Crowd signals for Fake news Detection

Vansh Kapoor
Guides: Prof. Nikhil Karamchandani, Prof. Abir Dey & Manish Jain

Department of Electrical Engineering
IIT Bombay

Outline

Motivation

- Project goal is to minimize the spread of misinformation in social networks by stopping the spread of fake news in this network.
- The vast volume spread of news make traditional human-based verification impractical
- Model capable of FND among vast dynamically generated news by using true labels from a smaller sample set.

Previous Work

- [2] leverages flagging activity of users to detect fake news & treats all flags equally reliable
- Recent work involves modeling network structures like ICM and NLP techniques
- Challenges: Limited availability of corpora and the substantial variability in the sources of fake news.
- [1] proposed an Online algorithm that uses Bayesian inference for FND and concurrently learns each user's flagging accuracy.

Problem Setup

Algorithm Labeling Algorithm

Input: social network graph $G = (U, E)$; labeling budget k per news
Initialize: active news $A^0 = \{\}$ (News not queried to Oracle).
for $t = 1, 2, \ldots, T$ **do**
    /* At the beginning of epoch t */
    Generate news X^t with $o_x \in U$ as the origin/source of $x \in X^t$.
    Update the set of active news as $A^t = A^{t-1} \cup X^t$. For all $x \in X^t$, do the following:
    Initialize users exposed to the news x as $\pi^{t-1}(x) = \{\}$.
    Initialize users who flagged the news x as $\psi^{t-1}(x) = \{\}$.

    /* During the epoch t */
    Algo selects a subset $S^t \subseteq A^t$ to get expert's labels given by $y^*(s) \in \{f, \overline{f}\}$ for all $s \in S^t$
    Block the fake news ($\forall s \in S^t$ such that $y^*(s) = f$, remove s from the network)
    Update the set of active news as $A^t = A^t \setminus S^t$

    /* At the end of epoch t */
    for all $a \in A^t$ **do**
        News a continues to propagate in the network. For all $a \in A^t$, do the following:
        News a propagates to more users $u^t(a) \subseteq U \setminus \pi^{t-1}(a)$; i.e., $\pi^t(a) = \pi^{t-1}(a) \cup u^t(a)$.
        News a is flagged as fake by users $l^t(a) \subseteq u^t(a)$; i.e., $\psi^t(a) = \psi^{t-1}(a) \cup l^t(a)$.
    end for
end for

Objective Function

- S^t: Set of news selected and given to the Oracle at timestep t
- $\pi^t(a)$: Set of affected nodes until time t by news a
- $\mathrm{val}^t(a) : \mathbb{E}_{\mathcal{D}}\left(|\pi^\infty(a)| \;\middle|\; \pi^m(a), m \leq t \right) - |\pi^t(a)|$ for an active news a

$$\mathrm{UTIL}(T) = \mathbb{E}\left[\sum_{t \in [T]} \left(\sum_{x \in S^t} \mathbb{I}\{x = \text{fake}\} \cdot \mathrm{val}^t(x) - \gamma |S^t| \right) \right]$$

Here γ is the trade-off parameter

Motivation for One-Step LookAhead

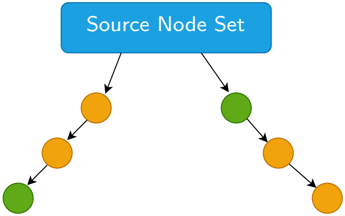


Figure: ICM Diffusion Model with high-reliability children nodes denoted in green

Notation

- $\pi^t(a)$: Set of affected nodes until time t by news a
- $\psi^t(a)$: Set of nodes/users who have flagged news a until time t
- $Y_u(x)$: label by user u assigned to x with true label $Y^*(x)$
- $\theta_{u,f} = P(Y_u(x) = f | Y^*(x) = f) \quad \theta_{u,\bar{f}} = P(Y_u(x) = \bar{f} | Y^*(x) = \bar{f})$
- $\beta^t(s)$: Unreliability of source node s

$$\mathcal{P}^t = \mathbb{P}(x = f | \psi(t), \theta_{u,f}, \theta_{u,\bar{f}}, \mathcal{S}(x))$$
$$= \frac{\prod_{u \in \psi(t)} \theta_{u,f} \prod_{u \in \pi(t)-\psi(t)} (1-\theta_{u,f})\beta}{\prod_{u \in \psi(t)} \theta_{u,f} \prod_{u \in \pi(t)-\psi(t)} (1-\theta_{u,f})\beta + \prod_{u \in \psi(t)} (1-\theta_{u,\bar{f}}) \prod_{u \in \pi(t)-\psi(t)} (\theta_{u,\bar{f}})(1-\beta)}$$

