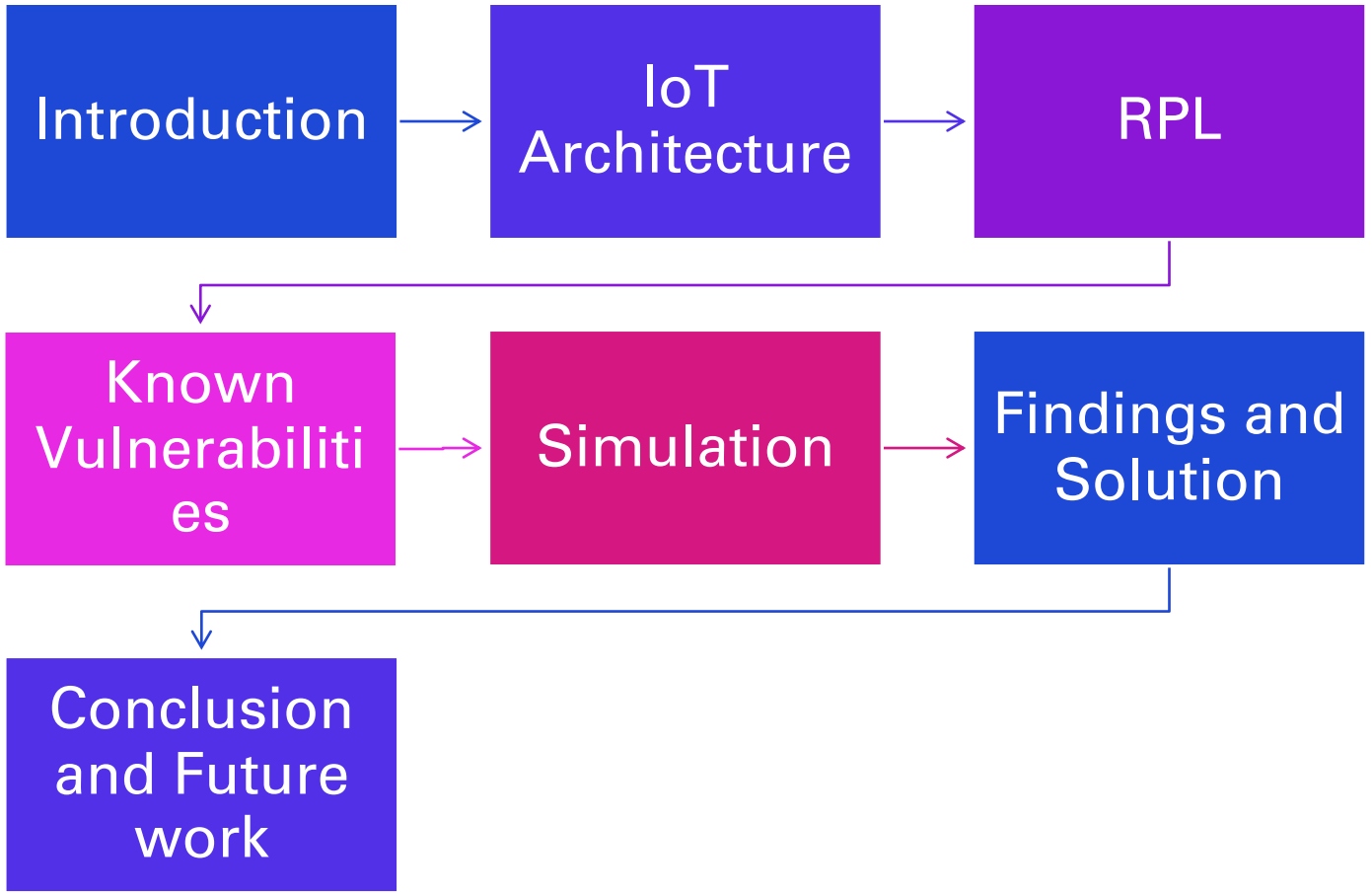
Investigation of security weakness and vulnerability in IoT routing protocol and solution

