Spy vs. Spy: Camouflage-based Active Detection in Energy Harvesting Motivated Networks

Cong Pu and Sunho Lim

Dept. of Computer Science, Texas Tech University

Abstract

Selective forwarding attack is one of well-known denial-of-service (DoS) attacks, and designing its countermeasure is critical and challenging. Detecting a forwarding misbehavior in multi-hop networks is non-trivial because it is hard to filter from node failure or packet collision. This paper proposes a new countermeasure, called camouflage-based active detection, in a rapidly emerging energy harvesting motivated networks (EHNets), where a set of self-sustainable nodes communicate directly or indirectly via multi-hop relays. Four adversarial scenarios motivated by energy harvesting and their potential forwarding vulnerabilities are analyzed. Each node actively disguises itself as an energy harvesting node, monitors any forwarding operation, and detects forwarding misbehaviors of lurk deep malicious nodes in EHNets. Extensive simulation experiments using OMNeT++ show that the proposed approach is highly detection-efficient compared to a hop-by-hop cooperative detection scheme in terms of detection latency and detection rate.

Introduction

❑ **Internet-of-Things (IoT)**

- ➢ A myriad of multi-scale sensors and devices (later in short, nodes) are seamlessly blended for a ubiquitous computing and communication infrastructure

❑ **Energy Harvesting Motivated Networks (EHNets)**

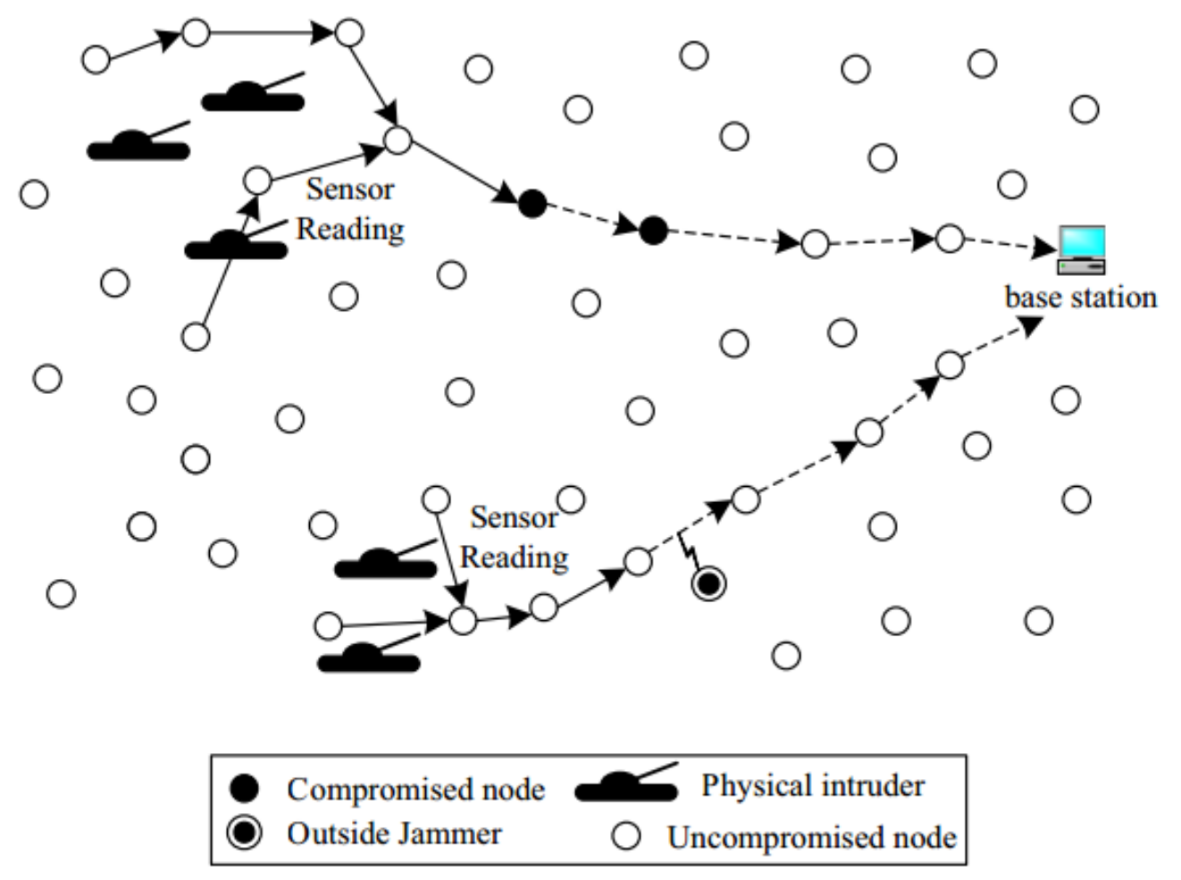
- ➢ A major building block for IoT applications
- ➢ Nodes harvest energy from an immediate environment (e.g., solar, wind, vibration, etc.)

