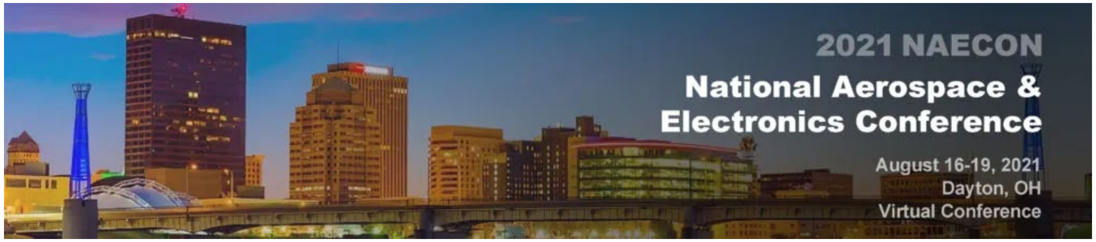
Detect Me If You Can: Mitigating DoS Attacks in the Energy Harvesting Internet of Things

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



2021 NAECON
National Aerospace & Electronics Conference
August 16-19, 2021
Dayton, OH
Virtual Conference

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

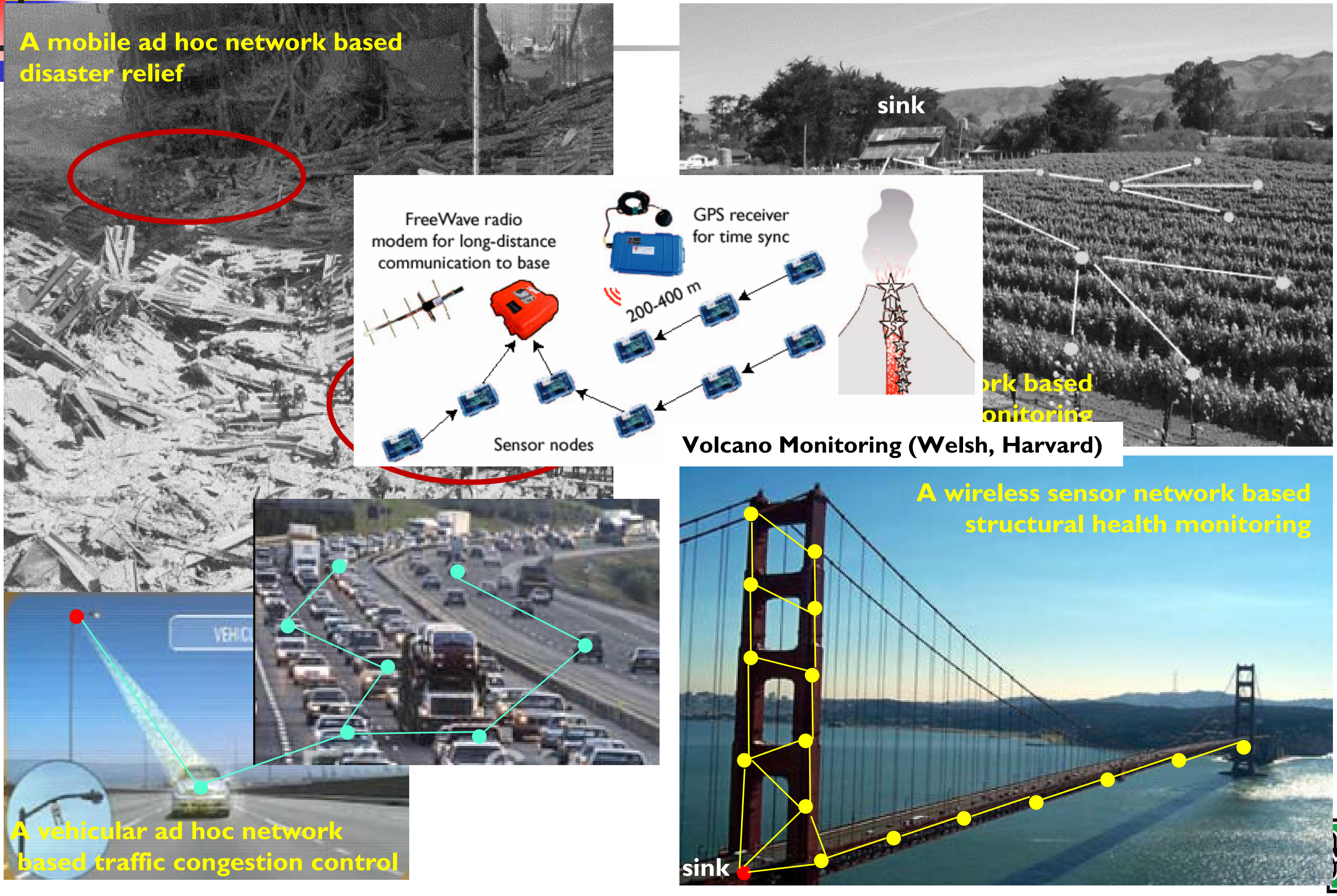
- More Work

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

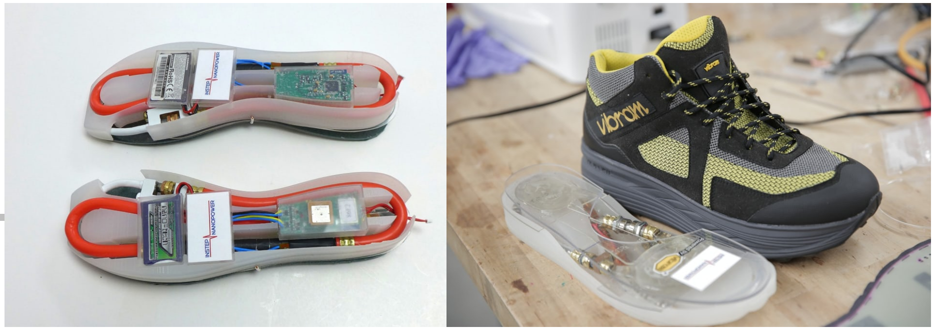
Introduction: Applications


A mobile ad hoc network based disaster relief
sink
FreeWave radio modem for long-distance communication to base
GPS receiver for time sync
200-400 m
Sensor nodes
ork based
onitoring
A wireless sensor network based structural health monitoring
sink
VEHICL
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



