中南大學
CENTRAL SOUTH UNIVERSITY

XXXX 论文

题目	xxxxxxx
学生姓名	xx
学　　号	xxxxxxxx
专业班级	xxxxx
指导教师	xxxx
学　　院	xxxxx
完成时间	xxxxxxx

中南大學
CENTRAL SOUTH UNIVERSITY

论文题目

学生姓名：xxx

学　　院：xxx 学院

专业班级：xxxx

指导老师：xxx 教授

二〇一九年十二月

摘要

提供了三个封面，取需

正文 宋体 小四，20 磅行距 最小值

标题从三号字体依次递减 最多三级标题

图片下方标题由文本框加入，设置布局格式为上下型环绕

目录

第一章 绪论

1.1 背景

xxxxxxx。

1.2 研究现状

第二章 xxxx 简介

2.1 XXXX

xxxxx。

2.2 XXXX

xxxx*[1]*。

$$\arg\max \mathcal{D}_p \ \mathcal{W}(\mathcal{D}', \theta_p^*)$$

第三章 xxxxx

3.1 xxxxxx

Algorithm 1 Poisoning Attack Algorithm

Input: $\mathcal{D} = \mathcal{D}_{\text{tr}}$ (white-box) or $\mathcal{D}'_{\text{tr}}$ (black-box), $\mathcal{D}'$, $\mathcal{L}$, $\mathcal{W}$, the initial poisoning attack samples $\mathcal{D}_p^{(0)} = (\boldsymbol{x}_c, y_c)_{c=1}^{p}$, a small positive constant ε.

$i \leftarrow 0$ (iteration counter)
$\boldsymbol{\theta}^{(i)} \leftarrow \arg\min_{\boldsymbol{\theta}} \mathcal{L}(\mathcal{D} \cup \mathcal{D}_p^{(i)}, \boldsymbol{\theta})$
repeat
  $w^{(i)} \leftarrow \mathcal{W}(\mathcal{D}', \boldsymbol{\theta}^{(i)})$
  $\boldsymbol{\theta}^{(i+1)} \leftarrow \boldsymbol{\theta}^{(i)}$
  for c = $1, \ldots, p$ **do**
    $\boldsymbol{x}_c^{(i+1)} \leftarrow \text{line\_search}\left(\boldsymbol{x}_c{}^{(i)}, \nabla_{\boldsymbol{x}_c} \mathcal{W}(\mathcal{D}', \boldsymbol{\theta}^{(i+1)})\right)$
    $\boldsymbol{\theta}^{(i+1)} \leftarrow \arg\min_{\boldsymbol{\theta}} \mathcal{L}(\mathcal{D} \cup \mathcal{D}_p^{(i+1)}, \boldsymbol{\theta})$
    $w^{(i+1)} \leftarrow \mathcal{W}(\mathcal{D}', \boldsymbol{\theta}^{(i+1)})$
  $i \leftarrow i + 1$
until $|w^{(i)} - w^{(i-1)}| < \varepsilon$

Output: the final poisoning attack samples $\mathcal{D}_p \leftarrow \mathcal{D}_p^{(i)}$

图一、xxxx 算法

3.2 xxxx

3.2.1 xxx

Xxxxxx。

3.2.2 xxx

Xxxx

Xxxx

第四章 结束语

Xxxxxxx。

感谢 xxxxx。

参考文献

[1] S. Alfeld, X. Zhu, and P. Barford. Data poisoning attacks against autoregressive models. In AAAI, 2016.