StateTrans

•HOME NETWORK SECURITY

Abstract:

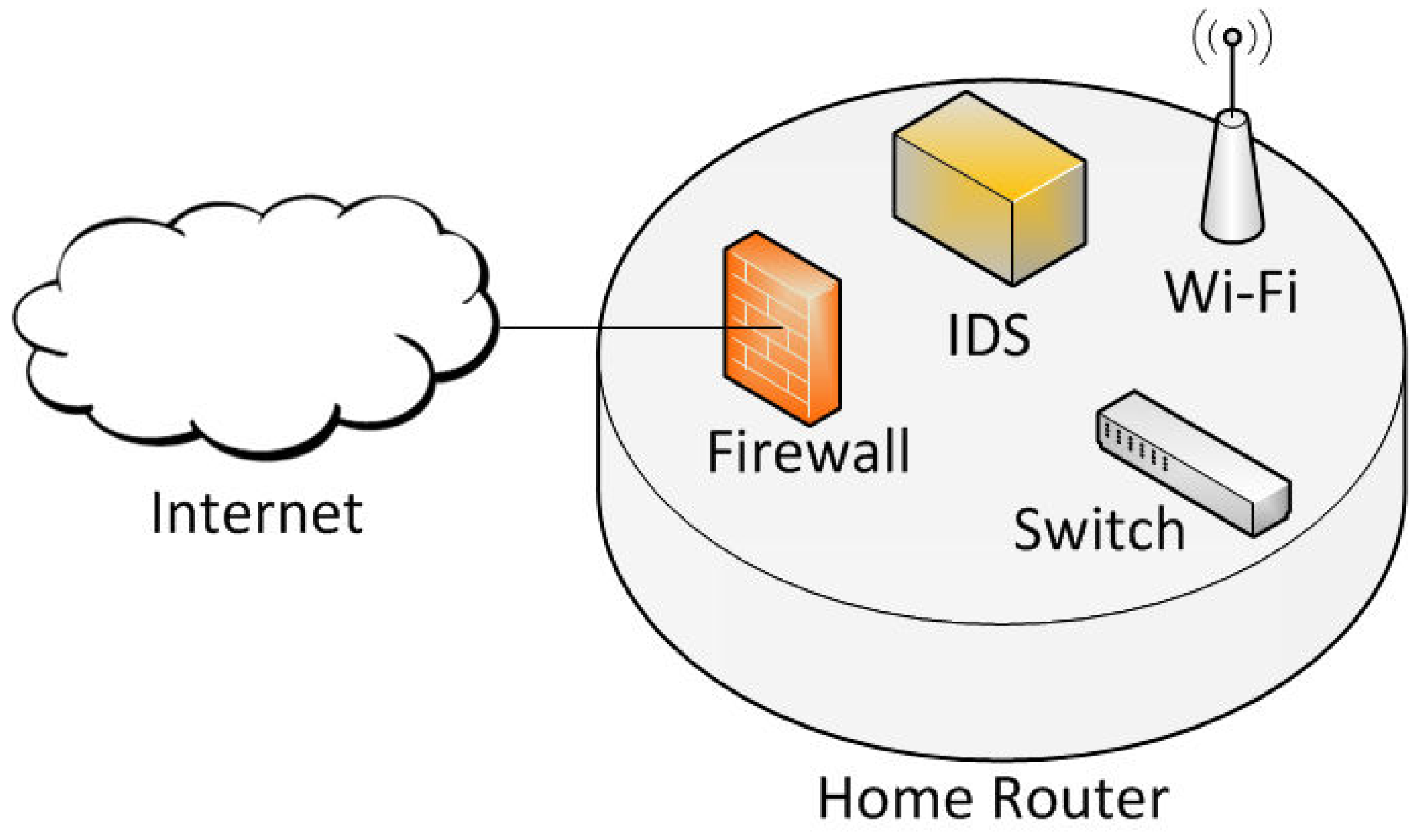
This diploma thesis deals with home network security and detection of intrusions in home network. The aim of this work is to design and implement a model for network intrusion detection system (NIDS), which can be easily deployed in home network. The model is based on stateful protocol analysis on network and transport layer. Profile is created for each device connected to network. Traffic is evaluated using these profiles in order to detect anomalies. Proposed NIDS is integrated into open source tool Ucollect. Furthermore, distributed approach to creation of firewall rules and employment of computational intelligence are discussed.

