A 1D-CNN Based Deep Learning for Detecting VSI-DDoS Attacks in IoT Applications

Tsogbaatar Enkhtur <tsogbaatar.enkhtur.ta4@is.naist.jp>

VSI-DDoS attacks

Goal and operation. The VSI-DDoS attack is a new form of application-layer short-burst low-rate DDoS attacks with aim to degrade the quality of service towards users.

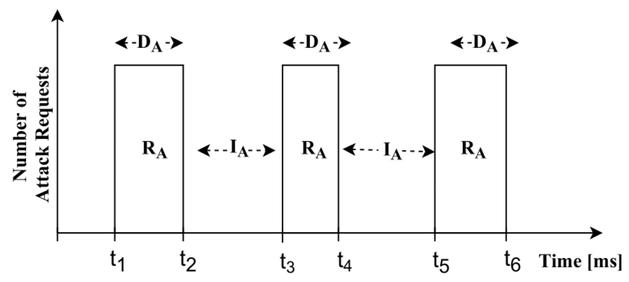


Figure 1: An illustration of VSI-DDoS attack, R_A indicates the degree of attack intensities per time period, duration of the attack D_A, and interval of the attack I_A .

Figure 2 illustrates how the VSI-DDoS attacks can seriously affect the QoS of the users for IoT applications.

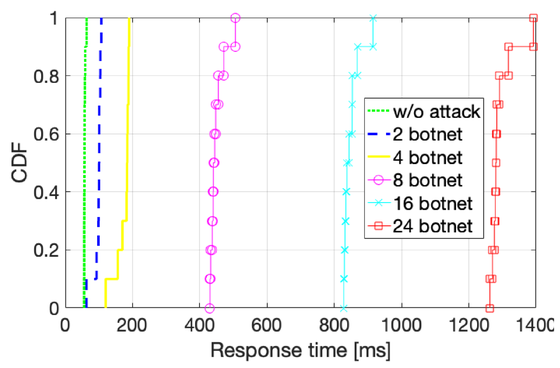
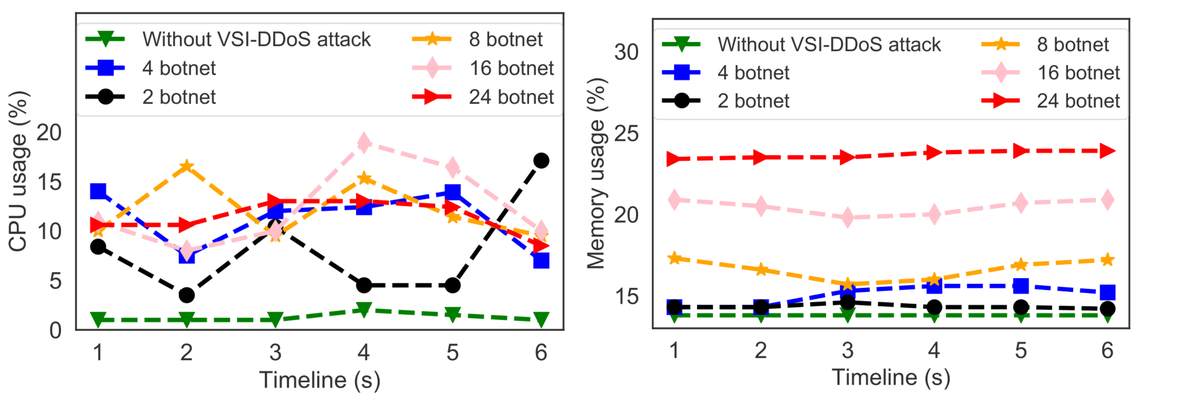


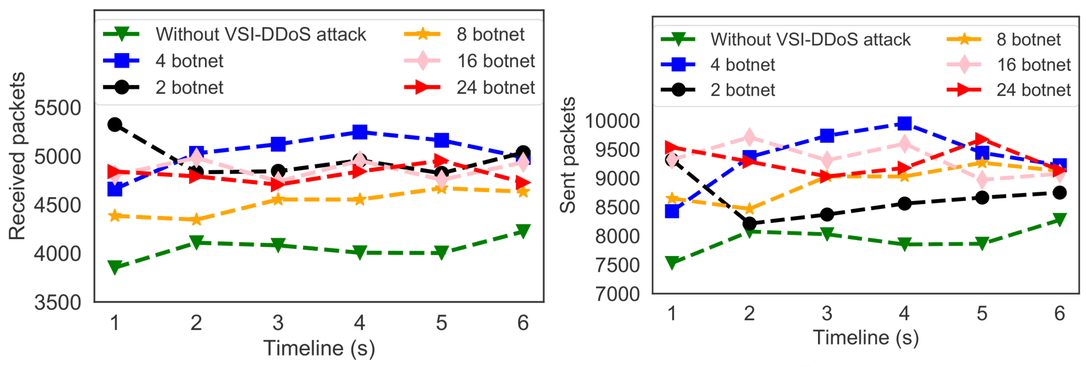
Figure 2: Cumulative density analysis of response time in presence and absence of VSI-DDoS attacks in IoT applications.

Detection adversity. Requests in VSI-DDoS attacks are similar to legitimate users' but they exhaust a server queues in milliseconds.



(a) CPU usage (b) Memory usage

Figure 3: CPU and memory usage of IoT application server with and without the VSI-DDoS attack.



(a) Received packets (b) Sent packets

Figure 4: Received and sent packets of IoT application server with and without the VSI-DDoS attack.