❑ **Problems:**

- ➢ Lack of physical protection in harsh environment
  - ▪ Node can be easily captured, tampered, or destroyed by an adversary
- ➢ An open nature of wireless communication
  - ▪ Adversary can overhear, duplicate, corrupt, or alter sensory data
- ➢ Lack of security requirements in network routing protocols
  - ▪ Adversary can disrupt network routing protocols or interfere with on-going communications

❑ **Attack:**

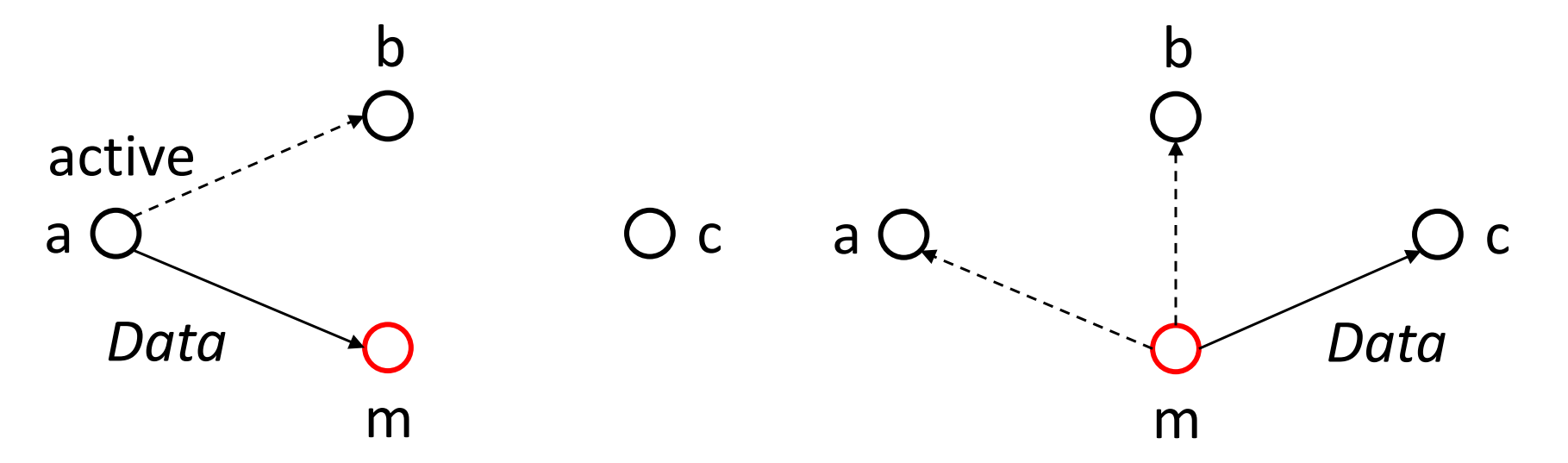
- ➢ Selective Forwarding Attack
  - ▪ A single or multiple malicious nodes randomly or strategically drop any incoming packet
  - ▪ Targeting the network routing vulnerabilities: *All nodes faithfully and collaboratively route packets to a sink*
- ➢ An example sensor network under selective forwarding attack



