LANCASTER UNIVERSITY

An Adaptive Approach to Network Resilience: Evolving Challenge Detection and Mitigation

Yue Yu, Michael Fry

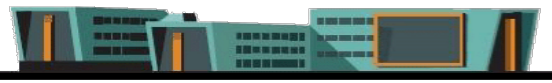
School of Information Technologies,
University of Sydney

Alberto Schaeffer-Filho,
Paul Smith, David Hutchison

School of Computing and Communications,
Lancaster University

8th International Workshop on
Design of Reliable Communication Networks (DRCN 2011)

October 10-12, 2011
Krakow, Poland



InfoLab21

Outline

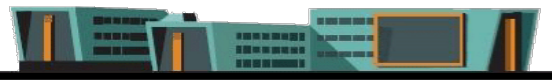
LANCASTER UNIVERSITY

① Motivation and Background
② Policy-based Management
③ Multi-stage Resilience Approach
④ Case-study: Protect ISP Network Against DDoS attacks
⑤ Evaluation: Resilience Simulation
⑥ Conclusion

Motivation

LANCASTER UNIVERSITY

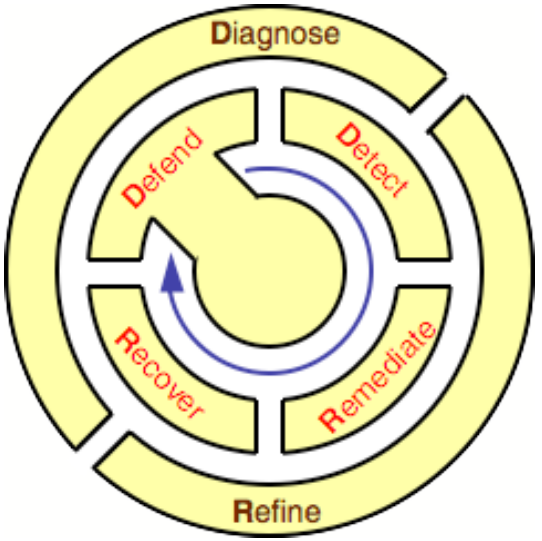
- **Computer networks need to become more resilient to a range of challenges that can impact their normal operation**
- **Network resilience**
  - Ability to provide and maintain an acceptable level of service in the face of various faults and challenges
    - **Malicious attacks**
    - **Misconfigurations**
    - **Hardware faults**
    - **Operational overload**
- **Requires identification of challenges in real-time, followed by the application of remedial actions**
- **Novel solution that enables the progressive, multi-stage deployment of resilience strategies**
  - Based on incomplete challenge and context information
  - Using policies to orchestrate the interactions between various resilience mechanisms
  - Incrementally identify the nature of a challenge and deploy appropriate mechanisms
- **Enable mitigation as early as possible**



