MARSHALL™
COMPUTER SCIENCE

Combating Advanced Vampire Attack: A Theil Index-Based Countermeasure in Internet of Things

Jacqueline Brown Advisor: Dr. Cong Pu
Weisberg Division of Computer Science, Marshall University

NASA WEST VIRGINIA SPACE GRANT CONSORTIUM

Abstract

Internet-of-Things (IoT) and its applications are rapidly increasing, where several of multi-scale sensors and devices are seamlessly blended. A major building block of IoT being IPv6-based Low Power and Lossy Networks (LLNs) which are leading to the further development of IoT applications. However, due to the shared wireless medium, lack of resources, physical protection, and security requirements of RPL protocol, LLNs are particularly vulnerable to Denial-of-Service (DoS) attacks. In this project, we propose a Theil index-based countermeasure to effectively detect and mitigate an advanced vampire attack.

Introduction

❑ The on-going miniaturization of electronic devices and the maturation of wireless communication technologies provide a solid foundation for the emergence and development of Internet of Things (IoT).

- ❖ **20.4** billion wirelessly connected devices will be available for IoT applications by 2020.
- ❖ Annual economic impact caused by IoT is to be in range of **$2.7** trillion and **$6.2** trillion by 2025.

❑ These smart and connected devices can cater to a variety of civilian and military IoT applications such as smart grids, smart transportation, smart cities, and smart homes.

❑ **Problems:**

- ❖ Lack of physical protection
  - ➢ Node can easily be captured, tampered, or destroyed by an adversary.
- ❖ Open nature of wireless communication
  - ➢ An adversary can overhear, duplicate, corrupt, or alter sensory data.

Contribution of Our Work

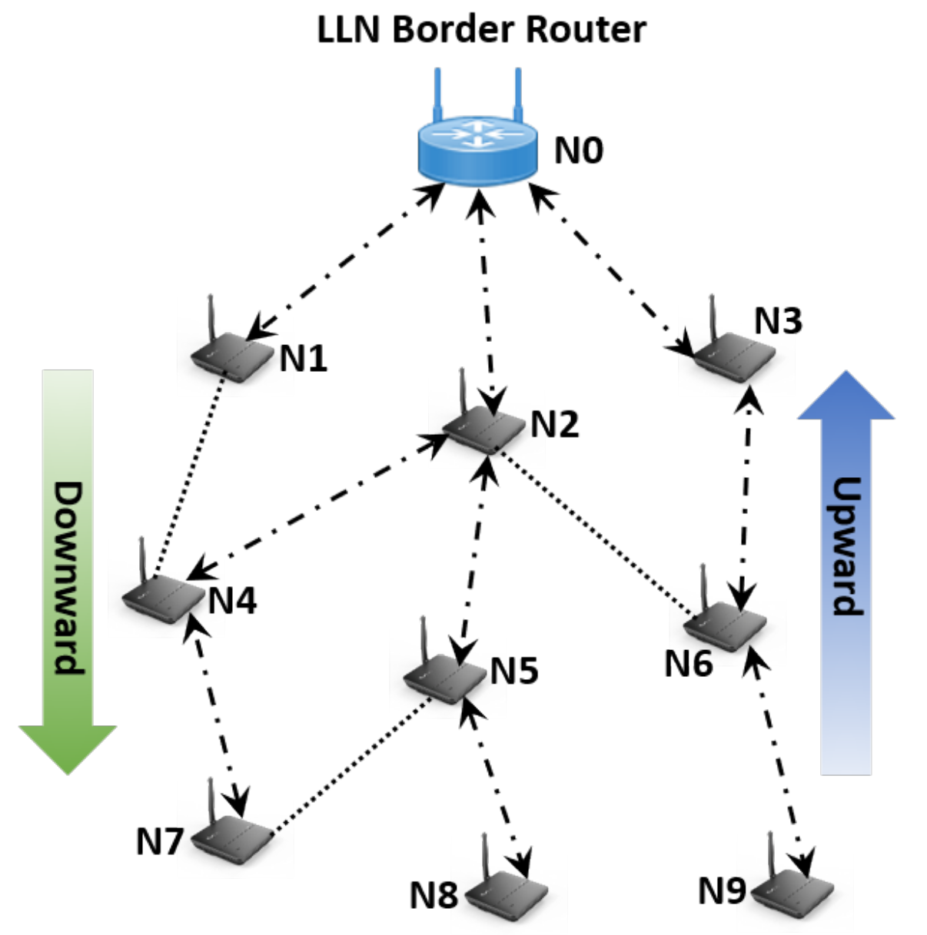
❑ A Theil Index-Based Countermeasure:

- ❖ Each node measures the distribution of destination MAC addresses in the received data packets to detect advanced vampire attack.

