Detect Me If You Can: Mitigating DoS Attacks in the Energy Harvesting Internet of Things

Cong Pu, Ph.D.
Dept. of Computer Sciences and Electrical Engineering
Marshall University
Huntington, WV 25705
Email: puc@marshall.edu
Outline

- Introduction and Research Motivation
- Attacks and Countermeasures
  - Adversarial Scenarios
  - EYES: Camouflage-based Active Detection
  - SCAD: Single Checkpoint Assisted Detection
  - EBAD: Explore-based Active Detection
- More Work
Introduction

- Internet-of-Things (IoT) and its applications are rapidly proliferating, where a myriad of multi-scale sensors and devices are seamlessly blended
  - 29 billion wirelessly connected devices will be available for IoT applications by 2022
  - Annual economic impact caused by the IoT is to be in range of $2.7 trillion and $6.2 trillion by 2025

- Wirelessly connected smart nodes under IoT will enhance flexible information accessibility and availability
  - Data mining
  - Cloud computing
  - Social networking
  - Computing power
  - Sensors and embedded devices
  - Wireless communications and networking technologies
Introduction:

Applications

A mobile ad hoc network based disaster relief

A wireless sensor network based structural health monitoring

A vehicular ad hoc network based traffic congestion control

Volcano Monitoring (Welsh, Harvard)
**Introduction: Limited Battery**

- For example, wireless sensor networks (WSNs),
  - Deployed in an unattended environment
  - Required to operate for a long period time
  - Hard to replace (or replenish) battery

"the U.S. Army will eliminate all the military batteries. Each soldier will equip self-powered (or battery-less) communication devices"

"the U.S. Army has invested about $4.2 million in the development of military Apps and the study of smart phone technology"
Introduction:
Energy Harvesting Motivated Networks

- **Energy harvesting (or scavenging)** from an immediate environment,
  - Extracting electric energy from various environmental sources for easy of battery energy replenishment
  - Vibrations, magnetic fields, thermal gradients, lights, *kinetic motions* (e.g., walk or run), and shock waves
- For example, vibration-sensitive energy harvesting WSNs

Introduction: Research Motivation

- Security threats
  - Lack of physical protection
    - Can be captured, tampered, or destroyed
  - Shared wireless medium
    - Can overhear, duplicate, corrupt, or alter data
  - Lack of security requirements
    - Vulnerable to Denial-of-Service (DoS) attacks
- DoS attacks
  - Target service availability rather than subverting the service itself
    - Disrupt network routing protocols or
    - Interfere on-going communications
  - Critical and challenging to develop DoS counterattack mechanisms
    - Sensitive sensory data & secure and reliable delivery

And this house is even more secure! The front door is four feet thick and made of solid titanium...
Selective forwarding attack

- Selectively forward any incoming packet
  - Randomly or strategically
- Target the network routing vulnerabilities of multi-hop networks
- Violate an implicit assumption of cooperative routing
  - Faithfully and collaboratively route packets
- Unlike blackhole attack
  - Simply refuse to forward any incoming packet
- Non-trivial to detect the forwarding misbehavior
  - Temporal node failures or packet collisions??

Energy Harvesting Motivated Attack: Adversarial Scenarios

- Charge-and-spend energy harvesting policy:
- Energy Harvesting State & Active State

Diagram showing the interaction between nodes a, b, c, and m with states and data flows.
Energy Harvesting Motivated Attacks: Adversarial Scenarios (cont.)

A vulnerable case: forwarding misbehavior!!
EYES: Camouflage-based Active Detection: Monitor-based Approach

- The basic idea is,
  - Actively disguises itself as an energy harvesting node on purpose
  - Pretend not to overhear
  - Monitor any forwarding operation
  - Spy vs. Spy

EYES: Camouflage-based Active Detection: Monitor-based Approach (cont.)

monitor ("spy")

overhear

a

b

Data

"harvest"

c

monitor

b

"harvest"

a

Data

m

harvest

m

Alarm

a

c

A vulnerable case: forwarding misbehavior!!

EYES: Camouflage-based Active Detection: Monitor-based Approach (cont.)

Target wireless sensor networks (WSNs) with multiple number of malicious nodes,

- Randomly selected a checkpoint node per-packet basis

---

**SCAD: Single Checkpoint Assisted Detection:**

**Acknowledgment-based Approach**

SCAD: Single Checkpoint Assisted Detection: Acknowledgment-based Approach (cont.)

TABLE II: The comparison* of detection strategies of forwarding misbehavior.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Collusive attack</th>
<th>Computation overhead</th>
<th>Communication overhead</th>
<th>Detection latency</th>
<th>Punishment</th>
<th>Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHEMAS [3]</td>
<td>N</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>N</td>
<td>Centralized</td>
</tr>
<tr>
<td>CAD [5]</td>
<td>N</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>N</td>
<td>Centralized</td>
</tr>
<tr>
<td>FADE [6]</td>
<td>Y</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>N</td>
<td>Centralized</td>
</tr>
<tr>
<td>Watchdog [8]</td>
<td>N</td>
<td>Low</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Stand-alone</td>
</tr>
<tr>
<td>HCD [12]</td>
<td>N</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>Y</td>
<td>Distributed</td>
</tr>
<tr>
<td>CAM [13]</td>
<td>N</td>
<td>Low</td>
<td>N</td>
<td>Low</td>
<td>N</td>
<td>Stand-alone</td>
</tr>
<tr>
<td>SCAD</td>
<td>Y</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>N</td>
<td>Centralized</td>
</tr>
</tbody>
</table>
EBAD: Explore-based Active Detection: Bait-based Approach

- Target mobile ad hoc networks (MANETs) with multiple number of malicious nodes.

**RREQ**: Route Request Packet

**RREP**: Route Reply Packet

**Fake RREP**

EBAD: Explore-based Active Detection: Bait-based Approach (cont.)

- Target mobile ad hoc networks (MANETs) with multiple number of malicious nodes,

- Intentionally broadcast an exploring RREQ with a fictitious destination node, eRREQ
EBAD: Explore-based Active Detection: Bait-based Approach (cont.)
More Work …

- Cryptography,

- Network Security,
  - "Energy Depletion Attack in Low Power and Lossy Networks: Analysis and Defenses", Cong Pu and Bryan Groves (CS Undergraduate), IEEE ICDIS, pp. 14--21, 2019. (Best Paper Award)

- Wireless Networks,
More Work ...

- **Mobile Computing,**

- **Information-Centric Networking,**

- **Currently working on,**
  - *Mutual Authentication and Key Agreement Protocol for Internet of Drones*
  - *Machine Learning based Service Scheduling for Internet of Drones*
  - *Mitigating Routing Misbehavior in Flying Ad Hoc Networks*
  - *A Secure Data Collection and Storage Mechanism for Internet of Drones*
Any Question?