Adversarial Neural Networks in Traffic Obfuscation

Steven R. Sheffey
Middle Tennessee State University

Ferrol Aderholdt
Middle Tennessee State University

Abstract

We live in a society. Gamers rise up! Israel will no longer oppress us.

1 Introduction

Internet censorship is bad

The TOR network helps circumvent internet censorship

Internet censors block tor

Pluggable transports, such as Meek hide tor traffic as benign-looking HTTPS traffic

However, this obfuscated traffic is easily identifiable through machine learning attacks on traffic patterns

2 Background

Censors block tor

tor introduced pluggable transports to disguise tor traffic to make it harder to block

Meek, one of these transports hides TOR traffic inside the encrypted payload of an HTTPS connection, using a technique known as domain fronting

Wang et al differentiated Meek traffic from HTTPs traffic by using machine learning algorithms on traffic pattern statistics

Obfuscating Meek traffic in a way that is resilient to these techniques remains an open problem

3 Related Work

foo

4 Methods

foo

5 Results

foo

6 Conclusions

foo

7 Availability

The traffic generation framework, feature extractor, and machine learning code for this work is open source, and can be accessed at `https://github.com/starfys/packet_captor_sakura`