SHENGLI YUAN, PH.D
IEEE SENIOR MEMBER
PROFESSOR, COMPUTER SCIENCE
UNIVERSITY OF HOUSTON-DOWNTOWN

TOOBA HASHMI
BS. COMPUTER SCIENCE
UNIVERSITY OF HOUSTON- DOWNTOWN

AGENDA


Introduction
IoT Architecture
RPL
Known Vulnerabilities
Simulation
Findings and Solution
Conclusion and Future work

Abstract

As an emerging technology, internet of things is rapidly revolutionizing the global communication network with billions of new devices deployed and connected with each other. Compared to traditional internet, IoT networks often operate in harsh environment that causes frequent traffic loss and delays; and IoT devices are often severally constrained in computational power, network bandwidth, and power supply. It is therefore imperative for IoT network to establish and maintain reliable and secure network connection. In this study, we focus our effort on RPL - routing protocol for low power and lossy networks, a dominate routing protocol designed by IEEE and IETF. We investigate new weakness and vulnerability in this protocol, especially in large and dense iot network, and develop mitigation solutions.

Introduction

- In 2015, IoT connected 4.9 billion things and will connect 25 billion things by 2020 (Gartner). Because it is an expansive and extensive network, the objects connected to it are susceptible to various security exploitations.
- As a safeguard against these attacks and exploitation, it is important to remember the various components of cyber security and protocol measures. Routing Protocol for Low Power and Lossy Networks (RPL), is standardized for routing in WSNs and IoT device Networks (Mangelkar, Dhage, & Nimkar, 2017).
- In this research project, we focused our effort on researching the protocol and the vulnerabilities within it and hope to further this research on alternative routing protocols.

