MARSHALL
COMPUTER SCIENCE

Combating Energy Depletion Attack: A Misbehavior-Aware Countermeasure in the Internet of Things

Bryan Groves Advisor: Dr. Cong Pu
Weisberg Division of Computer Science, Marshall University

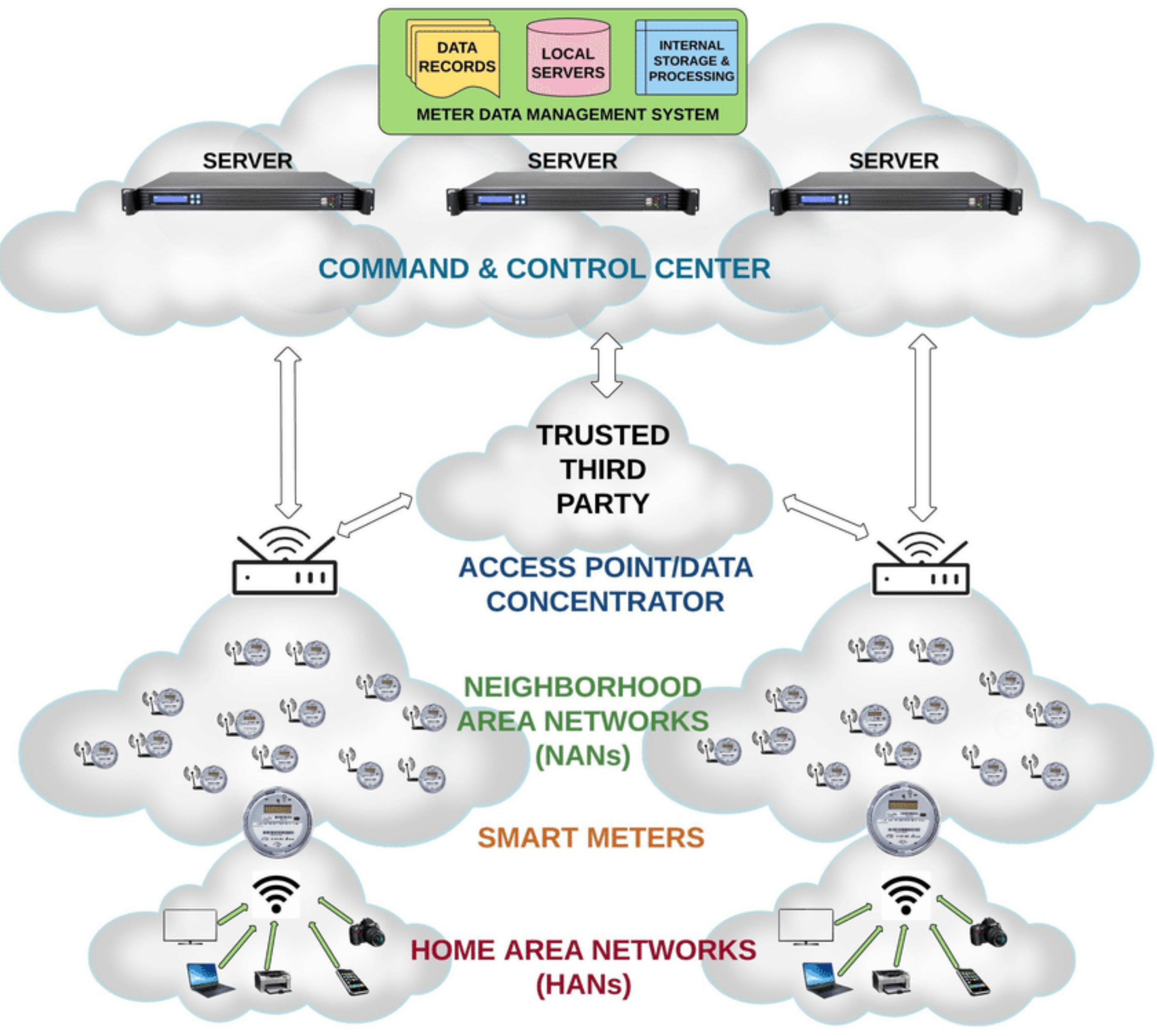
NASA WEST VIRGINIA SPACE GRANT CONSORTIUM

Abstract

With increasingly popular computing devices endowed with sensing and communicating capabilities, Low Power and Lossy Networks (LLNs) are rapidly emerging as an important part of ubiquitous computing and communication infrastructure. Due to the shared wireless medium, the lack of physical protection, and instinctive resource constraints, RPL-based LLNs are vulnerable to various Denial-of-Service (DoS) attacks. In this project, we propose a Misbehavior-Aware Detection (MAD) scheme against energy depletion attack in RPL-based LLNs.

