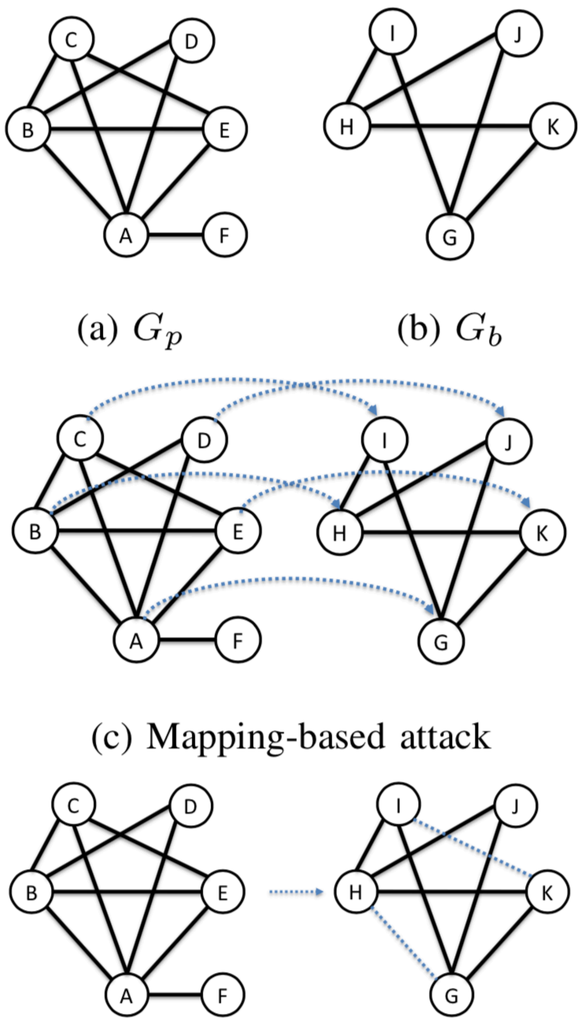
CERIAS

The Center for Education and Research in Information Assurance and Security

Online Social Network De-anonymization via Conditional Generative Adversarial Network Model

