Reviewer 2

1. There is major difference between the task of preventing the system from attacks and the task of finding a happened intrusion. The former is much more difficult and important than the latter.

Response 1: This has been revised as suggested. Please see p.4-5, lines 123-178, Section 2.

2. DDoS is different from DoS. The experiment setup in Figure 1 cannot simulate the distributed attacks.

Response 2:

1) Please refer to p.5, lines 183-184, "KALI generates... within the KALI VM."
2) Also, see p.6-8, lines 229-230, 236-237, 243-244, 250-251, 257-258, 264-265, "Attack command: … rand-source…". Hping3 emulates distributed attacks by generating random IP attack sources.

3. What is the contribution of the work? The authors should develop some algorithms to perform the anomaly detection automatically with better user interface.

Response 3:

1) For a clarification of the work's contribution, please refer to p.19, lines 480-493, "In this study... DDoS attack detection."
2) Regarding the anomaly detection algorithm, please refer to p.4-5, lines 123-178, Section 2.

4. There are always two squares under the x-axis in the Figures 12-34.

Response 4: The two squares below the x-axis in Figures 3-25 were automatically generated by PRTG. They indicate that the data was produced on the same day.