INTELLIGENT DETECTION OF BOTNETS USING MACHINE LEARNING AND DEEP LEARNING

1. The background context

Botnets are one of the most significant cyber threats of our time, capable of hijacking millions of devices to carry out destructive activities such as DDoS attacks, spam campaigns, and identity theft. Traditional signature-based detection systems struggle with identifying new and emerging botnets, leading to a significant gap in network security.

Recent advances in machine learning and deep learning techniques have shown tremendous potential in the field of botnet detection. These techniques can efficiently detect botnets by analyzing large-scale network traffic data and identifying patterns and anomalies associated with botnet activity.

In this context, the focus of this dissertation is to develop an intelligent detection system that uses machine learning and deep learning techniques to detect botnets accurately and in real-time. Our system aims to address the gaps and limitations of the existing botnet detection systems by using advanced machine learning algorithms to decrease false positives and improve detection accuracy. This system's techniques will include deeper neural networks, ensemble learning techniques, and unsupervised learning to detect new and emerging botnet threats.

The potential impact of this work is significant, particularly in the field of IoT security, where the number of connected devices is increasing exponentially. Effective detection of botnets is essential for the security and safety of IoT devices and networks. Therefore, the development of an intelligent botnet detection system that can handle large amounts of data efficiently and identify new and emerging botnet threats can be a significant contribution to the research community and beyond.

2. The objectives of this dissertation:

1. To identify the state-of-the-art techniques and best practices in botnet detection using machine learning and deep learning.

2. To develop an intelligent detection system that uses these techniques to detect botnets.

3. To validate the performance of the system against different types of botnets using simulation and real-world data.

4. To compare the performance of the system against existing detection systems in the market.

5. To critically reflect on the dissertation process and provide recommendations for future research.

3. The methodology:

The methodology followed for detecting botnets in the dissertation would involve the following steps:

1. **Literature review**: The first step would be to conduct a comprehensive literature review to identify the state-of-the-art techniques and best practices in botnet detection using machine learning and deep learning.

2. **Data collection and preprocessing**: The next step would be to create a dataset for training and testing the intelligent detection system. The dataset would be collected from various sources, including real-world botnet data sources and simulations.

3. **Feature extraction**: Feature extraction is the process of selecting and extracting relevant features from the collected dataset. Various machine learning and deep learning techniques would be applied in this step to extract the features that are relevant to detect botnet attacks.

4. **Model development**: The intelligent detection system would be developed using machine learning and deep learning techniques. The models used would be trained on the dataset created in step 2, and the features extracted in step 3.

5. **Performance evaluation**: The performance of the developed models would be evaluated against different types of botnets using simulation and real-world data. Various performance metrics such as precision, recall, and F1-score would be used to evaluate and compare the performance of the system against existing detection systems in the market.

6. **Critical reflection**: The dissertation would end with critical reflection on the dissertation process and recommendations for future research. Potential improvements to the detection system, limitations of the system, and future research directions would be discussed.

4. Special devices and software

A powerful computer system for training machine learning and deep learning models, software for data preprocessing and analysis, and access to real-world botnet data sources. I may need network simulators and botnet generators.

5. What is the new work that we are going to show

The new work that we are going to show in this dissertation is the development of an intelligent detection system that combines machine learning and deep learning techniques to accurately detect and classify botnet attacks in real-time. Our system will outperform existing detection systems in terms of accuracy and efficiency and will be able to identify new and emerging botnet threats.

Furthermore, we aim to demonstrate the effectiveness of our system in handling large amounts of data efficiently while reducing false positive detections. Additionally, we will use ensemble learning techniques and unsupervised learning to detect previously unknown botnet threats, which is a significant improvement over traditional signature-based detection methods. Our system will contribute to the advancement of the field of botnet detection using machine learning and deep learning, particularly in the context of IoT security, where the need for effective detection of botnets is crucial. Ultimately, our work will pave the way for future research that focuses on the development of even more sophisticated botnet detection techniques.