Background on Network Resilience

LANCASTER UNIVERSITY

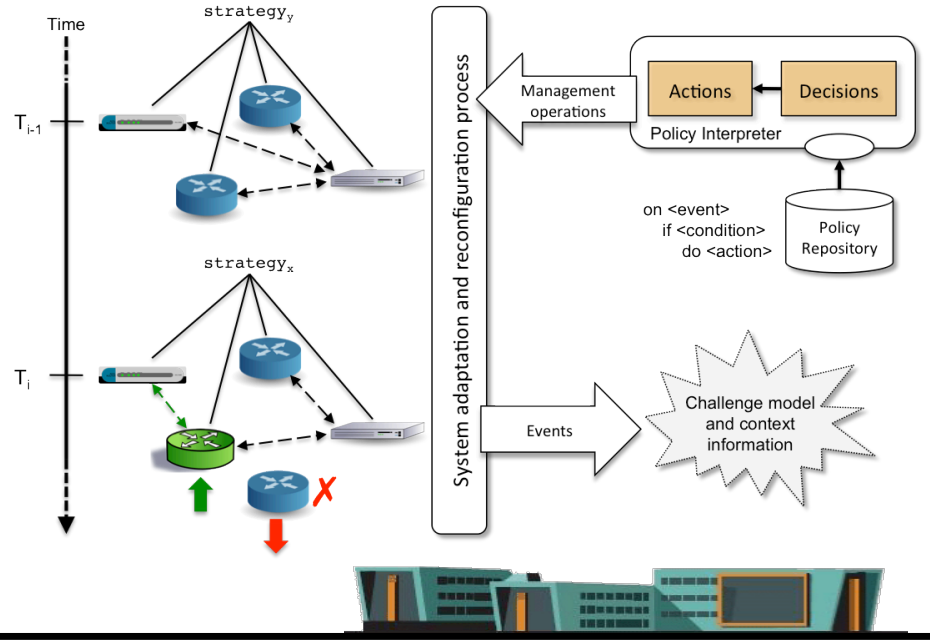
- **Network security and resilience framework: D^2R^2 + DR**
  - Real-time control-loop (D^2R^2): rapidly adapt to challenges and attacks and maintain an acceptable level of service
    - **Defend** against challenges to normal operation
    - **Detect** when adverse event occurs
    - **Remediate** the effects of adverse event
    - **Recover** to original normal operation
  - Offline control-loop (DR): enables term evolution of the system
    - **Diagnose** what caused the challenge
    - **Refine** operation to prevent it from happening again



- **Realising a framework for network resilience**
  - Often not clear how mechanisms for detection and remediation of challenges should be combined together to enforce effective resilience strategies

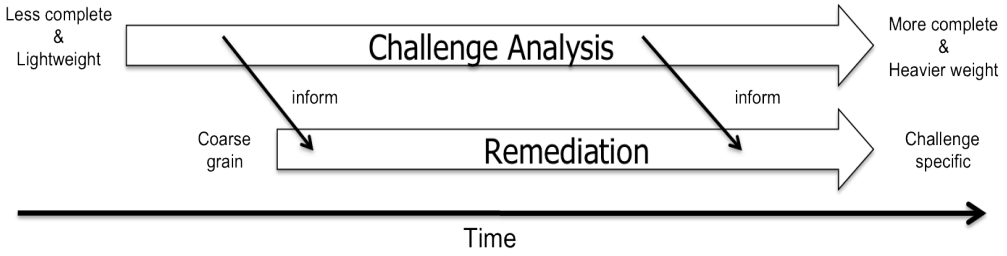
Policy-based Resilience Strategies

- **How to define configuration of resilience mechanisms, and how those configurations should evolve over time**
  - Management must be de-coupled from implementation of mechanisms
  - Configuration criteria change over time
    - **Requirements (e.g. SLAs)**
    - **Operation context (e.g. battery power)**
    - **Challenges (e.g. new types of attacks)**
  - Characteristics of monitoring and detection mechanisms vary
    - **Overheads, timescales, accuracy**
- **Using policies to define mechanisms configuration**
  - Modify management strategy without interrupting operation
    - **Re-configuration of operational parameters**
    - **Dynamic activation/deactivation of mechanisms**



Multi-stage Resilience Approach (1/2)

- **On-demand deployment and reconfiguration of mechanisms**
  - Use policies to refine detection and remediation strategies
  - Wide range of resilience mechanisms can be used
    - **Monitoring systems, tools to collect IP flow information, intrusion detection and classification systems, and mechanisms for mitigation, e.g. rate limiters**
  - Often not clear how they should be coordinated
    - **May span multiple autonomous systems and protocol layers**
- **Multi-stage challenge detection and remediation**
  - From lightweight detection to heavyweight analysis
  - From coarse-grain to tailored and fine-grain remediation