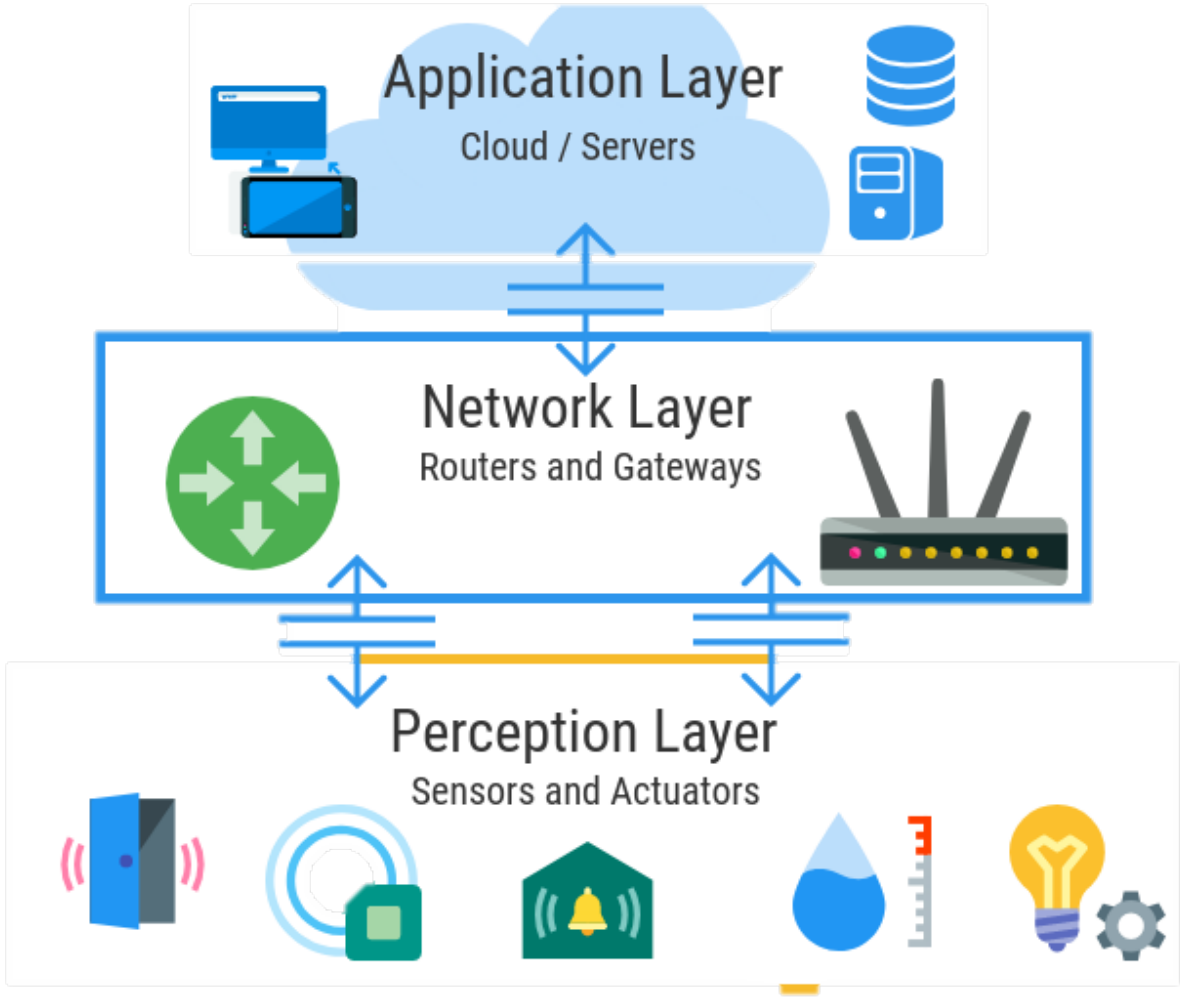
Common IoT Applications

Smart Grids promise to use information about the behaviors of electricity suppliers and consumers in an automated fashion to improve the efficiency, reliability, and economics of electricity.

Smart City refers to making a city more efficient by using IoT devices to solve complex problems particular to the city like water management, waste control, and emergencies.

Wearables such as Apple smart watches and Myso gesture control. These have the capability to also read your heartbeat and track steps, connect to eHealth applications.

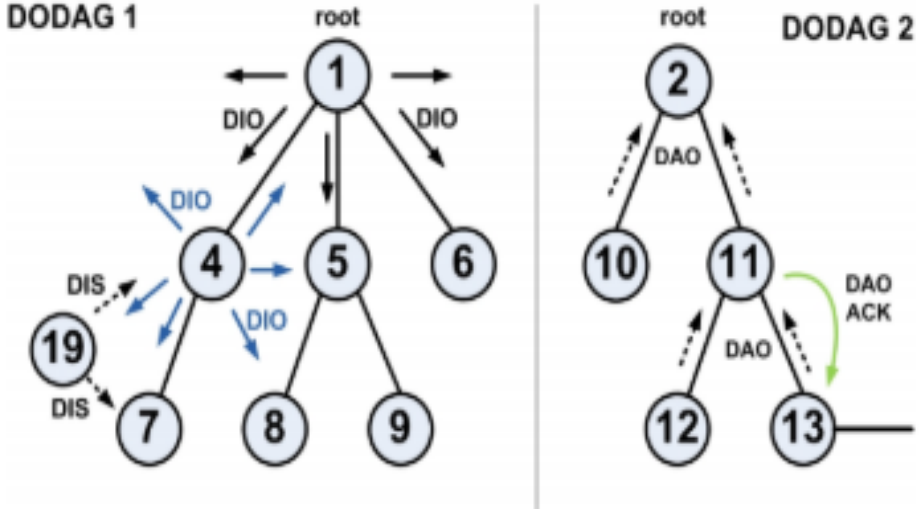
E-Health or connected health applications offer a means of mass data collection and pave the way for smart medical devices.



