Network Security

Ex. 1

**CensorSpoofer**

**Article Report**

Ron Meiry 301224283   
Slava Ustinov 309930006

Contents

[Article Summary 2](#_Toc388002863)

# Article Summary

## Introduction

In the past decade, the Internet was used extensively by independent users and groups as a platform for protest and organization against oppressive governments.

These events have caused such governments, China for example, to enforce a strong censorship policy against web-sites or services that were used extensively by protesters, such as Twitter and Facebook, to share ideas that are contrary to the government's political views.

## Goal

The article proposes a new scheme to allow users access to restricted web-sites, while remaining undetected by an attacker, which is an oppressive government in our case.

## Attacker Model

Our model adversary is of government level, meaning it has all plausible capabilities:

1. Full control over the network's infrastructure.
2. Ability to perform DPI, DNS hijacking, IP filtering and Packet injection.

Though our adversary is powerful, it's not omnipotent. For example, it's very unlikely that he's able to crack a modern day encryption (such as AES, RSA, etc.).