Learning Dynamic and Robust Defenses Against Co-Adaptive Spammers

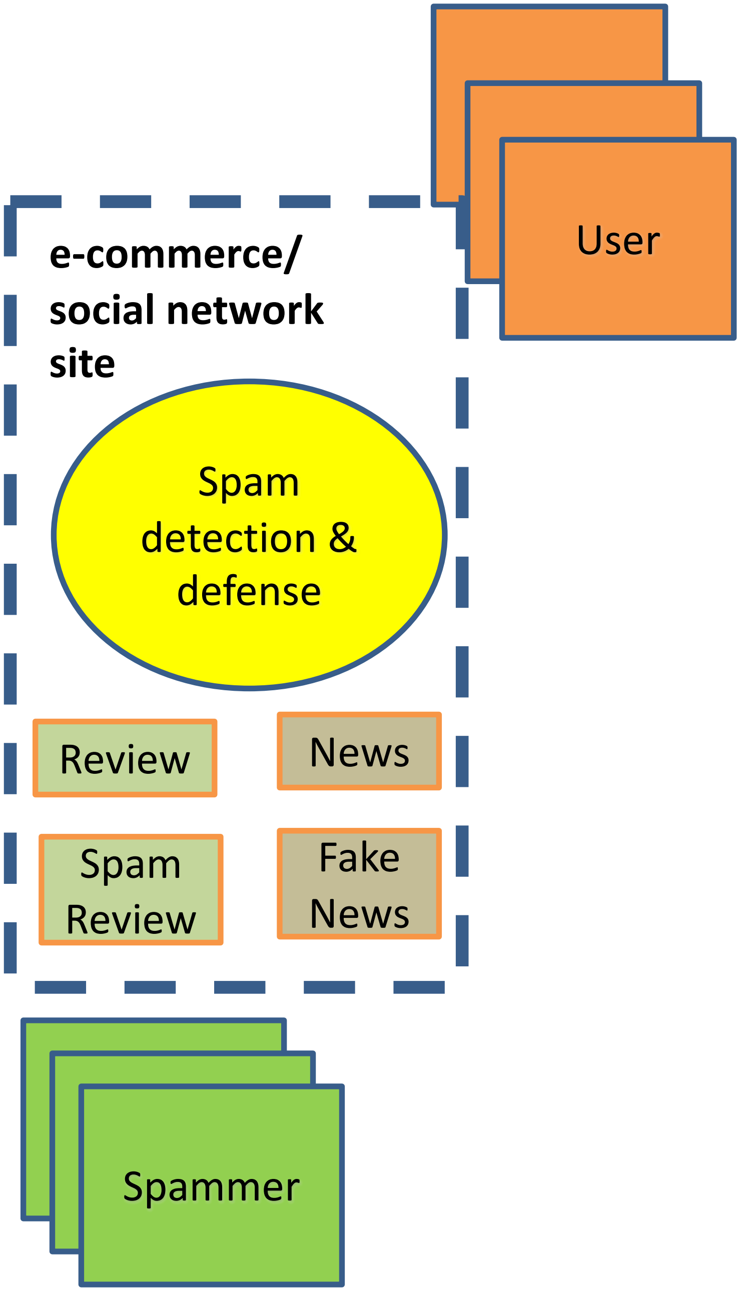
Challenge:

- Develop the next generation spam or fraud detection and defense technologies against intelligent spammers or fraudsters that learn to bypass traditional detectors.

Solution:

- Robust Detection of Adaptive Spammers by Nash Reinforcement Learning (KDD200)
- Deep Diffusive Neural Network based Fake News Detection from Heterogeneous Social Networks (ICDE2000)
- User Preference-aware Fake News Detection (SIGIR2021)
- Enhancing Graph Neural Network-based Fraud Detectors (CIKM200)

SaTC1930941, UIC, Philip S. Yu (PI)
e-mail: psyu@uic.edu



Scientific Impact:

- Insights into how and how much a spammer can bypass static detectors;
- Significant advances in modeling spammer-defender interactions
- Dynamic spam detections through continuous and reinforcement learning

Broader Impact and Broader Participation:

- Build a more trustworthy online environment, where business owners and professionals are encouraged to offer higher quality products and services
- Benefit consumers as they can rely on online contents, products and services more confidently,
- Train a good number of researchers, and educate a lot of students