Idealistic Scenario

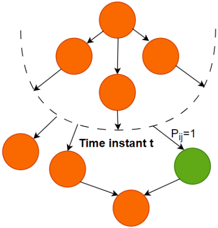


Figure: Idealistic Scenario at Time t

1. If news sent to the Oracle at time step t, then the utility function given by

$$UTIL(T) = \mathcal{P}^t \mathrm{val}(t) - \gamma$$

2. Utility function if we decide to wait for another time step given by

$$UTIL(T) = \mathcal{P}^t (\mathrm{val}(t+1) - \gamma)$$

Therefore if $(1 - \mathcal{P}^t)\gamma - \mathcal{P}^t(\mathrm{val}(t) - \mathrm{val}(t+1)) > 0$ it is optimal not to query the at t

Non-Idealistic Scenario

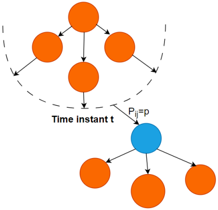


Figure: Non-Idealistic Scenario at Time t

$$\mathcal{P}_{\Theta_1} = \frac{1}{1 + (\frac{1}{\mathcal{P}^t} - 1)^{\frac{1-\Theta_{\bar{f}}}{\Theta_f}}} \qquad \mathcal{P}_{\Theta_2} = \frac{1}{1 + (\frac{1}{\mathcal{P}^t} - 1)^{\frac{\Theta_{\bar{f}}}{1-\Theta_f}}}$$

- Here $\mathcal{P}_{\Theta_1}$ and $\mathcal{P}_{\Theta_2}$ represent the probabilities of x being fake, given that the affected user u (Θ_f, $\Theta_{\bar{f}}$) flagged it and did not flag it, respectively.
- Observe that for if the user flags randomly ($\Theta_f = 0.5, \Theta_{\bar{f}} = 0.5$), rarely flags ($\Theta_f = 0, \Theta_{\bar{f}} = 1$) or always flags ($\Theta_f = 1, \Theta_{\bar{f}} = 0$) no advantage of one-step lookahead

Non-Idealistic Scenario: Continuation

- Expected Utility obtained if we wait for the next time-step

$$\begin{aligned}\mathbb{E}(UTIL(T+1)|\mathcal{H}^t) =& (\mathcal{P}^t\Theta_f + (1-\mathcal{P}^t)(1-\Theta_{\bar{f}})) \cdot U(\mathcal{P}_{\Theta_1}, t+1) \cdot (\mathcal{P}_{\Theta_1}(\mathrm{val}(t+1)) - \gamma) \\ &+ (\mathcal{P}^t(1-\Theta_f) + (1-\mathcal{P}^t)\Theta_{\bar{f}}) \cdot U(\mathcal{P}_{\Theta_2}, t+1) \cdot (\mathcal{P}_{\Theta_2}(\mathrm{val}(t+1)) - \gamma)\end{aligned}$$

- Here $U(\mathcal{P}_{\Theta_1}, t)$ is a step-function evaluated on $\mathcal{P}_{\Theta_1}(\mathrm{val}(t+1)) - \gamma$. This equation can also be interpreted in the following manner (both are inter convertible mathematically),

$$\begin{aligned}&\mathcal{P}^t \cdot \left(\mathbb{E}\left[U\left(\mathrm{Est}(t+1 \mid \mathrm{Est}(t), Y^*(x) = f) \cdot \mathrm{val}(t+1) - \gamma\right) \cdot (\mathrm{val}(t+1) - \gamma)\right]\right) \\ &+(1-\mathcal{P}^t) \cdot \left(\mathbb{E}\left[U\left(\mathrm{Est}(t+1 \mid \mathrm{Est}(t), Y^*(x) = \bar{f}) \cdot \mathrm{val}(t+1) - \gamma\right) \cdot (-\gamma)\right]\right)\end{aligned}$$

where $\mathrm{Est}(t)$ is a random variable denoting the estimate of the news being fake at time which conditioned on $\mathcal{H}^t$