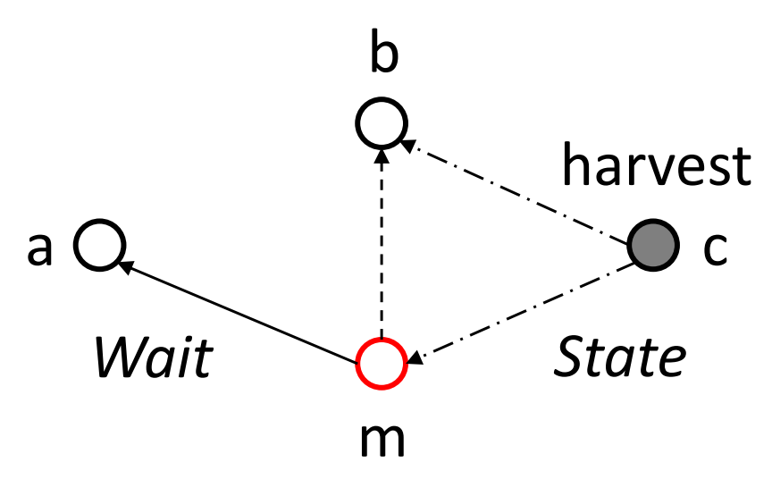
Energy Harvesting Motivated Attacks and Implications

❑ **A set of adversarial scenarios and its vulnerable cases in which a malicious node selectively drops any incoming packet without being detected in EHNets.**

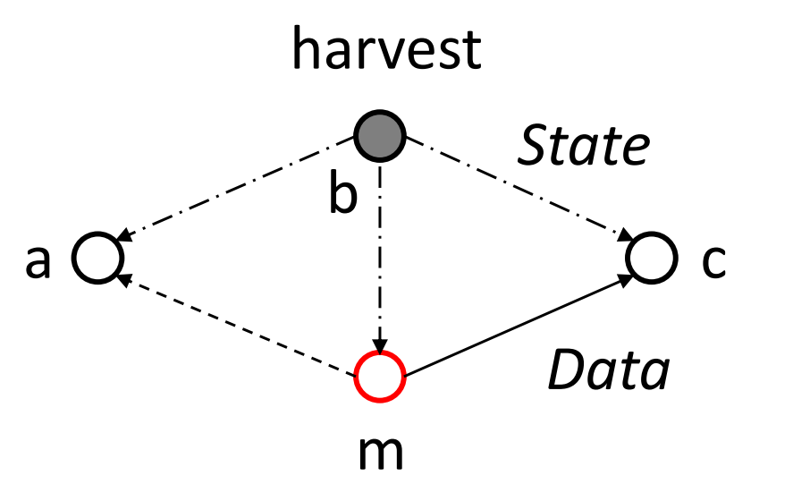
- ➢ A snapshot of network consisting of four energy harvesting enabled nodes:
  - ▪ Packet sender n_a
  - ▪ Packet receiver n_c
  - ▪ Forwarding candidate nodes n_b and n_m
- ➢ Scenario A:



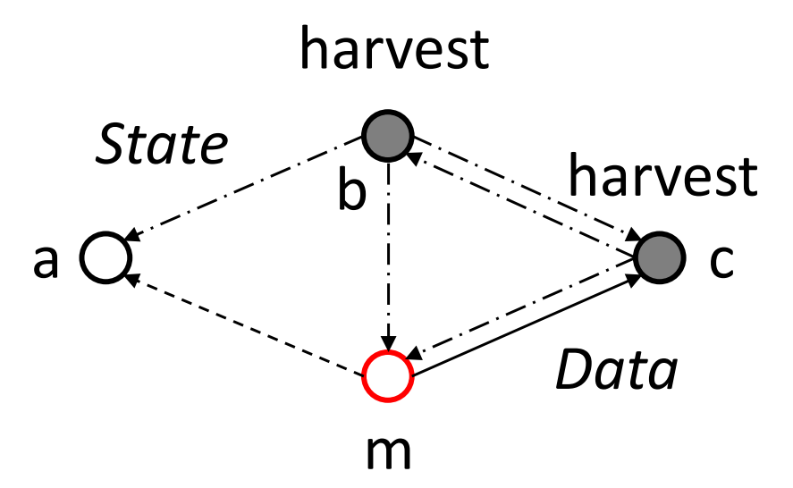
- ➢ Scenario B:



- ➢ Scenario C:

