# SVELTE
# Real-time intrusion detection in the Internet of Things

Shahid Raza, Linus Wallgren , Thiemo Voigt

Presented by Manbeer Singh

# Content

- Introduction
- Motivation
- SVELTE
- Components
- Algorithm
- Evaluation
- Extensions
- Conclusion

# Introduction

- Millions of smart objects
- 6LoWPAN (IPv6)
- Connected directly to Internet
- High Risk
- Attacker Can Access
- Intrusion Detection System is required
- IDS analyse network to detect error

# Motivation

- There are two types of existing IDS
- Signature based detections

  Match network behavior on basis of Signature of attacks

  Cannot deal with new attacks

  High Cost
- Anomaly based detections

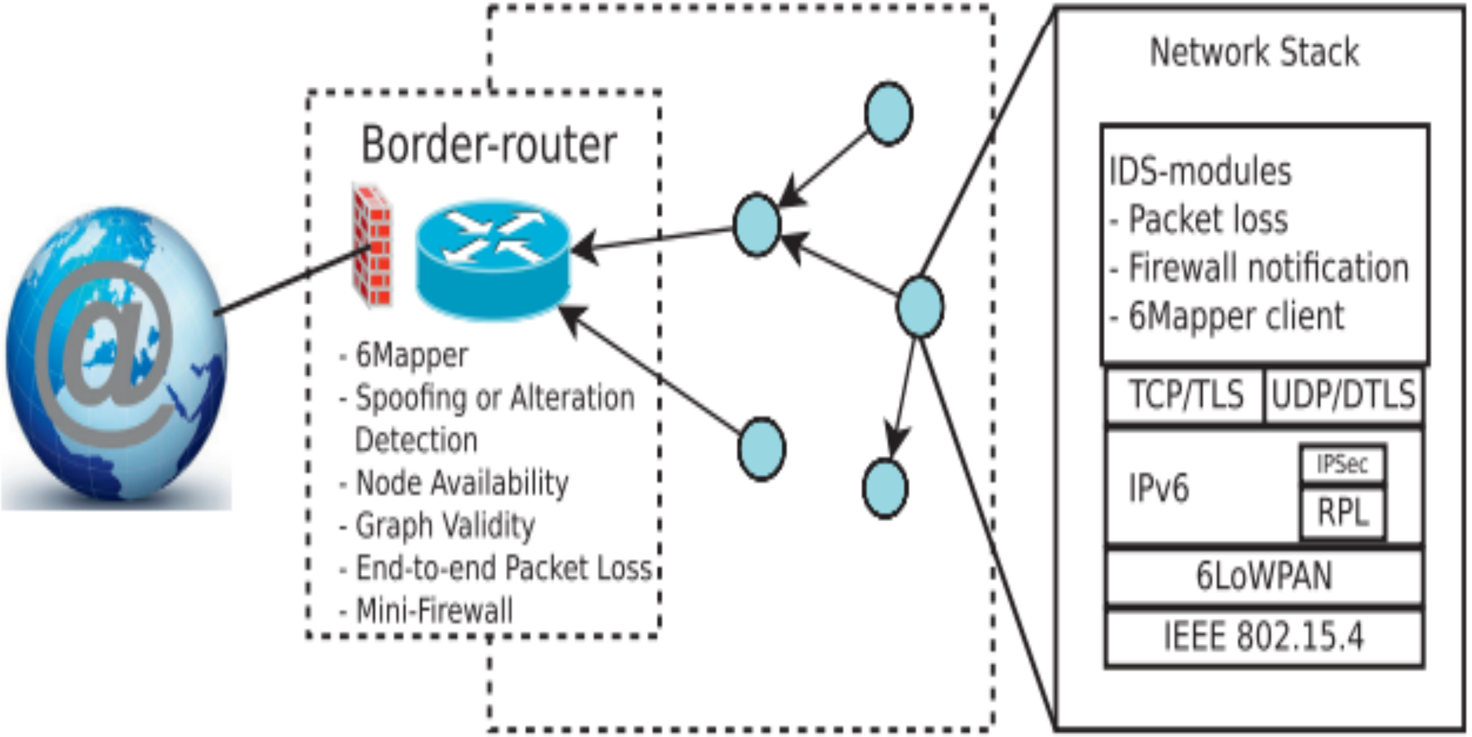
  determine the normal network behavior

  use ordinary behavior as baseline

  High Computation Time

# SVELTE

- A lightweight and effective IDS
- First IDS designed specially for IOT
- Have a integrated firewall



