Outside the Closed World: On Using Machine Learning For Network Intrusion Detection

Robin Sommer[1] Vern Paxson[2]

[1]International Computer Science Institute, and
Lawrence Berkeley National Laboratory

[2]International Computer Science Institute, and
University of California, Berkeley

Presented by Dylan Bersans

Novosibirsk State University
*THE REAL SCIENCE

Table of Contents I

Novosibirsk State University
*THE REAL SCIENCE

Table of Contents II

Novosibirsk State University
*THE REAL SCIENCE

Table of Contents

Novosibirsk State University
*THE REAL SCIENCE

Introduction

Figure: Amazon Logo

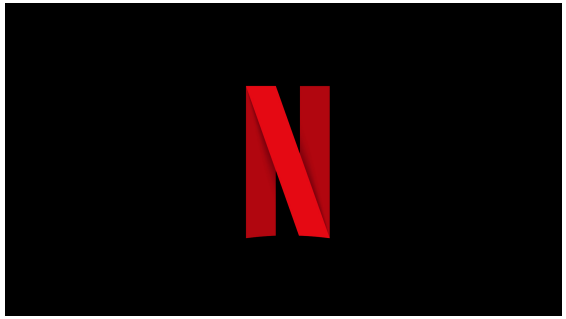

Figure: Netflix Logo

Figure: Natural Language procesing

Figure: Spam

Novosibirsk State University
*THE REAL SCIENCE

Table of Contents

Novosibirsk State University
*THE REAL SCIENCE

Machine learning in intrusion detection

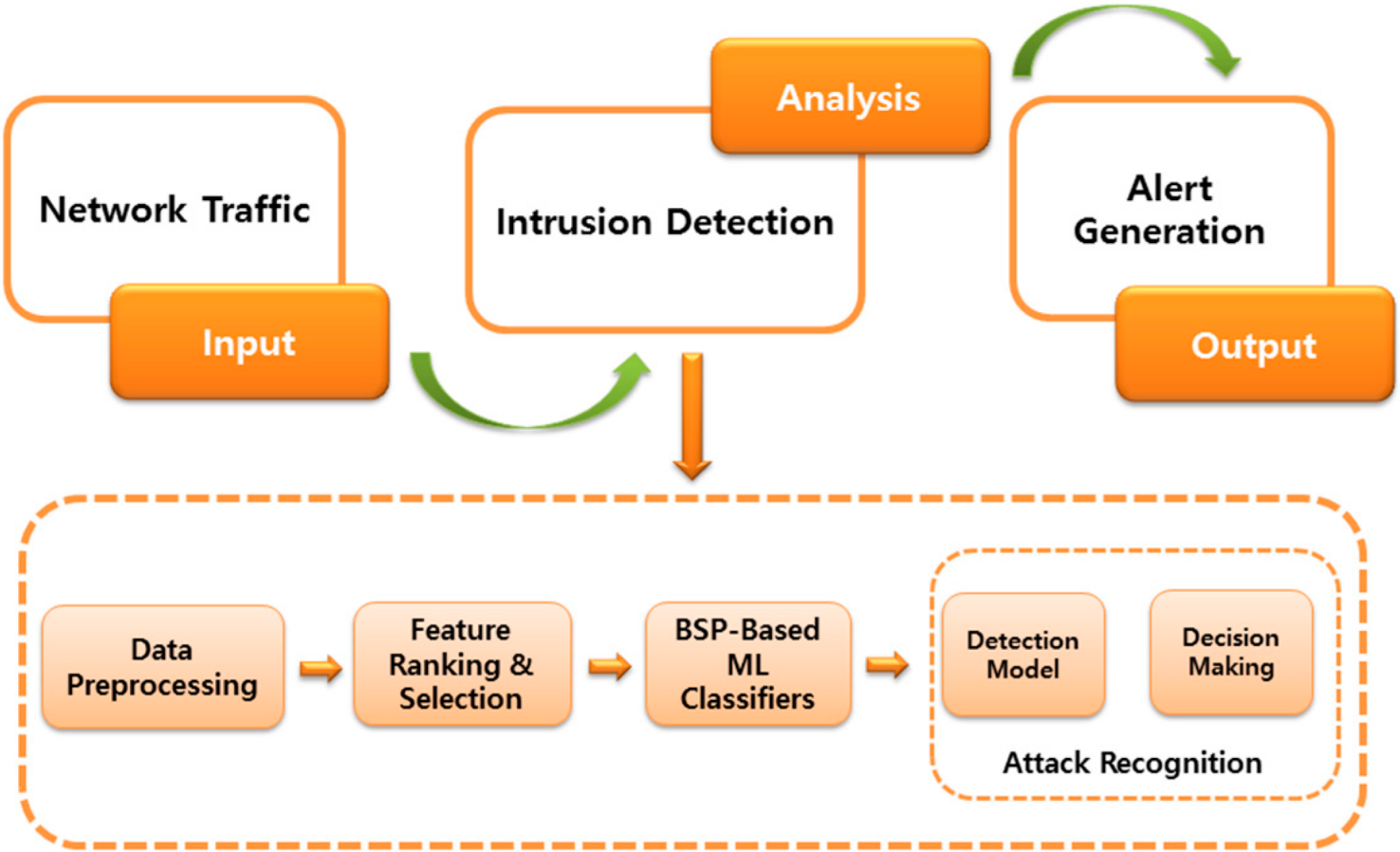

Figure: Machine Learning

Novosibirsk State University
*THE REAL SCIENCE

Table of Contents

Challenges of using machine learning

