CENTRE FOR
DOCTORAL TRAINING
in CYBER SECURITY

UNIVERSITY OF
OXFORD

EPSRC
Engineering and Physical Sciences
Research Council

CED3: Comparative Evaluation of DDoS Defences

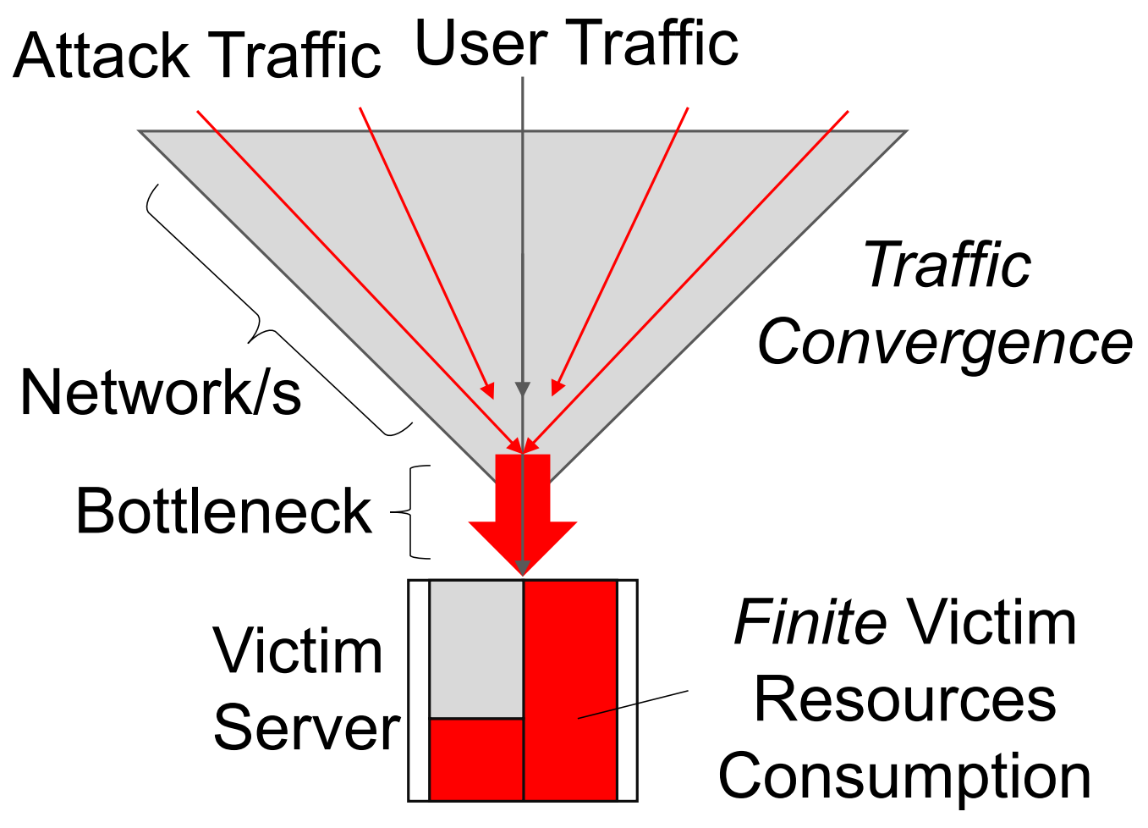
CED3 (Comparative Evaluation of DDoS Defences) is an evaluation method that aims to capture the usefulness of DDoS defenses in a way that is attacker-agnostic and allows defences to be objectively compared; thus addressing issues identified in the literature whereby defences shown to be effective would later be deemed ineffective, and where diversity of validation techniques made comparison infeasible. Success in this area would help organizations to make better decisions on which solutions to adopt, as well as facilitate collaborative selection of global solutions for the improved resilience and security of Internet infrastructure.