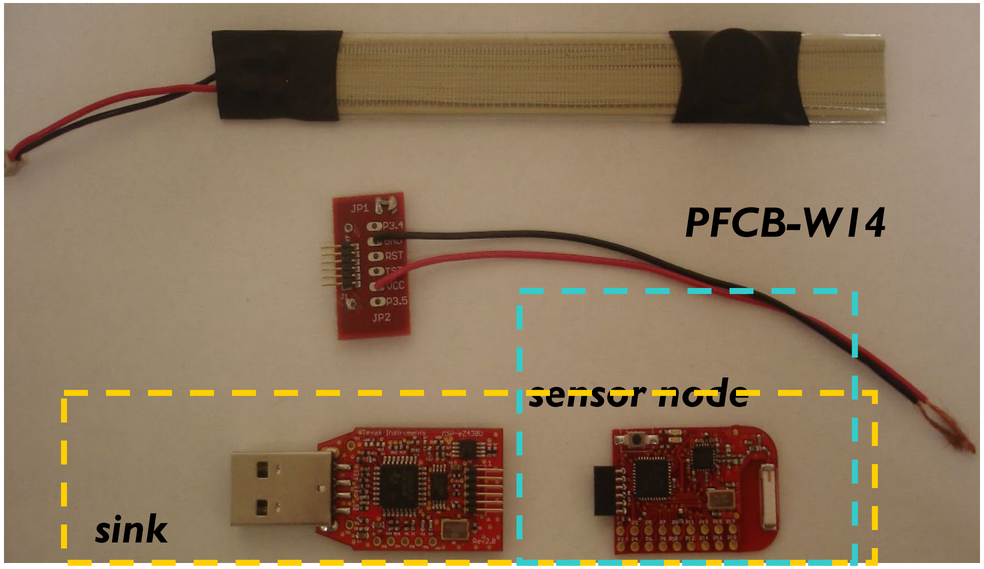
UW-Madison College of Engineering

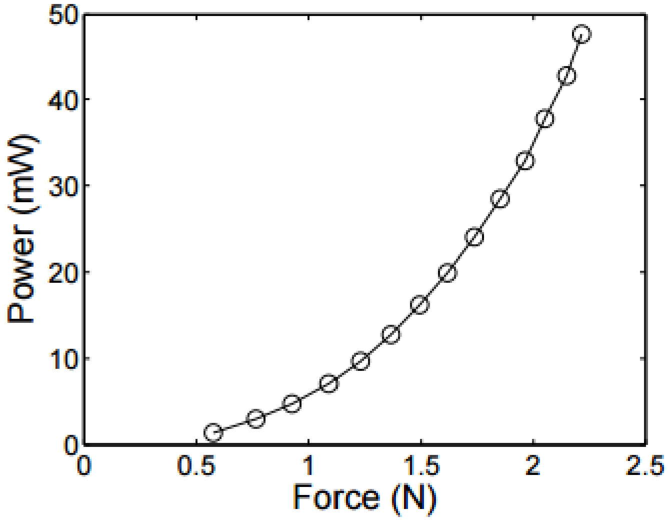
*"the **U.S. Army** will eliminate all the military batteries. Each soldier will equip **self-powered (or battery-less)** communication devices"*

*"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





Sunho Lim, Kimn Jung-Han, and Kim Hyeoungwoo, "Analysis of Energy Harvesting for Vibration-Motivated Wireless Sensor Networks." ICWN, 2010

Introduction:
Research Motivation

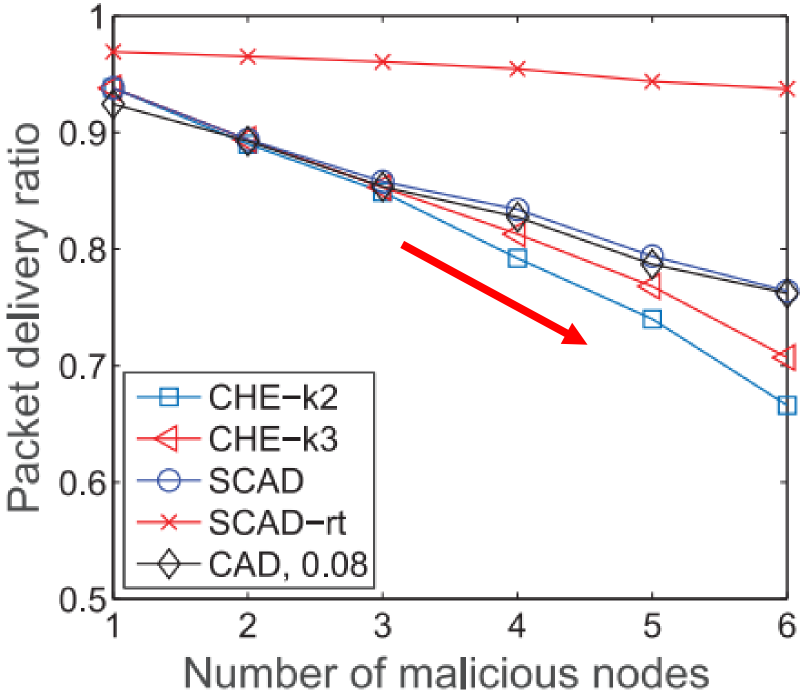
And this house is even more secure! The front door is four feet thick and made of solid titanium...

© 2002 by Paul Kocher

- 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

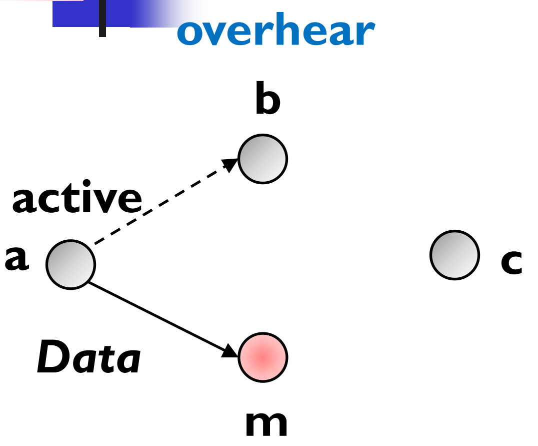
Forwarding Misbehavior: Selective Forwarding Attack

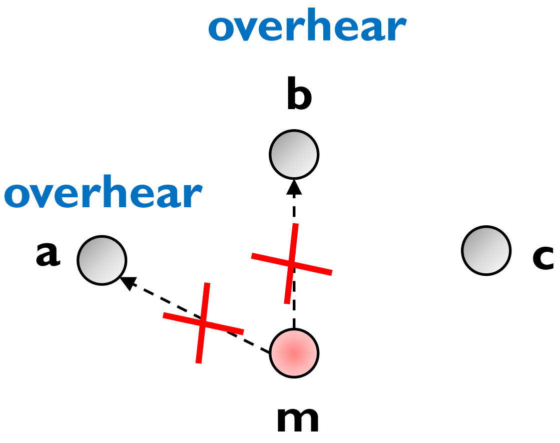
- Selective forwarding attack
  - Selectively forward any incoming packet
    - Randomly or strategically
  - Target the network routing vulnerabilities of multi-hop networks
  - Violate an **implicit assumption** of cooperative routing
    - Faithfully and collaboratively route packets
  - Unlike blackhole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

