RESILIENCE FOR FUTURE NETWORKING: DISTRIBUTED CHALLENGE DETECTION, IDENTIFICATION AND REMEDIATION

Yue Yu *Supervisor: Prof. Michael Fry*

Email: tinayu@it.usyd.edu.au

School of Information Technologies
FACULTY OF ENGINEERING & INFORMATION TECHNOLOGIES

MOTIVATION

• Part of the EU ResumeNet project (Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation) that is supported under the EU FP7 FIRE

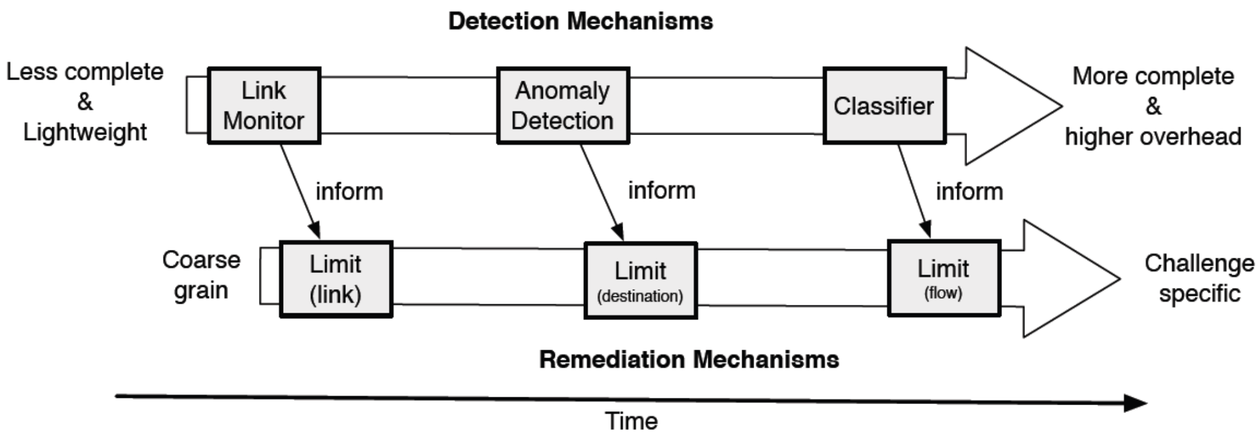
• Aim to make networks more resilient to a wide range of challenges including unintentional misconfigurations; malicious attacks from intelligent adversaries against the network hardware, software, or protocol infrastructure; environmental challenges of mobility, weak channels, unpredictably long delay; unusual but legitimate traffic load; provider failure

• Resilience means the ability of the network to provide an acceptable level of service in the face of significant challenges

• The focus of my research is on the network challenge detection, identification and remediation

MULTI-STAGE POLICY-DRIVEN APPROACH TO NETWORK RESILIENCE

• Coarse to fine grain challenge identification and remediation



• Detect the onset of challenges in real time that are impairing normal operation. Follow by remediate the damaging effects of the challenge and minimize its impact, to maintain an acceptable level of service. Then fully recover from the challenge by removing its root cause

• Provide a novel solution that enables the progressive multi-stage deployment of resilience strategies, based on incomplete challenge and context information

• Initially using lightweight detection and then progressively applying more heavyweight analysis, a key contribution of our work is the ability to mitigate a challenge as early as possible and rapidly detect its root cause

• The approach we proposed has the flexibility, reproducibility and extensibility needed to assist in the identification and remediation of various network challenges in the future

