Learning to Evade Jamming Attacks in the Wireless Networks Using Reinforcement Learning

SHI Shuyao
Department of Information Engineering
The Chinese University of Hong Kong
Shatin, Hong Kong
ss119@ie.cuhk.edu.hk

SONG Zirui
Department of Information Engineering
The Chinese University of Hong Kong
Shatin, Hong Kong
sz019@ie.cuhk.edu.hk

Abstract

Wireless networks are built on shared media, making it easy for attackers to launch intrusive attacks, which we called jamming attack. In our project, we established a simplified jamming attack model and environment for reinforcement learning, then tried to build an agent for defending attacker with different kinds of strategy, even without knowing the strategy of the attacker.

1 Introduction

In wireless networks, the media channels are easy and open in broadcasting, which makes the data forwarding between nodes susceptible to noise or interference. In particular, intentional interference is called jamming attack, and the attacker is called jammer. A more specific definition of a jammer is *an entity that is purposefully trying to interfere with the physical transmission and reception of wireless communications* (2). The attacker can quickly launch attacks after passively listening and obtain the communication frequency band of the current network node, also only attack when the agent is active, which is simple, low-cost and effective. Jamming attacks can severely interfere with the normal operation of wireless networks.

In response to this type of jamming attack, various technologies and strategies have emerged. The traditional method is to use complex physical layer technologies, such as direct sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS), which are applied in the military field. However, in practical applications, complex physical layer technologies are not suitable beyond the military area due the expensive cost. In view of this situation, various interference attack detection, defense, positioning, offensive and defensive game strategies based on the link layer and above are being proposed one after another.

In this project, by applying the reinforcement learning, we aim to train an agent to "learn" how to evade the attack from the different kinds of jammer, for defending the jamming attack without using the interference attack detection or positioning technology, and without knowing anything about the jammer's attack strategy.

1.1 Related work

A research team in the Zhejiang University has proposed four jamming attack models that can be used by an adversary to disable the operation of a wireless network (2), which are very typical and well-recognized. In our project, we will use these models as the baseline to generate the attacker model in our reinforcement learning environment.

In the field of defending jamming attack, a research team in the University of Maryland College Park tried to build an anti-jamming stochastic game for cognitive radio networks (1), in which it provides an approach for the problem that predicts and evades the transmissions of other agents as well as a dynamic jammer attack, i.e., focus on avoiding the collision under the multi-agent situation.

2 Framework

The agent (node 1) wants to send packets to the target (node 2) through a channel, the jammer will occupy and attack some channels, afterwards the packets sent from the occupied channel will fail, so the agent needs to move to other channels to evade the jamming attack. The strategy of the jammer may be various, and the agent needs to handle the attack without knowing the strategy of attacker.

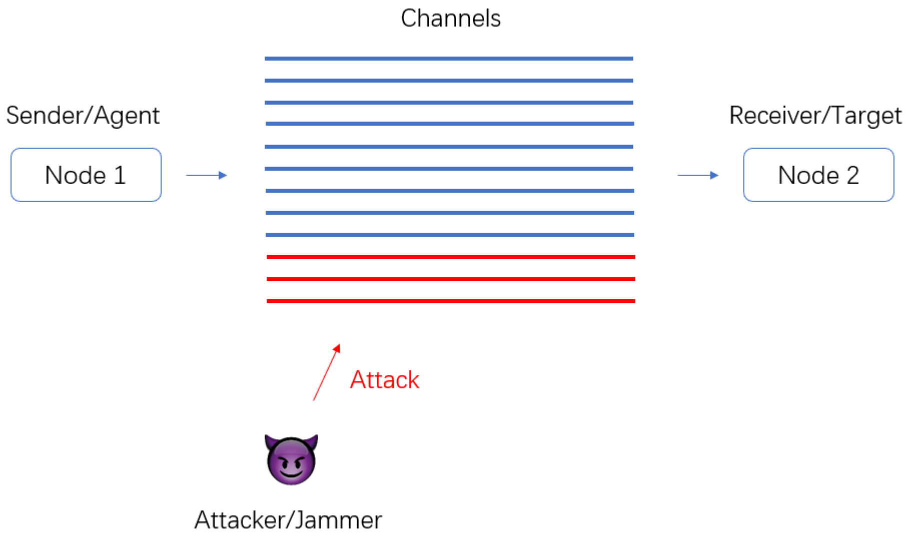

Figure 1: A simplified jamming attack model

- States: different channels.
- Actions: switch the channels, whether send the packet or not.
- Reward: if the agent sent the packet and receive the ACK signal from receiver, reward = 1; if the agent sent the packet but no ACK signal received, reward = -1; otherwise, reward = 0.
- Done: if all the packets are successfully sent by the agent and successfully received by the agent.