Research Motivation

❑ RPL Routing Protocol

- ❖ An IPv6-based proactive distance vector routing protocol designed for low power and lossy networks.

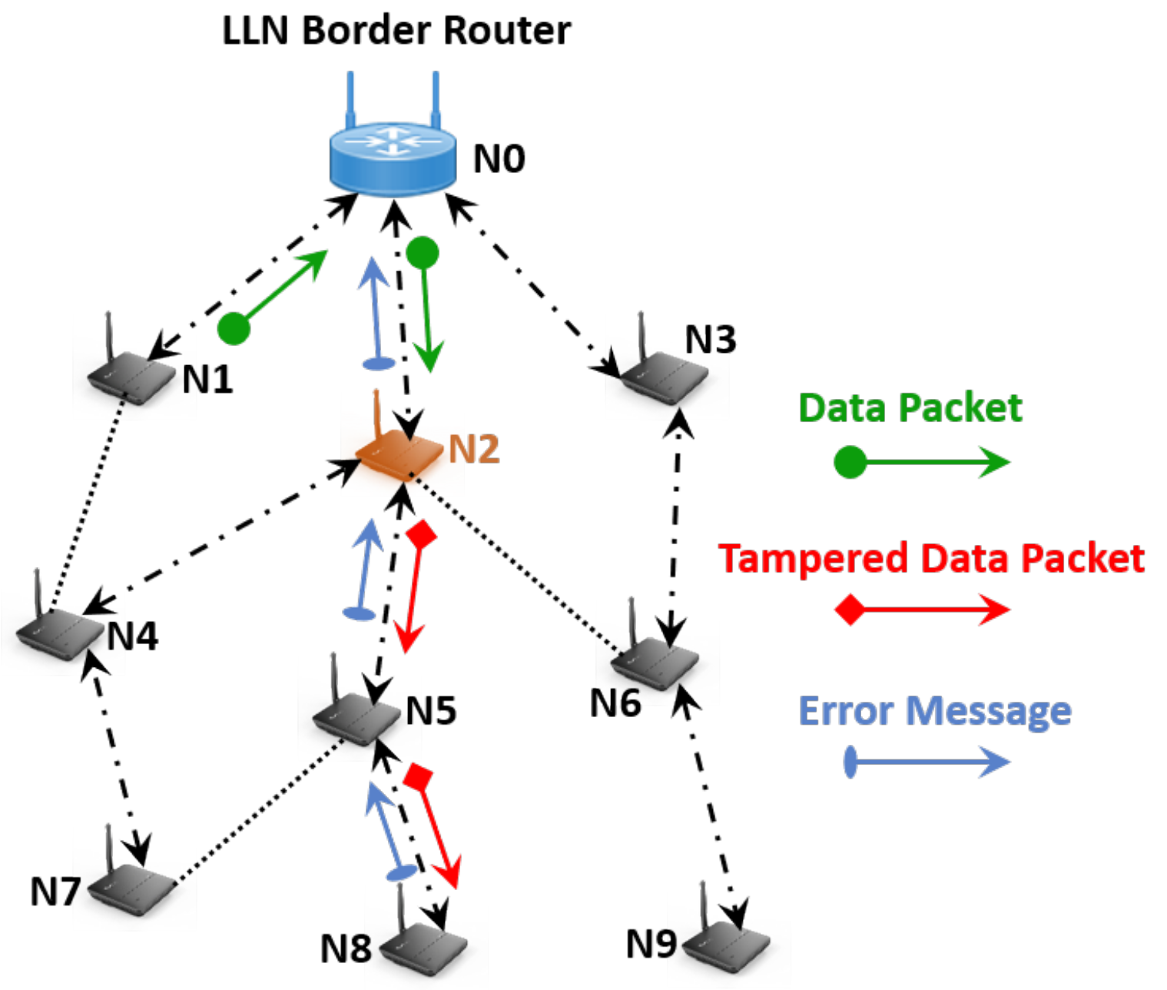


❑ RPL-based LLNs are vulnerable to various **Denial-of-Service (DoS) Attacks** that primarily target service availability.

- ❖ Lack of physical protection.
  - ➢ Nodes can be easily captured, tampered, or destroyed.
- ❖ Shared wireless medium.
  - ➢ Adversary can overhear, duplicate, corrupt, or alter data.
- ❖ Resource constraint.
  - ➢ Security mechanism greatly affects the performance of resource-constrained devices due to resource consumption.

