Deep Reinforcement Learning based QoS-aware Secure Routing for SDN-IoT

Aluri Jagan Mohini

Summer term 2020

In IoT system, To handle all the devices efficiently and to overcome the security issues, Software defined network(SDN) is incorporated into IoT. However, default routing protocols of SDN such as OSPF is vulnerable to the flow changes when the network is under attack. To overcome the above mentioned issue, Deep reinforcement learning based QoS-aware Secure routing Protocol (DQSP) is proposed in [1].

1 Introduction

- Importance of SDN-IoT[3].
- Limitations of default routing protocols in SDN controller.
- Comparison of deep reinforcement learning and supervised learning methods [2].
- Deep reinforcement learning based QoS-aware Secure routing Protocol(DQSP) in SDN-IoT.

2 PROBLEM DEFINITION AND ATTACK MODELS

2.1 Network Model and Problem Definition

- Packet forwarding process in traditional routing protocol.
- Limitations of traditional routing protocol.
- Workflow of Deep reinforcement learning based QoS aware secure routing protocol (DQSP).
  - Solution to achieve security and quality of service.

2.2 Attack Model

[1] focuses on the two attacks which SDN-IoT system is susceptible to and they are:

- Gray hole attack. [4].
- Distributed denial of service (DDoS) attack.

3 THE PROPOSED DQSP SCHEME

- Architecture of DQSP.
  - Describes the sensing layer, data layer, controller layer and their functions followed by agent layer.
- Related definitions of DQSP are stated in [1] to enable optimized routing.
- DQSP working algorithm is discussed in detail.
  - DDPG is adopted to enable efficient secure routing.
  - DDPG follows the classic actor-critic model in reinforcement learning.
  - Working of Sampling algorithm .
  - Working of DQSP Training algorithm.

4 RESULTS AND PERFORMANCE EVALUATION

4.1 Experiment setup

- Experiment is conducted by using tensor flow in the back end.
- The training network of DQSP is built and in that training network, DDGP agent will be trained.
- Finally, total rewards obtained in training process are updated.

4.2 Performance Evaluation

- Performance of DQSP is evaluated with respect to the following metrics,
  - Packet delivery ratio.
  - End-to-end delay.
- Results are compared against the state-of-art routing protocol OSPF.

5 Conclusion

As per experimental results.

References

[1] X. Guo, H. Lin, Z. Li, and M. Peng. "Deep Reinforcement Learning based QoS-aware Secure Routing for SDN-IoT". In: *IEEE Internet of Things Journal* (2019), pp. 1–1.

[2] Z. Xu, J. Tang, J. Meng, W. Zhang, Y. Wang, C. H. Liu, and D. Yang. "Experience-driven Networking: A Deep Reinforcement Learning based Approach". In: *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. 2018, pp. 1871–1879.

[3] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi. "Software Defined IoT security framework". In: *2017 Fourth International Conference on Software Defined Systems (SDS)*. 2017, pp. 75–80.

[4] J. Sen, M. G. Chandra, S. G. Harihara, H. Reddy, and P. Balamuralidhar. "A mechanism for detection of gray hole attack in mobile Ad Hoc networks". In: *2007 6th International Conference on Information, Communications Signal Processing*. 2007, pp. 1–5.