Student: Tianchong Gao; Advisor: Feng Li

A) Mapping based attack or generating based attack



(a) G_p (b) G_b

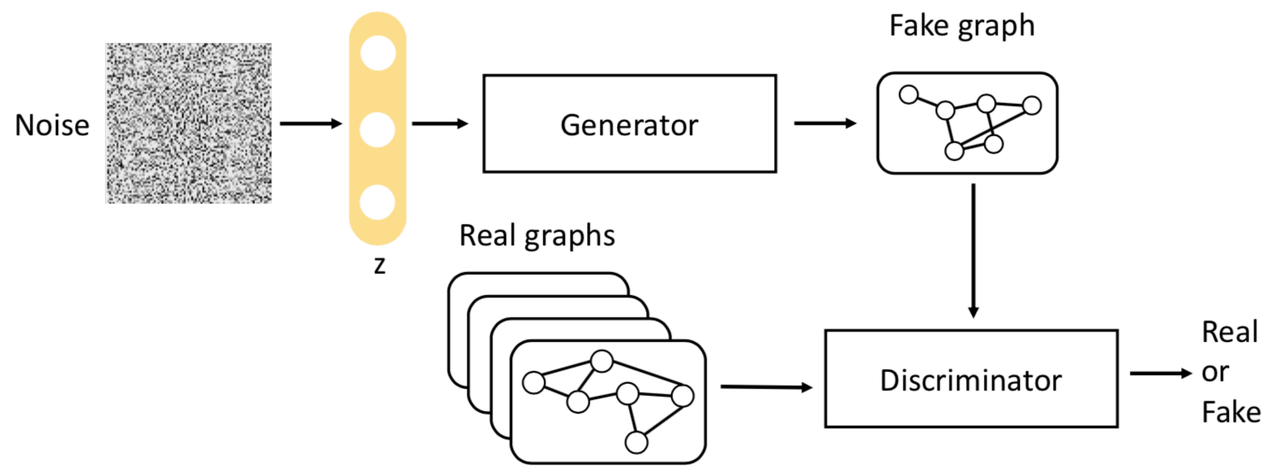
(c) Mapping-based attack

(d) Generating-based attack

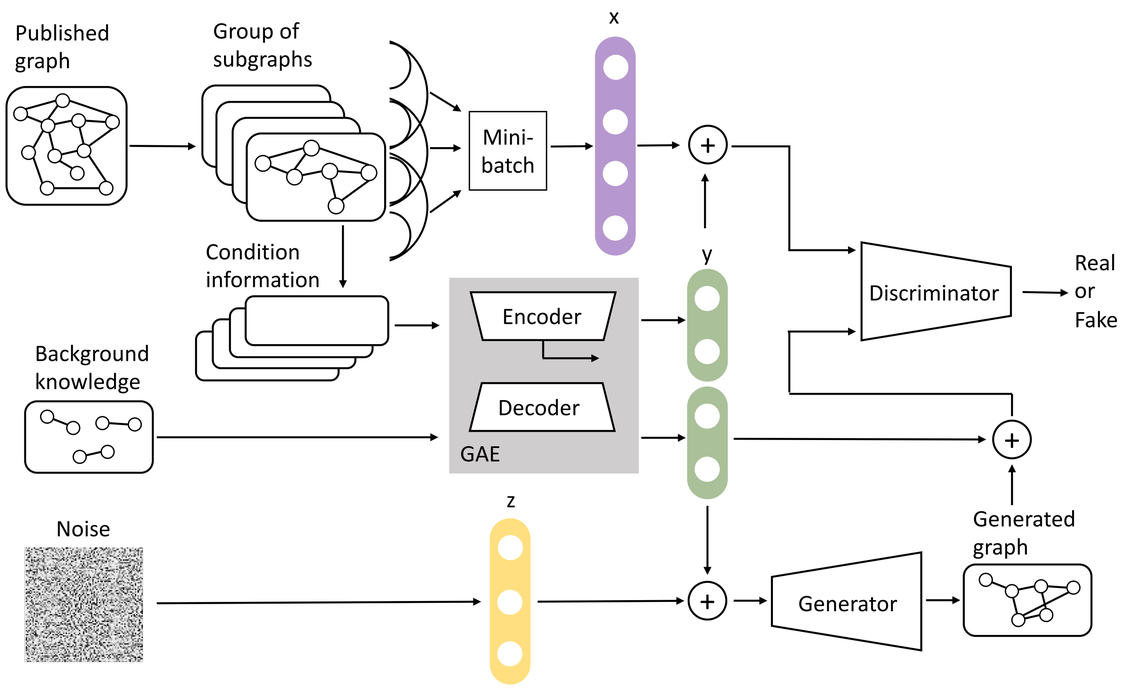
B) Problems of existing approach

- The published graph may partially cover / does not cover the target persons.
- The structure change, introduced by both the errors in adversaries' background knowledge and the noise in anonymization mechanisms, increases the difficulties of de-anonymization.
- The complexity of the graph structure makes it hard to find a global optimal mapping result.

B) Structure of GAN



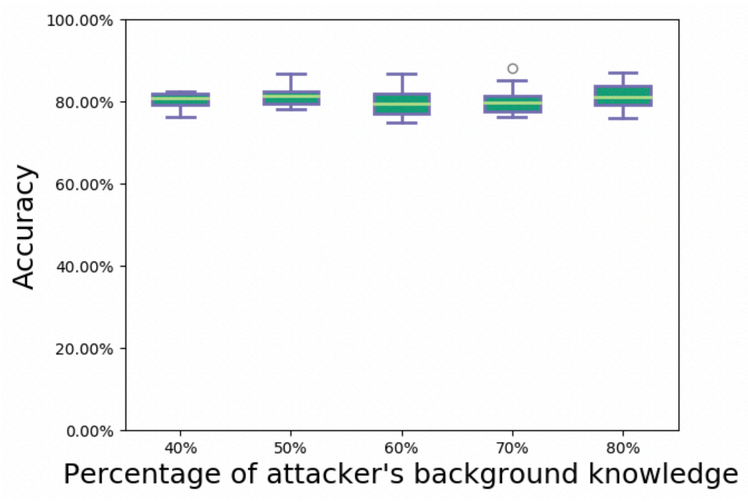
D) Framework Design



E) Highlights

- Published data embedding -> GAN model
- Background knowledge embedding -> CGAN model
- Graph structure embedding -> GNN and GAE model

F) Evaluation



Mapping-based attack success rate		
Prior knowledge	Original graph	Original graph + regenerated graph
40%	5.26%	17.89%
50%	7.37%	20.00%
60%	9.47%	47.37%
70%	10.53%	55.79%
80%	17.89%	65.26%

PURDUE UNIVERSITY Discovery Park

CERIAS