Author: ***Andikan Otung*** ***andikan.otung@cs.ox.ac.uk***

Scope & Foundations

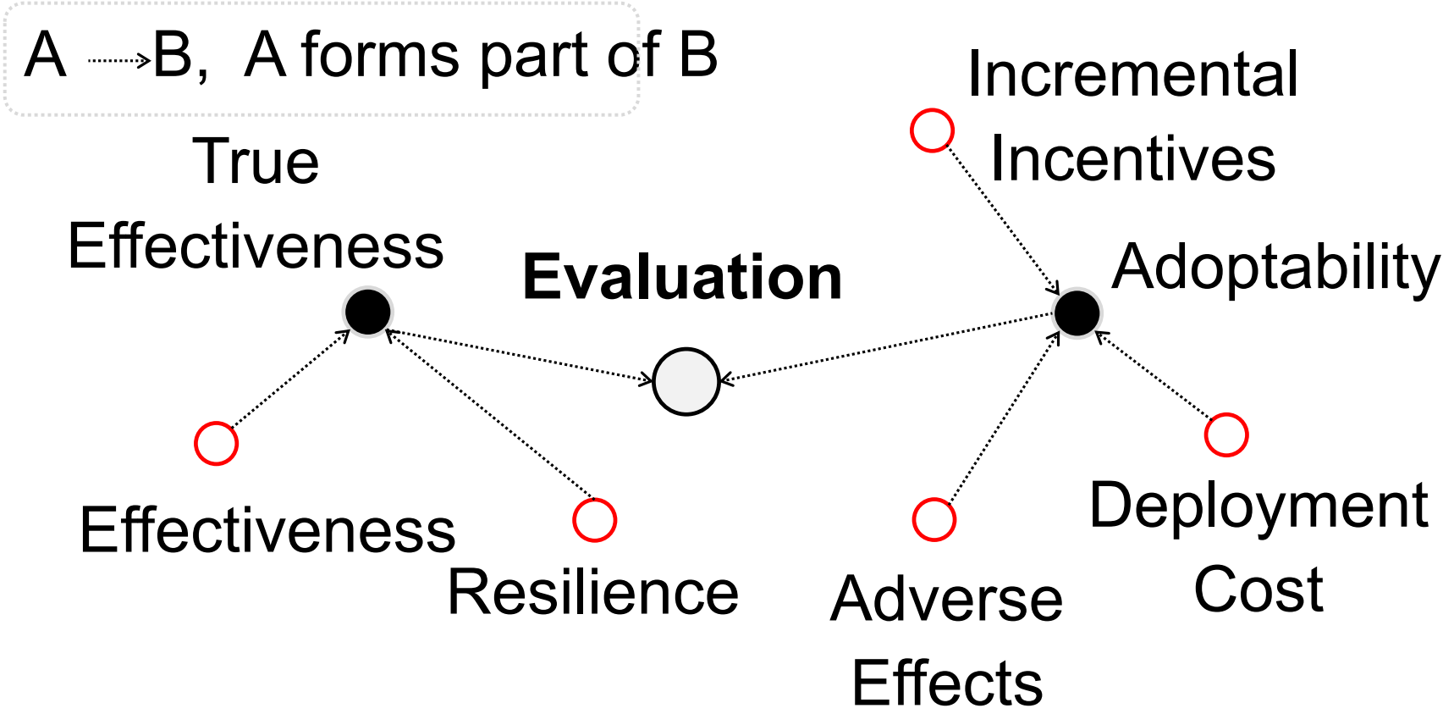
Since victim resources are finite, increasing attack strengths, which increase malicious resource consumption, eventually deprive the victim's clients of necessary resources to receive service. Thus we form the postulate of **Inevitable Theoretical Subversion**:

