are done
  – the **less efficiently** ERs are charged
  – the **shorter** their operation time.

Better measurement and **estimation** techniques are required to obtain the radio **power distribution** without feedback from ER.

Safety and Security Challenges in RF-Based Wireless Power Transfer Networks
Freerider ERs

- ETs equipped with omni-directional antennas - public energy sources
  - any ER inside their coverage can harvest energy.
    - although they did not request it.
- **Freerider ERs**
  - do not send charging requests & receive energy for free.
  - ETs are unaware of which ERs they are charging.
  - How to charge only registered or authorized ERs?

ETs can modify their RF transmission parameters at run-time, e.g. frequency and power.
Greedy – Cheating ERs

- **Greedy ERs** send charging requests to ETs **continuously**
  - may lead to other ERs receiving less power.
- ETs should implement **fair power transfer** mechanisms.
  - challenging to **estimate harvested energy precisely**
  - receive **feedbacks** from ERs
    - to get their energy levels
    - to optimize their power transmission parameters.
- **Cheating ERs** report their current energy level is low
  - receive more power from ETs.
Beamforming Attacks

- Multiple ETs emit RF waves at the same frequency band simultaneously
  - **constructive interference**: the phase differences of signals are negligible
    - the received power is greater than that of individual energy waves
  - **destructive interference**: the phase difference is large
    - leading to less harvested power

- Destructive interference is a potential threat
  - an attacker *deliberately* to decrease or destroy harvested energy at ERs

Turning off and listen the network, dynamically adapt their transmission parameters

Safety and Security Challenges in RF-Based Wireless Power Transfer Networks
Monitoring Attacks

- WPTNs can also be considered as wireless monitoring networks
  - malicious ERs that receive energy from ETs
    - disclose private information

- Example:
  - a malicious ER can be equipped with sensors
    - collect measurements
    - Localize people
Conclusions

- **IPDs** and **RF-based WPTNs** are emerging
- There are lots of **research opportunities** in this domain
  - Communication Protocols
    - Physical layer
    - MAC layer
    - Routing
    - Synchronization
  - Programming Platforms
  - Operating Systems
  - Safe and secure power transfer
  - Many more…
Thank You!