Frame Title

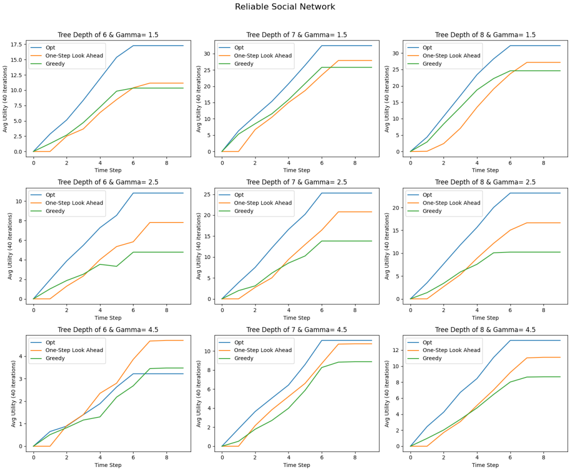


Figure: Performance Analysis of Algorithm with Depth of Tree and γ

Frame Title

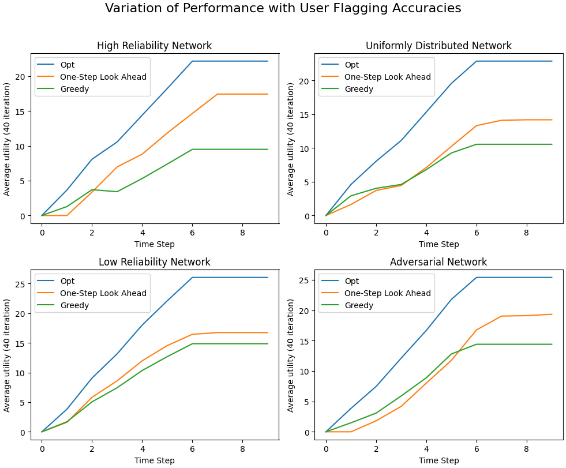
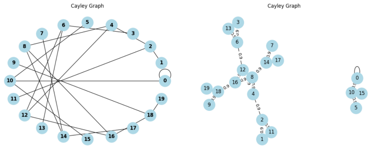


Figure: Performance Analysis of Algorithm with Variation in Social Network

Cayley Graphs



(a) Cayley Graph for $Z20$ group with generator 2 (b) Alternate view of 10a

Figure 10: Cayley Graph for $Z20$ group with a single generator

Figure: Cayley Graph for Z20 group with a single generator

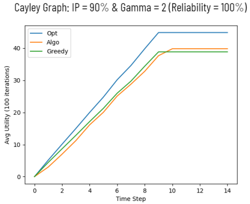


Figure: Performance Analysis of Algorithm for Realistic Social Networks

Its All About Estimation: Approximating One-Step Look-Ahead

$$\mathcal{P}^t \cdot \left(\mathbb{E}\left[U\Big(\mathsf{Est}(t+1 \mid \mathsf{Est}(t), Y^*(x) = f) \cdot \mathrm{val}(t+1) - \gamma \Big) \cdot (\mathrm{val}(t+1) - \gamma) \right] \right)$$
$$+(1-\mathcal{P}^t) \cdot \left(\mathbb{E}\left[U\Big(\mathsf{Est}(t+1 \mid \mathsf{Est}(t), Y^*(x) = \bar{f}) \cdot \mathrm{val}(t+1) - \gamma \Big) \cdot (-\gamma) \right] \right)$$

- For graphs with high influence probabilities $\mathrm{val}(t+1)$ is a nearly a constant constant and the independence assumption holds
- The main approximation is taking the Expectation inside the non-linear step-function

$$\approx \mathcal{P}^t \cdot \left(U\Big(\mathbb{E}\left[\mathsf{Est}(t+1 \mid \mathsf{Est}(t), Y^*(x) = f) \right] \cdot \mathbb{E}\left[(\mathrm{val}(t+1) \right] - \gamma \Big) \cdot \mathbb{E}\left[(\mathrm{val}(t+1) - \gamma) \right] \right)$$
$$+(1-\mathcal{P}^t) \cdot U\Big(\mathbb{E}\left[\mathsf{Est}(t+1 \mid \mathsf{Est}(t), Y^*(x) = f) \right] \cdot \mathbb{E}\left[(\mathrm{val}(t+1) \right] - \gamma \Big) \cdot (-\gamma) \Big] \Big)$$

