

On Understanding Normal Protocol Behaviour to Detect the Abnormal

P. Smith, D. Hutchison, M. Banfield, and H. Leopold

Computing Department
Lancaster University
{p.smith, dh}@comp.lancs.ac.uk

Telekom Austria AG
{mark.banfield, helmut.leopold}@telekom.at



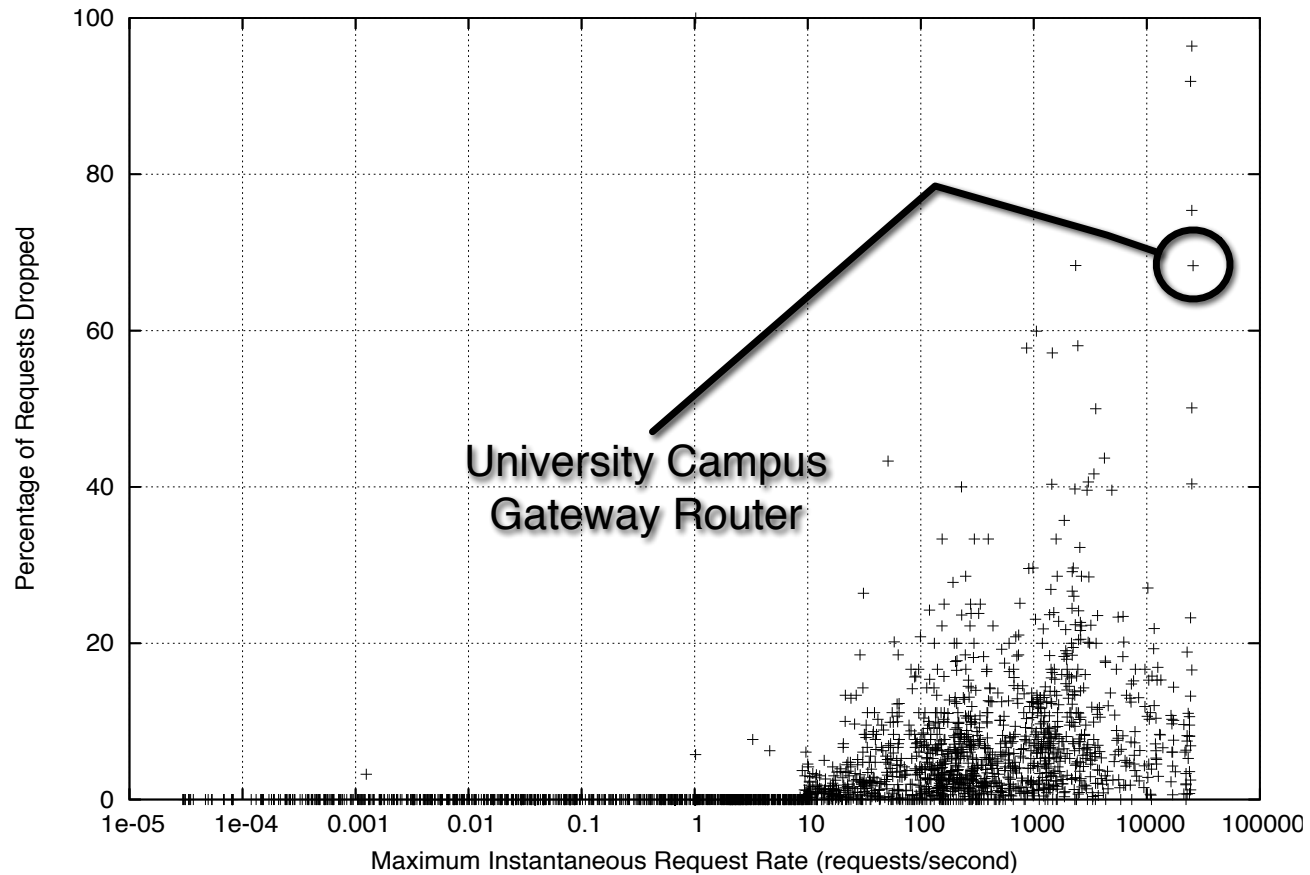
Our Thesis

Alone, a functional specification of a network protocol is insufficient when designing and parameterising systems that combat a range of network attacks – a non-functional specification (of normal protocol behaviour) is also necessary.