Any DDoS defence technique is theoretically surmountable by an attacker

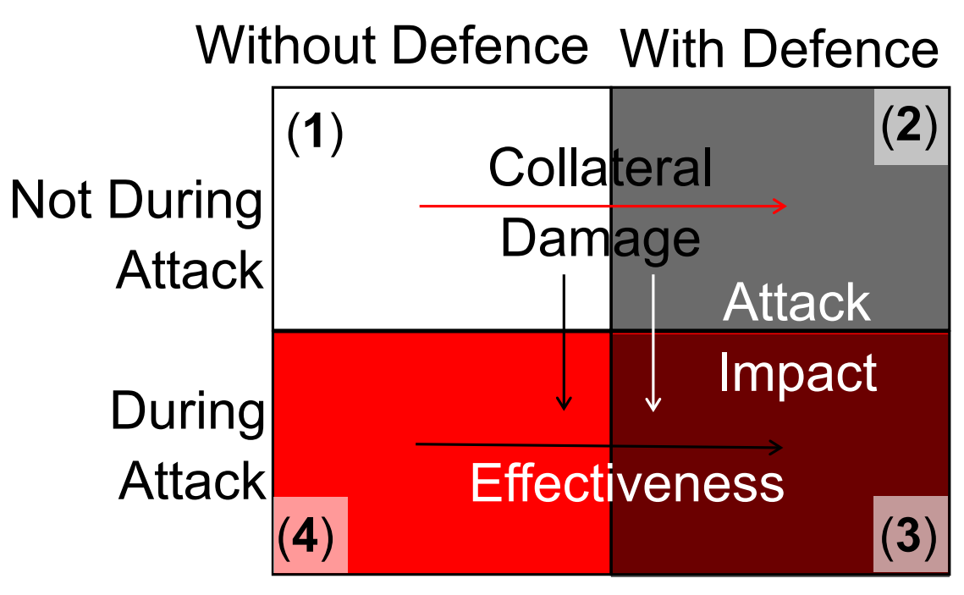


This postulate extends the paradigm of defence effectiveness evaluation from assessment of how well a defence would work, to consideration of what it would take to overcome it. Therefore we consider that:

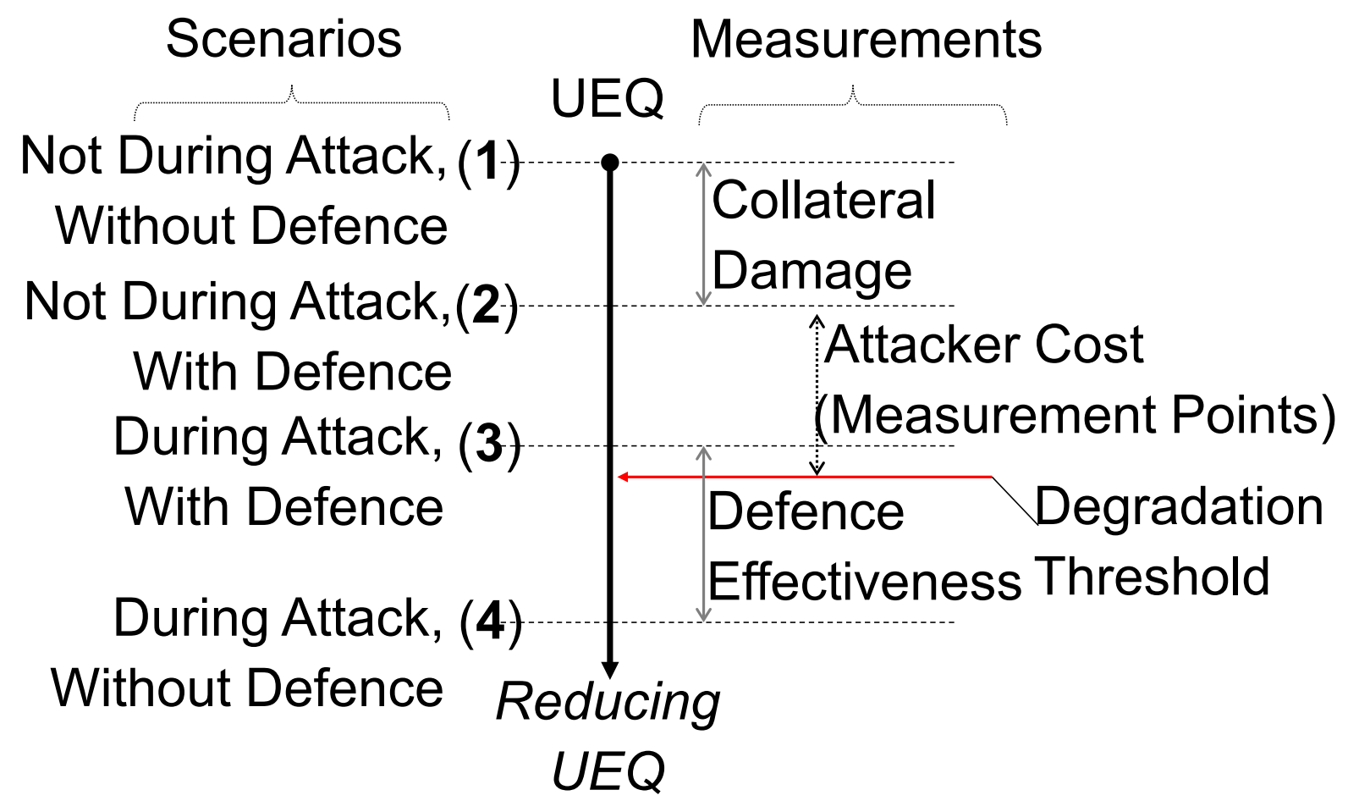
any truly representative measure of the effectiveness of a DDoS defence must incorporate the difficulty and or cost to the attacker in overcoming the defence.