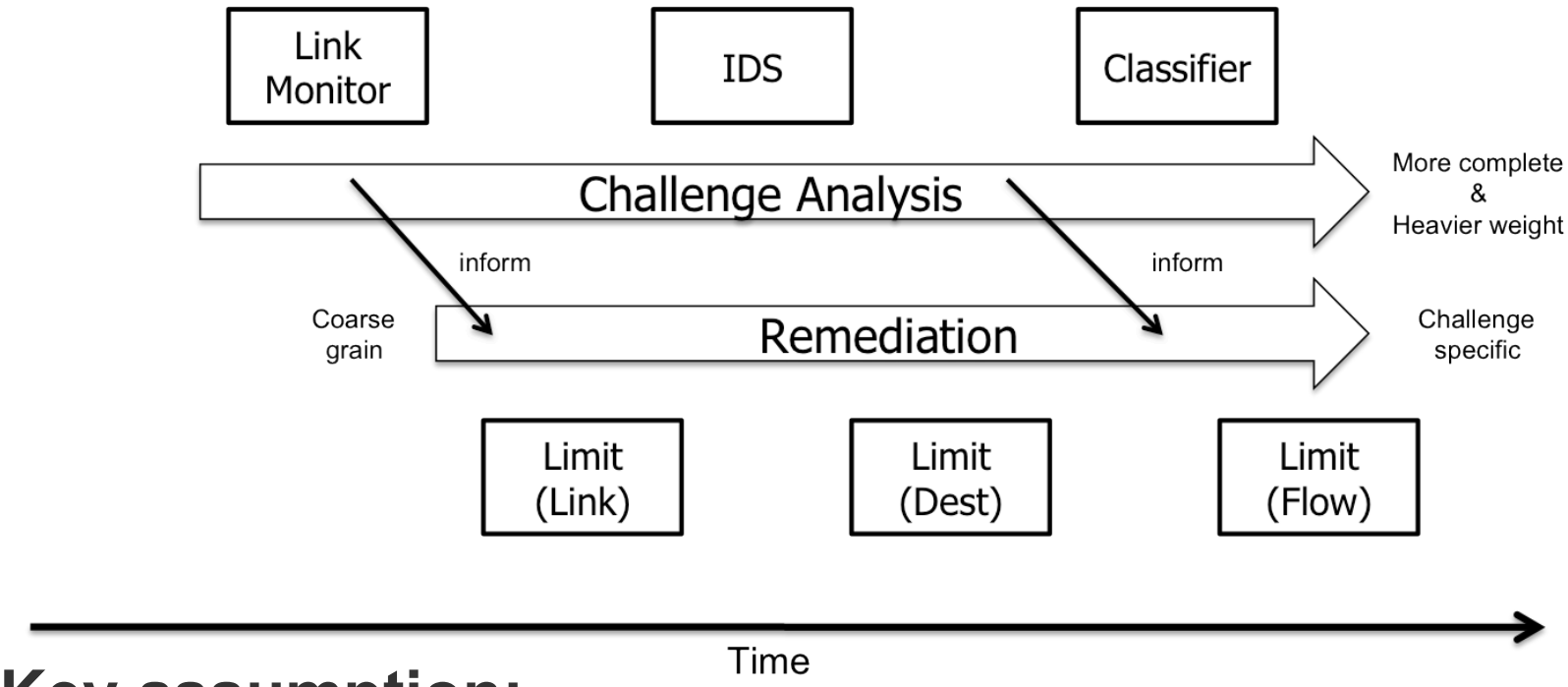


- **Remediation as early as possible to protect network and services**
  - Based on available (incomplete) information regarding challenges
  - Refine mitigation in real-time as new information becomes available

Multi-stage Resilience Approach (2/2)

LANCASTER UNIVERSITY

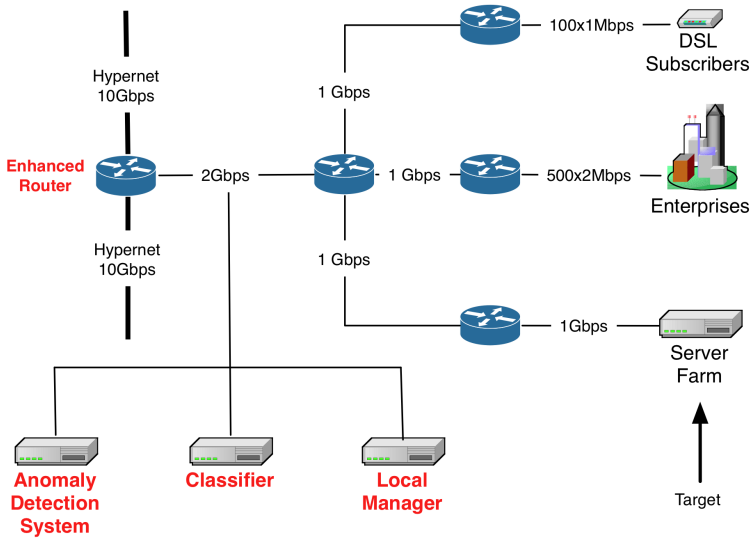
- **From coarse-grain to fine-grain remediation**

