MOTCHEBOUNG MOTCHEBONHE Félicien

MARAH NANA AWA

<< Machine Learning Methods for Computer Security>>

1. Introduction

1.1. Context

The emergence of the internet has changed the way we do things (business, personal live, communication …). Basing on data analysis and underlying methods of machine learning, the Internet generate enormous amount of data used for some system like Online advertisement, recommendation systems, consumer profiling and many others.

Unfortunately, the Internet is subjected to acts of abuse and cybercrime based on security breaches. These hackers operate in a stealth manner which increases the pressure of cyber security providers who must react to attacks to ensure the security of systems by using data-analysis technique to extract suspicious information in huge amounts of data. Their success will thus lead to the detection of the intrusions, which will cause the pirate to develop a new mechanism to escape this detection

It creates a game of cat and mouse between security companies and hackers, which raises the fundamental problem of what data analysis and machine learning techniques were originally conceived in the idea of faithful data and did not explicitly give information In the case of an attack by hackers. In addition, many studies show that data security instruments can be easily broken, thus raising the question of whether machine learning methods can be deployed at all in adversarial environments?.

1.2. Background

We are going to give an overview of Machine Learning

Machine learning is a method of data analysis that automates analytical model building. Using algorithms that iteratively learn from data, machine learning allows computers to find hidden insights without being explicitly programmed where to look.

Importance

Resurging interest in machine learning is due to the same factors that have made data mining and Bayesian analysis more popular than ever. Things like growing volumes and varieties of available data, computational processing that is cheaper and more powerful, and affordable data storage.

All of these things mean it's possible to quickly and automatically produce models that can analyze bigger, more complex data and deliver faster, more accurate results – even on a very large scale. And by building precise models, an organization has a better chance of identifying profitable opportunities – or avoiding unknown risks.

Evolution of machine learning

Because of new computing technologies, machine learning today is not like machine learning of the past. It was born from pattern recognition and the theory that computers can learn without being programmed to perform specific tasks; researchers interested in artificial intelligence wanted to see if computers could learn from data. The iterative aspect of machine learning is important because as models are exposed to new data, they are able to independently adapt. They learn from previous computations to produce reliable, repeatable decisions and results. It’s a science that’s not new – but one that’s gaining fresh momentum.

While many machine learning algorithms have been around for a long time, the ability to automatically apply complex mathematical calculations to big data – over and over, faster and faster – is a recent development. Here are a few widely publicized examples of machine learning applications you may be familiar with:

- The heavily hyped, self-driving Google car? The essence of machine learning.
- Online recommendation offers such as those from Amazon and Netflix? Machine learning applications for everyday life.
- Knowing what customers are saying about you on Twitter? Machine learning combined with linguistic rule creation.
- Fraud detection? One of the more obvious, important uses in our world today.

Who's using it?

Most industries working with large amounts of data have recognized the value of machine learning technology. By gleaning insights from this data – often in real time – organizations are able to work more efficiently or gain an advantage over competitors.

- **Financial services:** Banks and other businesses in the financial industry use machine learning technology for two key purposes: to identify important insights in data, and prevent fraud. The insights can identify investment opportunities, or help investors know when to trade. Data mining can also identify clients with high-risk profiles, or use cyber surveillance to pinpoint warning signs of fraud.
- **Government**: Government agencies such as public safety and utilities have a particular need for machine learning since they have multiple sources of data that can be mined for insights. Analyzing sensor data, for example, identifies ways to increase efficiency and save money. Machine learning can also help detect fraud and minimize identity theft.
- **Health care**: Machine learning is a fast-growing trend in the health care industry, thanks to the advent of wearable devices and sensors that can use data to assess a patient's health in real time. The technology can also help medical experts analyze data to identify trends or red flags that may lead to improved diagnoses and treatment.
- **Marketing and sales** : Websites recommending items you might like based on previous purchases are using machine learning to analyze your buying history – and promote other items you'd be interested in. This ability to capture data, analyze it and use it to personalize a shopping experience (or implement a marketing campaign) is the future of retail.
- **Oil and gas**: Finding new energy sources. Analyzing minerals in the ground. Predicting refinery sensor failure. Streamlining oil distribution to make it more efficient and cost-effective. The number of machine learning use cases for this industry is vast – and still expanding.
- **Transportation**: Analyzing data to identify patterns and trends is key to the transportation industry, which relies on making routes more efficient and predicting potential problems to increase profitability. The data analysis and modeling aspects of machine learning are important tools to delivery companies, public transportation and other transportation organizations

1.3. Problem and research questions

The problem is based on the following questions **whether machine learning methods can be deployed at all in adversarial environments? How to develop learning algorithms with provable security guarantees?**

2. Related works

3. Methodology employed

This paper present the solution of the problem in three themes. The first theme is Machine learning for security where the author present the security problems that can machine learning best help to solve and other scenario they are ill-suited for. He present also many other scientific and operational issues. The second theme is secure machine learning, where he presents the theorical limitations of worst case attacks against learning algorithms under different constraints and how can these constraints be used in practice for protecting learning methods against adversarial data. And the third theme is Future Applications of Secure Learning where the author present applications where learning techniques are used and can potentially be exposed to adversarial data and what experience from these applications can be used for development of general methodology of secure learning.