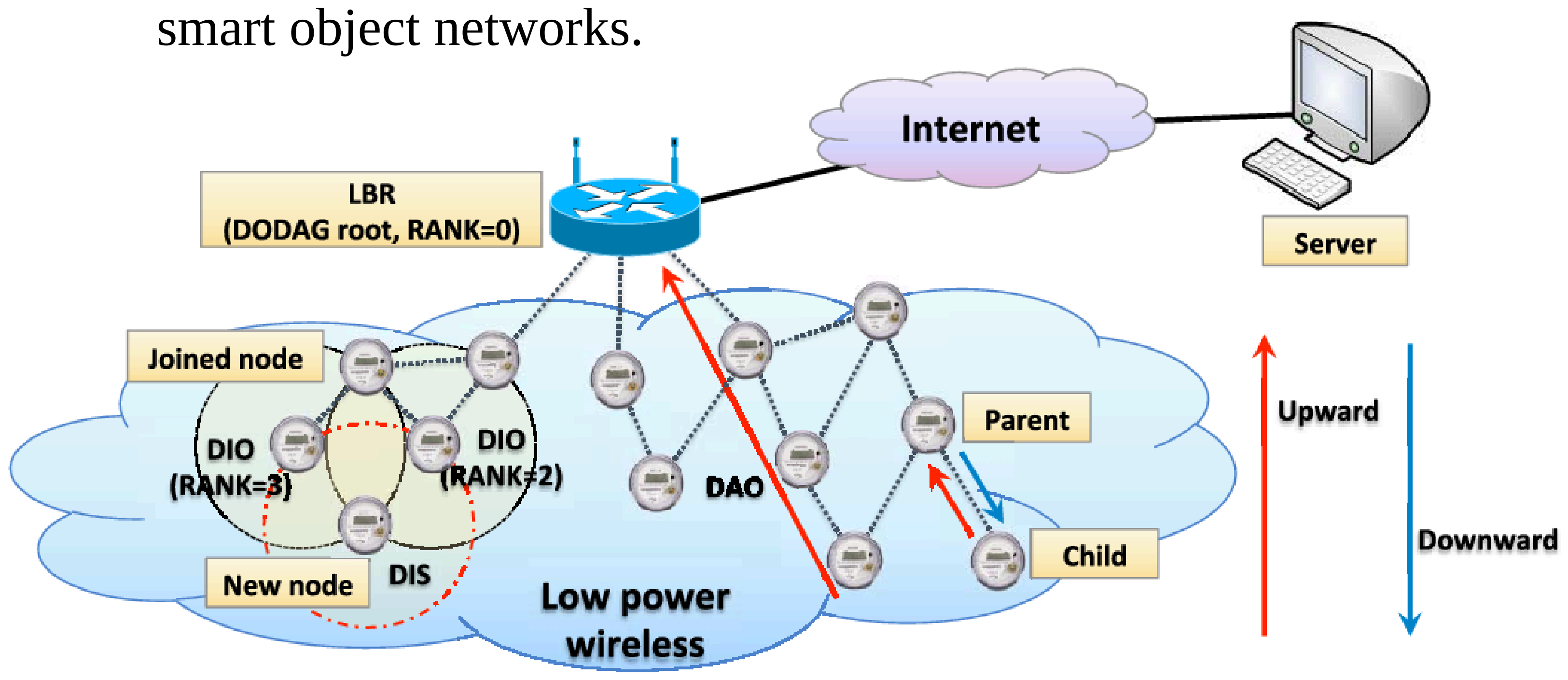
Introduction

- ❑ A rapidly growing pervasiveness and ubiquity of small and cheap computing devices (later nodes) endowed with sensing and communicating capabilities is leading the emergence of Internet-of-Things (IoT), and paving the way to the realization of IoT applications.
  - ❖ The number of wireless connected devices for IoT applications will rise to **50 billion** by the end of 2020.
  - ❖ Global spending on the IoT will also rise to **$1.7 trillion** by 2020.
- ❑ As a major building block of IoT, Low Power and Lossy Network (LLN) comprised of thousands of embedded networking devices employs the open and standardized IPv6-based architecture to connect with the larger Internet.

