

## Proposta para Dissertação de Mestrado em Engenharia Informática

### Título:

Deteção de Ataques do Tipo Low-rate Distributed Denial of Service Usando a Divergência de Kullback-Leibler

### Orientador:

Mário Freire (email: [mario@di.ubi.pt](mailto:mario@di.ubi.pt); página web: <http://www.di.ubi.pt/~mario/>)

### Sumário

Os ataques avançados de Distributed Denial of Service (DDoS) do tipo low-rate, que tentam imitar comportamentos de utilizadores legítimos, constituem uma das principais ameaças para aplicações, podendo ter um impacto significativo no negócio de uma empresa que se baseie o seu negócio na Web. Nesta dissertação pretende-se desenvolver um método para deteção de ataques avançados do tipo low rate usando a divergência de Kullback-Leibler.

### Objetivos

O principal objetivo desta dissertação consiste na definição e implementação de um método para deteção de ataques avançados do tipo low rate usando a divergência de Kullback-Leibler. O desempenho do método implementado deve ser avaliado experimentalmente, em termos de precisão e de consumo de recursos de computação, recorrendo a um trace de tráfego contendo ataques avançados DDoS do tipo low-rate.

### Tarefas a Realizar

São propostas as seguintes tarefas para a execução do trabalho de investigação e de desenvolvimento, conducente à elaboração da dissertação de mestrado:

- Tarefa 1. Estudo dos principais conceitos subjacentes à deteção de ataques do tipo Distributed Denial of Service e levantamento do estado da arte na deteção de ataques avançados do tipo Distributed Denial of Service.
- Tarefa 2. Estudo e comparação dos métodos existentes para deteção de ataques do tipo low-rate DDoS.

- Tarefa 3. Especificação e implementação de um método para deteção de ataques avançados do tipo low rate usando a divergência de Kullback-Leibler.
- Tarefa 4. Execução de testes e validação experimental do método implementado para deteção de ataques avançados do tipo low rate usando a divergência de Kullback-Leibler.
- Tarefa 5. Avaliação experimental do desempenho do método implementado, em termos de precisão e de consumo de recursos de computação, recorrendo a um trace de tráfego contendo ataques avançados do tipo low-rate DDoS.
- Tarefa 6. Escrita de um artigo científico sobre o trabalho de investigação realizado e escrita da dissertação de mestrado.

### Cronograma

A tabela seguinte representa a calendarização prevista para a execução das tarefas, em que a execução de uma dada tarefa num determinado mês é assinalada com um x.

Tarefa/mês	Set 18	Out 18	Nov 18	Dez 18	Jan 19	Fev 19	Mar 19	Abr 19	Mai 19	Jun 19
Tarefa 1	x									
Tarefa 2		x								
Tarefa 3			x	x						
Tarefa 4					x					
Tarefa 5						x	x			
Tarefa 6								x	x	x