# Morisita Index-Based Countermeasure against Sybil Attack in the Internet of Things

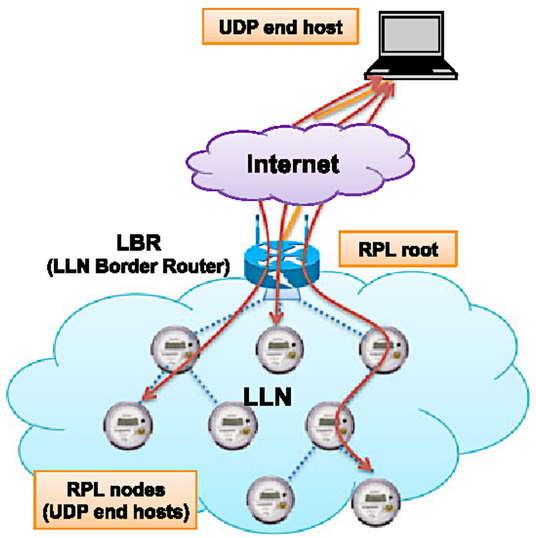

**Jacob Gressang**
**Advisor: Dr. Cong Pu**
**Weisberg Division of Computer Science, Marshall University**


## Abstract


With a rapidly growing number of physical objects being connected to the internet, the concept and applications of the Internet-of-Things (IoT) is coming to fruition in which a myriad of multi-scale sensors and devices are being seamlessly blended and communicate with each other. As a part of the emerging IoT technology, Low Power and Lossy Networks (LLNs) are being developed and defined in their functionality as a set of resource-constrained nodes with limitations in processing power, energy capacity, and available memory. From these limitations and the lack of security requirements / physical protection within RPL, the Routing Protocol for LLNs, lie Denial-of-Service attack vulnerabilities. Through investigating RPL and a DoS attack, called a sybil attack, it is clear that a statistical Morisita index-based countermeasure needs to be implemented to mitigate the sybil attack in RPL-based LLNs.

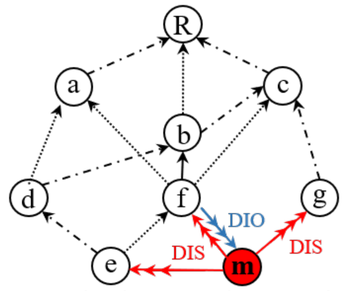

## Introduction

- Internet-of-Things (IoT) and its applications are rapidly proliferating, where a myriad of multi-scale sensors and devices are seamlessly blended
  - 20.4 billion wirelessly connected devices will be available for IoT applications by 2020
  - Annual economic impact caused by the IoT is to be in range of $2.7 trillion and $6.2 trillion by 2025
- With the increasing demand for resource-constrained nodes to be connected to Internet
  - Routing protocol for low power and lossy networks, referred to as RPL, has been standardized

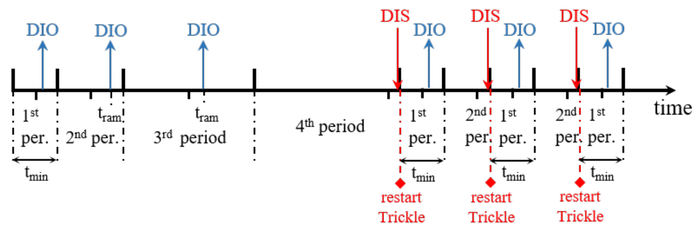



## Research Motivation

- 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.
- Denial-of-Service (DoS) attack: Sybil Attack
  - The malicious node multicasts a large number of DODAG Information Solicitation (DIS) messages with different fictitious identities
  - cause the legitimate nodes to restart the Trickle algorithm and broadcast an excessive number of DODAG Information Object (DIO) messages
  - drain down the energy resource of legitimate nodes, and finally causes the legitimate nodes to suffer from denial of service




*A snapshot of the network, where a malicious node $n_m$ multicasts the DIS message to probe for the DIO messages from adjacent nodes.*

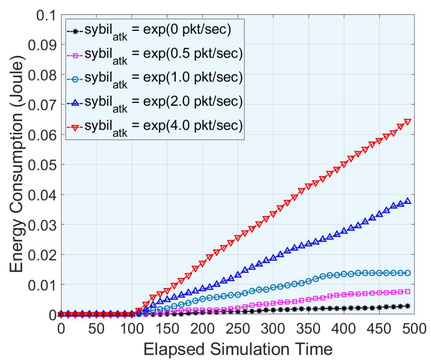


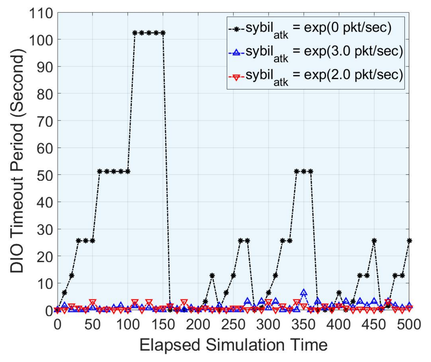

## Countermeasure

- **Morisita Index-Based Countermeasure**
  - **What is Morisita index??**
    - The Morisita index is a common method for analyzing spatial patterns
    - It is a statistical measure of dispersion based on the spatial Poisson process
  - **The characteristics of Morisita index**
    - When the MAC address ranges are equally distributed among all N classes, the Morisita index will reach or surpass the maximum value of 1.
    - When the MAC address ranges are distributed in clusters among all N classes, the Morisita index will remain closer to the minimum value of 0.
  - **Basic idea of countermeasure:**
    - Measure the dispersity of the identities in the received DIS messages to detect whether there is a sybil attack based on the Morisita index-based theory
    - If so, trigger the attack mitigation process to eliminate sybil attack
  - **Formula:**

$$C_D = \frac{2\sum_{i=1}^{S} x_i y_i}{(D_x + D_y)XY}$$

  - **Preliminary Results:**




## Acknowledgement


- This research was supported by NASA West Virginia Space Grant Consortium, Training Grant # NNX15AI01H