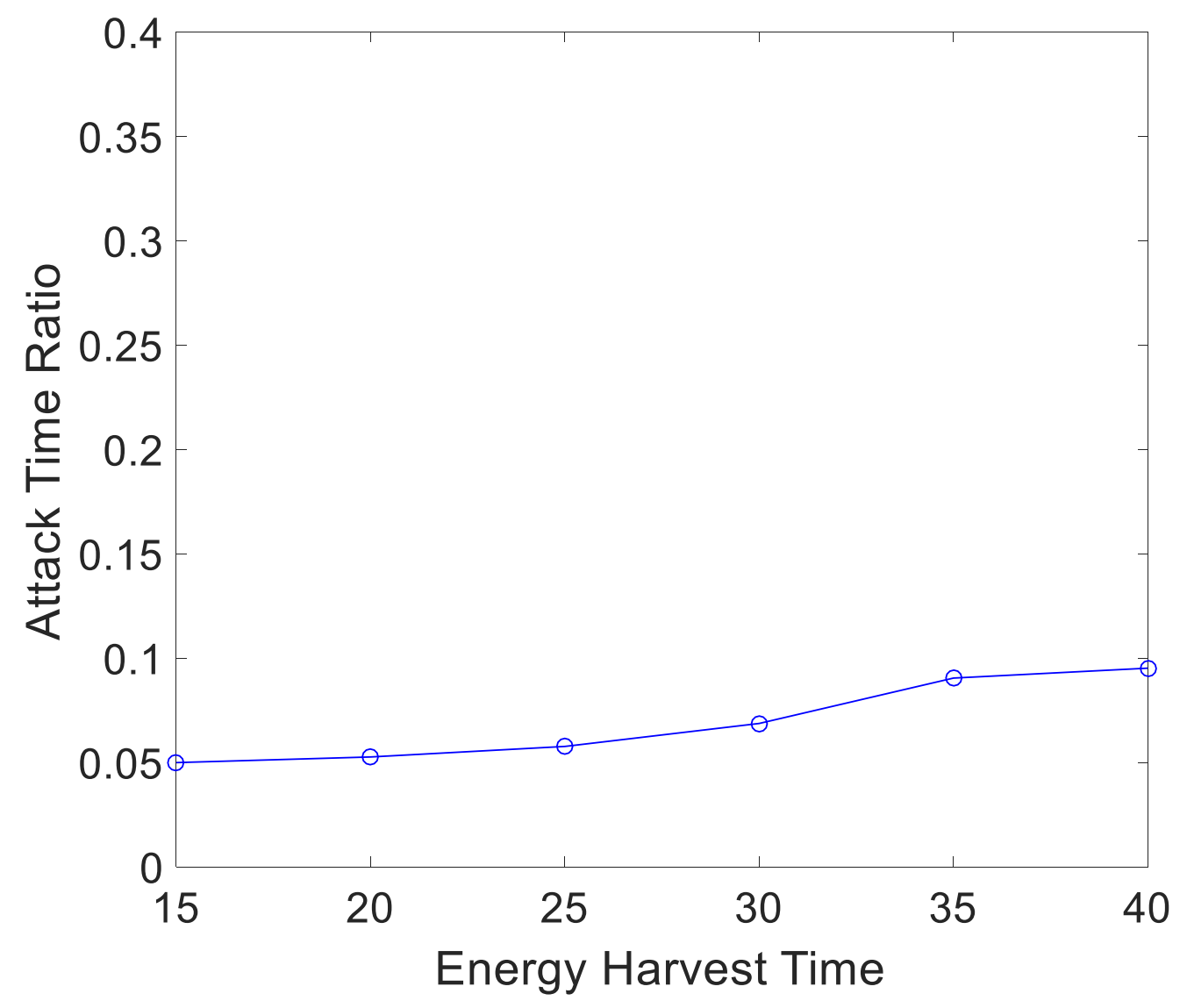


- ➢ Scenario D:



