# Empowering Elastic-honeypot as Real-time Malicious Content Sniffers for Social Networks

NSF Award #: 1948374

PI: Xu Yuan
University of Louisiana at Lafayette

## Background

**Problem:** Malicious contents have been adversely impacting users in social networks. It is critical of importance to develop effective mechanisms to capture and detect them.

**State-of-the-art**:

- Detecting spammers from blindly collected contents or accounts: low efficiency and only detect a small portion of spammers.
- Creating honeypot accounts as lures to attract spammers: has drawbacks in deployment flexibility, attribute variability, and network scalability, as it involves considerable human efforts.

**Goal:** We propose a novel malicious contents gathering system, collecting contents that are far more likely of including spammers' activities so as to detect and remove them.

## Motivation

- Large amounts of users are suffering spammy behaviors.
- The diversity of user attributes meeting spammer's taste.
- Many users have the intrinsic property as honeypot in spammer attraction.
- Relieve manual construction overhead of honeypots.

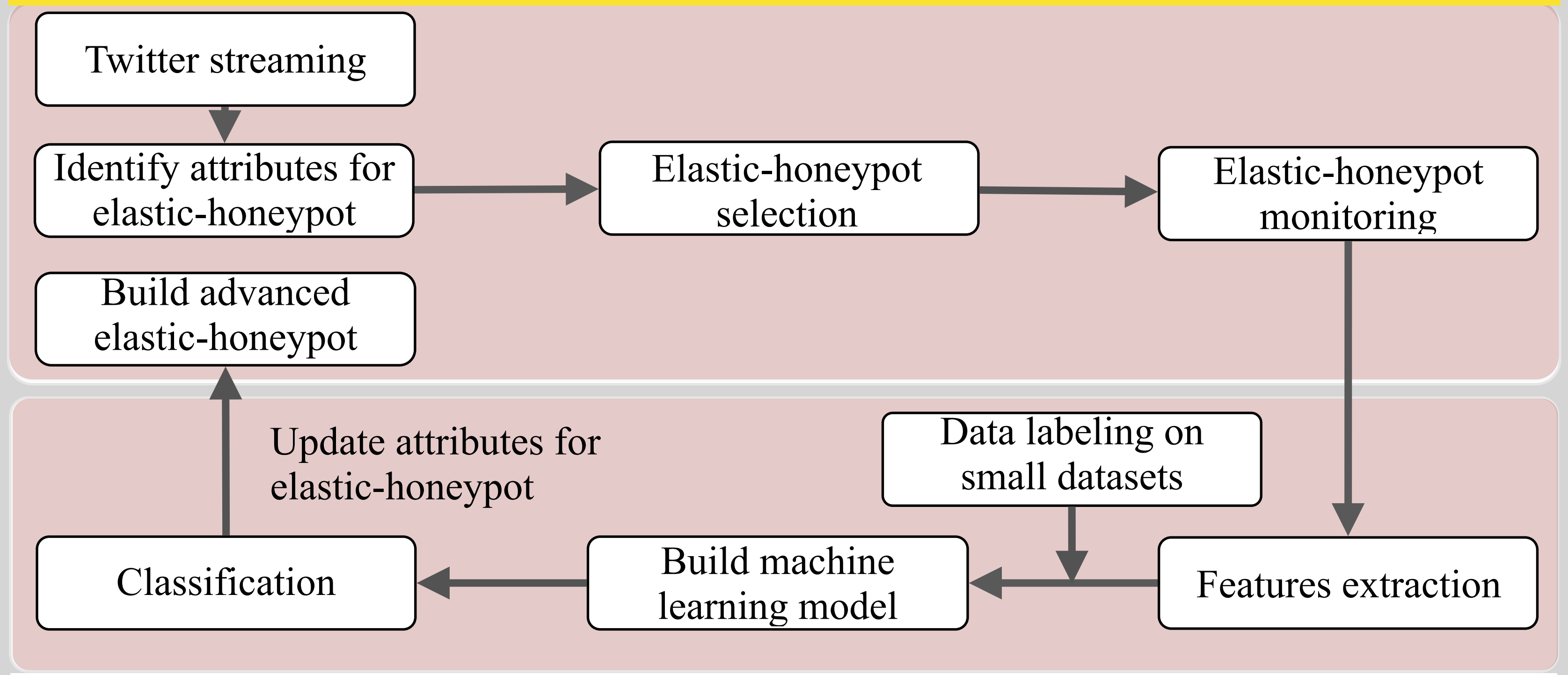
## Elastic-Honeypot

- Elastic-honeypot is constructed on the top of normal users.
- Taking advantages of users diversity and screening attributes that attract spammers' tastes.
- collecting tweets that are far more likely of including spammers' activities.
- Easily to be scaled up to an arbitrarily sized network.
- Can quickly migrate to new users or new attributes to adapt the change of spammers' taste.