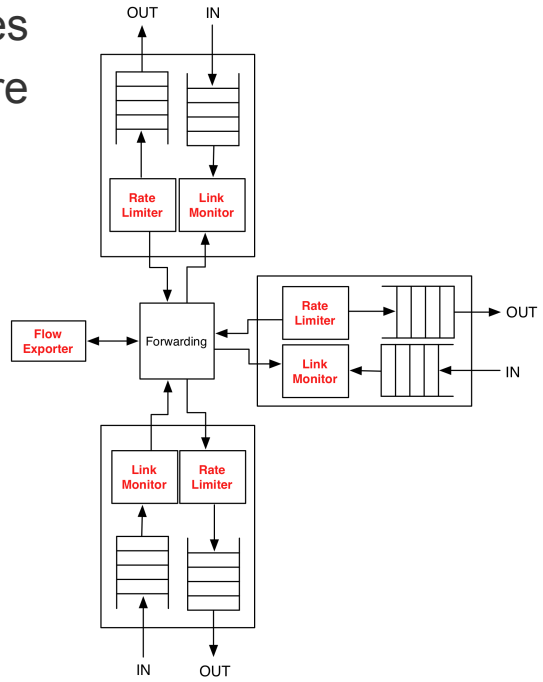


- **Key assumption:**
  - *Mechanisms that yield coarse-grain findings about a challenge are more timely and have lower overhead than those that provide more fine-grain information*

Case-study (1/2)

- **Protect access network of an ISP from the effects of DDoS attacks**
  - Resource starvation attack targeted at web server hosted on the server farm
  - Attack has the potential to disrupt other hosted services
  - Important to mitigate rapidly to protect the infrastructure