# Components

- 6LoWPAN Mapper

  Get the information about network

  construct it using RPL (IPv6 routing Protocol)
- Intrusion detection in SVELTE

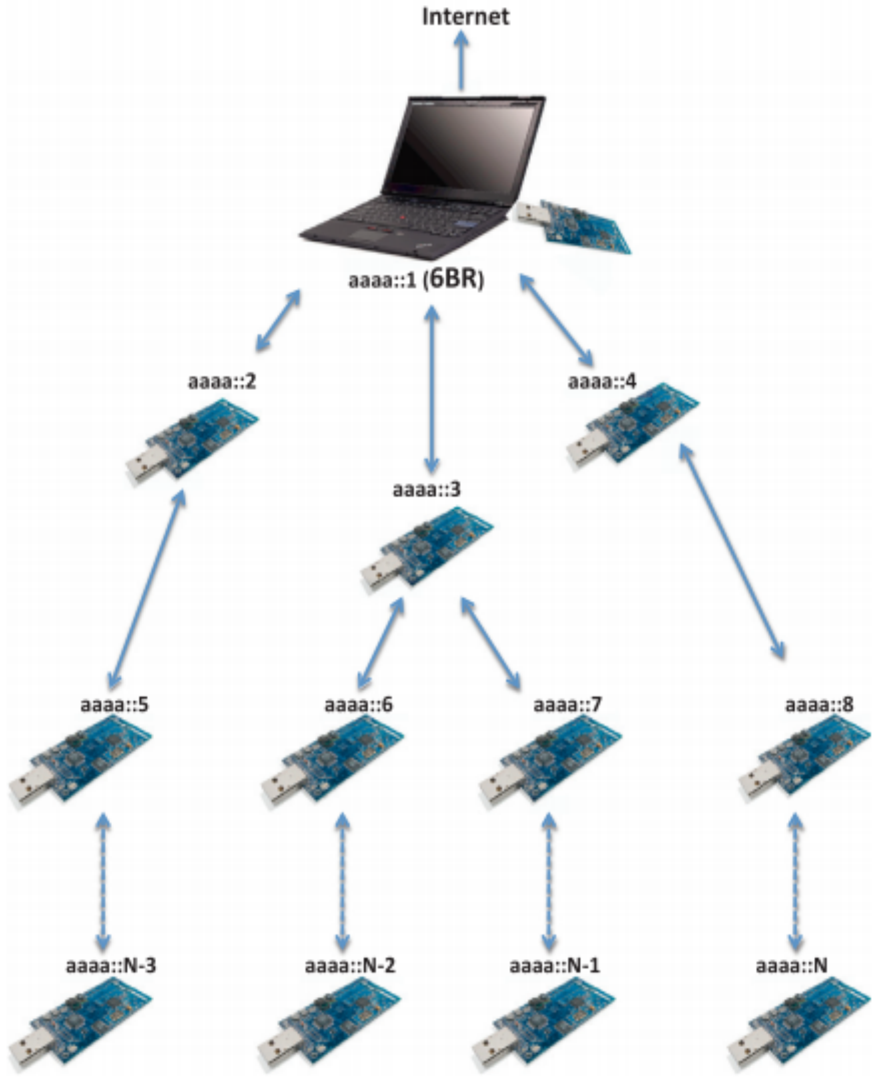
  Detect disturbance by analysing the mapped data
- Distributed mini-firewall

  Filter traffic (unwanted)

# RPL Protocol

- Each node has ID
- Rank increases (from root to node )
- Uses RPL DODAG ( Direction oriented Directed Acyclic Graph)

  Support two modes 1. Uni-directional 2. Bi-Directional
- Every node has capability to find direct of flow



# Intrusion detection

- Network graph inconsistency detection

  Attacker can create inequality in network

  Send wrong information by node

  It checks the node IDs rank assigned by 6mapper component

  If node IDs and ranks are not according assigned values, alarm is raised

- Checking node availability

  Check if all nodes working properly or not

  Keeps log of each node create a whitelist of nodes

  Compare white list with total nodes

# Intrusion detection

- Routing graph validity

  Attacker can change the flow of network

  It check routing of graph

  Detect sinkhole attacks by analysing network tropology

  Rank decreases from child to root

- End-to-end packet loss adaptation

  It alternate path if packet is not received by destination

# Mini-firewall

- Intrusion detection protects network internally
- Mini-Firewall protect network from global attackers
- Attacking is very easy for hosts out of network
- It filters the external nodes
- By comparing threshold value of local host with external host