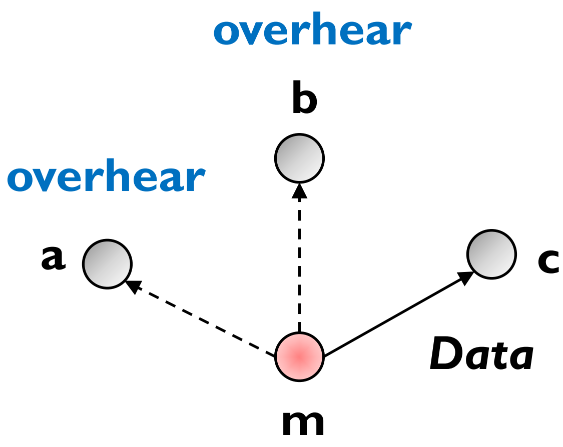


Cong Pu and Sunho Lim, A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation, IEEE Systems Journal (Impact Factor: 3.931), vol.12, iss. 1, pp. 834--842, 2018.

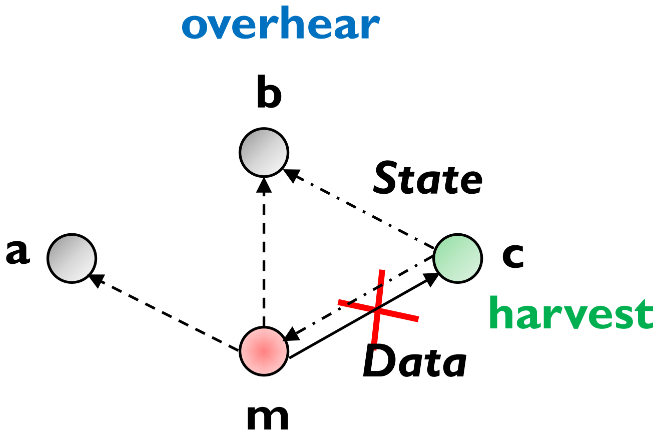
Energy Harvesting Motivated Attack: Adversarial Scenarios

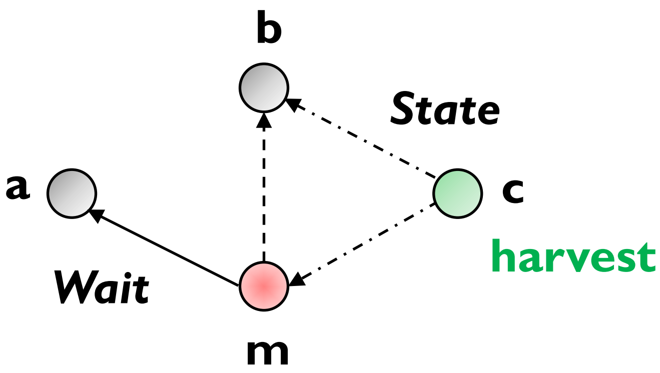




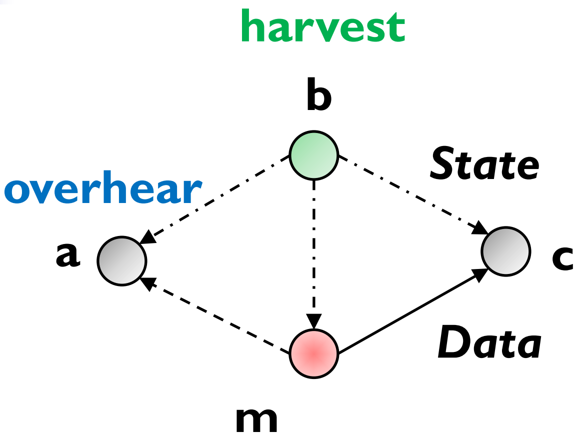


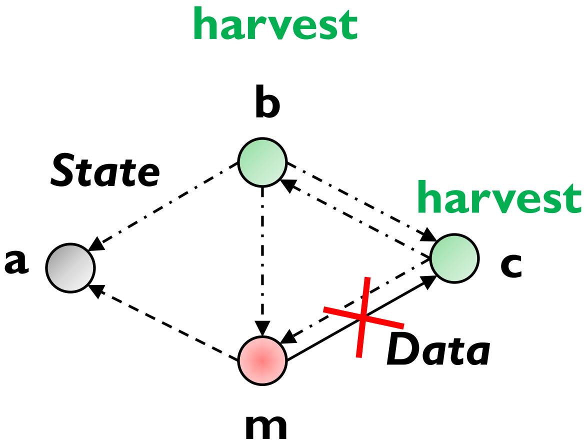
- *Charge-and-spend* energy harvesting policy:
  - Energy Harvesting State & Active State





Energy Harvesting Motivated Attacks: Adversarial Scenarios (cont.)

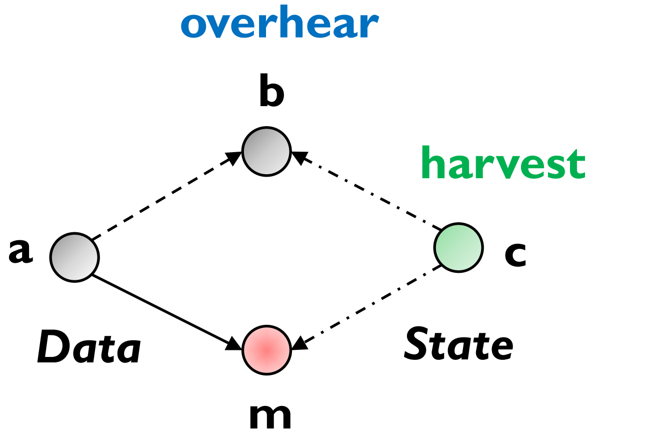




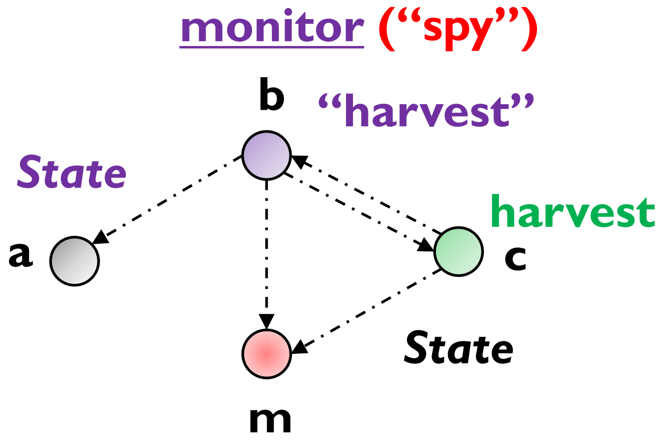
a vulnerable case:
forwarding misbehavior!!