❑ **Attack Time Ratio**

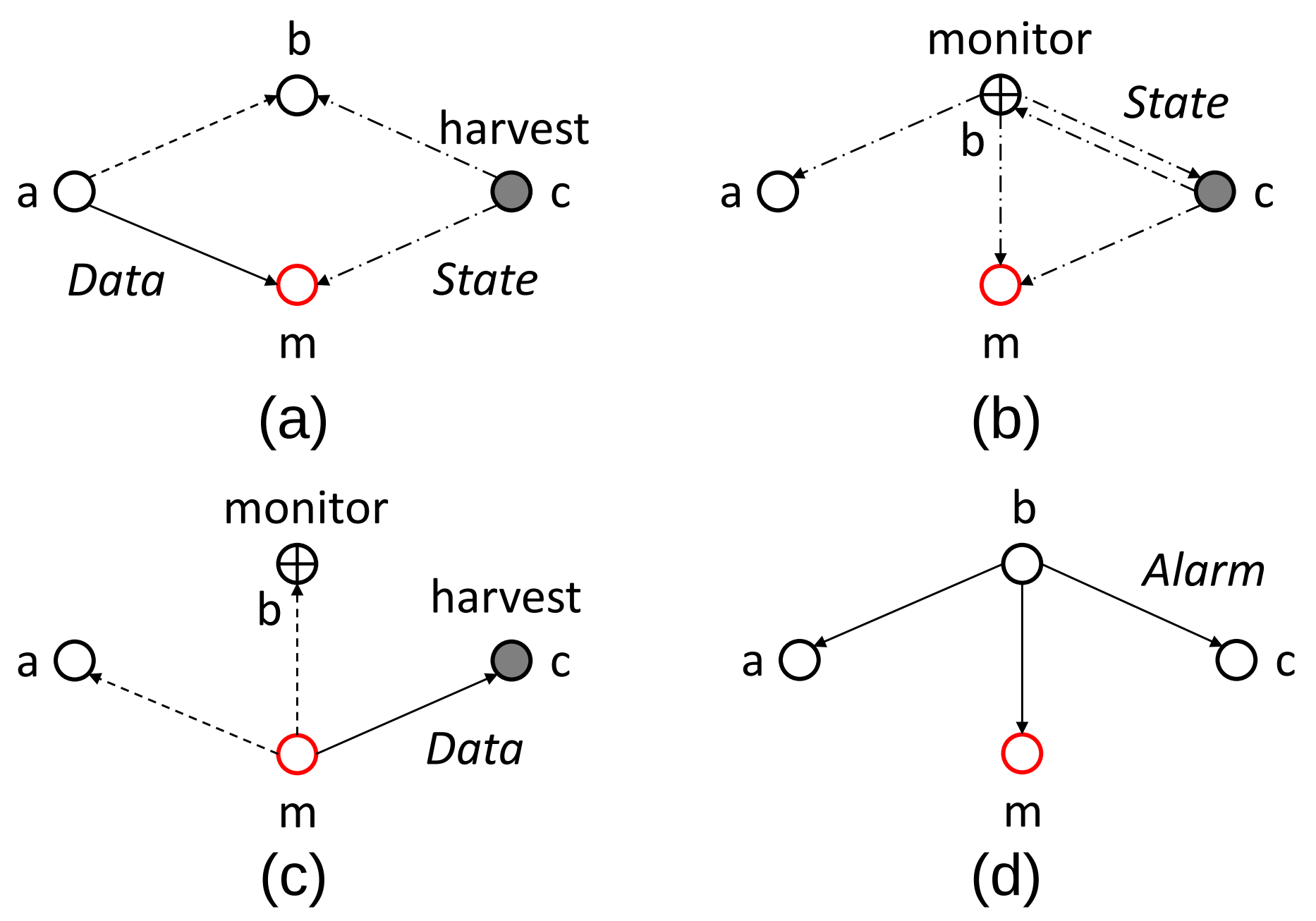
- ➢ How frequently a malicious node can show its forwarding misbehaviors in terms of attack time ratio
- ➢ t_{at} / t_{tot}
  - ▪ t_{at} is total attack time of forwarding misbehaviors
  - ▪ t_{tot} is total observation time