# Evaluation

- Experiment setup

  Test on Cooja (network simulator) with Linux

- SVELTE detection and true positive rate

  Evaluate the number of defective nodes

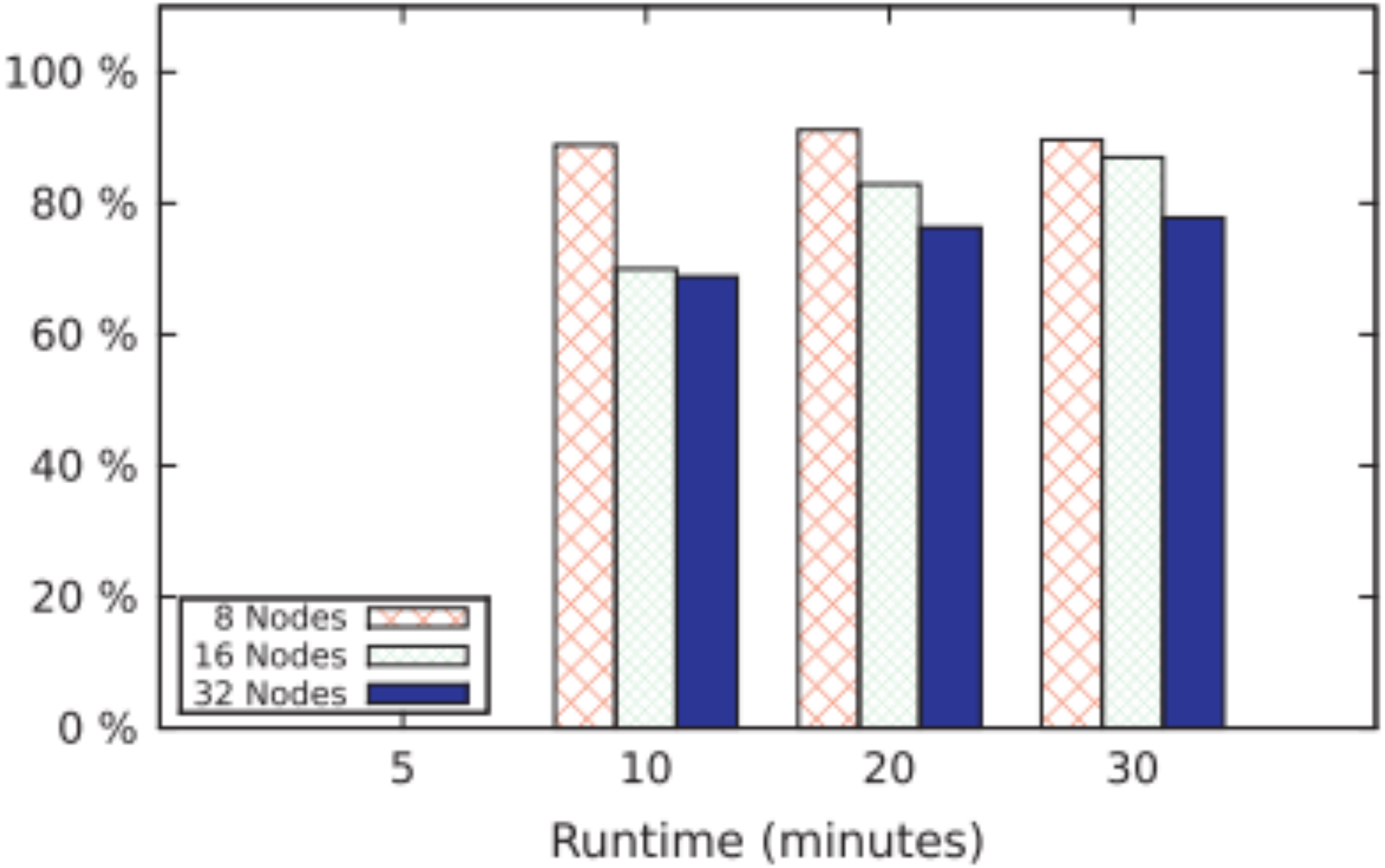
- Energy overhead