Existing attack models can be divided into several categories based on the ability and intelligence of the attacker. One type of attack does not consider channel status, including constant jammer, deceptive jammer and random jammer.There are also attacks based on channel status called reactive jammer.We will select some attack models as opponents and use reinforcement learning to train our agent in the game flow. So that it can avoid being attacked by strategically selecting channels.

3 Experiments

3.1 Setting up the environment

We have implemented the environment.py (Go `https://github.com/CupCupRay/IERG6130` to see the details) contains the environment for the reinforcement learning.

The jamming attack in the real-world has some constraints in terms of energy consumption, and computing power, etc. We want to make the environment as much close as possible to the practical situation, therefore, we take four jamming attack models: constant jammer, deceptive jammer, random jammer, and reactive jammer as the baseline in designing the strategies for jammer in our reinforcement learning environment.We have designed five different attacker strategies with the guidelines from (2):

1. Constant jammer, focus on several channels to continuously attack;

2. Constant jammer, continuously randomly choose several channel to attack;

3. Random jammer, switch back and forth between sleep and active, when active it focus on several channels to attack;

4. Random jammer, switch back and forth between sleep and active, when active it will randomly choose several channels to attack;

5. Reactive jammer, which can passively listen and obtain the communication channel used by agent, and attack.

3.2 Reinforcement learning method

In our project, we applied model-free based, policy gradient with/without baseline reinforcement learning with 2 independent policy networks for action "switching the channel" and action "send packet".

Since in our environment, there are huge action space and the environment itself is dynamic, which means the agent need to decide not only which channel to go, but also when to send the packet, also the attacked channels may switch due to the attacker's strategy, meanwhile, the attacker's strategy may also change from time to time. Furthermore, the mechanism of wireless communication determined that the rewards in packet transmission is delayed, the agent may receive the ACK signal from the target after sending many another packets.

3.3 Performance Metrics

In order to evaluate our agent, we need to introduce some characteristics and metrics that indicates the effectiveness of a jammer, as well as the performance of the agent.

- Packet Send Ratio (PSR): The ratio of packets that are successfully sent out by agent compared to the number of packets it intends or needs to send out.
- Packet Delivery Ratio (PDR): The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender, i.e., the ratio of packets that are successfully received by the receiver compared to the total packets successfully sent by the agent.

The Packet Send Ratio (PSR) intuitively indicates the packets sending rate of the agent, assume the bandwidth is not a concern under normal circumstances, then the strategy of agent when to send the packet will determine the performance of the Packet Send Ratio (PSR).

During the packets sending, the jamming attack will make the packets send by the agent (i.e., the packet is sent successfully) fail to receive by the receiver (i.e., not successfully received by receiver, if the agent doesn't receive the ACK signal from the receiver, the agent needs to resend the duplicate packet, which will cause the decrements of the Packet Delivery Ratio (PDR).

Therefore, one of the challenge of the agent is to find a trade-off of whether send packets or not. If the agent send too much packets in dangerous channel, the Packet Delivery Ratio (PDR) will be low because many successfully sent packets are not well received by the receiver, however, if the agent is very cautious in sending the packets, the Packet Send Ratio (PSR) will be bad due to the low packets sending rate.

3.4 Result

Here we show the results that during the 10,000 iterations of training by applying both policy gradient with/without baseline. Before showing the training result, we claim the practical meaning of the performance metrics:

- Higher Packet Send Ratio (PSR) means higher packet transmission rate during the wireless communication.

- Higher Packet Delivery Ratio (PDR) means lower packet loss rate during the wireless communication.