IoT Architecture

RPL: Routing protocol for low power and lossy networks

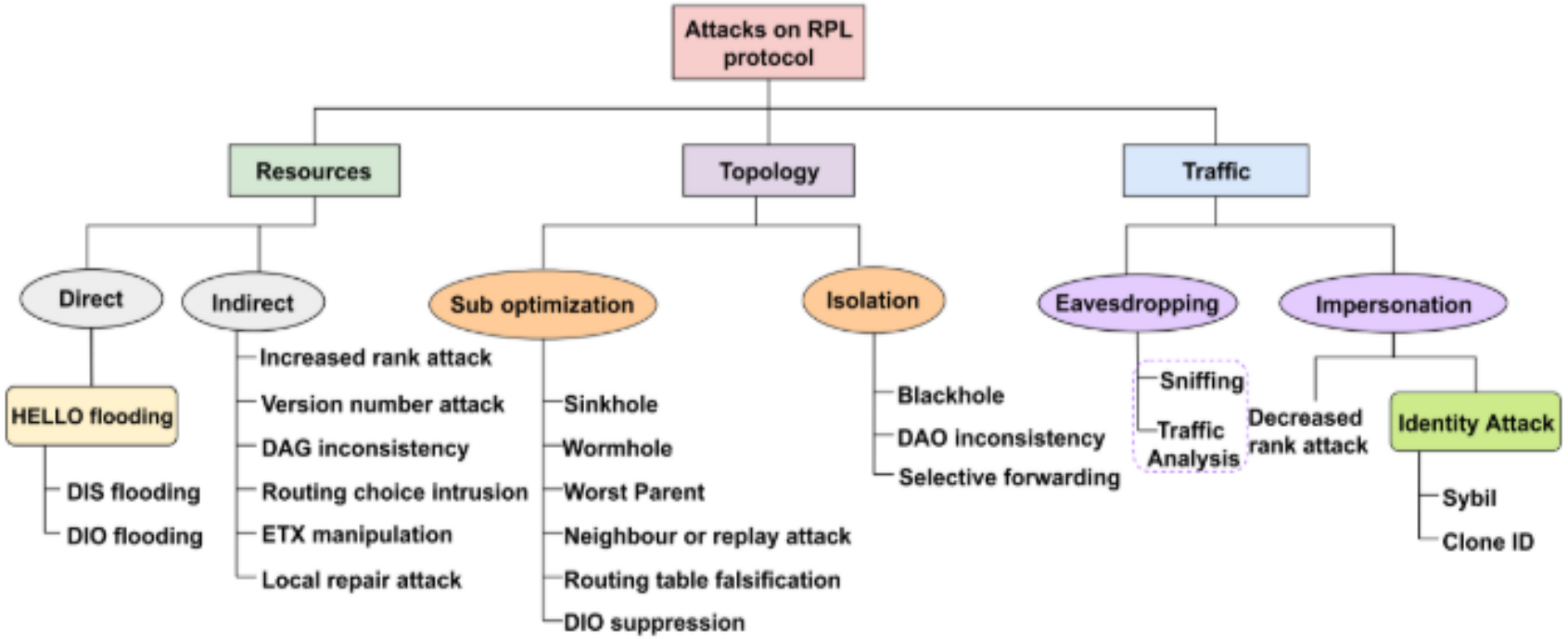
- In RPL, the IoT devices are interconnected using mesh and tree topology to build a destination oriented directed acyclic graph (DAG).
- The DAG characterizes a tree-like structure that indicates the default routes between nodes in the LLN. In the DAG, a node may associate to multiple parent nodes. The destinations nodes, known as sinks, provide routes to the Internet and as the roots of the DAGs.
- RPL enabled networks have the prospective data rate is low and communication is prone to high error.



Constraints

- Internal memory constraint
  - Unable to run sophisticated operating system, algorithms, and protocols.
- Computational capability constraint
  - Unable to support complex routing algorithms and encryptions
- Power constraint
  - Energy consumption is one of the most important areas related to improving the RPL.
  - Energy consumption in RPL is handled by a trickle timer. However, the trickle timer is ineffective in dynamic environments, often resulting in high energy loss and failed packet delivery.

Known Vulnerabilities and Attacks



Vulnerabilities and Attacks Examples

- During a sybil attack, malevolent nodes can falsely cast messages with different and fake ids to cause working nodes to also transmit and pass on illicit messages. This malicious node spoofing will take up memory space and present nodes to be fully connected.
- Another example of vulnerability has to do with interdependence. IoT devices can implicitly be controlled by conflicting rules and behaviors. For example, if a smart thermometer detects over heating, it can act by opening windows of the house. However, it does not take into consideration the risk on security.
- A large system or device can be compromised via outside interference because lightweight IoT devices do not have the memory management unit for complicated encryption methods.