We name this characteristic **True Effectiveness** and it forms a key part of the comprehensive evaluation outputs illustrated. The effectiveness **ε** of a defence and its collateral damage are empirically obtained by contrasting the difference between the user-experienced quality of service (UEQ) from the different test scenarios illustrated. Degradation in UEQ is captured by measuring changes in delay, jitter, packet loss and transaction time.

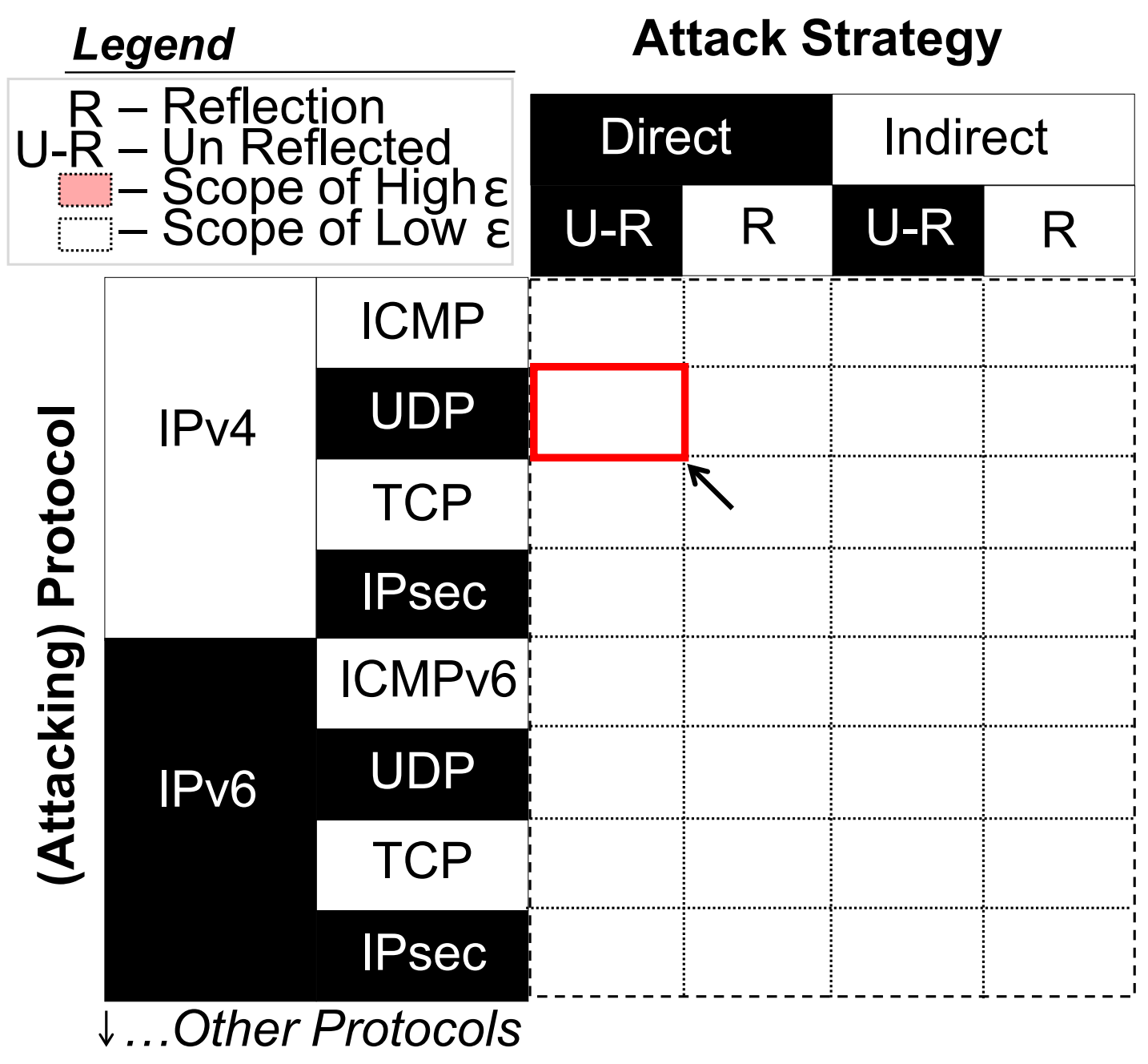


Of the four categories of DDoS defence techniques (alleviation, resource enlargement, vulnerability reduction and defence by offence) CED3 is applicable to all whose real-time in-attack impact can be measured. Therefore techniques that prevent attacks from occurring, such as deterrence, lie out of scope.


Scenarios
UEQ
Measurements
Not During Attack, Without Defence (1)
Not During Attack, With Defence (2)
During Attack, With Defence (3)
