CHAPTER SIX

CONCLUSION

This research presented a new scheme for detecting and mitigating DDoS attacks in the SDN environment based on the elapsed time between attack successive packets. The new scheme has proposed to analyse parameters used by the existing solutions for detecting DDoS attacks in SDN, design the scheme to detect and mitigate Low-rate DDoS attacks, flooding DDoS attacks and DDoS attacks that changing from high volume to low volume in SDN and evaluate the performance of the proposed scheme in defending different DDoS attacks in SDN environment. The new scheme is aimed to overcome the drawbacks of the existing solutions. In this chapter, we will give a research summary in section 6.2. In section 6.3, we list the study's contributions and, in section 6.4 the possible future work is finally suggested.

6.1 Study summary

This thesis was organized into six chapters. The first chapter provided an introduction to this study. This chapter presented the research problem followed by the objectives. Then, the significance of the research and scope presented.

Chapter two presented a background study on the common DDoS attacks and SDN. The literature review started by presenting an introduction to DDoS attacks. Then, SDN fundamentals elaborated in details. Next, SDN controllers discussed and, the benefits of SDN mentioned. Also, the effect of the DDoS attacks

on SDN structure presented. Moreover, this chapter presented the literature on the commonly used techniques for detecting and mitigating DDoS attacks over SDN. The literature presented the pros and cons of the solutions that used these techniques and ended with a detailed comparison between the solutions in terms of the parameters used, measured overhead and, the accuracy achieved. The main techniques discussed: machine learning technique and entropy technique. Chapter two also discussed the common mitigation techniques used for mitigating DDoS attacks.

The research methodology discussed in chapter three. Firstly, it introduced performance evaluation techniques. Then, details of the selected network simulator presented. Moreover, chapter three discussed the simulation experiments design, experiments hardware and software, validation and verification and the network performance evaluation metrics.

Chapter four introduced a new scheme for detecting DDoS attacks based on the elapsed time between the successive attack packets and mitigating them based on changing the values of the Idle-timeout and hard-timeout of the flows that contain these packets to terminate them at time of detection. The three phases of the proposed scheme presented in this chapter. In phase one, we discussed in details how we collect the statistical information from both the SDN controller and the OpenFlow switch. Then, phase two discussed in details how the detection function in the proposed scheme worked. Finally, the mitigation function explained in phase three. The algorithm of detecting and mitigating DDoS attacks presented.

Chapter five discussed implementing and evaluating the proposed phases of the scheme in chapter four. This chapter presented four extensive experiments to

evaluate the performance of the proposed scheme under different experimental scenarios. The performance of the proposed scheme was evaluated for each experiment in terms of overhead (CPU usage), accuracy and false alarms. For the first three experiments, we compared the performance enhancements with all previous studies presented in chapter two. For the last experiment, we compared the results with the results obtained by the scheme in experiment three for confirming the results validity. For the comparison, we used Mininet emulator to obtain the results of one performance metric: CPU usage. We plotted graphs to make a comparison of the accuracy and false alarms more obvious. Two comparison tables presented after each mixture traffic case in each experiment in this chapter to compare enhancements of the proposed scheme to previous machine learning based works and entropy-based works. One comparison table presented in chapter five, section 5.4.

As a result, the new scheme showed better performance compared to the previous machine learning based studies in terms of overhead and better performance compared to the previous entropy based studies in terms of accuracy and false alarms.

6.2 Study Contributions

Producing an efficient and less complex solution with low false alarms for detecting DDoS attacks is an active study area. Many improvements have been proposed to enhance the performance of DDoS defense solutions over SDN in the past few years. Nevertheless, there is no optimal solution, as solutions use different detection techniques to distinguish the attack packets from legitimates. The existing solutions achieved high accuracy but they suffer from either increase the overhead or the false alarms or both of them at the same time. Also, the existing solutions do not detect

attacks that change the attack volume during the time of the attack in addition to the lack of researches that consider detecting the low-rate DDoS attacks. All of these were the motivations behind the research.

The main aim of this study was to propose a new scheme to enhance the DDoS defense solutions performance over SDN structure. This objective was carried out by a serious of connected contributions, including:

- A novel parameter the elapsed time between the successive attack packets which was not used before to detect flooding DDoS attacks and to enhance the DDoS attacks defense solutions performance in SDN.

- A new detection function to detect both flooding DDoS attacks and low-rate DDoS attacks. The new detection function also detects the DDoS attack packets change from the high volume of packets to the low volume and vice versa.

- A new mitigation function to drop the attack packets from the controller and to terminate the attack flows that contain these attack packets from the switch by making the idle timeout equals zero and, the hard timeout equals one at the time of the attack.

- Decreasing the overhead (CPU usage) produced by both machine learning technique based solutions and entropy technique based solutions to detect DDoS attacks from up to 70% to 34.3% in detecting UDP flood DDoS and 29.9% in detecting both of the UDP and SYN attacks that mixed in a same mixture traffic.

- Achieving high accuracy 99.85% in detecting the UDP flood attacks and low-rate of SYN attack that mixed with normal traffic in same mixture traffic with very low overhead 29.9% and low false alarms 0% compared to the mentioned solutions.

- Lowering false alarms ranging from 10% to 70% in most of the entropy technique based solutions to 0%.

- Achieving high accuracy of 99.47% with low measured overhead of 2.5% in detecting low-rate SYN attack in SDN.

6.3 Future Work

This research opens up further avenues for investigations. In this section, we present some of the future work recommendations. Hopefully, this research will be further extended and improved. The following summarizes some of these recommendations.

In this research, we proposed a new scheme to detect and mitigate single-vector DDoS attacks in SDN. For future work, this scheme could be enhanced to detect and mitigate Multi-Vector DDoS attacks or what is called "DDoS of Things". Another recommended future work is to use a testbed (real environment) to test the new proposed scheme. The testbed will obtain more reliable results; however, it is expensive.