As we observed, Tesla’s autopilot system development is based on neural network (NN). Lets has a brief introduction of how Tesla’s autopilot system works. It used the camera in the car to observe the environments and take control of the car by NN, just like a human observes the environment nearby and drive the car. It looks too good to be true, but there are some problems hidden inside this magic box and it takes time for Tesla to solve them.

The first problem that NN encounter is the bias of their original dataset is. The training of the neural network requires a massive amount of data, and thanks to the contribution of Facebook, Google, etc, those massive amounts of data is much easier to obtain than before. However, the original dataset contains a brunch of the same type of photos, which lead to NN bias in some type of circumstances, but in the real-life, it may not be the case and it may cause some fatal accident. Furthermore, since most of the photos from the internet are taken by human since they will upload to their social media, the dataset is biased to human’s taken photo instead of the actual case Tesla is facing, i.e. taken the photo by machine. Research points out that there is a massive difference between a human’s taken photos and a robot’s taken photos. So in the real case, there may not be enough photos for Tesla to train their model. To solve this situation, Tesla needs to spend a lot of resources to clean the dataset; also, they need to obtain the photo by itself under different circumstances such as raining, storm, snowing, whereas sometimes it is hard to obtain the photos of some situations such as dust storm or hail.

Another problem that NN encounter is the way it inferences the photo it received is different from how human inference the photo. One example is the Convolution network identify if there is an animal behind the photo is by the blurred background, instead of finding the animal itself, so if the photo is not blurred, NN can still not identify there is an animal in there even there is an animal behind the picture. Tesla has to understand how their NN works and ensure that it works in ever circumstances, either by changing the hierarchy of the NN such as using a much advance model or understand how NN works and find some solution to fit the data that the NN requires. Of course, both solutions require resources and time, as it is not an easy task to dig inside a black-box model.

Furthermore, NN can be tricked by some artificial photos. Researchers successfully make some photos by noise to let the NN misclassify it is another object. It is not a problem in the normal case because it does not harm others even NN predict the result wrongly, but when it comes to a car, then it can cause massive damage or even fatal accident. We cannot ignore the fact that there is a possibility that people try to attack the system, and it is very dangerous to leave this kind of possibilities to the public.

In conclusion, we have discussed different aspect that Tesla’s autopilot system encounter. Although most cases can be solved by resources and Tesla probably already tackle it, Tesla should take a serious look at the possible attacks by others on the system. In general, the system already mature enough, but in my opinion, it should be a support system for driving instead of dominating the whole driving process.