## Technical Challenges

- Elastic-honeypot's activities have to be utterly transparent to users, for obeying Social networks' security and privacy policy
- How to determine the top ones meeting spammers' taste, from the wide variety of attributes and billions of users
- How to shift across accounts to maintain high efficiency
- How to handle spammer taste drift issues
- How to develop efficient classification solutions and handle feature drift

## Technical Approaches

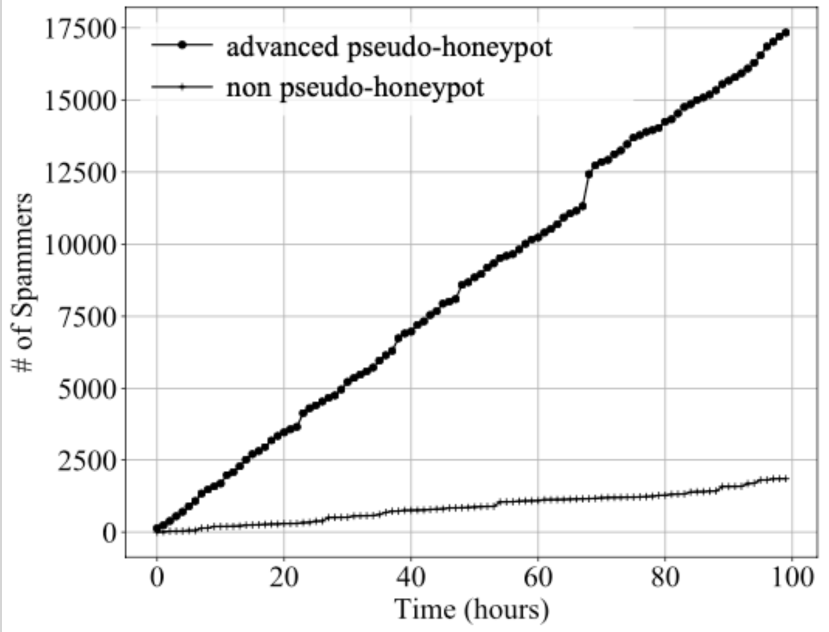

Twitter streaming
Identify attributes for elastic-honeypot
Elastic-honeypot selection
Elastic-honeypot monitoring
Build advanced elastic-honeypot
Update attributes for elastic-honeypot
Data labeling on small datasets
Classification
Build machine learning model
Features extraction

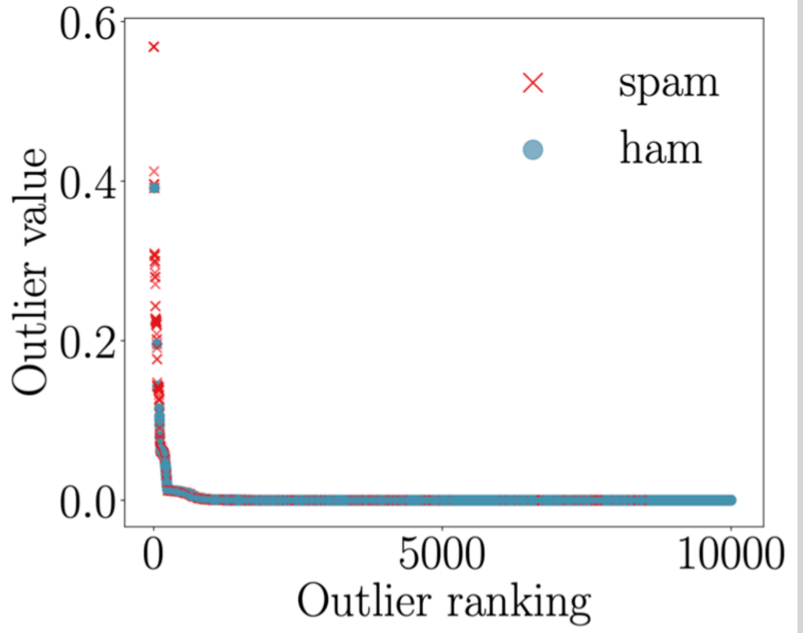
- Social network APIs: Twitter Streaming API, Reddit API, Facebook/Instagram Search API, etc
- Selecting attributes from a large pool and refining to get effective ones, graph clustering methods to identify victims
- Analyzing and predicting users' activity patterns to determine the shift behaviors of Elastic-honeypot
- Developing graph-based and outlier-based classification solutions
- A fully-fledge system including real-time data gathering and real-time detector

## System Evaluations

**Experiments:** create a 100-node pseudo-honeypot network and run 300 hours. We manually label 1,290 spams and 5,517 non-spams.

Then, we create a 100-node pseudo-honeypot networks and run a total of 100 hours.





| Honeypot mehtod | Time | Running duration | Honeypots | Spams | Spammers | Efficiency |
|---|---|---|---|---|---|---|
| Stringhini *et.al.* [1] | 2010 | 11 months | 300 | – | 15, 857 | 0.0067 |
| Lee *et.al.* [2] | 2011 | 7 month | 60 | – | 36, 000 | 0.12 |
| Yang *et.al.* [3] | 2014 | 5 month | 96 | 17, 000 | 1, 159 | 0.0034 |
| Yang *et.al.* [3]'s advanced system | 2014 | 10 days | 10 | – | – | 0.087 |
| Advanced pseudo-honeypot system | 2018 | 50 hours | 50 | 7, 370 | 2, 301 | 0.92 |

## Scientific and Border Impacts

- Developing a novel, lightweight, and real-time system for effectively gathering and classifying manic-likely contents
- Gathering a large-sized dataset for use in AI and cybersecurity areas
- Novel solutions advancing the field and boosting the system robustness
- Real-world implementations and deployments yield valuable experience and software toolkits
- Research opportunities for graduate and undergraduate students
- Summer tutorials for educating and engaging undergraduate students with entry-level knowledge