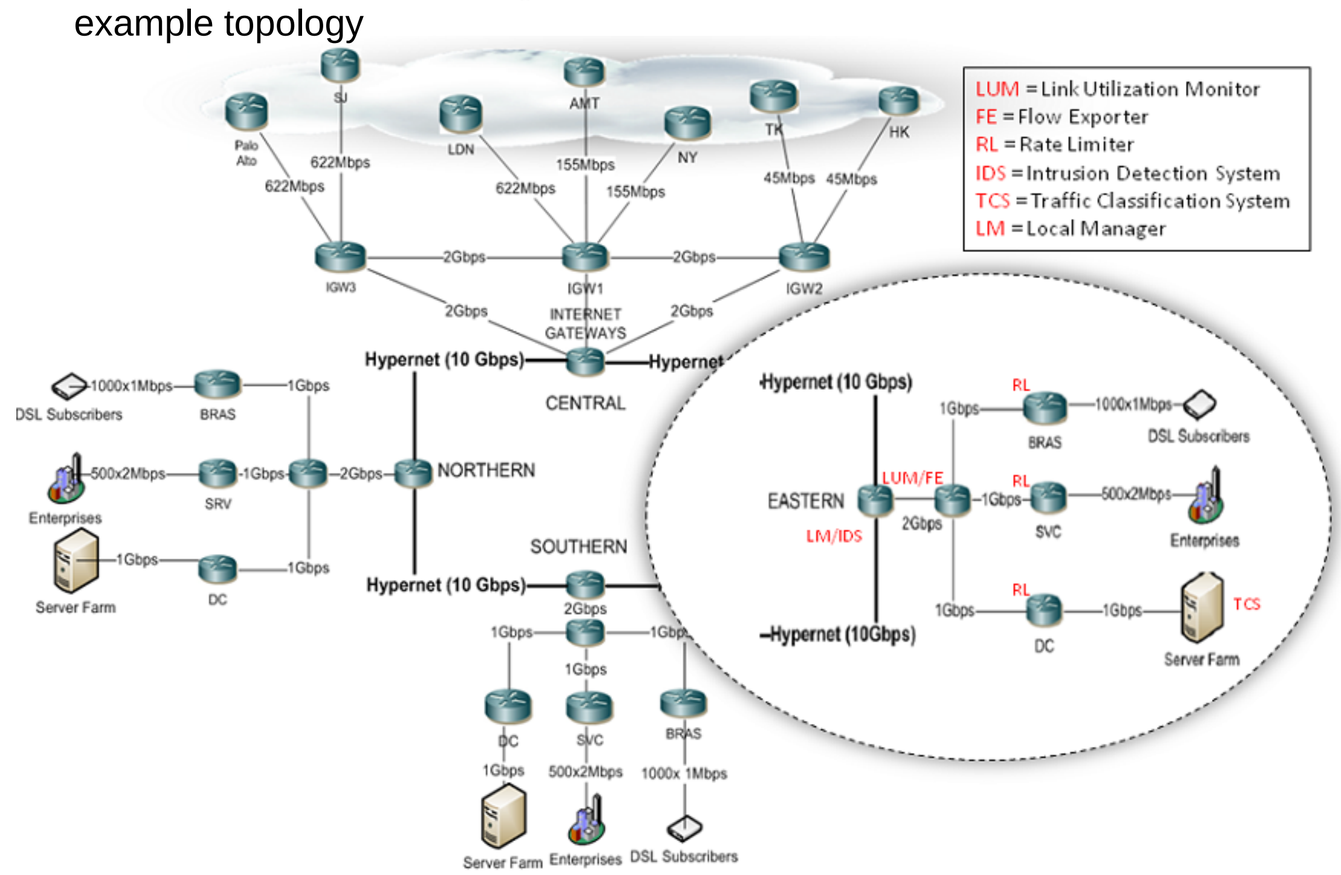
EXPERIMENTAL SCENARIOS

• The example topology shows the mechanisms used to ensure resilience of the network to high-traffic volume challenges

• The aim is to provide protection to the access network of an Internet Service Provider (ISP)

• The DDoS attack originating from the 10Gbps Hypernet toward a Web service hosted at the server farm has the potential to disrupt other hosted services (on the server farm), and the ISP's enterprise and domestic customers

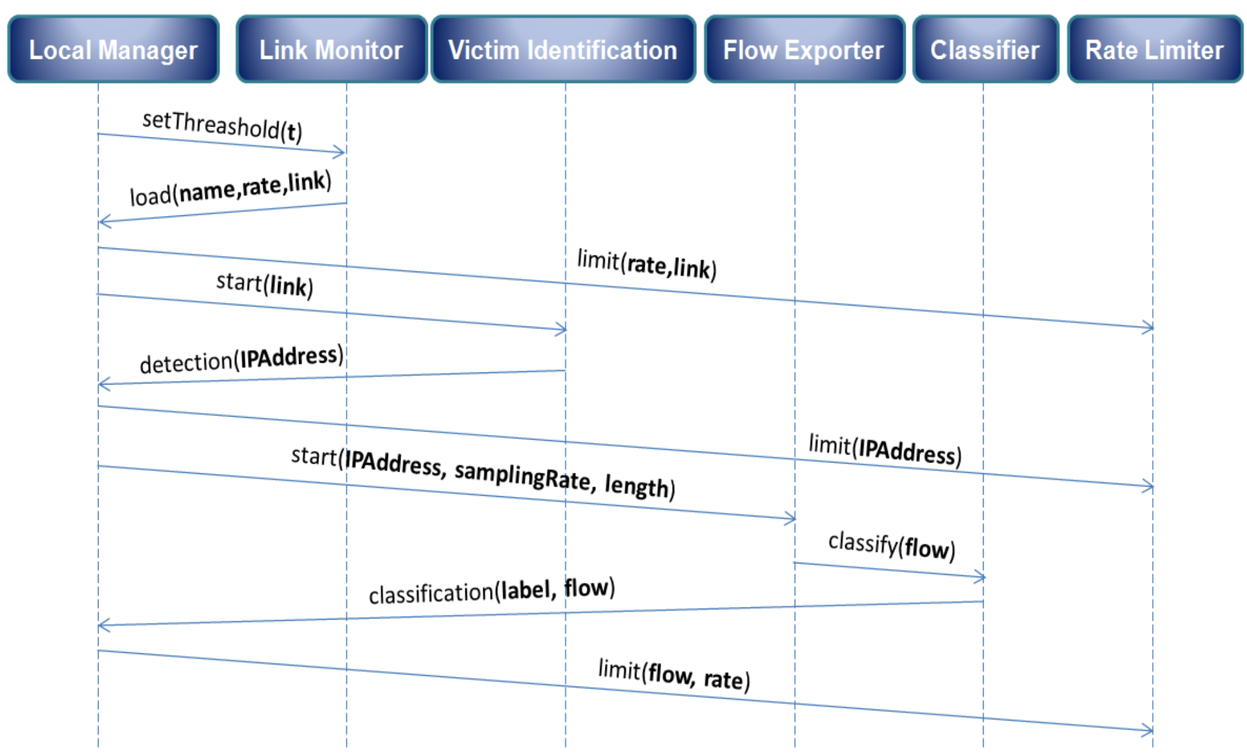
• Our experiment is using network simulator OMNeT to simulate the example topology