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

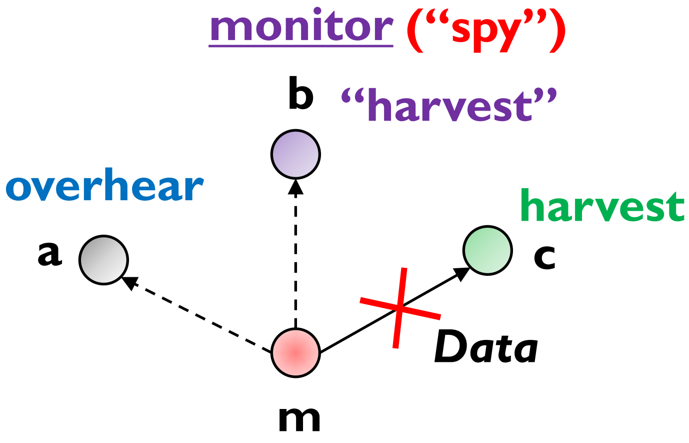


disguise itself as an energy harvesting node randomly
→ a vulnerable case

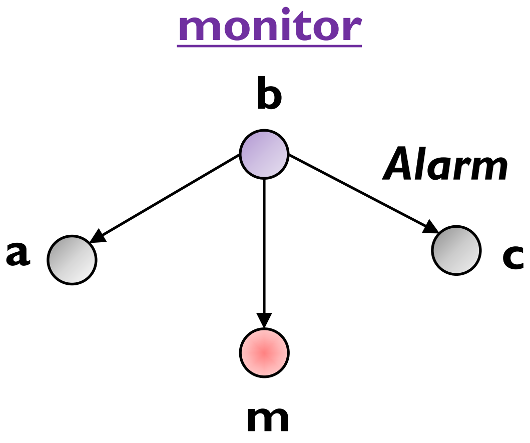


Cong Pu, Sunho Lim, Byungkwan Jung, and Jinseok Chae. "EYES: Mitigating Forwarding Misbehavior in Energy Harvesting Motivated Networks", Elsevier Computer Communications (Impact Factor: 3.167), Vol. 124, pp. 17--30, 2018.

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

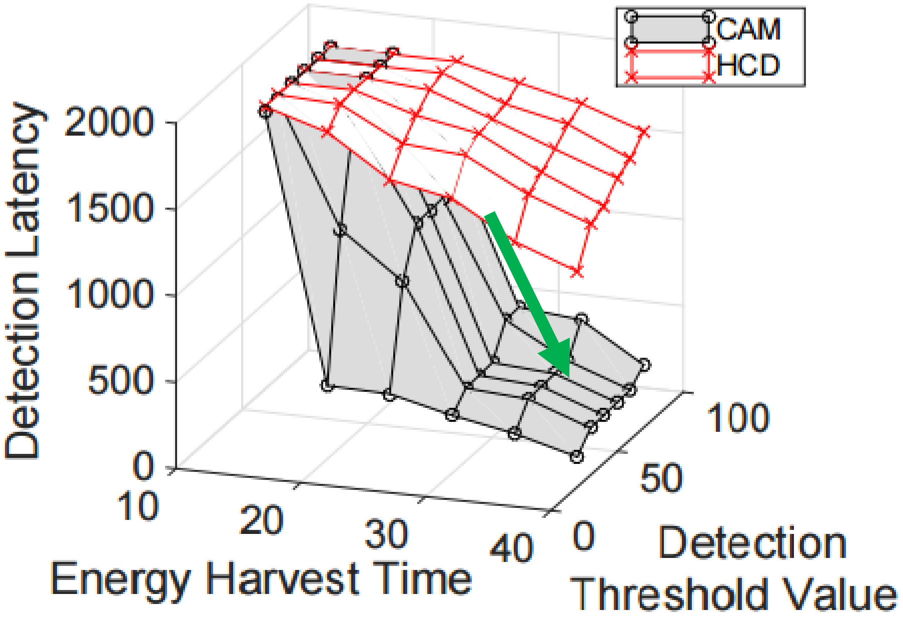


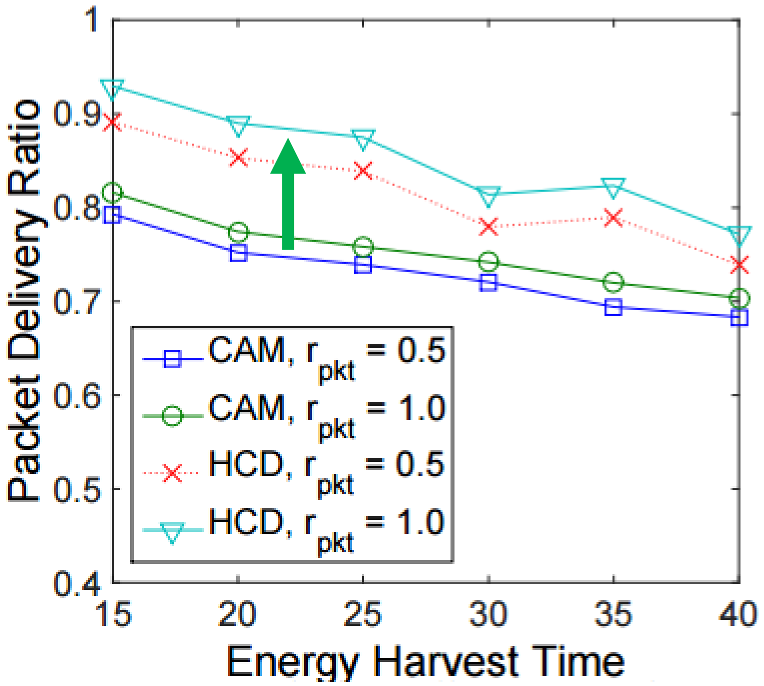
a vulnerable case:
forwarding misbehavior!!