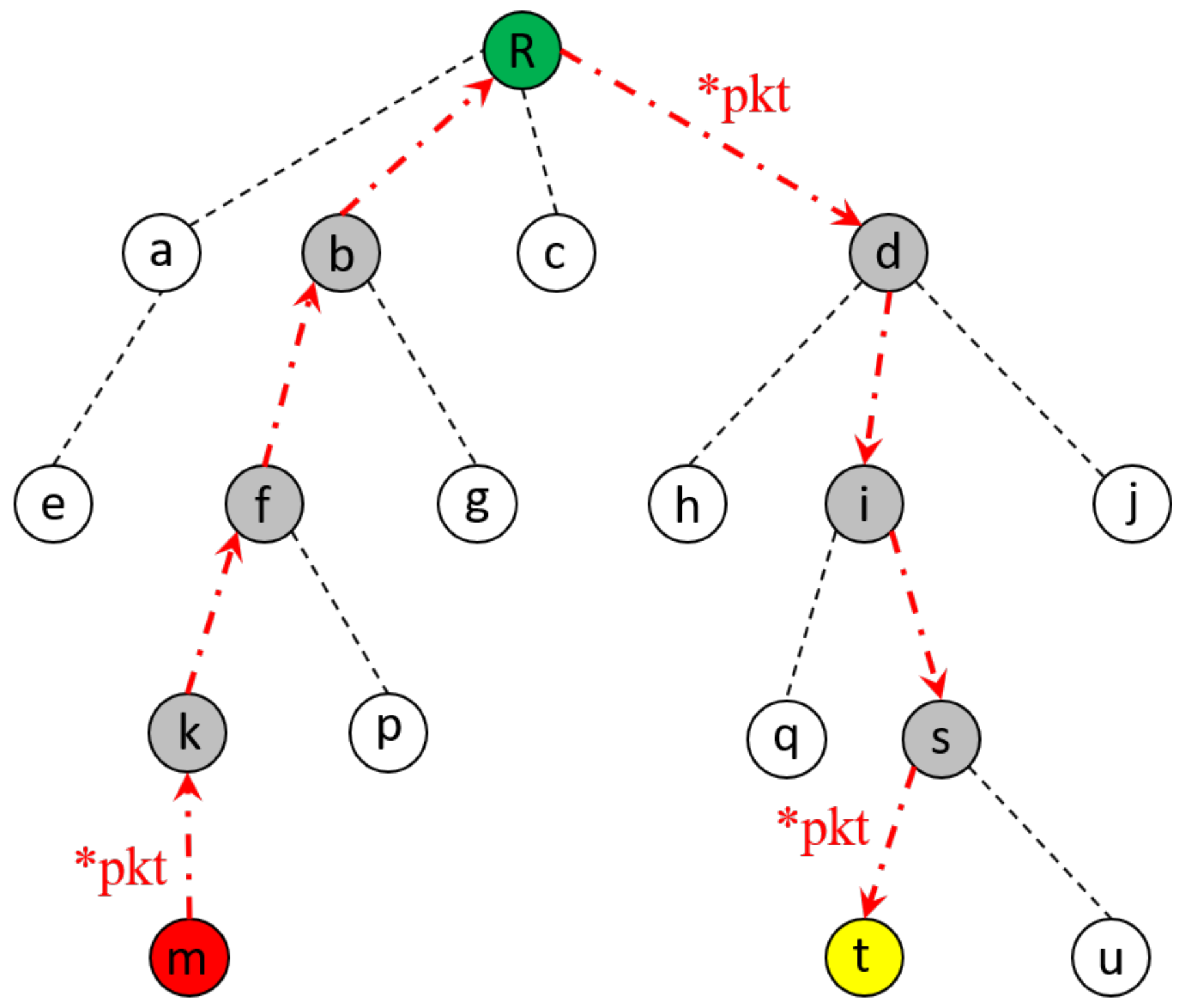

DATA RECORDS
LOCAL SERVERS
INTERNAL STORAGE & PROCESSING
METER DATA MANAGEMENT SYSTEM
SERVER
SERVER
SERVER
COMMAND & CONTROL CENTER
TRUSTED THIRD PARTY
ACCESS POINT/DATA CONCENTRATOR
NEIGHBORHOOD AREA NETWORKS (NANs)
SMART METERS
HOME AREA NETWORKS (HANs)