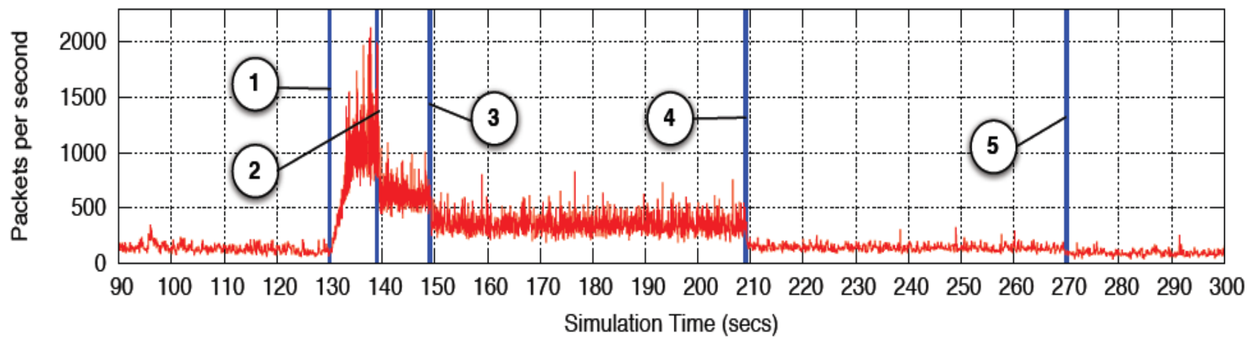


USER CASE: INCREMENTAL DDOS DETECTION AND REMEDIATION

• An approach to DDoS attack resilience that incrementally improves remediation as more fine-grain information about the nature of the attack is gleaned from detection and classification

• Resilience mechanisms are realized as a number of policy-enabled Managed Objects that must co-operatively enforce the resilience of the network



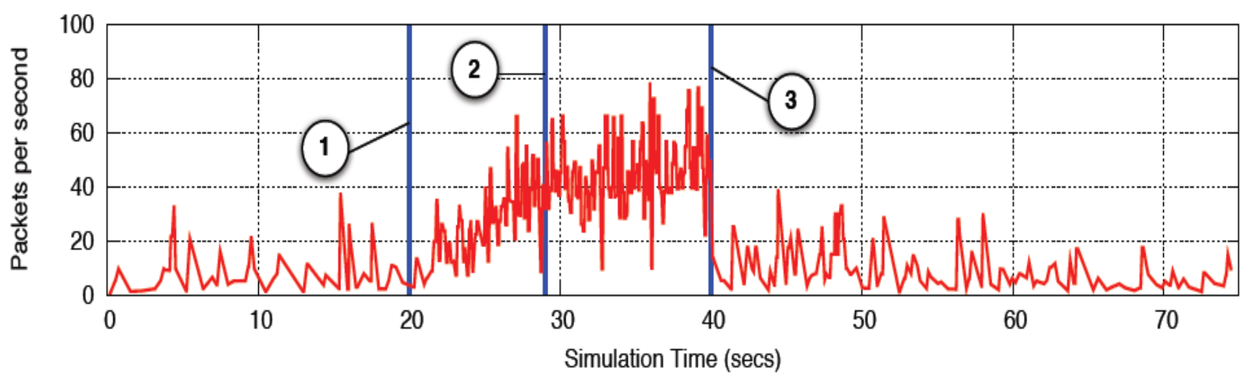


USER CASE: INCREMENTAL WORM DETECTION AND REMEDIATION

• An innovative approach to detect and mitigate different types of worm propagation.

• The worms could be noticed soon upon their first appearance

• Effectively and automatically stop or reverse the propagation of the network worms after the worms are identified.



FUTURE WORK

• To explore the generality of our approach we intend to develop and implement case studies for a variety of challenges including malicious (e.g. Botnets) and non-malicious (e.g., faults and router misconfigurations) challenges

• Evaluate the benefits of this approach

• Develop formal models of challenges, which can then be mapped onto policy-based detection algorithms

THIS RESEARCH IS SPONSORED BY