During Attack, Without Defence (4)
Collateral Damage
Attacker Cost (Measurement Points)
Defence Effectiveness
Degradation Threshold
Reducing UEQ

Defence Map

The CED3 defence map presents the true effectiveness of a defence in the context of the landscape of possible attacks that affect it. The map achieves this via a simple taxonomy of attributes that enable distinction between attack-types. Outlined on the map is the section under which the 3 defences were simulated. The value entered on the map would be the change in lowest cost for an attacker to cross the UEQ threshold when the defence is deployed compared to when no defence is deployed.


Legend

R – Reflection
U-R – Un Reflected
🟥 – Scope of High ε
□ – Scope of Low ε

Attack Strategy

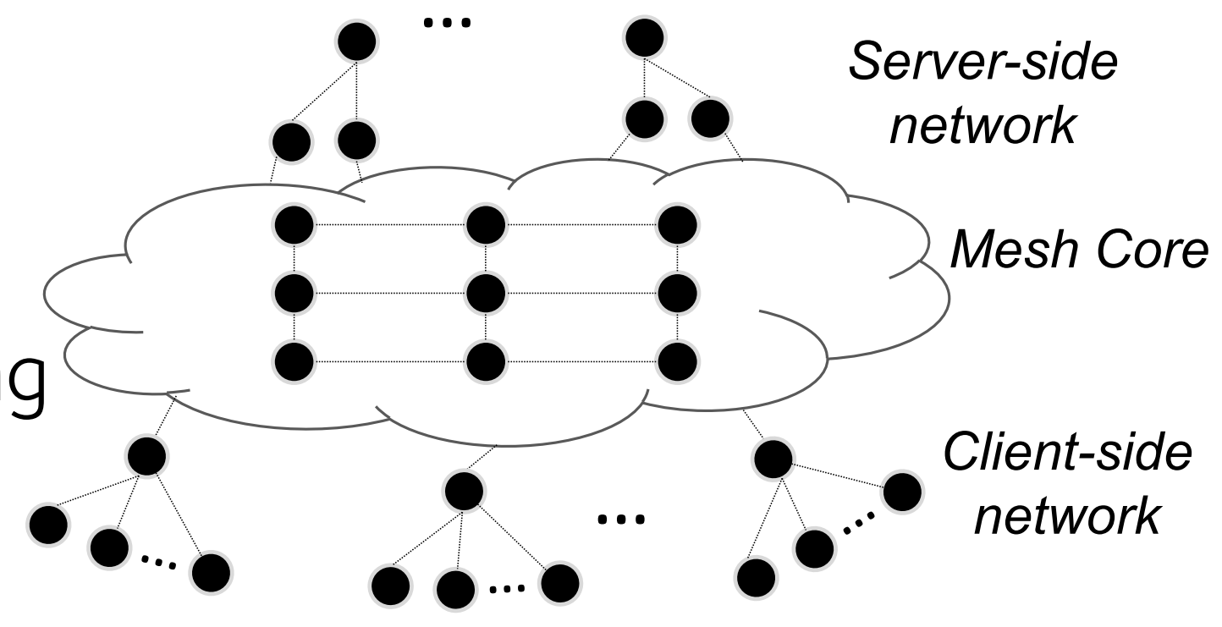
(Attacking) Protocol		Direct		Indirect	
		U-R	R	U-R	R
IPv4	ICMP				
	UDP				
	TCP				
	IPsec				
IPv6	ICMPv6				
	UDP				
	TCP				
	IPsec				