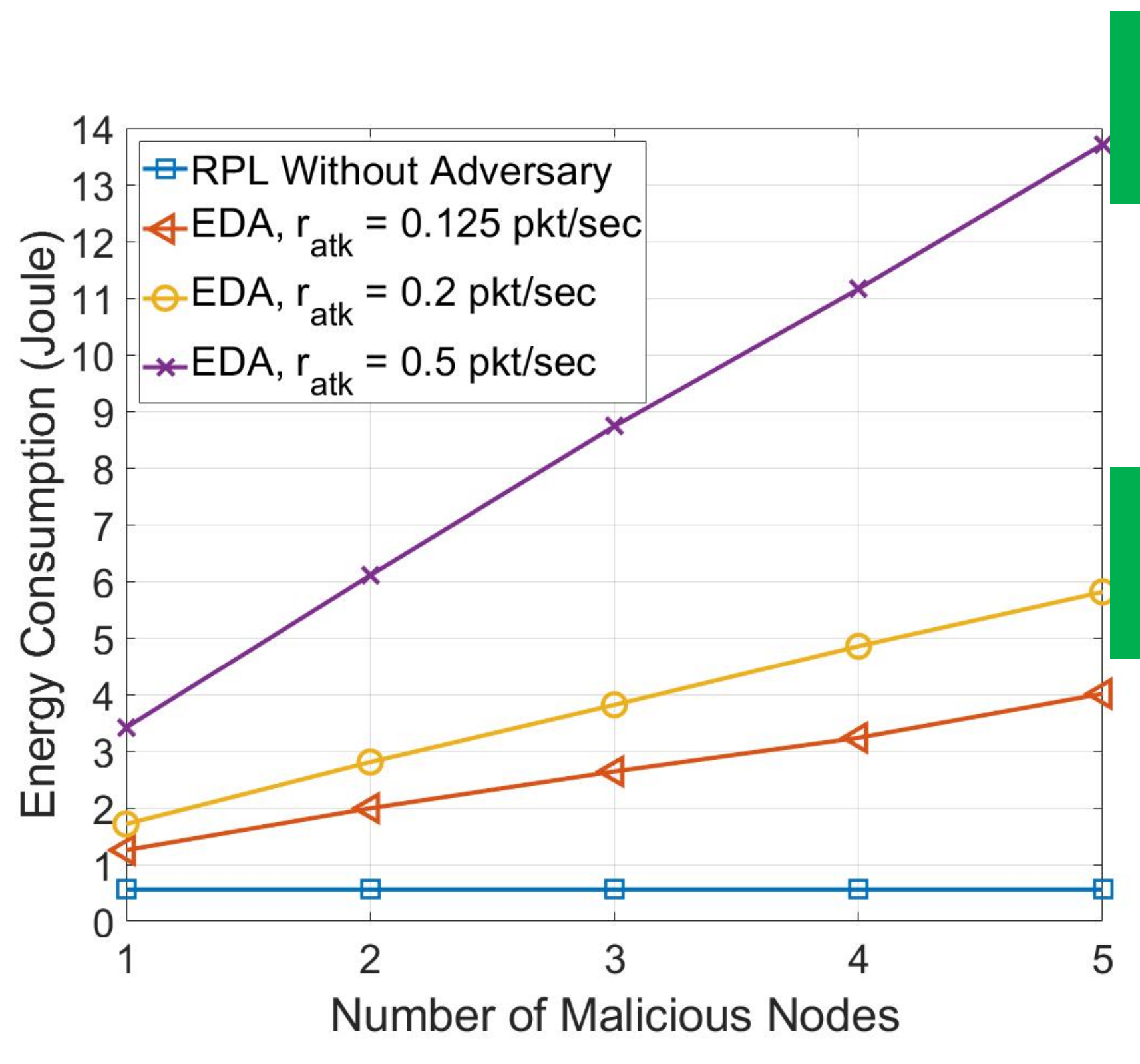
Research Motivation

- ❑ RPL Routing Protocol
  - ❖ Provides both efficient and reliable communication for IP smart object networks.