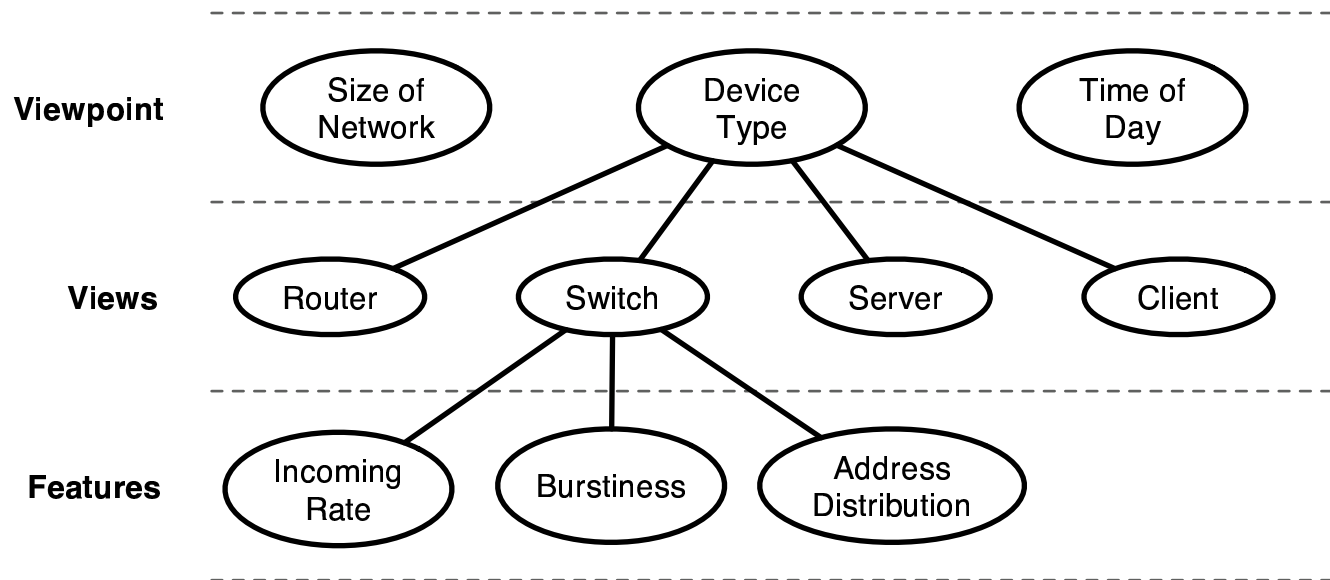
Motivation

- Current intrusion detection systems
 - Perform protocol checking against a functional specification
 - Can limit protocol message rates
- Protocols can exhibit abnormal behaviour because of an attack yet still behave according to their functional specification
- Advanced attackers can learn thresholds and operate below them

Case Study: Controlling Anomalous ARP Behaviour



Viewpoints, Views, and Features



An example set of viewpoints, views, and features for the ARP protocol

Uses for Operational Specifications

- Smart stacks
 - End-systems perform protocol message checking
 - Can we determine if a protocol message is good or bad?
- Intrusion detection systems
 - Specification could be used as input to an IDS that does normal behaviour checking
 - Could be based on a programmable edge router (*e.g.*, LARA++)

Issues

- Stealth attacks
 - Can systems developed as we are proposing catch stealth attacks?
 - Higher fidelity specifications give stealth attacks less room to manoeuvre
 - Potential trade-off between fidelity of specification and false positives
- What are the useful protocols, viewpoints, views, and features?
 - Potential for over specification, and where to stop specifying
- What are the side effects of detecting attacks in this way?
 - Consequences of false positives on a mitigation system
 - Confidence thresholds

Conclusions

- To build systems that detect advanced network attacks, a specification of normal protocol behaviour is essential
- Example applications
 - Smart stacks
 - Intrusion detection systems

More information:

<http://www.comp.lancs.ac.uk/resilinet>

