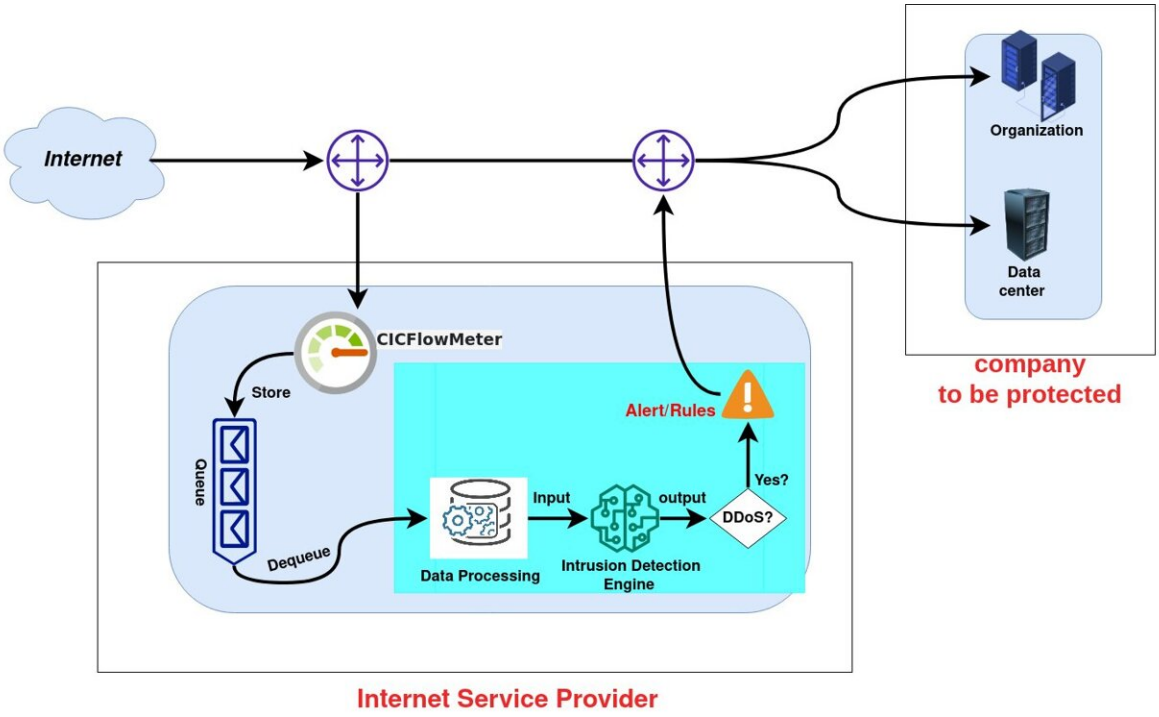
A new AI-based tool to detect DDoS attacks

February 28 2023, by Ingrid Fadelli



IDS deployment on the ISP. Credit: Mustapha et al

Cybercriminals are coming up with increasingly savvy ways to disrupt online services, access sensitive data or crash internet user's devices. A cyber-attack that has become very common over the past decades is the so-called Distributed Denial of Service (DDoS) attack.

This type of attack involves a series of devices connected to the internet,

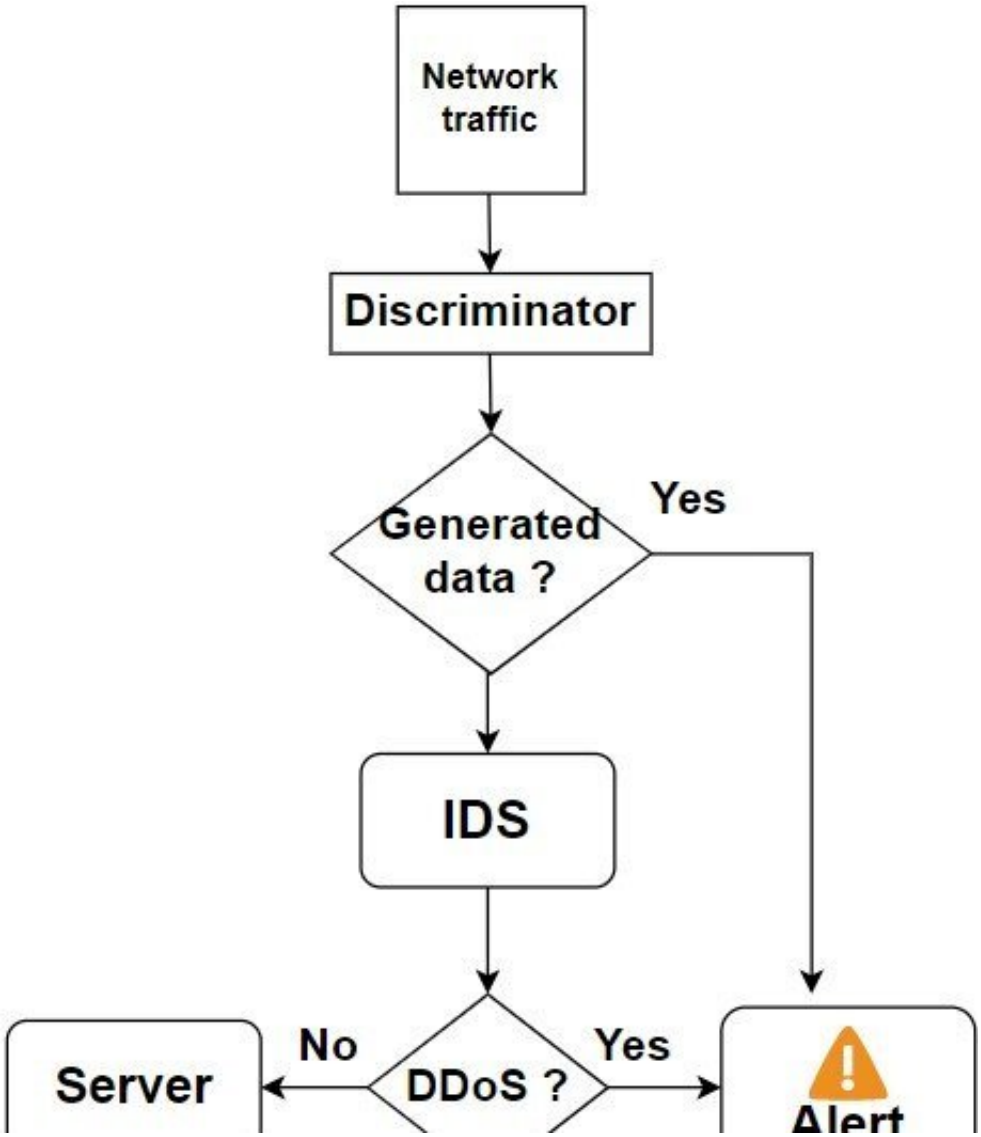
which are collectively referred to as a "botnet." This "group" of connected devices is then used to flood a target server or website with "fake" traffic, disrupting its operation and making it inaccessible to legitimate users.