Objectives:

- Analyze home network security
- Design and implement a model for network intrusion detection system (NIDS) for home network
- Integrate into existing open-source solution

Implementation:

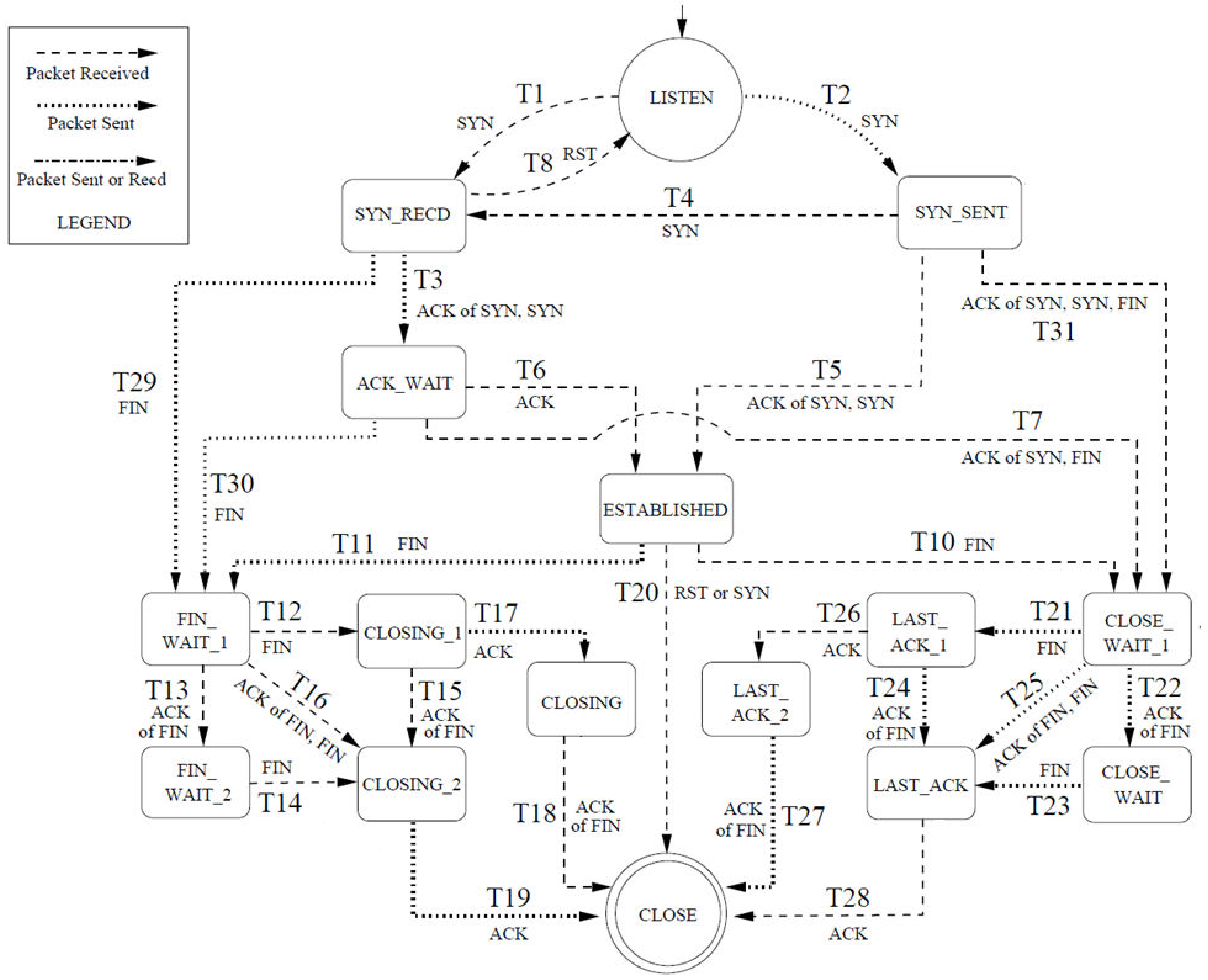
- Plugin for Ucollect
  - Daemon for collecting and analyzing network data
  - Part of Turris project (by CZ.NIC)
  - Open HW & SW based on OpenWrt
- Two approaches for integration into home network
  - Integration into router
  - Deployment on dedicated device
- Lightweight resource-friendly implementation to allow deployment on upper-class home routers



Integration of NIDS directly into home router.