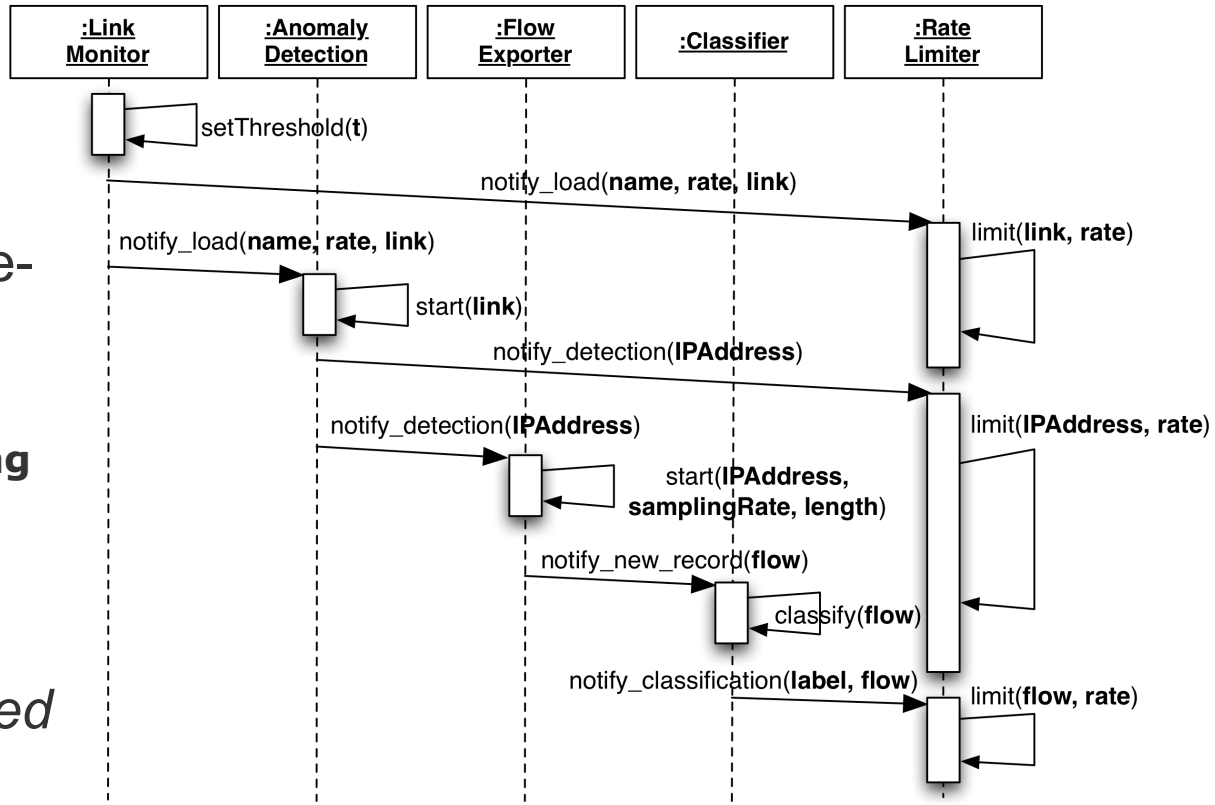




  - Topology showing the mechanisms used to ensure resilience of the network to high-traffic volume challenges
    - **A physical device such as a router will typically implement several management functions, e.g., a link monitor and an IP flow exporter**

Case-study (2/2)

- Policies are used to define the management strategy to contain the attack
  - **Easy to add or remove policies**
- Incrementally improve remediation as more fine-grain information is obtained
  - **From various monitoring systems**
- Resilience mechanisms realised as a number of policy-controlled *Managed Objects*



Resilience Simulation (1/4)

- **Difficult to evaluate complex resilience strategies**
  - Manage multiple detection and remediation mechanisms dynamically
  - Must be activated on demand, subject to conditions observed during run-time
  - As opposed to hardcoded protocols
- **Simulation of policy-based resilience strategies**
  - Integration of network simulator and policy framework
  - Policies specify required adaptations based on conditions observed during run-time

    - **High link utilisation**
    - **Malicious attacks**
    - **Equipment failures**

    <<< Event triggered condition-action (ECA) rules >>>

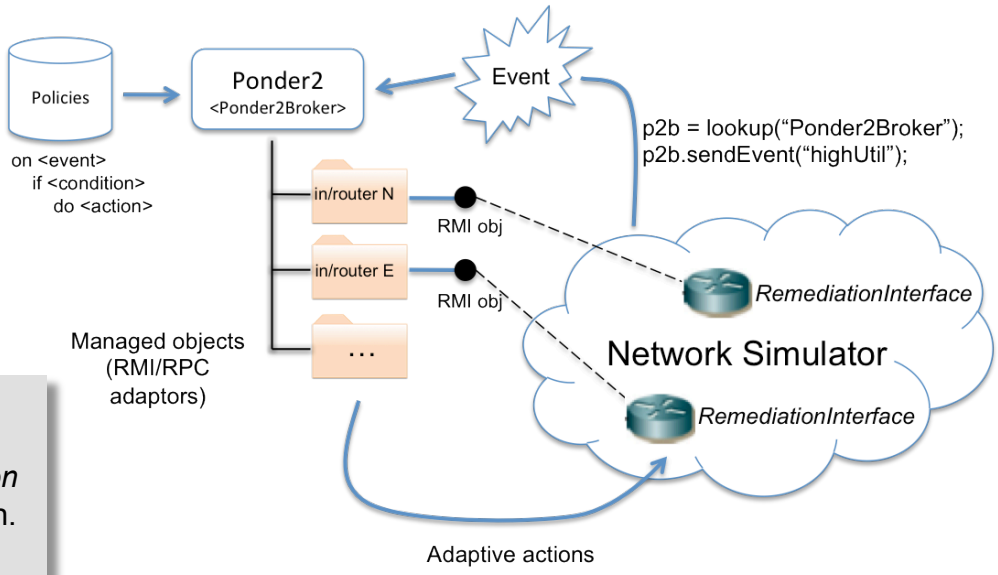
    ```
    on AnomalyDetectorMO.highRisk(link,src,dst)
        if (LinkMonitorMO.getUtilisation() >= 75%)
            do RateLimiterMO.limit(link,60%)
    ```