To protect their website or servers from DDoS attacks, businesses and other users commonly use firewalls, anti-malware software or conventional intrusion detection systems. Yet detecting these attacks can be very challenging today, as they are often carried out using generative adversarial networks (GANs), machine learning techniques that can learn to realistically mimic the activity of real users and legitimate user requests.

As a result, many existing anti-malware systems ultimately fail to secure users against them.

Researchers at Institut Polytechnique de Paris, Telecom Paris (INFRES) have recently developed a new computational method that could detect DDoS attacks more effectively and reliably. This method, introduced in a paper published in *Computers & Security*, is based on a long short-term memory (LSTM) model, a type of recurrent neural network (RNN) that can learn to detect long-term dependencies in event sequences.

"Our research paper was based on the problem of detecting DDoS attacks, a type of cyber-attacks that can cause significant damage to online services and network communication," Ali Mustapha, one of the researchers who carried out the study, told Tech Xplore. "While previous studies have explored the use of deep learning algorithms to detect DDoS attacks, these approaches may still be vulnerable to attackers who utilize machine learning and deep learning techniques to create adversarial attack traffic capable of bypassing detection systems."



IDS model architecture. Credit: Mustapha et al

As part of their study, Mustapha and his colleagues set out to devise an entirely new machine learning–based approach that could improve the resilience of DDoS detection systems. The method they proposed is based on two separate models that can be integrated into a single intrusion detection system.

"The first model is designed to determine whether the incoming network

traffic is adversarial and block it if it is deemed fraudulent," Mustapha explained. "Otherwise, it is then forwarded to the second model, which is responsible for identifying whether it constitutes a DDoS attack. Depending on the outcome of this analysis, a corresponding set of rules and an alert system are employed."

The DDoS detection tool proposed by this team of researchers has numerous advantages over other intrusion detection systems developed in the past. Most notably, it is robust and can detect DDoS attacks with high levels of accuracy, it is adaptable, and it could also be tailored to meet the unique needs of specific businesses or users. In addition, it can be easily deployed by internet service providers (ISPs), while protecting them against both standard and adversarial DDoS attacks.

"Our study yielded several noteworthy results and accomplishments," Mustapha explained. "Initially, we evaluated high-performance models that are trained to identify standard DDoS attacks, testing them against adversarial DDoS attacks generated through Generative Adversarial Networks (GANs). We observed that the models were relatively ineffective at detecting these types of attacks; however, we were able to refine our approach and enhance it to detect these attacks with an accuracy exceeding 91%."

Initial tests conducted by Mustapha and his colleagues yielded very promising results, as they showed that their system could also detect more sophisticated attacks specifically engineered to fool machine learning algorithms. To demonstrate their tool's potential further, the researchers also carried out a series of tests in real-time. They found that the system satisfied the real-time DDoS attack detection requirements, extracting and analyzing network packets in a limited amount of time and without causing substantial network traffic delays.

The promising method presented in this paper could soon be integrated

within existing and newly developed security systems. In addition, it might inspire the development of similar machine learning techniques for detecting DDoS attacks.

"As we look ahead to future work, it will be essential to assess the efficacy of our IDS when challenged with adversarial attacks generated by alternative models," Mustapha added. "Additionally, we need to explore the implementation of online learning algorithms, which enable the IDS to continuously update its model in real-time as it analyzes new data. By integrating an incremental update feature, the IDS could retain its effectiveness in detecting evolving attack techniques."

More information: Ali Mustapha et al, Detecting DDoS attacks using adversarial neural network, *Computers & Security* (2023). DOI: 10.1016/j.cose.2023.103117