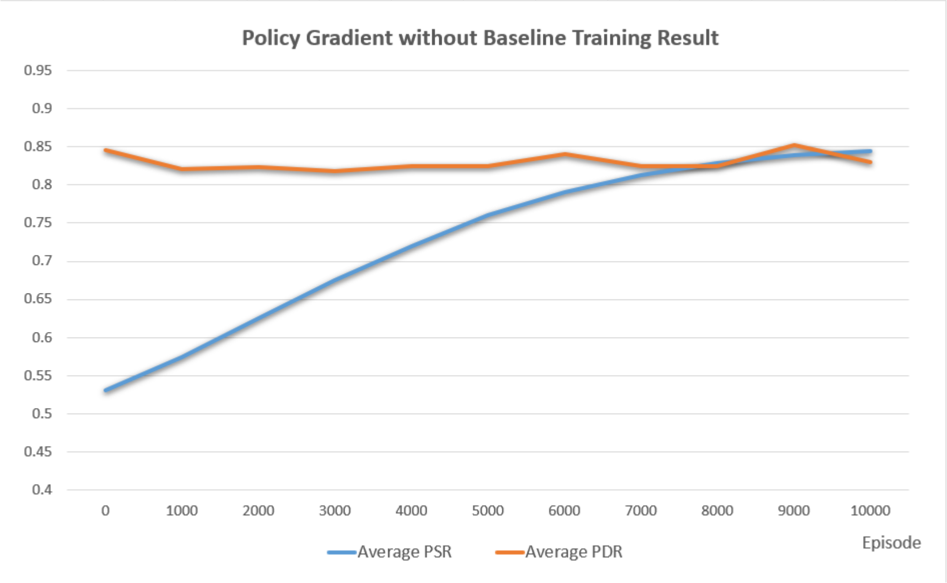

Figure 2: Policy Gradient without Baseline

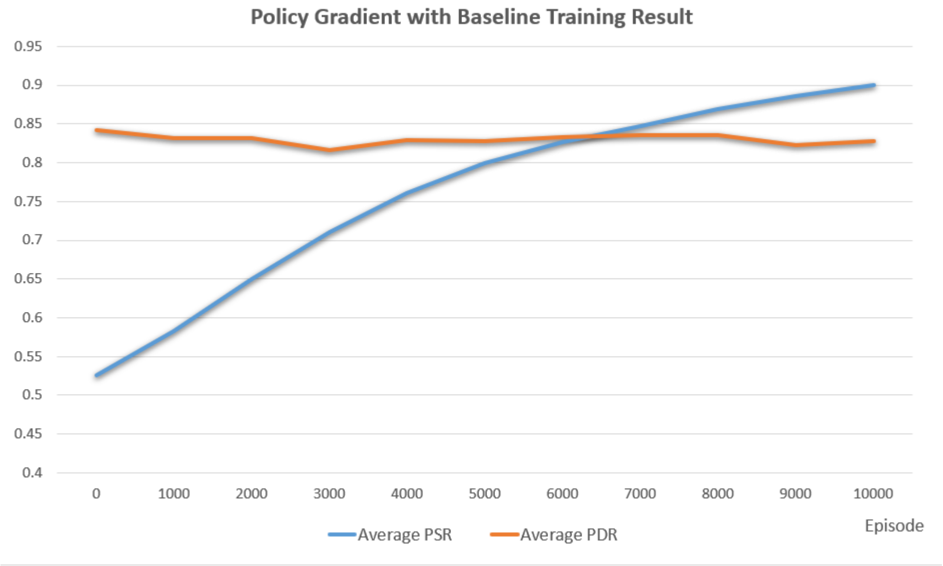

Figure 3: Policy Gradient with Baseline

From the figures above we can conclude that both policy gradient with baseline and without baseline is evidently effective in stably increasing the Higher Packet Send Ratio (PSR). Meanwhile, the Higher Packet Delivery Ratio (PDR) is in a relatively stable state, which is not bad news since the agent improves the packet transmission rate as well as keep the packet loss rate in an acceptable range (about 15%). So overall, the quality of wireless communications has been improved even in the presence of jamming attacks.