  Measured SVELT's power consumption

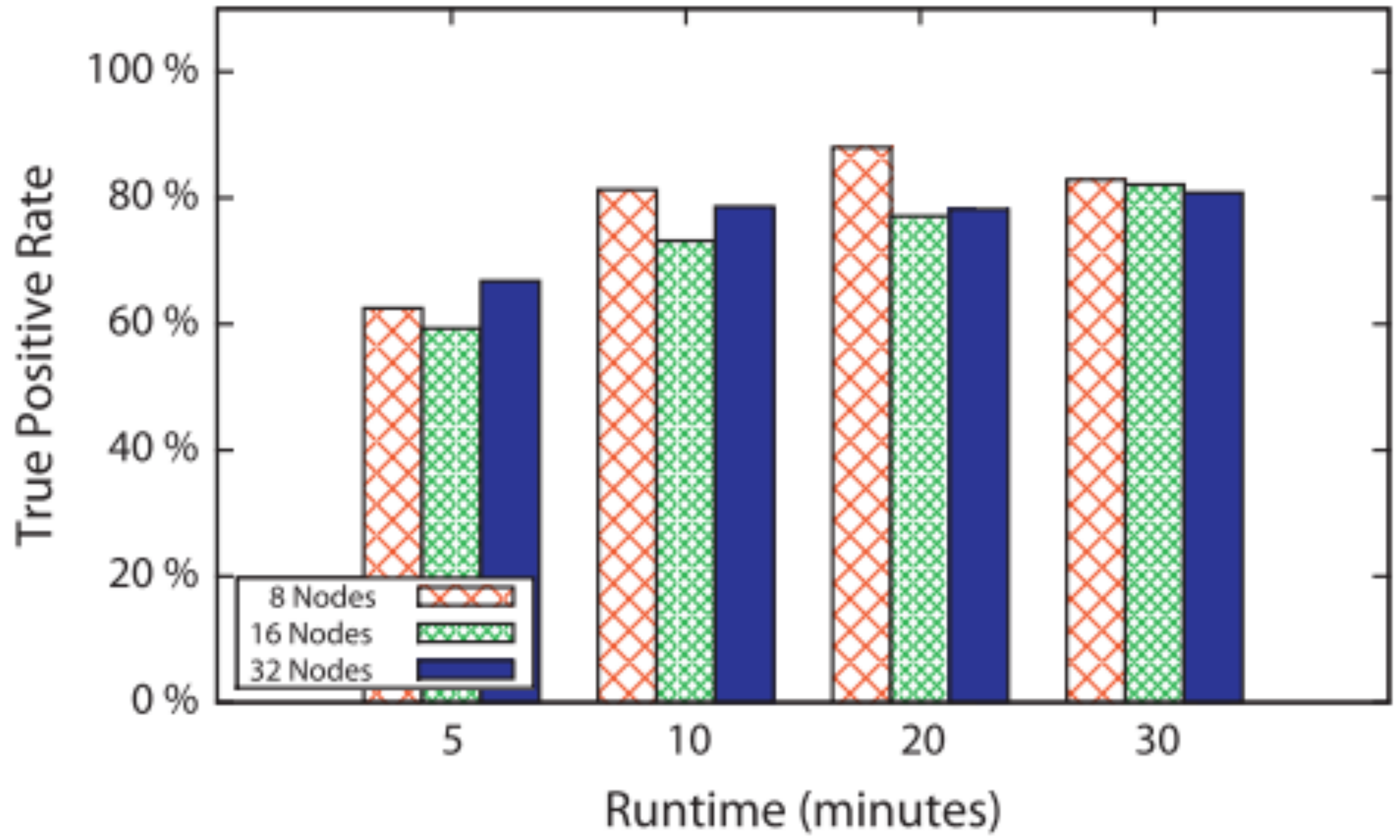
- Memory consumption

  Showed the RAM requirements

# SVELTE detection and true positive rate Sinkhole Attacks

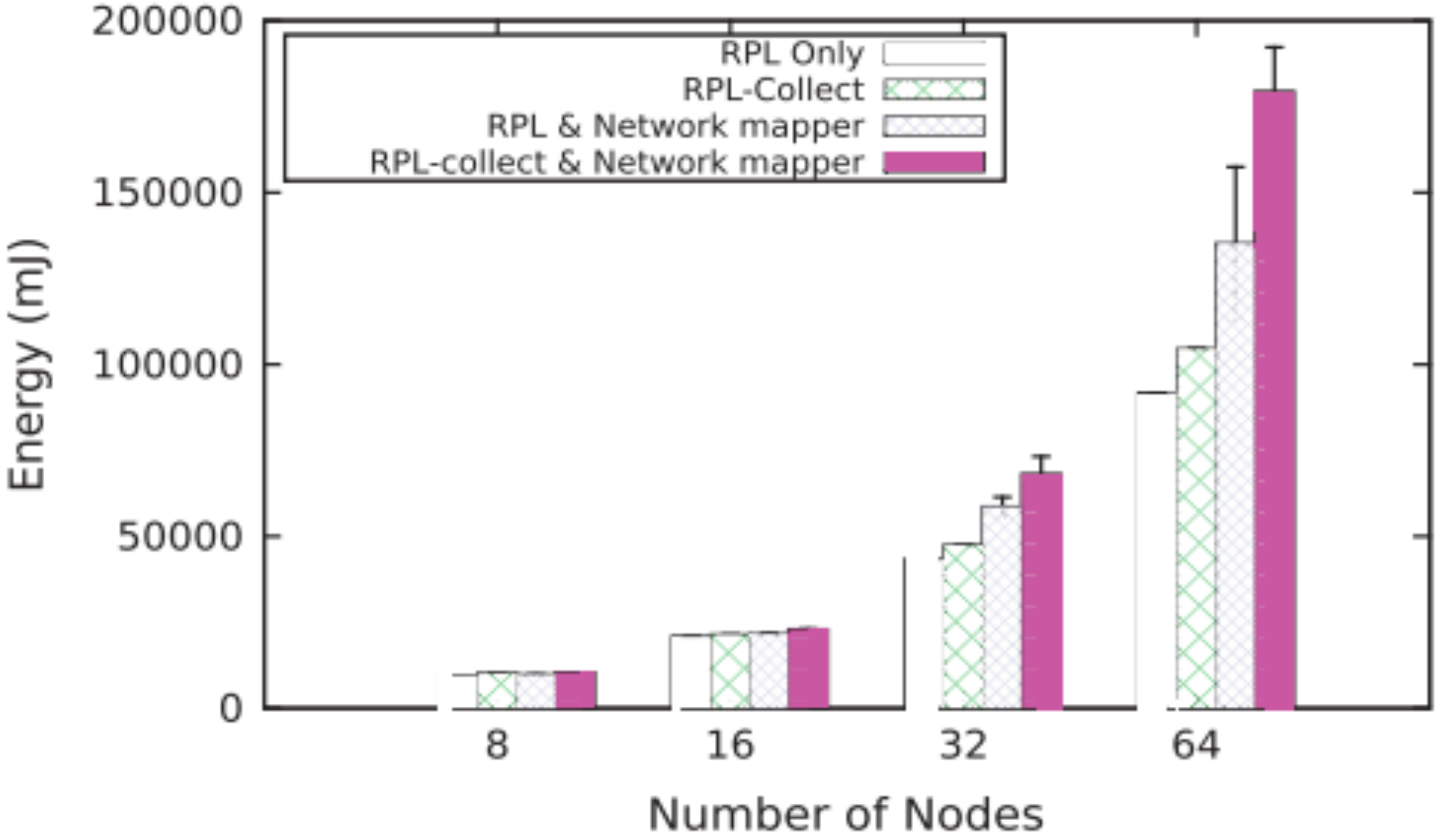


# Selective Forwarding Attack



(a) *Lossy* network suffering from selective forwarding attack

# Energy overhead



(a) Energy usage for the entire network (with *duty cycling*) in 30 minutes.