***Cong Pu**, Sunho Lim, Byungkwan Jung, and Jinseok Chae. "EYES: Mitigating Forwarding Misbehavior in Energy Harvesting Motivated Networks", Elsevier Computer Communications (Impact Factor: 3.167), vol. 124, pp. 17--30, 2018.*

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



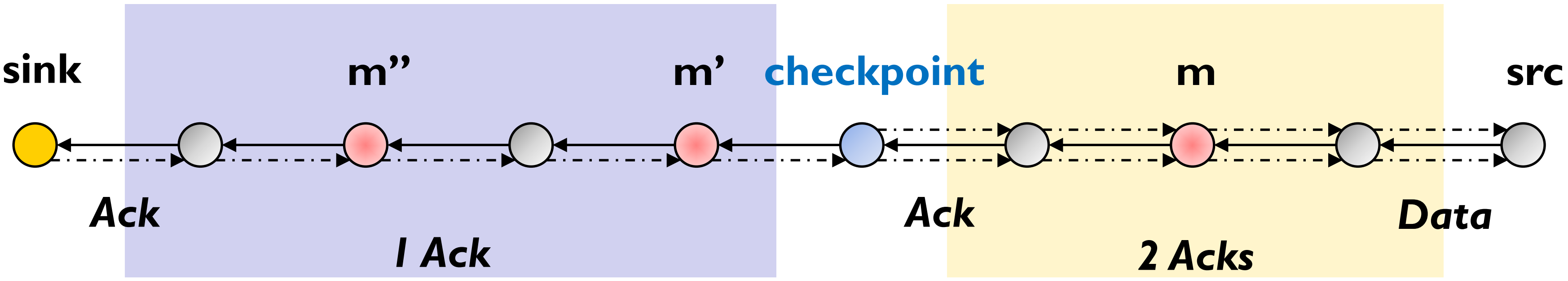


***Cong Pu**, Sunho Lim, Byungkwan Jung, and Jinseok Chae. "EYES: Mitigating Forwarding Misbehavior in Energy Harvesting Motivated Networks", Elsevier Computer Communications (Impact Factor: 3.167), Vol. 124, pp. 17--30, 2018.*

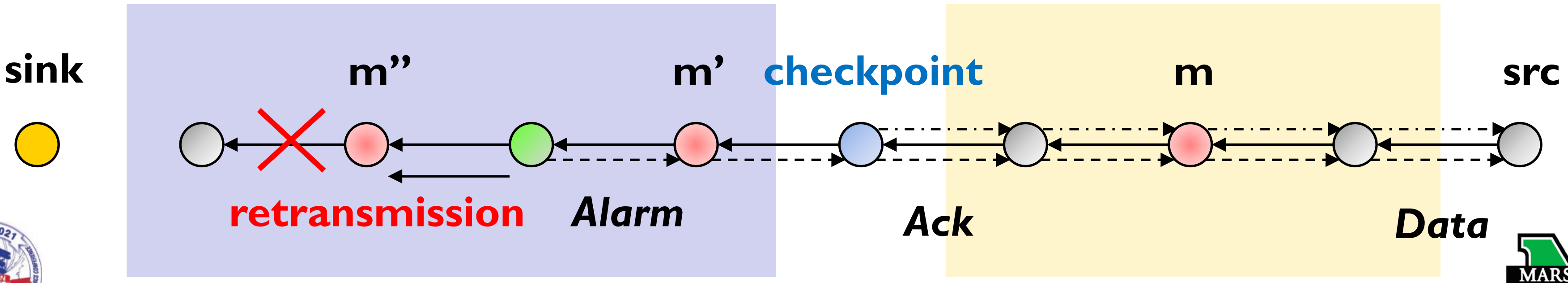
Cong Pu *and Sunho Lim, A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation, IEEE Systems Journal (IF: 3.931), vol. 12, iss. 1, pp. 834--842, 2018.*

SCAD: Single Checkpoint Assisted Detection: Acknowledgment-based Approach

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

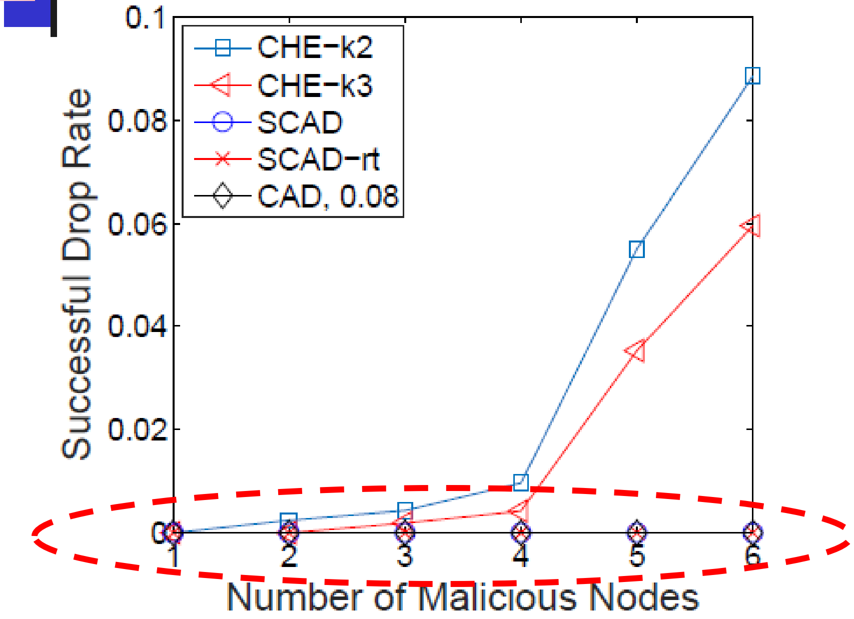


- **Randomly selected a checkpoint node per-packet basis**



Cong Pu *and Sunho Lim, A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation, IEEE Systems Journal (IF: 3.931), vol. 12, iss. 1, pp. 834--842, 2018.*

