# Article information:

Generative Poisoning Attack Method Against Neural Networks - 百度学术
[https://xueshu.baidu.com/usercenter/paper/show?paperid=9034c3b27bab678eef804ad5fa534960=xueshu\_se](https://xueshu.baidu.com/usercenter/paper/show?paperid=9034c3b27bab678eef804ad5fa534960&site=xueshu_se)

# Article summary:

1. This article examines the possibility of applying traditional gradient-based methods to generate poisoned data against neural networks.

2. A generative method is proposed to accelerate the generation rate of the poisoned data, using an auto-encoder (generator) and a target NN model (discriminator).

3. Experiments show that the generative method can speed up the poisoned data generation rate by up to 239.38x compared with the direct gradient method, with slightly lower model accuracy degradation.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

The article is generally reliable and trustworthy in its presentation of information regarding generative poisoning attack methods against neural networks. The authors provide a detailed overview of their research, including a description of their proposed generative method and results from experiments conducted to test its efficacy. The authors also provide a countermeasure for detecting such attacks, which adds further credibility to their work.

However, there are some potential biases in the article that should be noted. For example, the authors do not explore any possible counterarguments or alternative approaches to their proposed method, nor do they discuss any potential risks associated with it. Additionally, while they present evidence for their claims in terms of experiment results, they do not provide any evidence for why their proposed approach is superior to other existing methods or why it should be adopted over them. Furthermore, while they mention that their proposed approach has slightly lower model accuracy degradation than other methods, they do not provide any details on how much lower this degradation is or what implications this may have for real-world applications of their approach.

# Topics for further research:

* Generative poisoning attack countermeasures
* Risks associated with generative poisoning attacks
* Comparison of generative poisoning attack methods
* Real-world applications of generative poisoning attacks
* Model accuracy degradation of generative poisoning attacks
* Advantages of generative poisoning attacks over other methods

# Report location:

<https://www.fullpicture.app/item/008047893d75fb790db8824bf22fc99c>