❑ In an **advanced vampire attack**, a malicious node

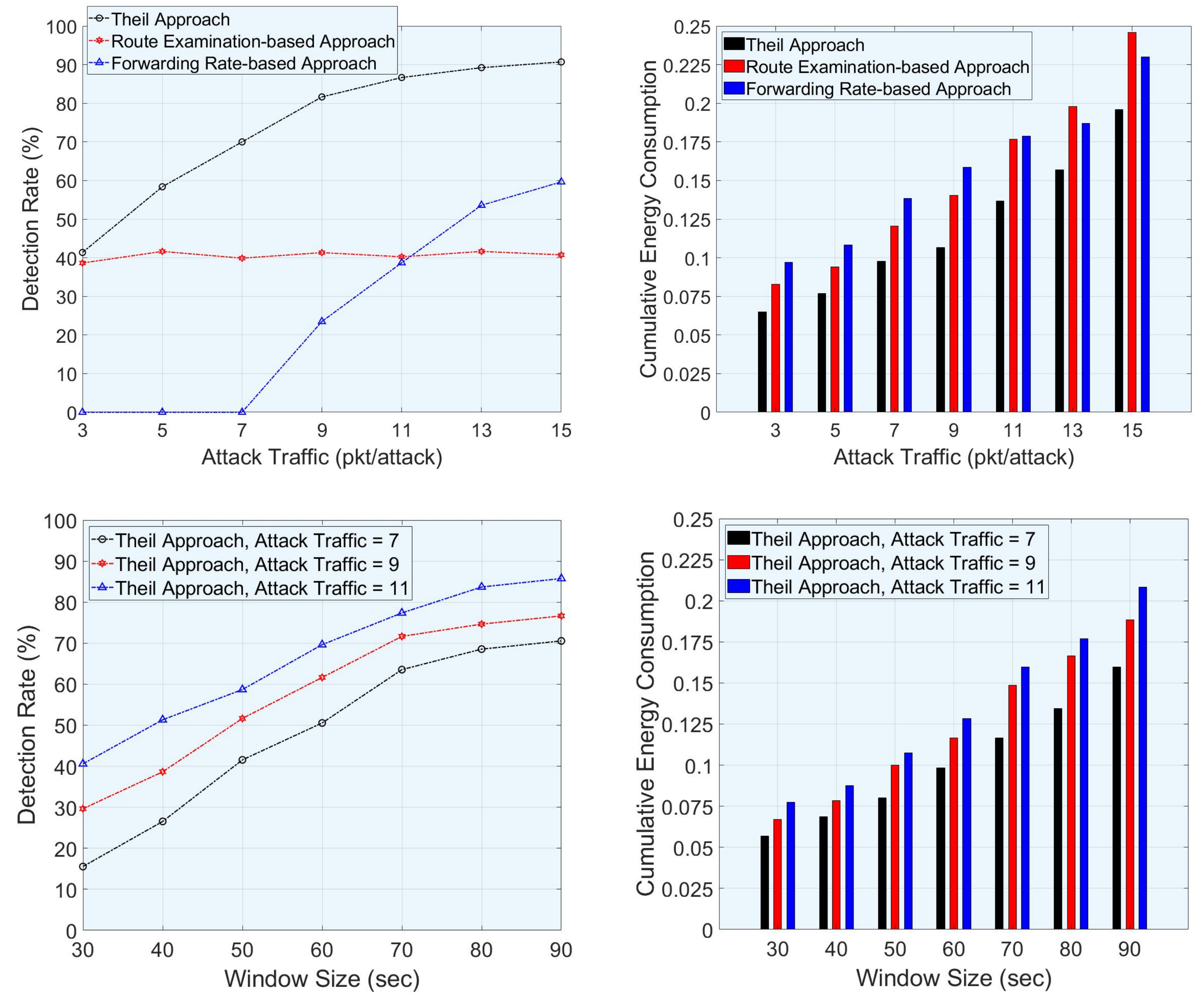
- ❖ manipulates the source route header of received packets, then generates and sends the invalid packet with a fictious route to legitimate nodes.
- ❖ When the legitimate node receives the invalid packets with a fictious route the packets are dropped since the receiving node cannot forward the packets with the piggybacked route, then replies an error message back to the DODAG root.
- ❖ The mass error messages from legitimate nodes causes denial of service in LLN networks.



Countermeasure

❑ **Theil Index-Based Detection**

- ❖ Designed based on Theil index theory, which can be viewed as a measurement of non-evenness or non-randomness of samples among all classes. In particular, if the samples are evenly distributed among all classes, a higher Theil index value can be observed. While a lower Theil index value indicates that the samples are not distributed evenly among all classes.
  - ➢ Each intermediate node records the destination MAC address of the received data packet within a specific window (ω).
  - ➢ Once the advanced vampire attack is detected, the attack mitigation procedure is triggered at the intermediate node who is the next hop of the suspected adversary to eliminate the attack by reducing the number of accepted data packets from the adversary.
- ❖ Performance Evaluation



Acknowledgement

❑ This research was supported by NASA West Virginia Space Grant Consortium, Undergraduate Research Fellowship Affiliate Award, and Marshall University, Summer Undergraduate Research Experience (SURE) Award.