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



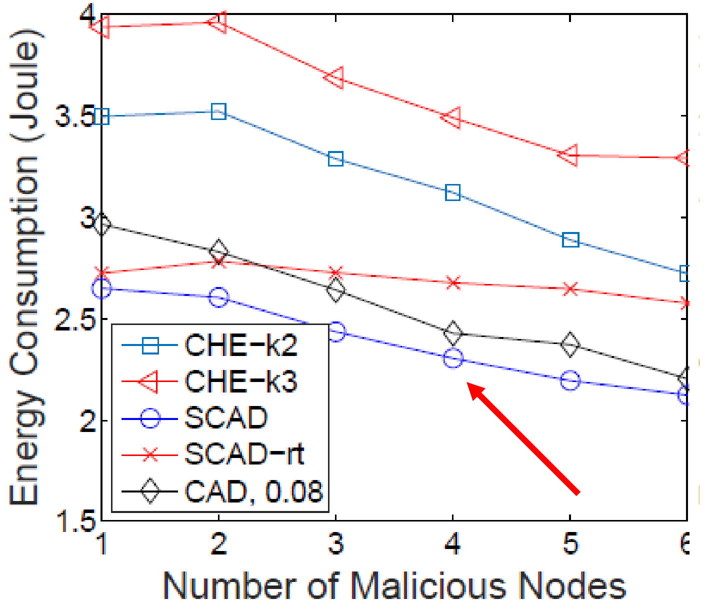
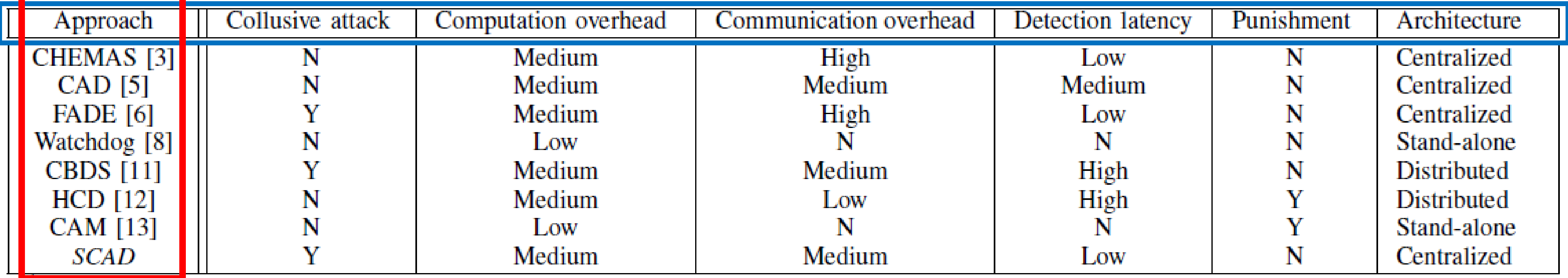


TABLE II: The comparison† of detection strategies of forwarding misbehavior.

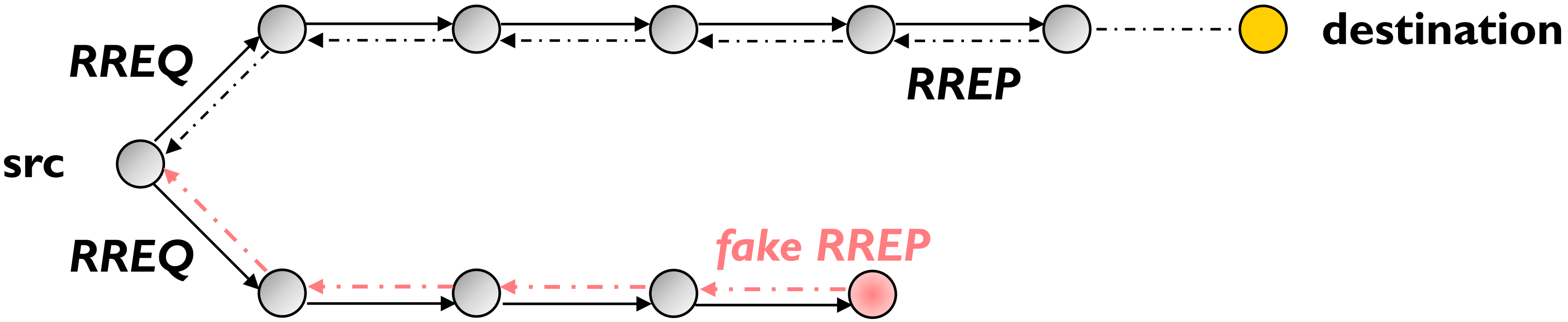


Approach	Collusive attack	Computation overhead	Communication overhead	Detection latency	Punishment	Architecture
CHEMAS [3]	N	Medium	High	Low	N	Centralized
CAD [5]	N	Medium	Medium	Medium	N	Centralized
FADE [6]	Y	Medium	High	Low	N	Centralized
Watchdog [8]	N	Low	N	N	N	Stand-alone
CBDS [11]	Y	Medium	Medium	High	N	Distributed
HCD [12]	N	Medium	Low	High	Y	Distributed
CAM [13]	N	Low	N	N	Y	Stand-alone
SCAD	Y	Medium	Medium	Low	N	Centralized

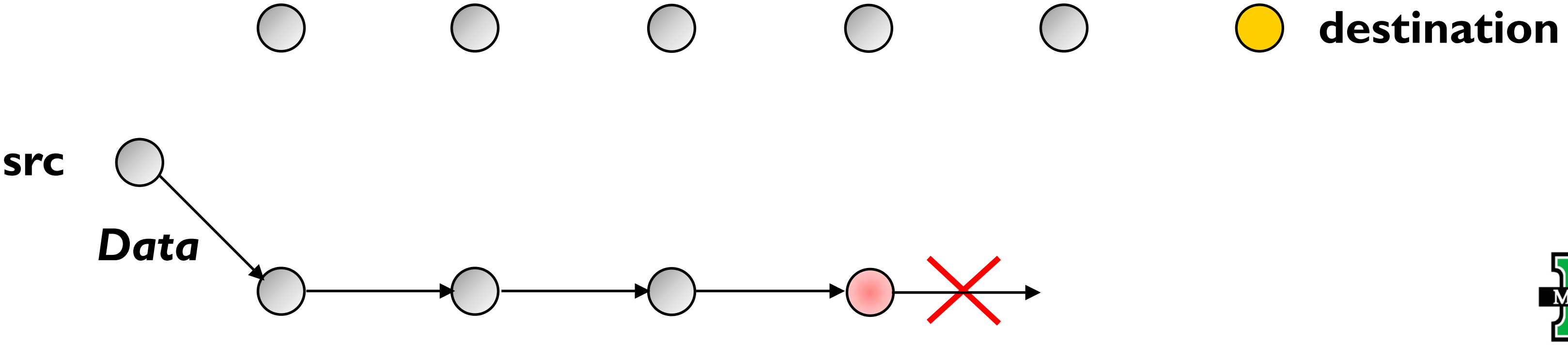
Cong Pu, Sunho Lim, Jinseok Chae, and Byungkwan Jung, "Active Detection in Mitigating Routing Misbehavior for MANETs", Springer Wireless Networks (Impact Factor: 2.602), vol. 25, iss.4, pp. 1669—1683, 2019.