Model:

- Based on stateful protocol analysis in combination with anomaly detection
- Monitoring of transitions in protocol state machine
  - L2 & L3 layer
- Artificial states for stateless protocols
- Profile created for each connected device
- Anomaly detection (current traffic vs. profile)
- Statistical approach used for evaluation
- Computation intelligence approaches can be employed



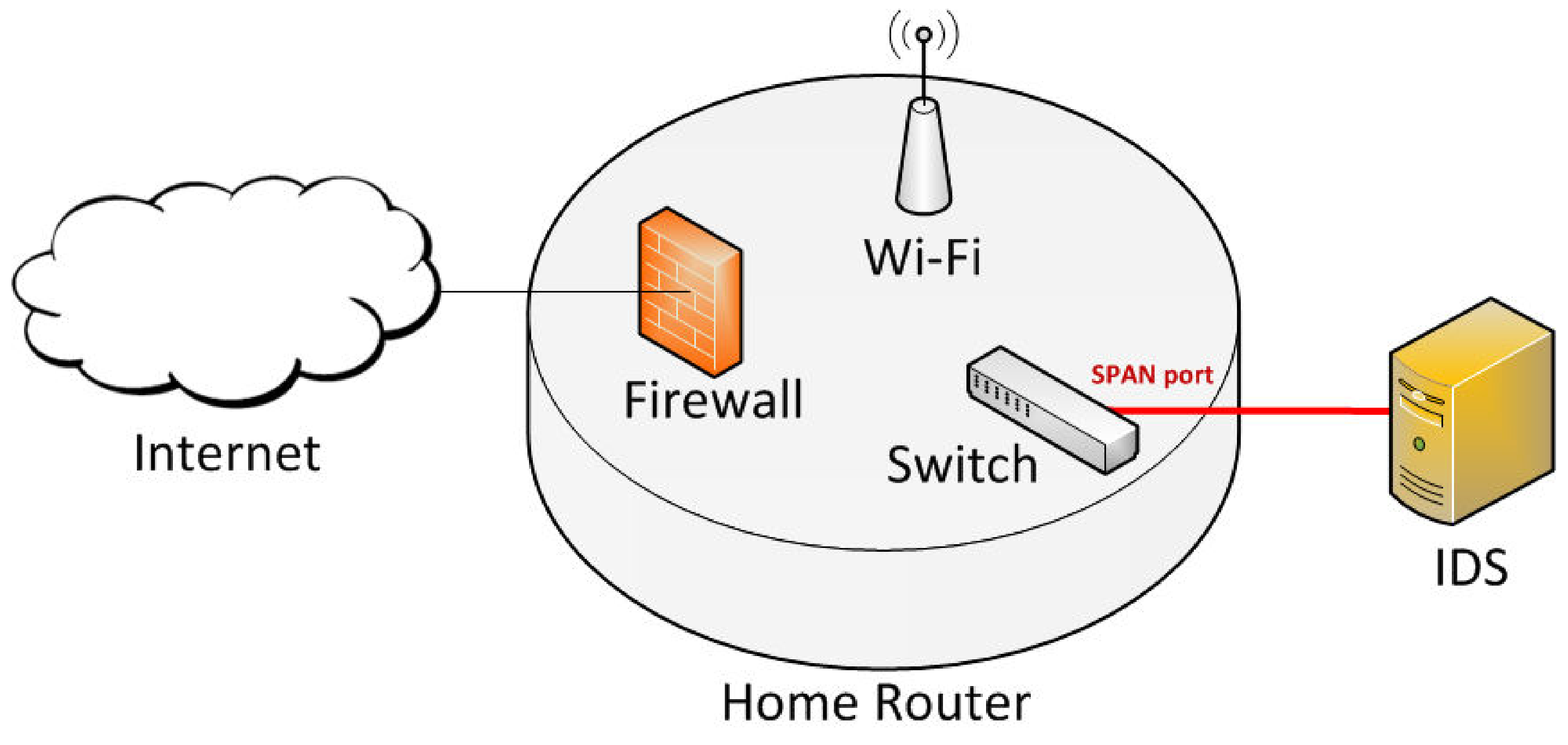
TCP protocol state machine

Contact:

Author: Ing. Tomáš Morvay

E-mail: tomasmorvay@gmail.com

Supervisor: doc. Ing. Ladislav Hudec, CSc.



Integration of NIDS into network using dedicated device

Experimental results

Traffic type	Number of connections	True Positives	True Positive Rate
Normal traffic	100	98	98 %
TCP SYN scan (nmap)	10	10	100 %
TCP CON scan (nmap)	10	10	100 %
TCP XMAS scan (nmap)	10	0	0 %
DOS útok (hping3)	100	97	97 %

Acknowledgement:

This work was partly sponsored by the Eset Research Centre and Scientific Grant Agency of the Slovak Republic, grant No. VEGA 1/0836/16 “Methods and algorithms for improving efficiency and multimedia content delivery in IP networks”.