Problem statement

Given the data of **n** th different time-series with length T, i.e.,$x = (x_1; x_2; x_3;\cdots; x_n)^T$, and collected data from multiple IoT applications in the presence and absence of VSI-DDoS attacks. We aim to achieve the following three goals:

- VSI-DDoS datasets, i.e., generating a VSI-DDoS IoT applications dataset with diverse attack scenarios and
- make it public.
- VSI-DDoS detection, i.e., detecting VSI-DDoS attacks in IoT applications to alleviate QoS interruption.
- Experimental analysis, i.e., carry out exhaustive experimental analysis using both testbed and benchmark datasets with diverse attack scenarios.

Contribution

- We prepare a new VSI-DDoS IoT applications dataset with diverse attack scenarios and made it available for public use to fill the research gap.
- We propose a 1D-CNN deep learning approach to detect VSI-DDoS attacks early for IoT applications.
- The experimental evaluation illustrates the performance of the proposed approach using testbed datasets. We carry out experiments on benchmark datasets as well to compare with baseline models.

Dataset

We evaluate our proposed 1D-CNN deep learning approach using two datasets: (i) testbed data, and (ii) benchmark data. **Testbed data:** We used Time Series Benchmark Suite (TSBS), which simulates data streaming from a set of trucks belonging to a fictional trucking company in IoT application.

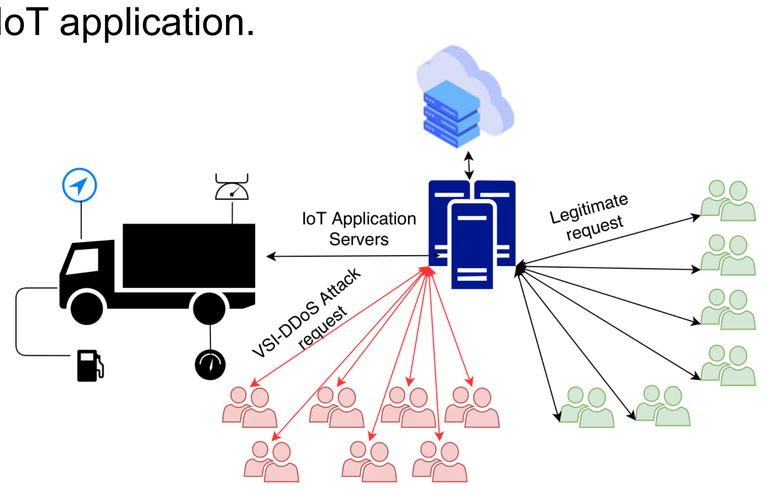


Figure 5: Experimental testbed setup and topology

Proposed CNN-Based Detection Model

We first introduce the problem we aim to study, then we elaborate the proposed 1D-CNN-based deep learning for detecting VSI-DDoS attacks in IoT applications to combat QoS degradation of services towards users. A system architecture of 1D CNN-based VSI-DDoS detection is shown in Figure 6.

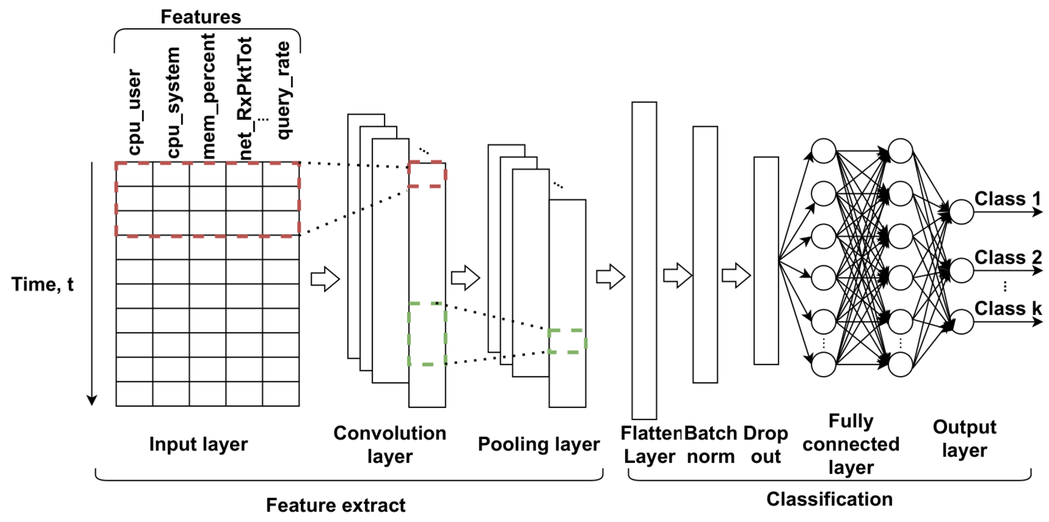


Figure 6. A system architecture for 1D CNN-based VSI-DDoS detection

Result

Figure 7 shows the accuracy of each model. The experiment results show that our 1D-CNN model has the highest accuracy compared with LSTM and the other baseline machine learning methods.

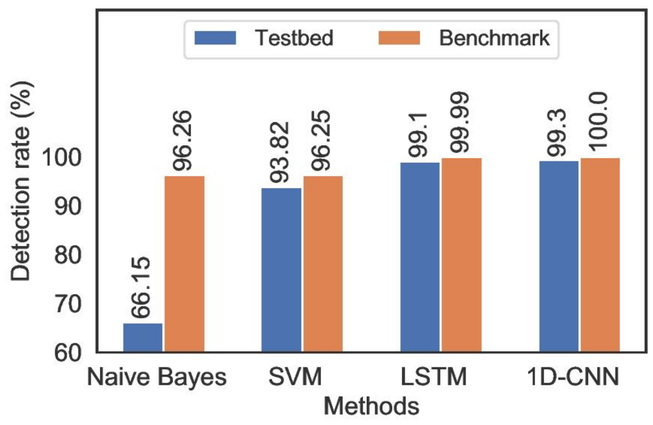


Figure 7. Comparison of proposed method with baseline models