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**

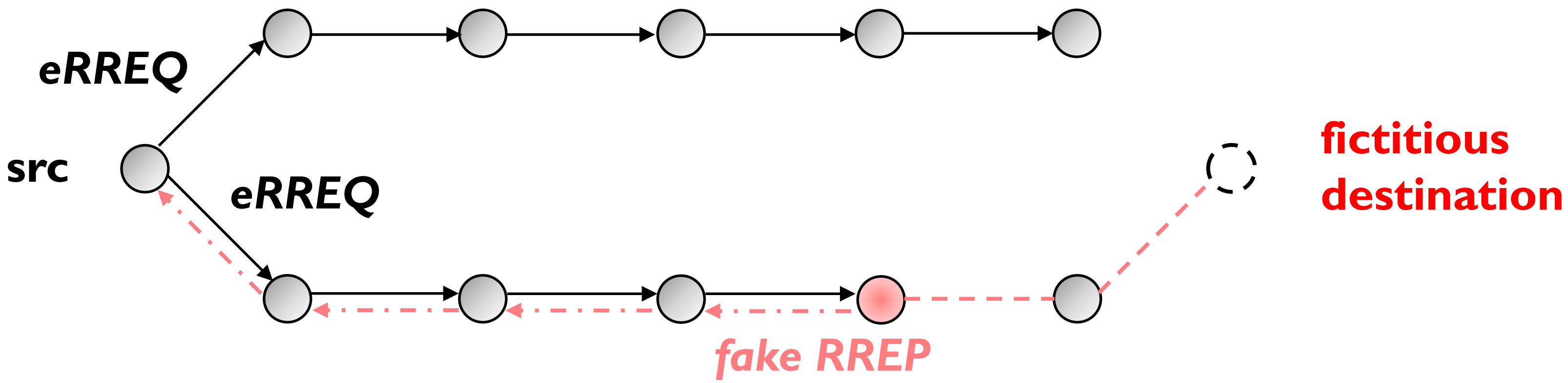


Cong Pu, Sunho Lim, Jinseok Chae, and Byungkwan Jung, "Active Detection in Mitigating Routing Misbehavior for MANETs", Springer Wireless Networks (Impact Factor: 2.602), vol. 25, iss.4, pp. 1669—1683, 2019.

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

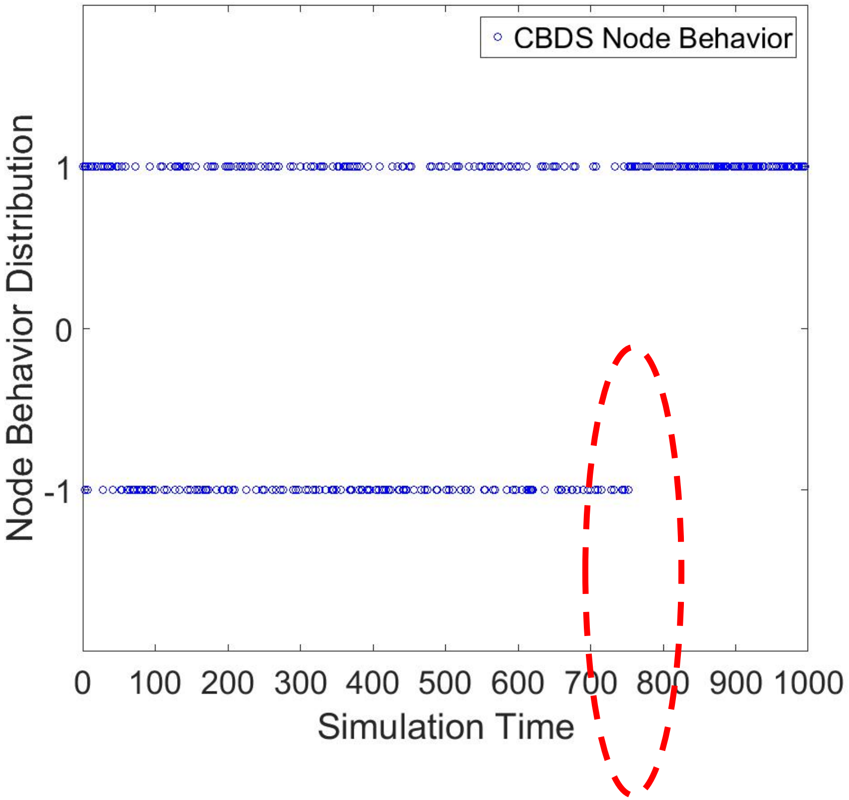
- Target mobile ad hoc networks (MANETs) with multiple number of malicious nodes,

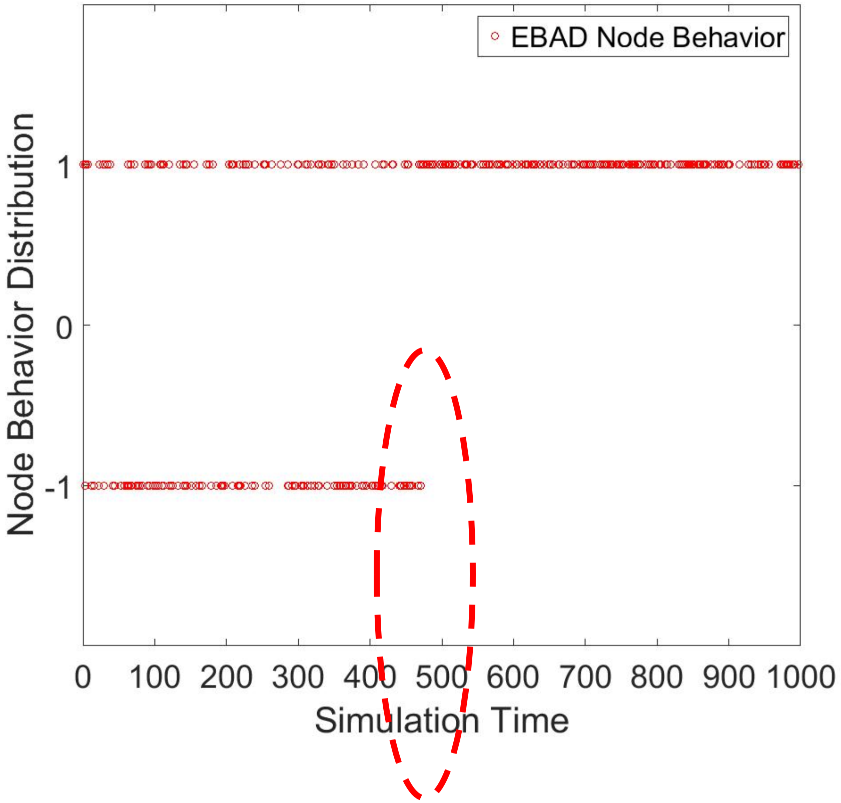
- **Intentionally broadcast an exploring RREQ with a fictitious destination node, *eRREQ***