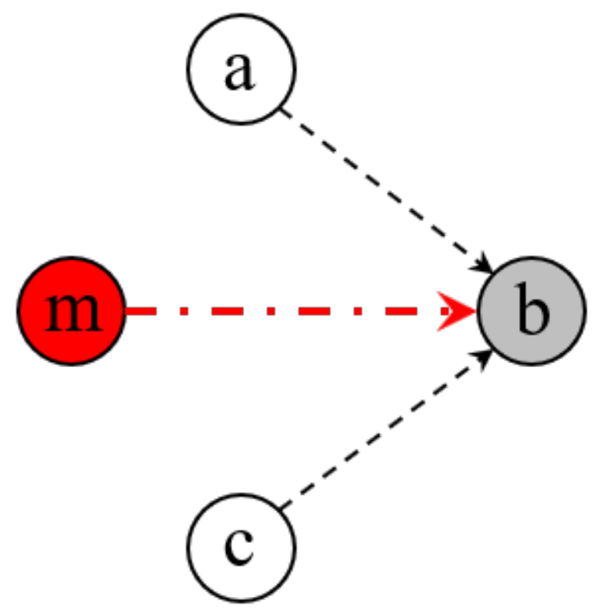
- ❑ RPL-based LLNs are vulnerable to various **Denial-of-Service (DoS) Attacks** that primarily target service availability.
  - ❖ Lack of physical protection.
    - ➢ Nodes can be easily captured, tampered, or destroyed.
  - ❖ Open nature of shared wireless medium.
    - ➢ Adversary can overhear, duplicate, corrupt, or alter data.
  - ❖ RPL is not originally designed to consider the security requirements for DoS attacks.
    - ➢ Security mechanism greatly affects the performance of resource-constrained devices.
- ❑ In **energy depletion attack**, a malicious node
  - ❖ intentionally generates and sends a large number of packets to legitimate node to excessively consume the energy resource of intermediate nodes located along the forwarding path,
  - ❖ finally causes denial of service in resource-constrained networks.





Countermeasure

- ❑ **Misbehavior-Aware Detection**
  - ❖ Each node maintains a count of the number of received packets from its one-hop neighbor node within a specific time window, and then compares the count with a dynamically calculated threshold to detect potential malicious node.
    - ➢ Each node maintains an Observation Table (OT) to record the number of received packets from each neighbor node during an observation window (ω).
    - ➢ Each node also maintains a Detection Table (DT) to record the number of detected forwarding misbehaviors of each neighbor node.
    - ➢ At the end of each observation window, each node examines Observation Table (OT) and Detection Table (DT), and calculates a threshold value as the reasonable number of received packets from neighbor node within observation window.
    - ➢ When the number of detected forwarding misbehaviors of suspected node reaches a threshold (φ), the detecting node broadcasts an *Isolate* packet to its one-hop neighbor nodes to prevent them from receiving or accepting any packet from the suspected malicious node.
  - ❖ A snapshot of network



Observation Table (OT)

nid	***rp***	***ts***
a	5	t_{cur}
m	15	t_{cur}
c	4	t_{cur}

$$T_{pkt} = \frac{\sum_{i=nid}^{G} wt_i \cdot rp_i}{|G|}.$$

$$wt_i = 1 - \frac{c_{mis}^{i}}{\sum_{j=nid}^{G} c_{mis}^{j}}.$$

$$T_{pkt} = \frac{\sum_{i=nid}^{G} \left(1 - \frac{c_{mis}^{i}}{\sum_{j=nid}^{G} c_{mis}^{j}}\right) \cdot rp_i}{|G|}.$$

Experimental Environment

Contiki
The Open Source OS for the Internet of Things

MATLAB

Acknowledgement

❑ This research was supported by NASA West Virginia Space Grant Consortium, Training Grant #NNX15AI01H, and Marshall University Undergraduate Creative Discovery Scholar and Undergraduate Research Scholar Award.