Simulation Results

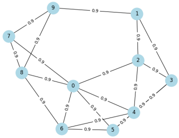
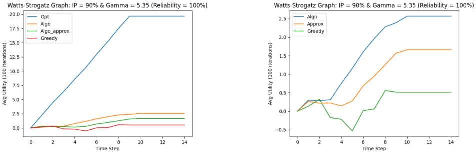


Figure: Watts-Strogatz graph with 10 nodes



(a) Gamma = 5

(b) Gamma = 5.35%

Figure: Performance Evaluation for Algo Appprox

- Increase in γ has a higher effect on the Greedy algorithm, which is intuitive as the effective decrease for one-step look ahead is $\Delta\gamma \cdot \beta$ whereas for Greedy its simply $\Delta\gamma$.

Moving Towards the Learning Setting

Logarithmic Regret Bound on Source Reliability Algorithms

- Consider a setting where decisions regarding querying the Oracle are made immediately upon news generation
- In this we are learning the source reliability of the algorithm

Theorem

The Regret suffered by the corresponding learning algorithm based on Thompson Sampling $\frac{4}{\gamma-\beta}\ln T + 2(\gamma - \beta)$

Intuition:

- Notice here that this problem of ours can be converted into a 2-armed bandit, where the action here is to choose or not whether to query to the Oracle for the news.
- Also in this setting, the rewards for one of the arms is deterministic and 0 .

Diversion: PSRL

Notation: For every episode k of fixed horizon τ, we run the optimal policy μ_{M_k} for the MDP M_k, whose parameters (rewards and transition probabilities) are obtained from posterior sampling (Thompson sampling) based on the history H_{t_k}.

We define the regret incurred by a reinforcement learning algorithm π up to time T to be

$$\text{Regret}(T, \pi) := \frac{1}{T} \sum_{k=1}^{T/\tau_e} \Delta_k,$$

where Δ_k denotes regret over the kth episode, defined with respect to the MDP M^* by

$$\Delta_k = \sum_{s \in \mathcal{S}} \rho(s) \left(V_{\mu^*,1}^{M^*}(s) - V_{\mu_k,1}^{M^*}(s) \right),$$

with $\mu^* = \mu^{M^*}$ and $\mu_k \sim \pi_k(H_{t_k})$ and ρ the initial state distribution

Theorem

Theorem If f is the distribution of M^*, then,

$$E\left[\mathit{Regret}(T, \pi_\tau^{PS})\right] = O\left(\tau S \sqrt{AT \log(SAT)}\right)$$

Regret Analysis for One-Step LookAhead

One-step look-ahead approach, which allows for a maximum of 2 steps to make the decision on whether or not to query the oracle.

Claim: An optimal policy (which knows the user parameters and the network transition probabilities) will carry out a one-step look ahead approach at $t = 1$ and at $t = 2$ (final step of the episode) will act greedily for each of the news N.

Theorem

The corresponding learning algorithm (via posterior sampling) suffers a $O(\sqrt{T \log(T)})$ *regret wrt. the optimal algorithm (that knows the user reliability as well as the social network) that takes a maximum of 2 steps to make its decision for any news.*

Explorations

1. Multi-Oracle setting with known Oracle parameters
2. Approach to approximate flagging activity by majority algorithm
3. Regret Bounds wrt. Opt

References

1. **Detecting Fake News in Social Networks via Crowdsourcing**
   Sebastian Tschiatschek, Adish Singla, Manuel Gomez-Rodriguez, Arpit Merchant, Andreas Krause
2. **Leveraging the Crowd to Detect and Reduce the Spread of Fake News and Misinformation**
   J. Kim, B. Tabibian, A. Oh, B. Schoelkopf, M. Gomez-Rodriguez
3. **(More) Efficient Reinforcement Learning via Posterior Sampling**
   Ian Osband, Dan Russo, Benjamin Van Roy