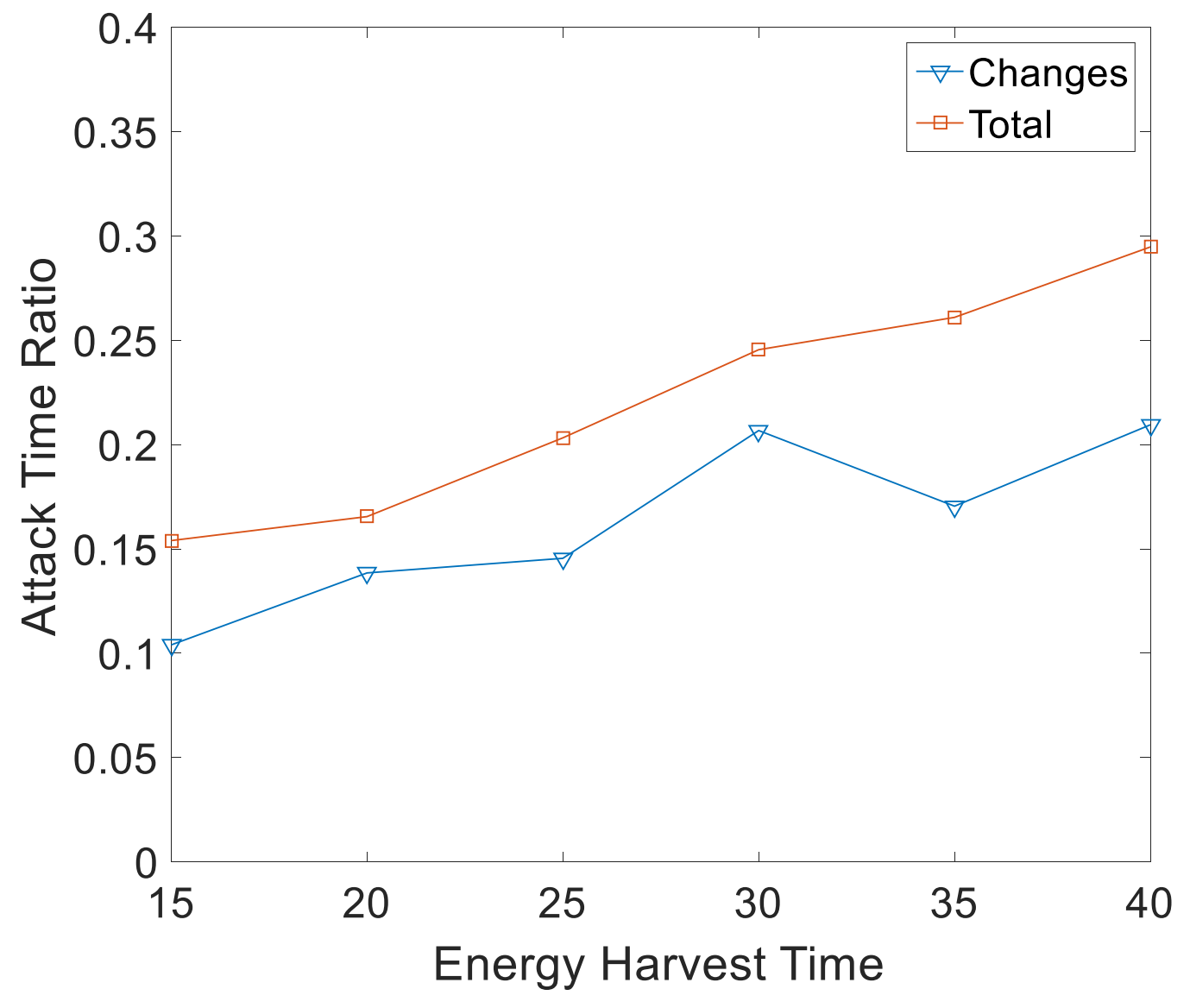
Camouflage-based Active Detection (CAM)

❑ **Basic Idea**

- ➢ Each node *actively* disguises itself as an energy harvesting node on purpose and pretends not to overhear, and then monitor any forwarding operation of its adjacent nodes to detect a lurking deep malicious node
- ➢ A snapshot of the proposed CAM scheme