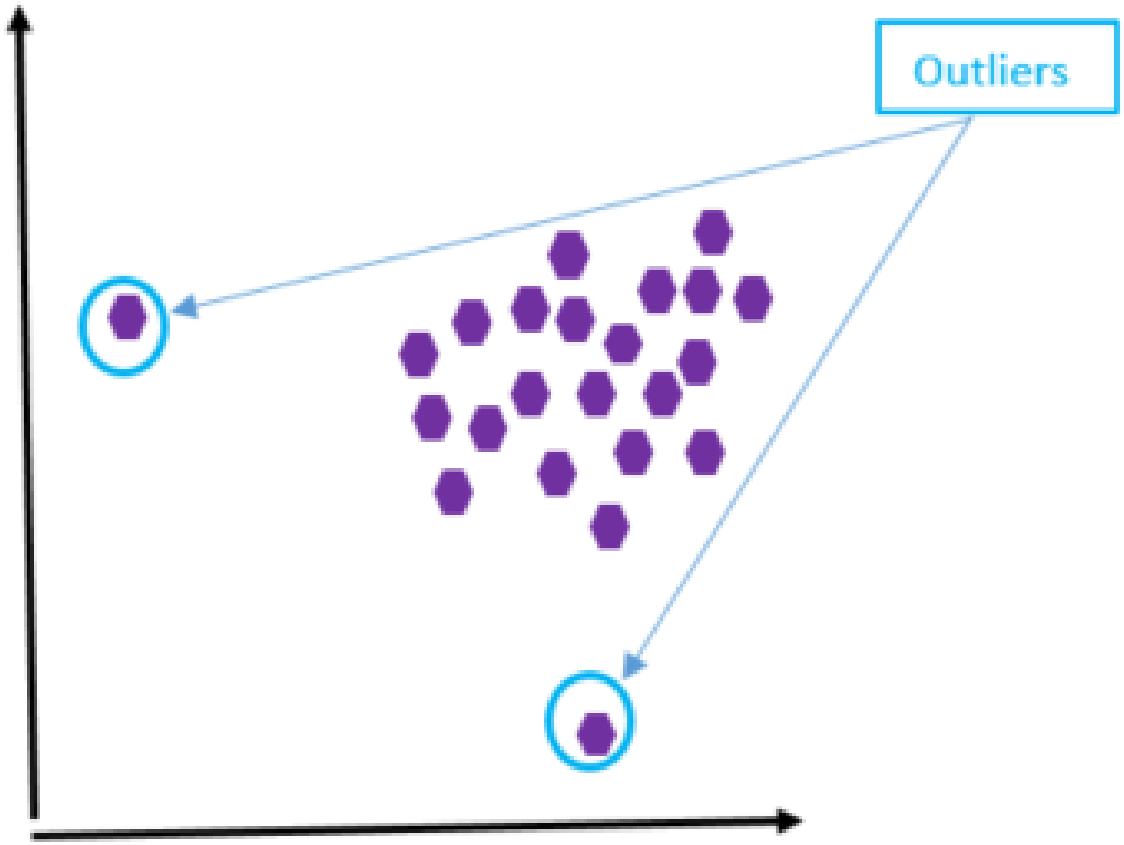

Figure: Outliers

Novosibirsk State University
*THE REAL SCIENCE

High Cost of errors

Figure: Error Cost

Novosibirsk State University
*THE REAL SCIENCE

Semantic Gap

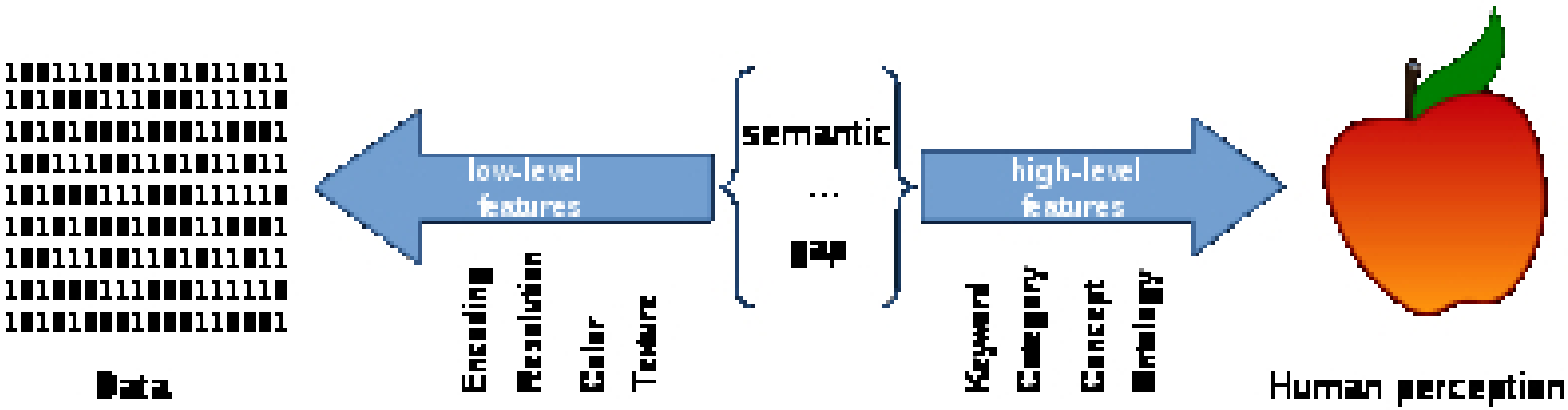

Figure: Semantic Gap

Diversity of network Traffic

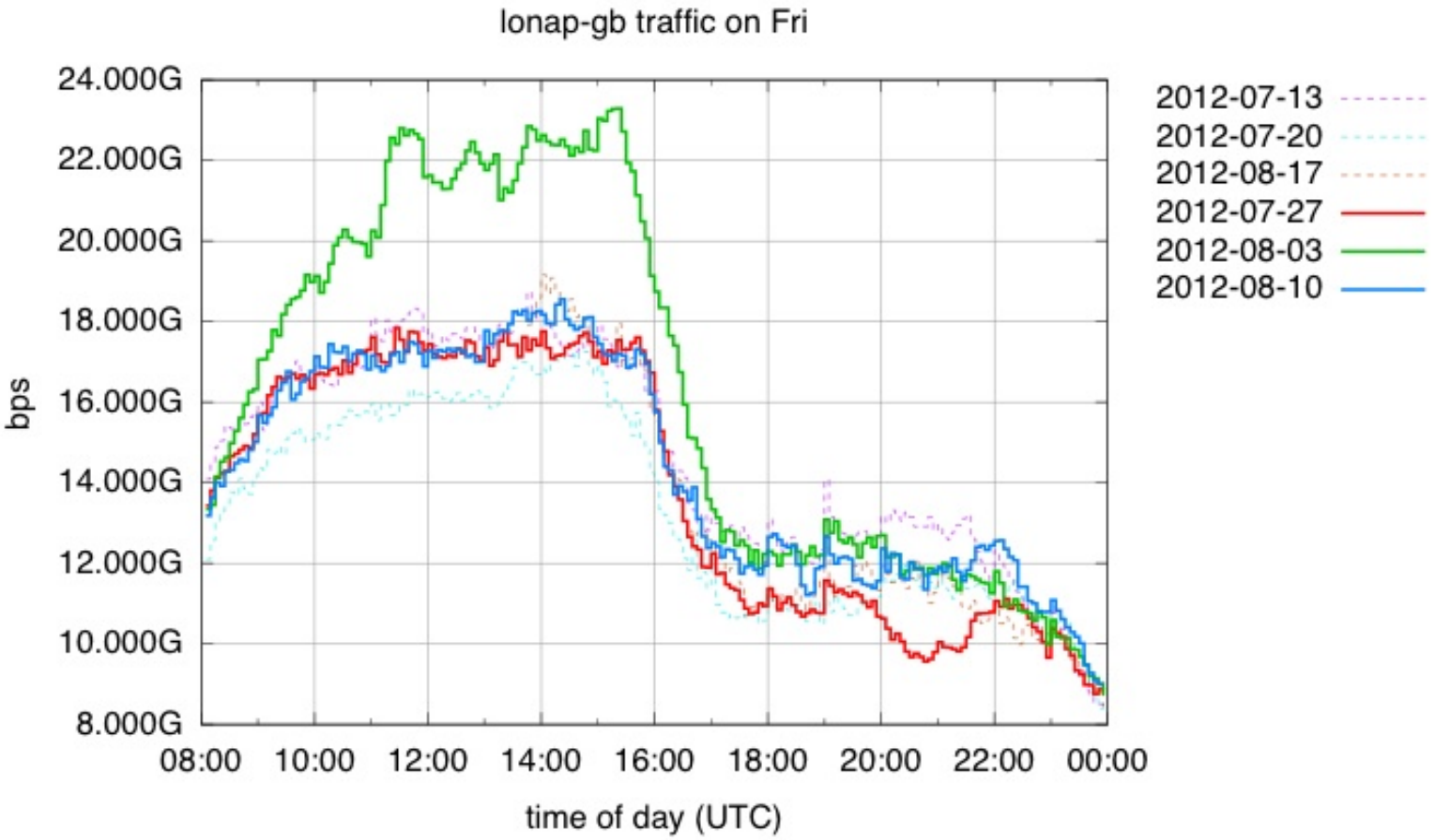

Figure: Network Traffic

Novosibirsk State University
*THE REAL SCIENCE

Table of Contents

Novosibirsk State University
*THE REAL SCIENCE

Table of Contents

Novosibirsk State University
*THE REAL SCIENCE