开场

Good morning everyone, I’m 王曦 and this is my team. We’re grateful for the opportunity to present this topic, Intrusion Detection System and Impact of IDS on Humans.

Our world is moving fast towards the era of the Internet of Things (IoT), which connects all kinds of devices to digital services and brings significant convenience to our lives. With the rapid increase in the number of devices connected to the IoT, there may exist more network vulnerabilities, resulting in more network attacks. Under this dynamic IoT environment, an effective intrusion detection system (IDS) is urgently needed to detect attacks with low-latency and high accuracy. To alleviate this problem, a multi-objective evolutionary convolutional neural network(MECNN) was proposed for intrusion detection system, which is run on the fog nodes of Fog computing on IoT.

We skipped the CNN part since people are too familiar with it. In the first part we’ll begin with MECNN. In the second part we’ll introduce Fog Computing. In the third part we’ll talk about Intrusion Detection System. The last part we’ll share our opinions on Impact of IDS on Humans.

Part 4, Impact of IDS on Humans

Positive impact:

1. Real-time monitoring: IDS can monitor network traffic in real-time, allowing for immediate identification and response to potential threats.

2. Early warning: IDS can detect anomalies or patterns indicating a potential attack before it occurs, giving security teams time to prevent or mitigate the threat.

3. Customization: IDS can be customized to fit the specific needs of an organization, allowing them to tailor their security measures to their unique environment and requirements.

4. Reduced risk: By detecting and responding to potential attacks early, IDS can significantly reduce the risk of data breaches, theft, or other cyber-attacks.

5. Compliance: Many industries require compliance with regulatory standards. IDS can help organizations meet these requirements by providing continuous monitoring and alerts in case of suspicious activity.

Negative impact:

1. False positives: IDS may generate false positives, flagging legitimate traffic as potential threats and creating unnecessary alerts that can lead to alert fatigue.

2. Complexity: IDS can be complex to configure and maintain, requiring significant expertise and resources on the part of the organization.

3. Cost: Implementing and maintaining IDS can be expensive, particularly for small or medium-sized organizations with limited budgets.

4. Limitations: IDS rely on pattern matching and signature-based detection techniques, which may limit their ability to detect novel attacks or sophisticated threats.

5. Privacy concerns: IDS may capture and analyze sensitive data, raising concerns about privacy and compliance with data protection laws.