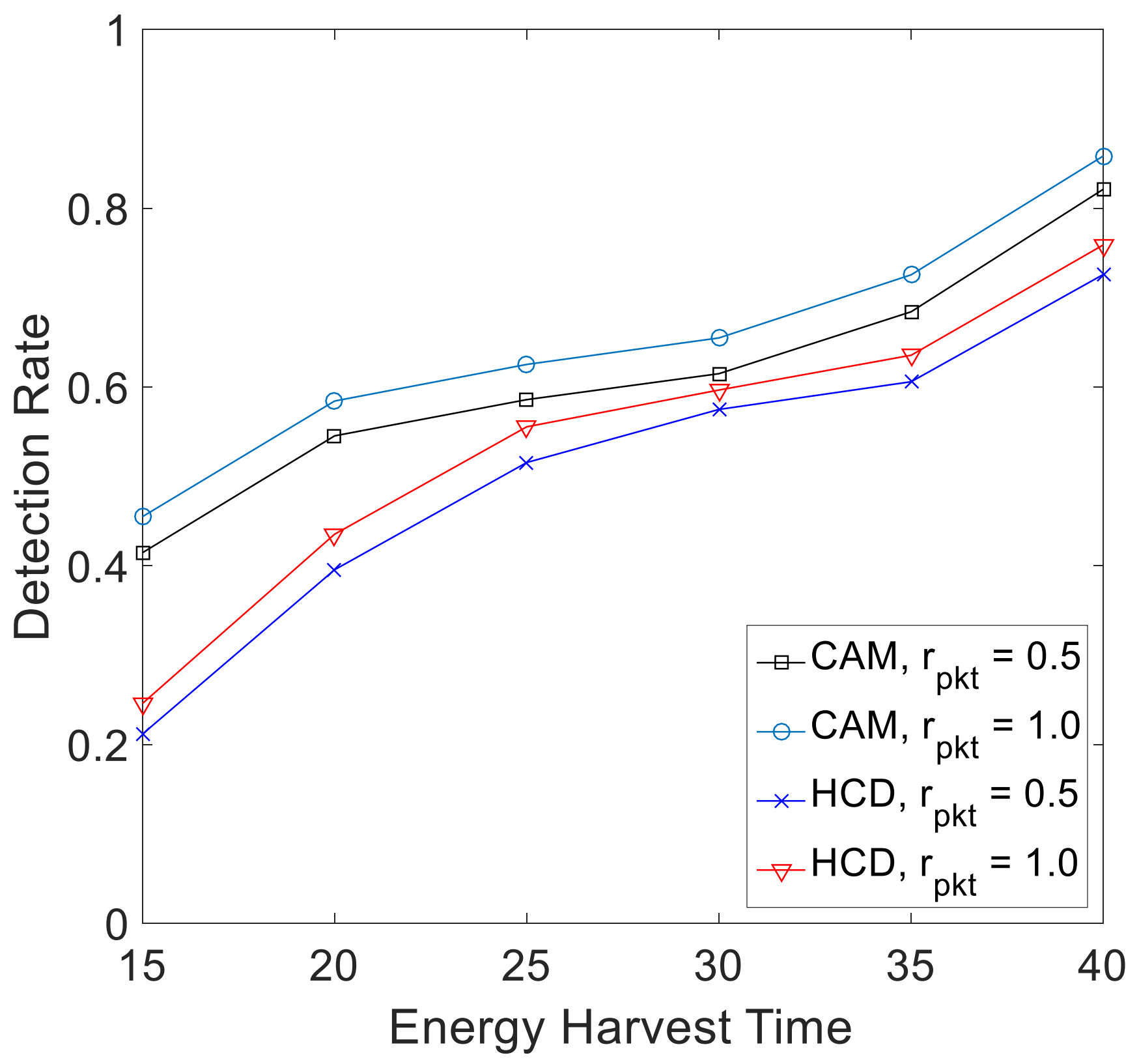


- ➢ Changes of Attack Time Ratio

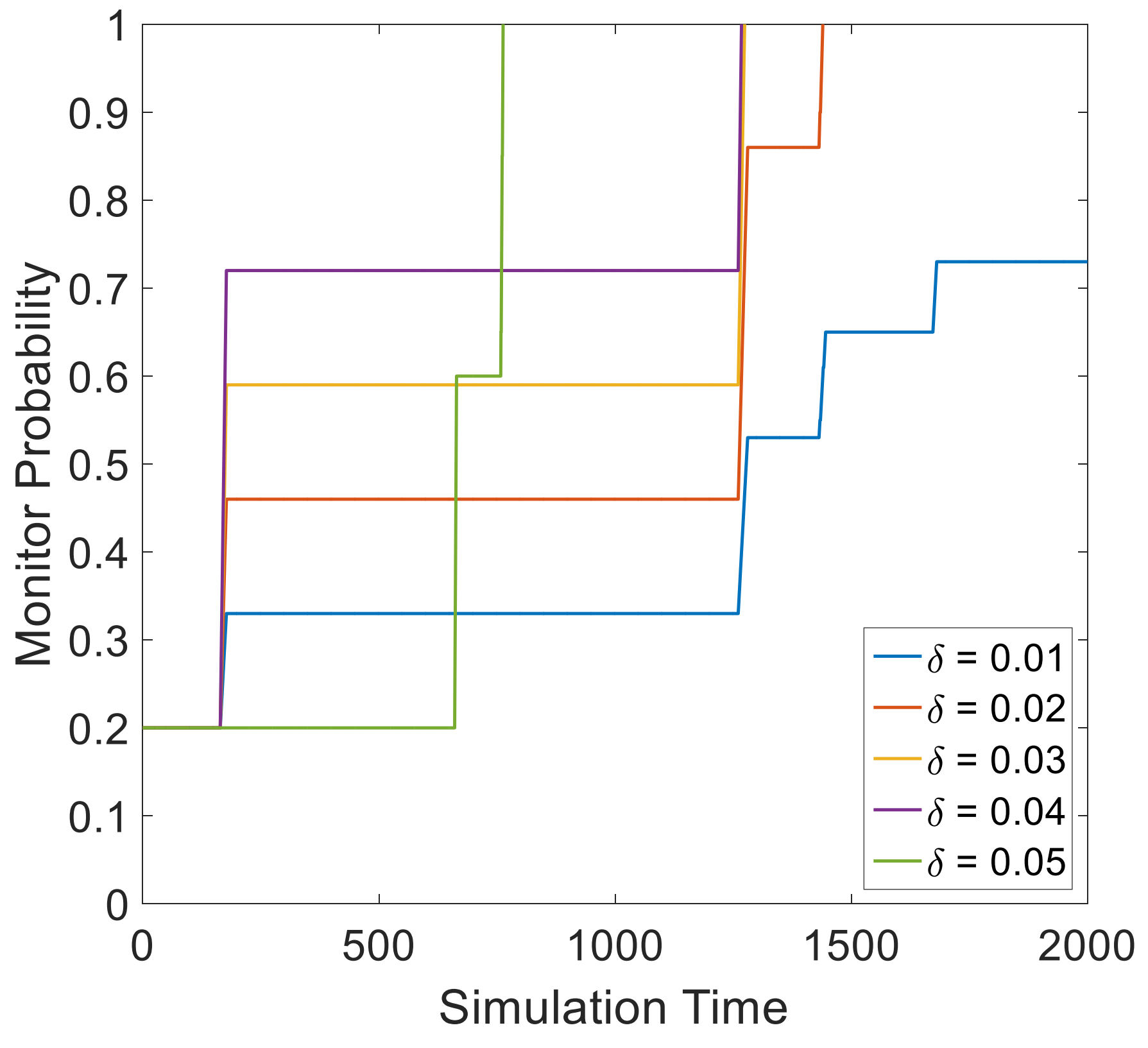


Performance Evaluation

❑ **Detection Rate**



❑ **Monitor Probability**



Concluding Remarks

The proposed countermeasure achieves better performance in terms of detection rate and detection latency compared to the existing hop-by-hop cooperative detection scheme, and suggest a new approach to detect lurk deep malicious nodes in EHNets.

References

❑ **Cong Pu**, and Sunho Lim. "Spy vs. Spy: Camouflage-based Active Detection in Energy Harvesting Motivated Networks." In *Military Communications Conference, MILCOM 2015-2015 IEEE*, pp. 903-908. IEEE, 2015.

❑ **Cong Pu**, and Sunho Lim. “A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation." IEEE Systems Journal (IF: 1.98).To Appear, 2016.

❑ **Cong Pu**, Tejaswi Gade, Sunho Lim, Manki Min, and Wei Wang. "Light-Weight Forwarding Protocols in Energy Harvesting Wireless Sensor Networks." In *Military Communications Conference (MILCOM), 2014 IEEE*, pp. 1053-1059. IEEE, 2014.