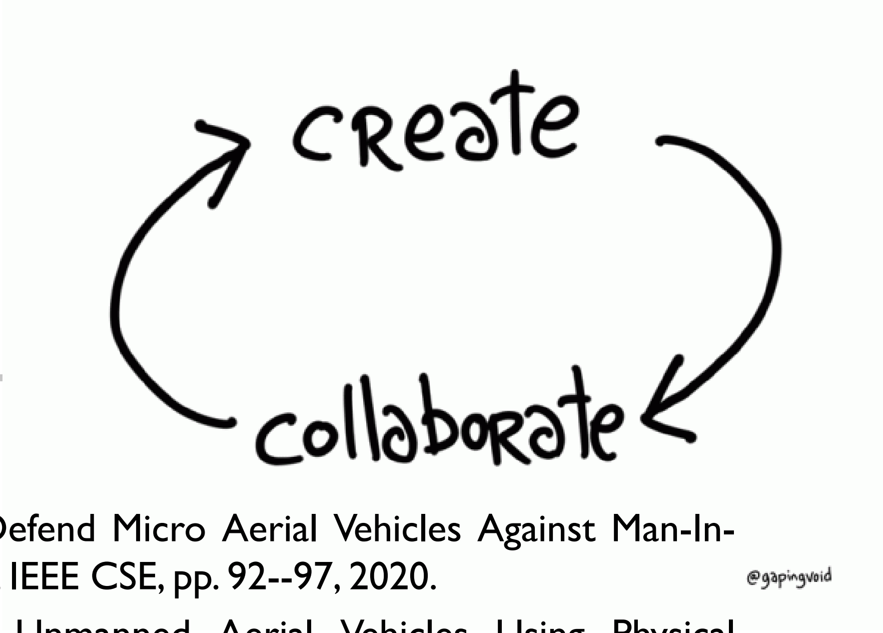
Cong Pu, Sunho Lim, Jinseok Chae, and Byungkwan Jung, "Active Detection in Mitigating Routing Misbehavior for MANETs", Springer Wireless Networks (Impact Factor: 2.602), vol. 25, iss.4, pp. 1669—1683, 2019.

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



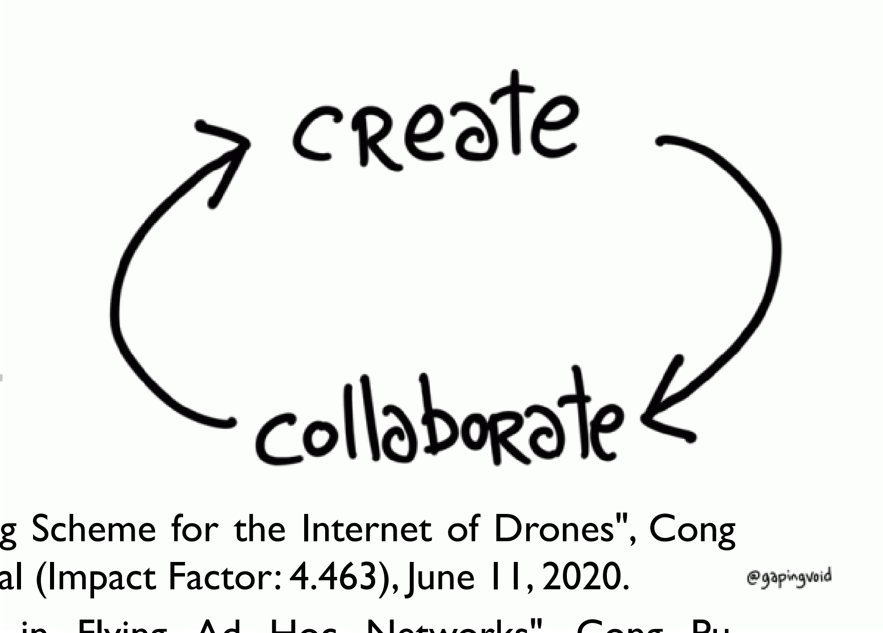


More Work …



- **Cryptography,**
  - "Lightweight Digital Signature Solution to Defend Micro Aerial Vehicles Against Man-In-The-Middle Attack",Yucheng Li and Cong Pu, IEEE CSE, pp. 92--97, 2020.
  - "Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System", Cong Pu and Yucheng Li, IEEE LANMAN, pp., 2020.
- **Network Security,**
  - "Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses", Cong Pu, IEEE Internet of Things Journal (Impact Factor: 9.936),Vol. 7, Iss. 6, pp. 4937--4949, 2020.
  - "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,**
  - "Light-Weight Forwarding Protocols in Energy Harvesting Wireless Sensor Networks", Cong Pu, Tejaswi Gade, Sunho Lim, Manki Min, and Wei Wang, IEEE MILCOM, pp. 1053--1059, 2014.
  - "A Novel Energy Harvesting Aware IEEE 802.11 Power Saving Mechanism", Yigitcan Celik and Cong Pu,WASA, pp. 14--26, 2018.

More Work …



- **Mobile Computing,**
  - "Psched: A Priority-Based Service Scheduling Scheme for the Internet of Drones", Cong Pu and Logan Carpenter, IEEE Systems Journal (Impact Factor: 4.463), June 11, 2020.
  - "Stochastic Packet Forwarding Algorithm in Flying Ad Hoc Networks", Cong Pu, Proceedings of the IEEE MILCOM, pp. 494--499, 2019.
- **Information-Centric Networking,**
  - "ProNDN: MCDM Based Interest Forwarding and Cooperative Data Caching for Named Data Networking", Cong Pu, Journal of Computer Networks and Communications, Vol. 2021, pp. 1--16, 2021.
  - "Self-Adjusting Share-Based Countermeasure to Interest Flooding Attack in Named Data Networking", Cong Pu, Nathaniel Payne, and Jacqueline Brown, IEEE CPSCom, pp. 142--147, 2019.
- **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?