

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

Robin Sommer¹ Vern Paxson²

¹International Computer Science Institute, and
Lawrence Berkeley National Laboratory

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

Presented by Dylan Bersans

Table of Contents I

- 1 Introduction
- 2 Machine learning in intrusion detection
- 3 Challenges of using machine learning
 - Outlier Detection
 - High Cost of errors
 - Semantic gap
 - Diversity of network Traffic
 - Difficulties with Evaluation
 - Difficulties of data
 - Mind the gap
 - Adversarial Setting

4 Recommendations for using machine learning

- Understanding the Threat Model
- Keeping the scope Narrow
- Reducing the costs
- Evaluation
 - Working with data
 - Understanding results

5 Conclusion

Table of Contents

- 1 Introduction
- 2 Machine learning in intrusion detection
- 3 Challenges of using machine learning
- 4 Recommendations for using machine learning
- 5 Conclusion



Figure: Amazon Logo



Figure: Netflix Logo



Figure: Natural Language processing



Figure: Spam

Table of Contents

- 1 Introduction
- 2 Machine learning in intrusion detection
- 3 Challenges of using machine learning
- 4 Recommendations for using machine learning
- 5 Conclusion

Machine learning in intrusion detection

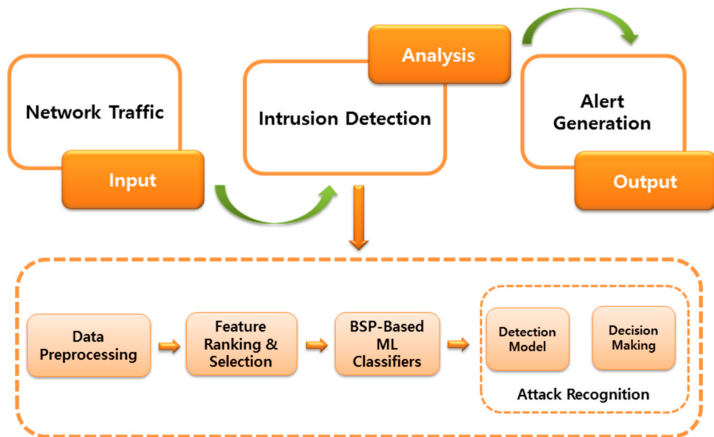


Figure: Machine Learning

Table of Contents

- 1 Introduction
- 2 Machine learning in intrusion detection
- 3 Challenges of using machine learning**
 - Outlier Detection
 - High Cost of errors
 - Semantic gap
 - Diversity of network Traffic
 - Difficulties with Evaluation
- 4 Recommendations for using machine learning
- 5 Conclusion

Challenges of using machine learning

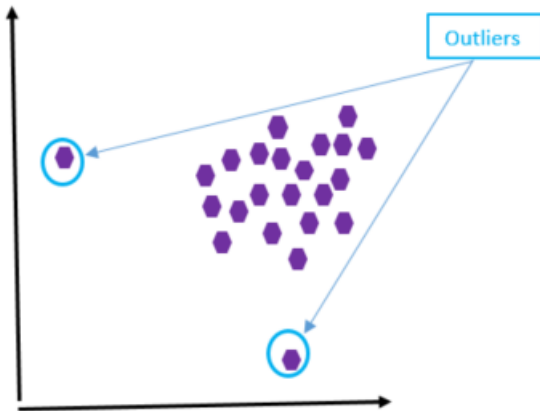


Figure: Outliers

High Cost of errors



Figure: Error Cost

Semantic Gap

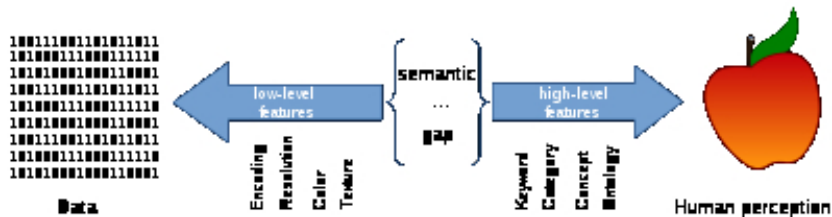


Figure: Semantic Gap

Diversity of network Traffic

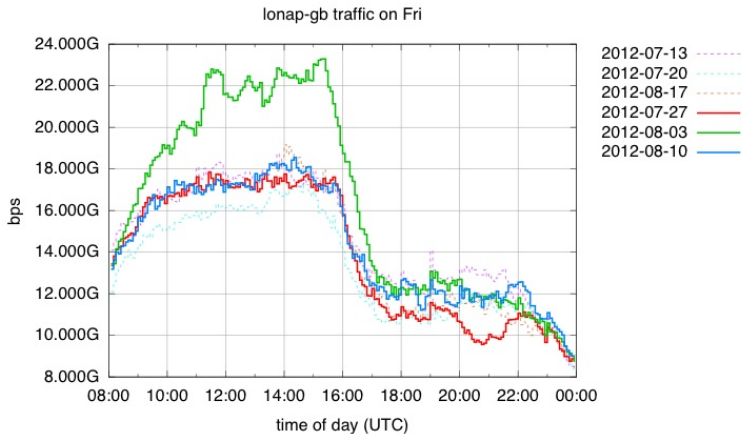


Figure: Network Traffic

Table of Contents

- 1 Introduction
- 2 Machine learning in intrusion detection
- 3 Challenges of using machine learning
- 4 Recommendations for using machine learning
 - Understanding the Threat Model
 - Keeping the scope Narrow
 - Reducing the costs
 - Evaluation
- 5 Conclusion

Table of Contents

- 1 Introduction
- 2 Machine learning in intrusion detection
- 3 Challenges of using machine learning
- 4 Recommendations for using machine learning
- 5 Conclusion