↓ *…Other Protocols*

Conclusions

From the created postulates, the CED3 method was successfully used to compare the true effectiveness of the 3 defences: Passport, TrustGuard and Increasing the Victim Capacity. By considering the lowest cost for an attacker to effect DoS, CED3 was able to identify *doubling the victim capacity* as the most effective defense mechanism under the conditions tested. CED3 demonstrates the value in using theoretical analysis to drive empirical data acquisition in order to support objectivity in DDoS defence evaluation.

Experiment

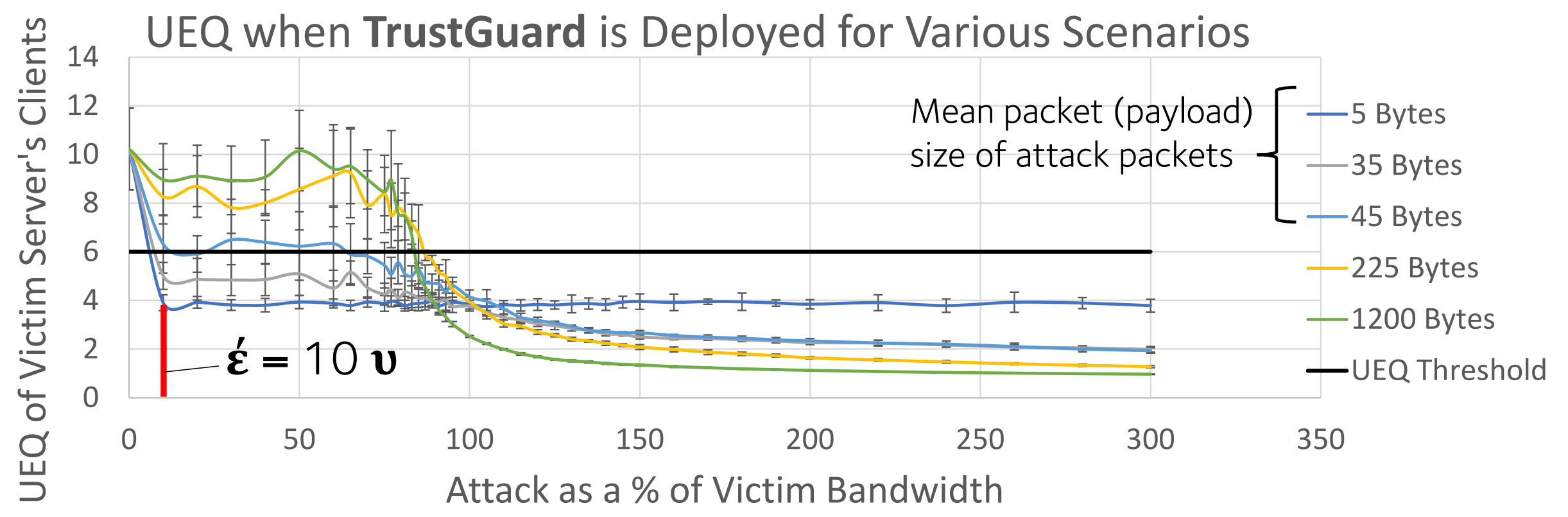


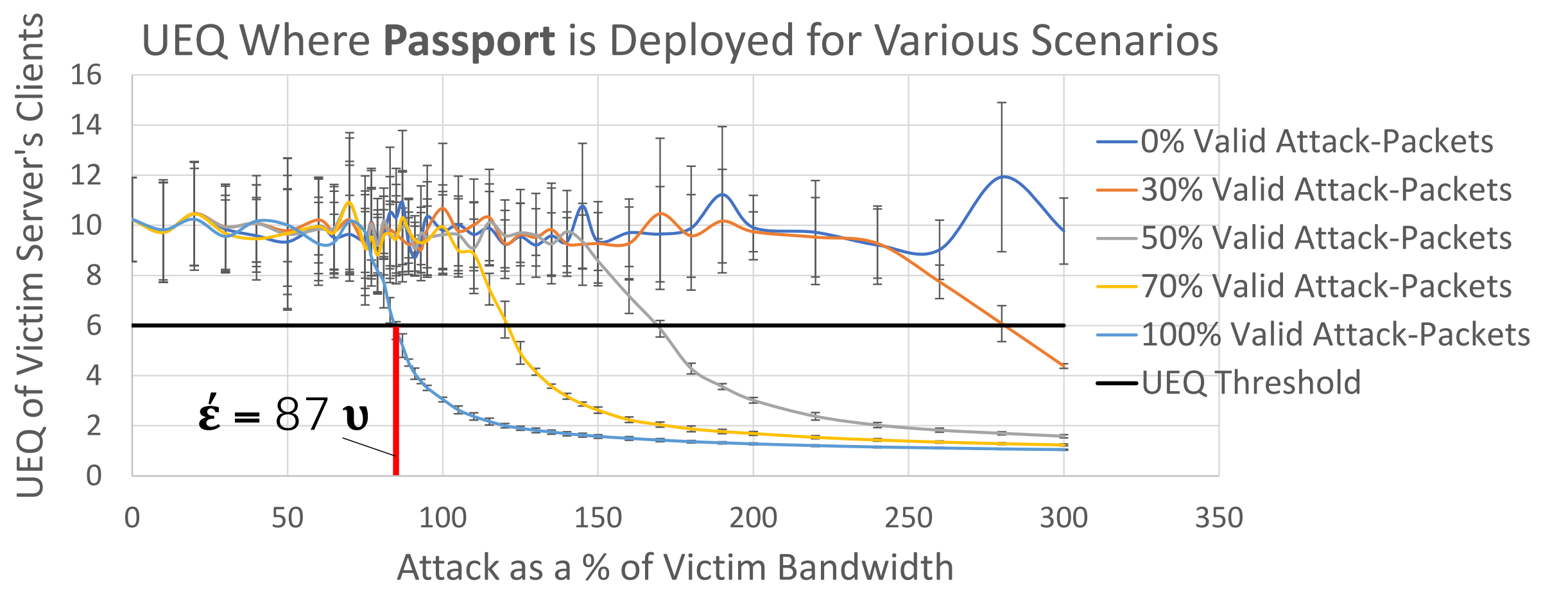
The CED3 method was applied to three DDoS defences: *Passport*, *TrustGuard* and increasing the victim capacity. A network topology of more than 500 nodes was constructed in C++ using the NS3 software, with a mix of benign UDP and TCP traffic flows between 10 servers. Thousands of scenarios were run on a computing cluster * taking hundreds of thousands of CPU hours to complete. Each defence was tested under attacks of increasing strength, in addition to an attribute of the attacker – that the particular defence under test is sensitive to (packet size for TrustGuard and % of valid packets for Passport) – being adjusted. For a each scenario, the UEQ of users of the victim server, φ_V^n was given by the equation:

