Mitigating Spam DODAG Information Solicitation Attack in Low Power and Lossy Networks

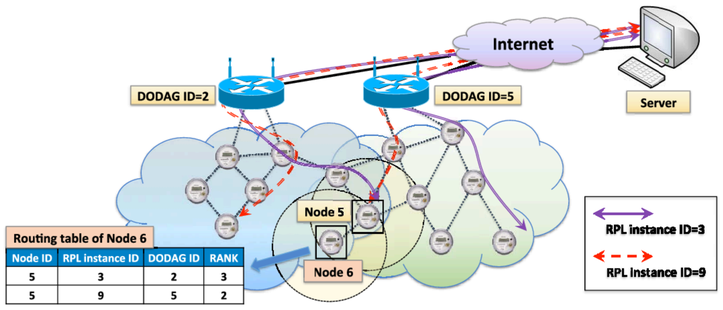
Bryan Groves **Advisor: Dr. Cong Pu**
Weisberg Division of Computer Science, Marshall University

Abstract

As a major building block of IoT, Low Power and Lossy Network (LLN) that consists of a set of resource-constrained nodes in terms of communication, computation, memory, and energy plays an essential role in the realization of ubiquitous computing and communication paradigm. In spam DIS attack, a malicious node multicasts a large number of DODAG Information Solicitation (DIS) messages with different fictitious identities to cause the legitimate nodes to restart the Trickle algorithm and broadcast an excessive number of DODAG Information Object (DIO) messages, which drain down the energy resource of legitimate nodes, and finally make the legitimate nodes suffer from denial of service.

Introduction

- Routing Protocol for Low Power and Lossy Network (RPL) is a novel approach to provide efficient and reliable communication for IP smart object networks.
- RPL forms a Destination Oriented Directed Acyclic Graph (DODAG) with the root being the access point.



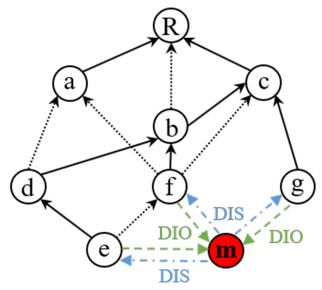
Routing table of Node 6

Node ID	RPL instance ID	DODAG ID	RANK
5	3	2	3
5	9	5	2

- RPL-based LLNs are vulnerable to various Denial-of-Service (DoS) Attacks.
  - 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 sensory data.
  - RPL is not originally designed to consider the security requirements for DoS attacks.
    - Security mechanism greatly affects the performance of resource-constrained devices.

Spam DIS Attack

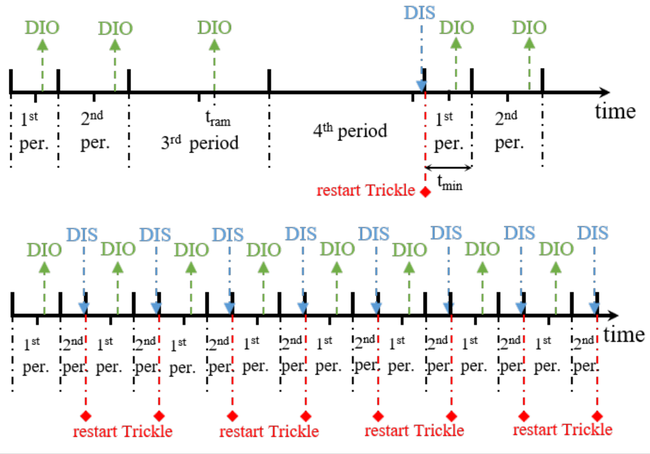
- **In Spam DIS attack**, the malicious node multicasts a large number of DODAG Information Solicitation (DIS) messages with different fictitious identities.
  - Primarily targets the vulnerability of DIO transmission mechanism in RPL by violating an implicit assumption.
- Legitimate nodes restart the Trickle algorithm and broadcast an excessive number of DODAG Information Object (DIO) messages.
  - Legitimate nodes drain resources by broadcasting messages.
  - Legitimate nodes are unable to communicate and suffer from denial of service.



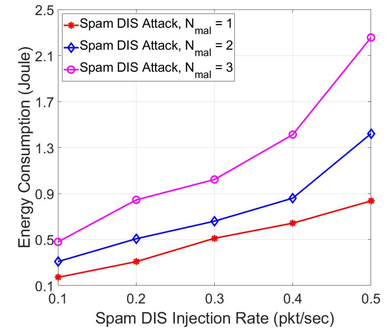
A snapshot of the network, where a malicious node n_m multicasts the DIS message to probe for the DIO messages from adjacent nodes.

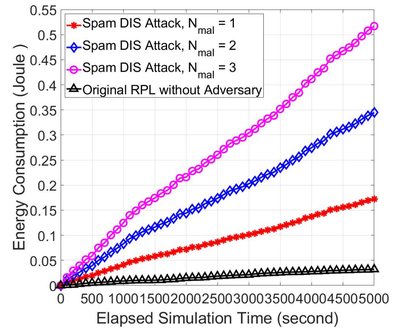
Trickle Algorithm

- A density aware local communication primitive with an underlying consistency model to guide the message transmissions.
- The emission rate of DIO messages is dynamically adjusted according to the stability of routing information.

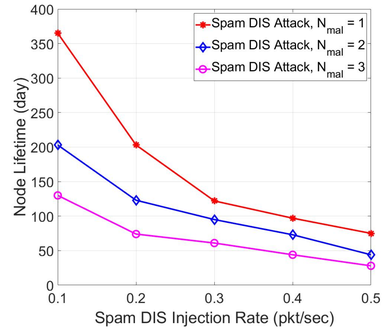


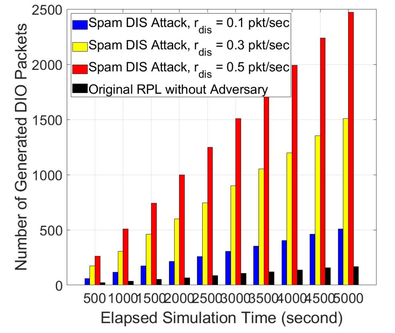
Experimental Study





The performance of energy consumption against spam DIS message injection rate and elapsed simulation time.





The performance of node lifetime and number of generated DIO packets against spam DIS message injection rate and elapsed simulation time.

Future Work

- Develop a monitor-based detection scheme to efficiently mitigate the spam DIS attack.
- Conduct extensive simulation experiments through Contiki Cooja and OMNET++ to evaluate the performance of the proposed scheme.

Contiki — The Open Source OS for the Internet of Things

OMNeT++ INET FRAMEWORK

Acknowledgement

This research is supported by 2019 NASA West Virginia Space Grant Undergraduate Fellowship Program.