  - Observe how policies affect operation of simulated components
    - **Evaluate resilience strategies before deployment in the network, e.g. routers**

Resilience Simulation (2/4)

- **Integration between OMNeT++ simulator and Ponder2 framework**
  - Policies can be added, removed, enabled and disabled
  - Resilience mechanisms: instrumented objects in the simulation
    - **Most are additions to the standard Router module**
    - **Activated on demand, subject to conditions observed during run-time**
    - **XMLRPC integration: mechanisms export a management interface as a call-back proxy**
  - Simulation platform for
    - **Experiment different topologies**
    - **Analysis of anomaly scenarios**
    - **Implement resilience strategies**

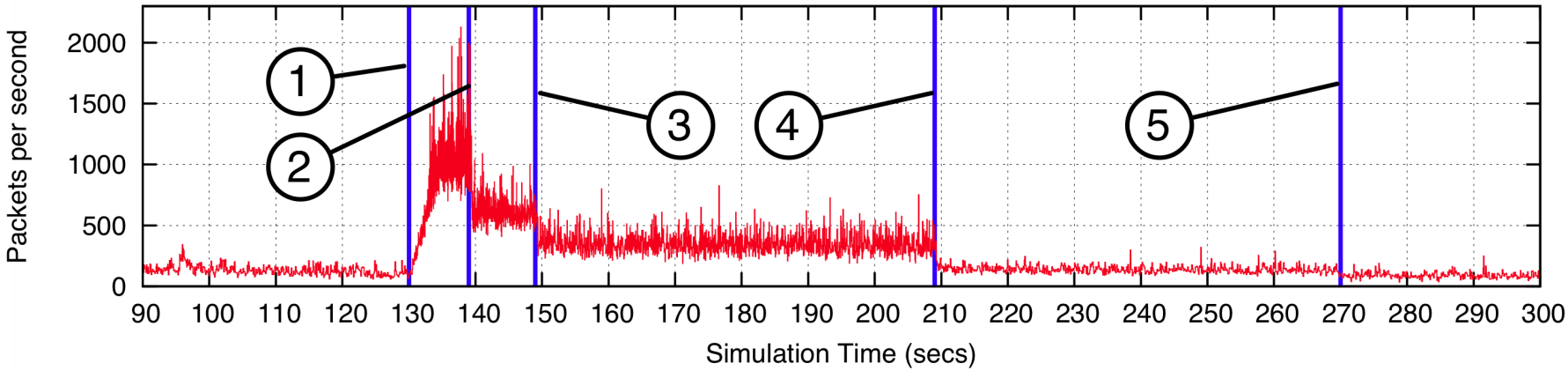
http://ponder2.net



A. Schaeffer-Filho, P. Smith, and A. Mauthe. **"Policy-driven Network Simulation: a Resilience Case Study"**. In: *Proceedings of the 26th ACM Symposium on Applied Computing (SAC 2011)*, ACM. Taichung, Taiwan. March 2011. p. 492-497.

Resilience Simulation (3/4)

- **Policy-based DDoS remediation**
  - Topology: 14 stub Autonomous Systems connected by 6 transit AS
    - **Victim AS attacked by 39 DDoSZombie hosts**
    - **1005 hosts generate background traffic to a number of other servers**
  - Resilience functions carried out at the edge of the AS network