Then let's compare these two algorithm with each other,

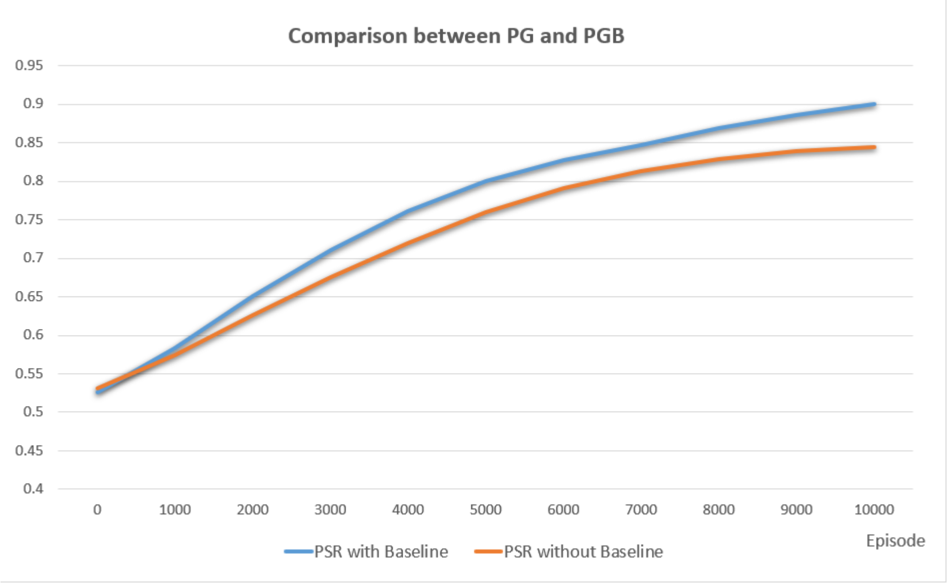

Figure 4: Comparison between PG and PGB

From the figure above we can conclude that, compare to the policy gradient without baseline, the policy gradient with baseline has better performance in training the agent in terms of the Higher Packet Send Ratio (PSR).

4 Sensitivity to Hyper-parameters

Among the hyper-parameters, the most practically related parameter are the "number of channels" and "attacker's strategy", actually, the real world's jamming attack varies greatly depends on the dynamic ambient, constrained budget (one of the feature of jamming attack is low-cost), etc. Therefore, we would like to modify the hyper-parameters to test the sensitivity of the agent towards different situations.

We take the agent trained using policy gradient with baseline as the tester, and we set the "number of channels" various to show that whether the performance of the agent is sensitive with the "number of channels" in the environment. The figure.5 shows the result of the evaluation.

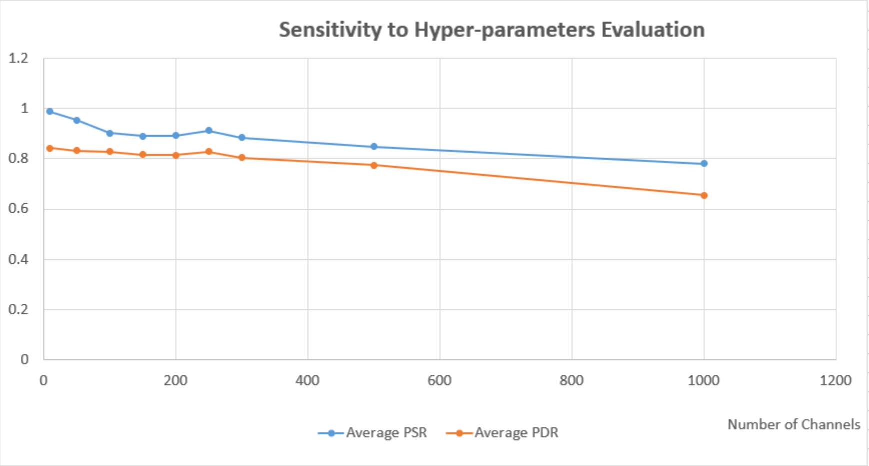

Figure 5: Sensitivity to Hyper-parameters Evaluation

As we can see, when the number of channels is limited in a small range, the performance of the agent is good as the original evaluation. However, if the number of channels goes to larger, the both PDR and PSR will become worse, but fortunately, in the practical wireless communication scenario, the number of channels will not be so large, normally there will be at most five hundred channels(2). In conclusion, our agent can basically fulfill all the practical usage in evading the wireless communication jamming attack.

5 Conclusion

In our project, we aimed to train an agent that can "learn" how to evade the attack from the different kinds of jammer, without knowing anything about the jammer's attack strategy. We built several attacker models in our environment and makes them closer to the practical wireless communication scenario.

We apply the policy gradient with and without baseline algorithms in training the agent, the result shows that the both of the algorithms are effective for increasing the Packet Send Ratio (PSR), which is an important metric in wireless communication that indicates the packets transmission rate, among them, the policy gradient with baseline has better performance. Meanwhile, the Packet Delivery Ratio (PDR) keeps stable while the training, which indicates the packets loss rate.

Due to the limitation of time, we did not perform more iteration training. In future work, we will find the convergence point of these algorithms and conduct more analysis and make further improvements.

References

[1] B. Wang, Y. Wu, K. R. Liu, and T. C. Clancy. An anti-jamming stochastic game for cognitive radio networks. *IEEE journal on selected areas in communications*, 29(4):877–889, 2011.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 46–57, 2005.