4. Results found and Perspectives

We are going to present results of this paper in the three themes mentioned.

In the first theme, Machine learning for security, the author present the security problems that can machine learning best help to solve and other scenario they are ill-suited for.

For the author the classical security application of machine learning is detection of malicious activity in operating systems data or network traffic: “intrusion detection systems”. Some work in intrusion detection followed learning approaches like anomaly detection, rule inference and supervised learning. The limited use of learning-based methods in the general intrusion detection context is the necessity for a precise focus on the semantics of specific applications. For example in the case of web application security. Due to their versatility, it is next to impossible to devise signatures for specific attack patterns. However, learning systems overcome this difficulty by automatically inferring models of benign application-specific traffic. Such models can be used to detect malicious web queries, to detect logical state violations in web applications, and even to develop reactive mechanisms such as reverse proxies or the sanitization of web queries. Another crucial contribution of learning-based systems lies in the realm of dynamic malware analysis. To acquire novel malware, most anti-virus vendors deploy sophisticated systems which, for such of them, have been successful in collecting masses of data, resulting in an urgent need for tools to automatically analyze novel malware. So, one of the first methods for malware analysis based on reports from its execution in a sandbox used hierarchical clustering to infer groups of related malware. Another approach based on supervised learning enabled classification of malware into known families as well as detection of novel malware strains. Subsequent research has improved scalability of the above mentioned methods and verified their feasibility for large-scale malware attribution. The synergy between machine learning and malware analysis has been exploited for automatic signature generation (ASG). However, the key weakness of such methods was their susceptibility to attacks, which made it possible to evade a deployed system or increase its false alarm rate. JavaScript is also used for detection of drive-by-downloads and malicious non-executable files. Static analysis of JavaScript token sequences has been successfully deployed for detection of drive-by-downloads and JavaScript-bearing malicious PDF documents. Another form of static analysis with a focus on PDF document structure was instrumental in recently developed highly effective methods for detection of PDF malware. Dynamic analysis of JavaScript string allocations combined with classification of string payloads has been successfully used for in-browser detection of drive-by-downloads.

The author present at the end of the first theme some open issues and future research directions for machine learning for security:

- Integration of machine learning with security mechanisms
- Reactive approaches
- Machine learning for offensive security

In the second theme, secure machine learning, the author presents the theorical limitations of worst case attacks against learning algorithms under different constraints and how can these constraints be used in practice for protecting learning methods against adversarial data.

Depending of the part of the data controlled by an attacker, a learning algorithms can present different behavior. Some of them can be surprisingly tolerant to wrong labels assigned by an attacker during training. On the other hand, by controlling attributes of the data, an attacker can construct inherently difficult learning problems, in which the error rate can be nearly as high as the fraction of data under the attacker's control.

The open issues and research direction of this theme are:

- Formalization of Secure Learning
- Empirical Evaluation
- Development of Secure Learning Approaches
- Data sanitization
- Secure Learning and Data Privacy

The third theme presents the future application where do adversaries attack next. These applications are :

- Spam filtering
- Advertising
- Social media spam
- Plagiarism Detection and Authorship Identification
- Copyright Enforcement
- Computer Vision Systems: Present and Potential Attacks
- Sentiment analysis

5- Most important publication for this work

- Battista Biggio, Blaine Nelson, and Pavel Laskov. Poisoning attacks against Support VectorMachines. In International Conference on Machine Learning (ICML), 2012.
- Cynthia Dwork. Differential privacy. In International Colloquium on Automata, Languages and Programming, Part II (ICALP), pages 1–12, 2006.
- Marius Kloft and Pavel Laskov. Online anomaly detection under adversarial impact. In International Conference on AI and Statistics (AISTATS), pages 405–412, 2010.
- Marius Kloft and Pavel Laskov. Security analysis of online centroid anomaly detection. Journal of Machine Learning Research, 13:3133–3176, 2012.

- Daniel Lowd and Christopher Meek. Adversarial learning. In ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), pages 641–647, 2005.
- Roberto Perdisci, David Dagon, Wenke Lee, Prahlad Fogla, and Monirul Sharif. Misleading worm signature generators using deliberate noise injection. In IEEE Symposium on Security and Privacy, pages 17–31, 2006.