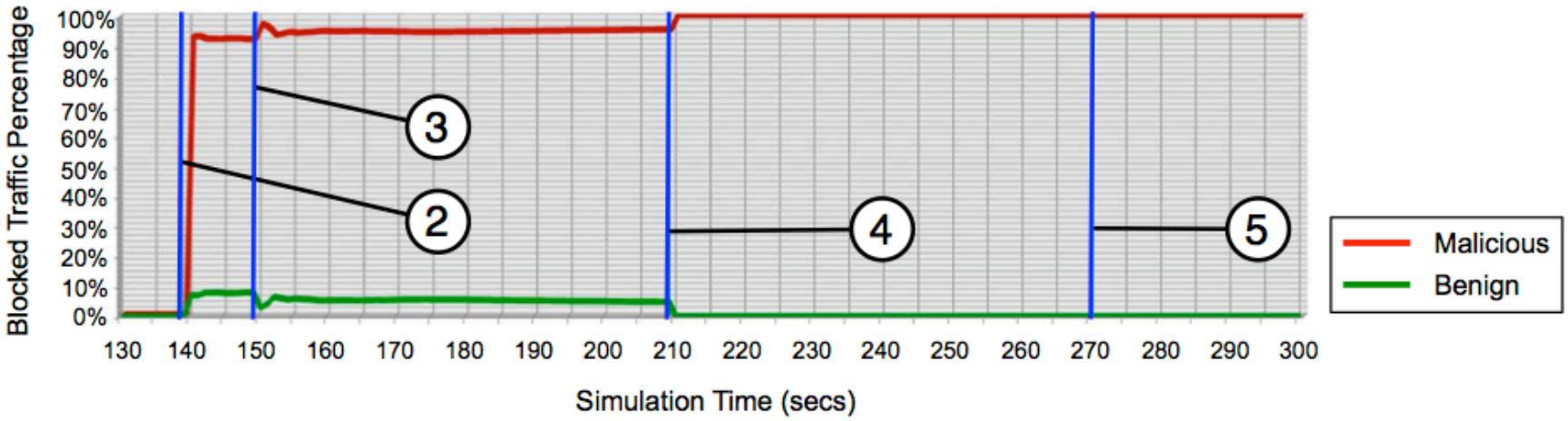


  - Progressive detection and tailored remediation of the attack

① Attack starts
② Rate limit the entire link
③ Rate limit all traffic towards the victim
④ Rate limit only the attack flow
⑤ All attack flows is successfully classified

Resilience Simulation (4/4)

- **Policy-based DDoS remediation**
  - Malicious and benign traffic dropped at different stages of the multi-level resilience strategy
    - **Increasing the percentage of malicious traffic limited (red), and conversely decreasing the percentage of legitimate traffic limited (green)**



  - Progressive detection and tailored remediation of the attack

① Attack starts
② Rate limit the entire link
③ Rate limit all traffic towards the victim
④ Rate limit only the attack flow
⑤ All attack flows is successfully classified

Conclusion (1/2)

- **On-demand deployment and reconfiguration of resilience strategies**
  - How a challenge can be dealt with by initially using:
    - **Lightweight detection and then progressively applying more heavyweight analysis**
    - **Coarse-grain remediation to minimise disruption, which then moves towards more fine-grain remediation**
  - Policies that rely on incomplete challenge and context information
    - **Elaborate the configuration of mechanisms deployed in the network**
  - Simulation platform can be used to analyse different types of challenges and the resource trade-offs involved
    - **Evaluate the effects of detection and remediation mechanisms**

Conclusion (2/2)

- **Commercial systems offer automated intrusion response based on detected signatures only**
  - May require a human operator to interpret anomalous behaviour and take discretionary actions
  - Traditionally, system administrators have had the perception (which is not entirely wrong) that the automatic launch of remedies might create additional security risks
- **Advantages of the multi-stage, policy-based approach**
  - Policies can be carefully crafted and evaluated on the simulation environment
  - Permits introducing intermediate stages of remediation
    - **System can operate with limited performance until definite cause is reliably identified**
  - On-demand deployment of mechanisms not only applicable to resilience,
    - **Energy-awareness, QoS, etc**

LANCASTER UNIVERSITY

An Adaptive Approach to Network Resilience: Evolving Challenge Detection and Mitigation

Yue Yu, Michael Fry

School of Information Technologies,
University of Sydney

Alberto Schaeffer-Filho,
Paul Smith, David Hutchison

School of Computing and Communications,
Lancaster University

Thank You!