# Memory Consumption

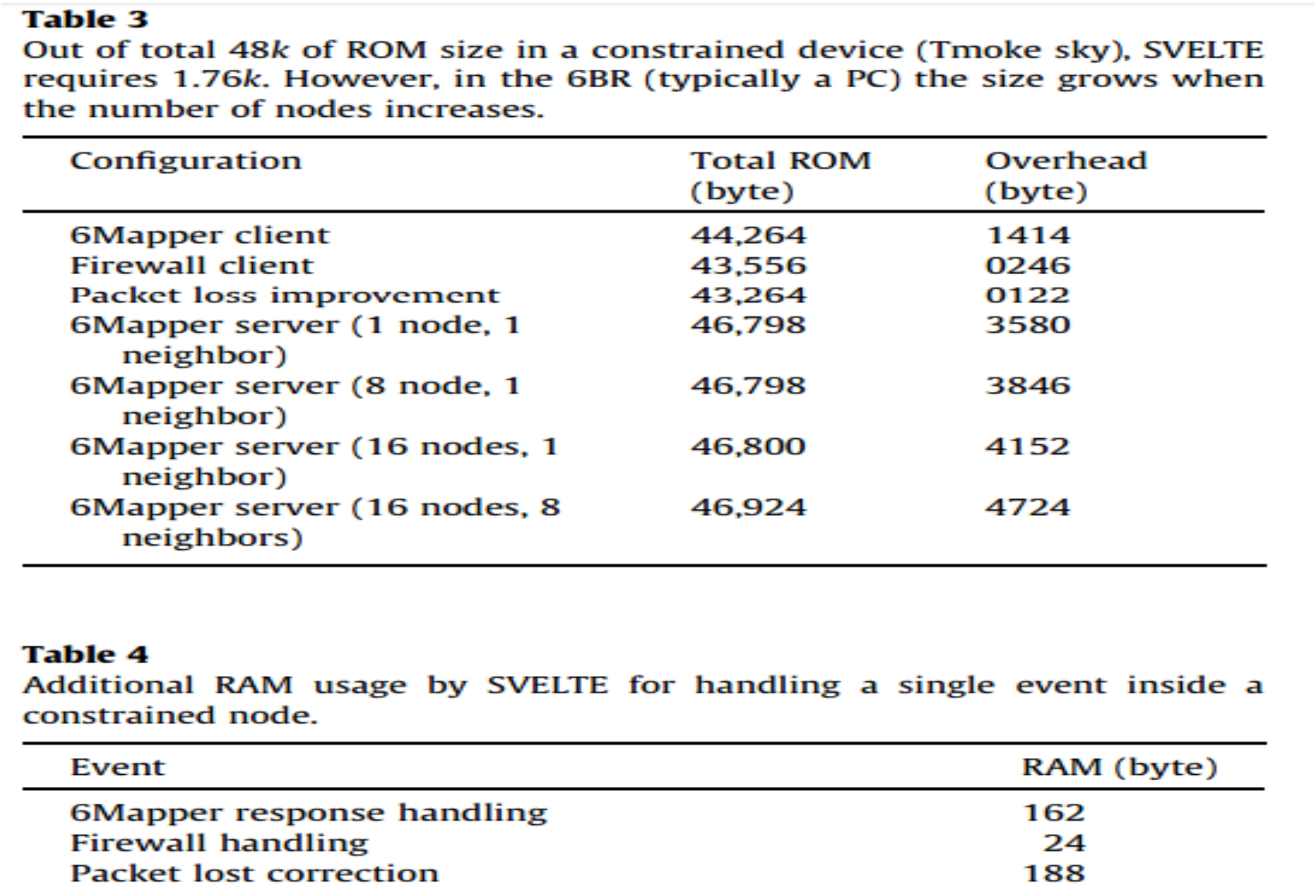


**Table 3**
Out of total 48*k* of ROM size in a constrained device (Tmoke sky), SVELTE requires 1.76*k*. However, in the 6BR (typically a PC) the size grows when the number of nodes increases.

| Configuration | Total ROM (byte) | Overhead (byte) |
|---|---|---|
| 6Mapper client | 44,264 | 1414 |
| Firewall client | 43,556 | 0246 |
| Packet loss improvement | 43,264 | 0122 |
| 6Mapper server (1 node, 1 neighbor) | 46,798 | 3580 |
| 6Mapper server (8 node, 1 neighbor) | 46,798 | 3846 |
| 6Mapper server (16 nodes, 1 neighbor) | 46,800 | 4152 |
| 6Mapper server (16 nodes, 8 neighbors) | 46,924 | 4724 |

**Table 4**
Additional RAM usage by SVELTE for handling a single event inside a constrained node.

| Event | RAM (byte) |
|---|---|
| 6Mapper response handling | 162 |
| Firewall handling | 24 |
| Packet lost correction | 188 |

# Extensions

- Easily extendable
- Can do wormhole detection
- Pinpoint the filter node

Improves accuracy to detect selective forward attacks

# Conclusion

- 6LoWPAN network main part of IOT
- Security of 6LoWPAN network very important
- SVELTE , First IDS for IOT
- Working with selective forwarding attacks , altered information and sinkhole
- Extendable