Problem Statement

We liked to find out, especially for large and dense IoT networks:

- How RPL tree converges while the network density and size increase with difference internal memory sizes?
- How different the power consumptions of the nodes in the network are?

Simulation

Contiki is an operating system with a focus on low power IoT devices. Cooja allows the large and small networks of Contiki motes to be simulated.

For the project, Z-motes were used. One as a sink and the others as sender nodes.

Experiments over the course of 5, 10, 15, 20, 25, 30 motes and the energy consumption were evaluated.

Findings

- The constraints on the internal memory allocated for the routers' routing table and the neighboring table have a significant impact on RPL tree's ability to converge.
- The CPU power consumption is significantly higher in the nodes with many descendant nodes than the nodes with less or no descendant nodes.

Findings - storing mode

- Once the network density becomes high enough, a router may exhaust its memory for the neighboring table
- Router stops adding additional neighbor nodes to the RPL tree, nor forwarding information of additional neighbors to the root, thus causing the RPL tree incomplete and nodes disconnected from the tree

Findings - storing mode

- If the network density is not high, but the network size becomes high enough, a router may not exhaust its memory in the neighboring table.
- But the number of its descendant nodes may still become high enough to exhaust its memory in the routing table
- Router stops adding additional descendant nodes to the RPL tree, nor forwarding information of additional nodes to the root, causing the RPL tree incomplete and nodes disconnected from the tree.

Findings – non-storing mode

- Memory constraints on the neighboring table and routing table do not influence the RPL tree's ability to converge.
- Relay on source routing

Preliminary sample data

Memory capacity	3 max entries in neighboring and routing table	5 max entries in neighboring and routing table	7 max entries in neighboring and routing table	10 max entries in neighboring and routing table
Final number of nodes in RPL tree	0/35	6/35	32/35	35/35

Table 1. Network with 1 sink node and 35 sender nodes. All in storing mode

Preliminary sample data

1 sink 10 senders	1 sink 20 senders	1 sink 30 senders	1 sink 40 senders
3.2	3.4	3.9	4.3

Table 2. CPU power consumption ratios between the non-RPL-root node with the most descendants and the one with the least descendant. All senders are in storing mode.

Preliminary sample data

1 sink 10 senders	1 sink 20 senders	1 sink 30 senders	1 sink 40 senders
3.0	3.4	4.9	16.9

Table 3. CPU power consumption ratios between the non-RPL-root node with the most descendants and the one with the least descendant. All senders in non-storing mode.

Security Vulnerabilities on Availability

- When the IoT devices are in storing mode by default, the constraints on their internal memory may severely hinder the RPL tree's ability to converge in a large or dense network, even without any attacks.
- A malicious node capable of spoofing MAC and IP addresses can easily exhaust the neighboring table and the routing table on some nodes, causing part of the network disconnected. The damage is more severe if the malicious node is deployed near the nodes close to the root.
- The RPL tree structure cause much higher power consumptions on the nodes with more descendant nodes in the RPL tree, which is more so when the nodes are in non-storing mode. Once the power is depleted on some nodes, the network becomes disconnected.

Proposed Solutions

- Limit the number of nodes in each tree below the capacity of the neighboring table and the routing table
- The root in each tree serve as a proxy for all the nodes inside the tree, minimizing the need for them communicate with outside world.
- Roots are equipped with much more resources, communicating with advanced routing and security measures.

Conclusion and Future Work

- Constraints on internal memory and power supply create significant security vulnerabilities
- Implement and test our proposed solutions
- Network reliability issues

Acknowledgements

First and foremost, thank Dr. David Nicol for his guidance and insights throughout this project. This project wouldn’t have succeeded without his leadership.

Also thank our student assistant Jaron Mink for his dedication and hard work.

Equally grateful for the supports from Dr. Beth White of ORISE and Ms. Andrea Whitesell of Critical Infrastructure Resilience Institute.