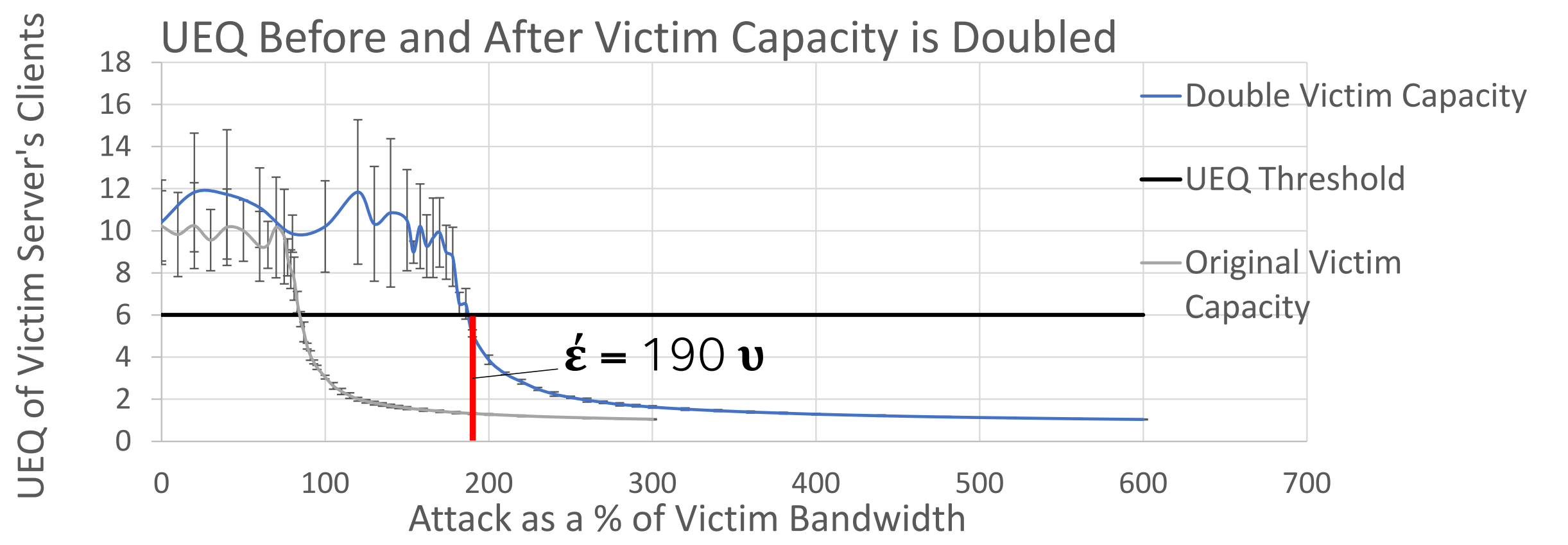
$$\varphi_V^n = \frac{K_1}{a_L\overline{\boldsymbol{\mu}_L^n} + a_D\overline{\boldsymbol{\mu}_D^n} + a_J\overline{\boldsymbol{\mu}_J^n} + a_T\overline{\boldsymbol{\mu}_T^n} + K_2}$$

The multiplicand $\overline{\boldsymbol{\mu}_X^n}$ represents the mean of the measured metric x, in the n'th quadrant, where x is either L, D, J or T; denoting: loss, delay, jitter or transaction time. The multipliers of the form a_X are coefficients and K_1 and K_2 are constants. The $\overline{\boldsymbol{\mu}_X^n}$ values were measured in quadrant (3) but were expressed as % changes from their respective (D, J or T) values in quadrant (1), where quadrant (n) refers to a labelled section in the diagram on the left.

Results







The true effectiveness (ἑ) of these defences is the cost associated with the lowest attack size required to take the UEQ below the threshold. These costs are marked on the diagrams in *attack units* (υ), and assume a trivial cost for an attacker to set its packet size and packet validity.

*Richards, Andrew. (2015). University of Oxford Advanced Research Computing. Zenodo.10.5281/zenodo.22558