instituto de telecomunicações

MAP tele DOCTORAL PROGRAMME IN TELECOMMUNICATIONS

ATNoG

Workshop MAP-Tele 2013
20 June 2013 - Porto

Nuno Rodrigues, António Nogueira, Paulo Salvador
nuno@ipb.pt, nogueira@av.it.pt, salvador@ua.pt

Modeling and Analysis of Network Resilience: The Security Perspective

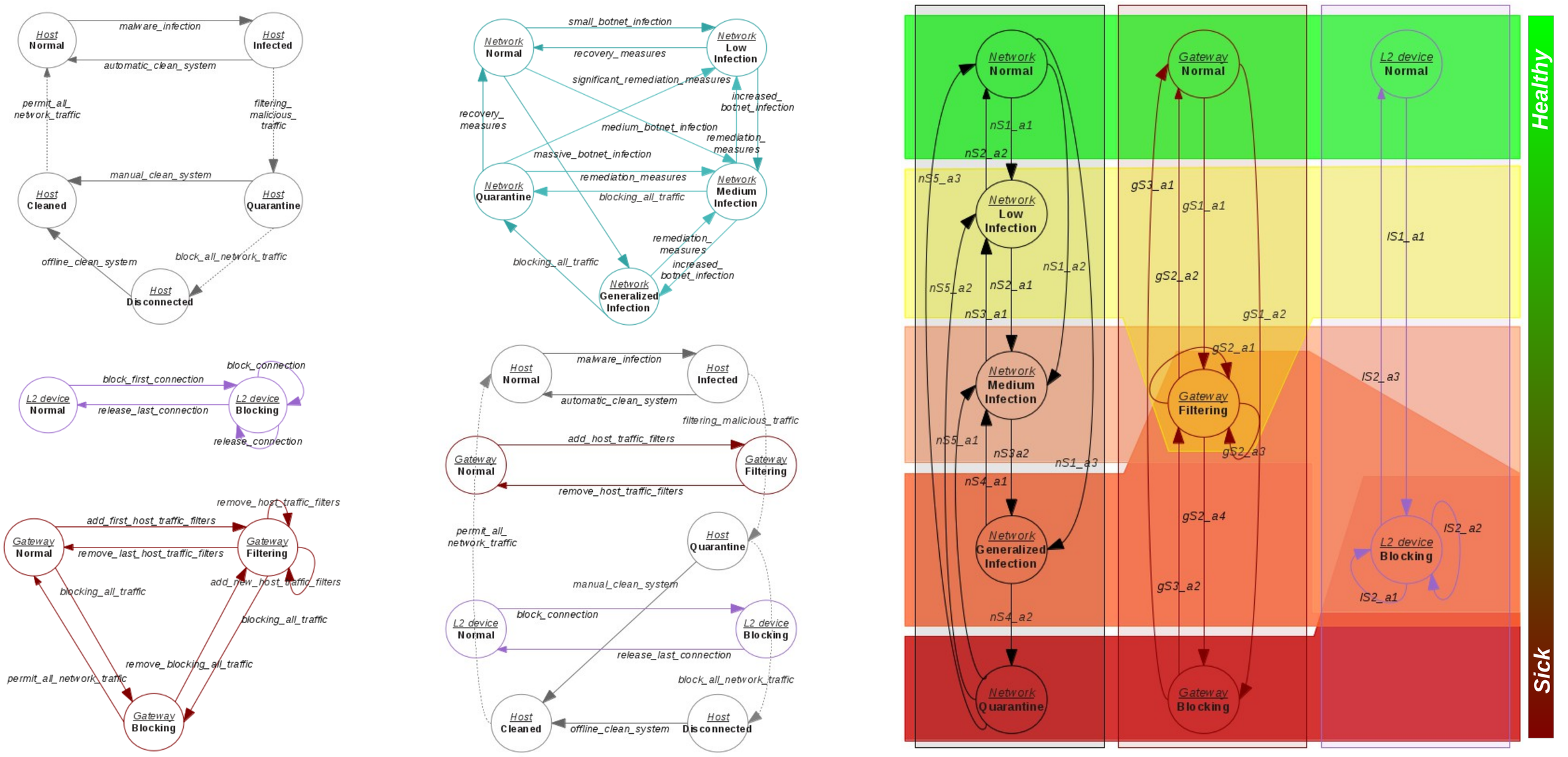
Motivation

- The increased **impact of global Internet in our daily lives is a continuous challenge** for those who are responsible for their design, planning, implementation and administration.
- As the **Internet becomes more important** to citizens, organizations and nations, more **pressure** is placed in their **reliability**, **availability** and **security** or, in other terms, in its **Resilience**.
- Because **Internet was not initially designed to support the actual levels of responsibility** in the global economy, it **is now evident that new paradigms and enhancements are needed to make this a resilient network**.
- From the three disciplines that mainly characterize network resilience, **security is one of the most challenging**. In fact, the range of security threats that nowadays affect Internet is immense and increasingly complex, with the beginning of a new era where the concept of cyber-wars between nations becomes reality.
- One of the most relevant security threats is the **malware** and **botnet** phenomenon. **Despite the development of several different types of countermeasures to fight these threats during more than a decade, this continues to be a field with big challenges and where new and solid improvements are needed.**

Objectives

- **Characterization and classification of the botnet threats** in terms of their impact in a **network resilience** perspective
- Definition of an **analytical model** that can **characterize the different network states** in terms of these **security threats**
- Definition of a **framework and architecture** to **manage** the different **network states** identified under the scope of the referred model
- Implementation of a prototype of the proposed architecture, for **validation and demonstration purposes**

Modeling ... and characterization of the different network states in terms of botnet threats



Next steps...

- Inferring the **network model parameters**, from real and/or reliable network data
- Definition of an **analytical model framework** that will facilitate the prediction of future network states
- **Development of a prototype, for validation and demonstration** of the proposed model

Expected Results

- Is expected that the proposed framework can **help network managers** plan short-term or long-term network reconfigurations and upgrades or **design new strategies for network management**, traffic routing, service provisioning and other critical network operational issues
- The correct planning and location of network failures due to security flaws can greatly **increase network operation efficiency** and **optimize Quality of Service** (QoS) parameter values

universidade de aveiro

instituto de telecomunicações