

Social Network Analysis
Prof. Tanmoy Chakraborty
Department of Computer Science and Engineering
Indraprastha Institute of Information Technology, Delhi

Chapter - 10

Lecture - 03

So, last day we have discussed you know one type of you know cyber attack in terms of sock puppets and puppet masters. So, today we will discuss another application another so, again cyber security related applications. And, today we will see how to identify collusive activities in online social network. So, let me start by you know telling you a story, you know and this is really I mean that this is useful to motivate the problem.

So, when I joined triple IIT in 2017 I was given a responsibility of you know promoting a workshop. So, triple IIT D, you know started you know thinking of a organizing a workshop and I was new. So, I was given the responsibility of you know promoting the workshop on social network and that time I was not that social media savvy. So, I just wrote a simple post about the workshop on Twitter, assuming that you know this is a since this is about a scientific event, it would automatically attract audience ok.

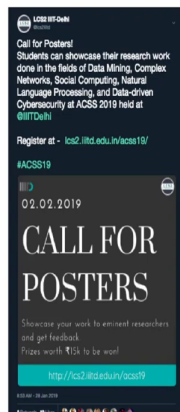
(Refer Slide Time: 01:31)

Sockpuppet Network

- A sockpuppet network is constructed from the Similar View Network by introducing an additional constraint
- According to Bu et al. (2013), puppetmasters have similar writing styles
- They prune SVN by adding additional authorship identification techniques
- Community detection algorithms on sockpuppet network can determine which sockpuppets belong to a certain sockpuppet group



(Refer Slide Time: 01:37)



5 Retweets in 3 days ??

Fun fact – Our lab has 37 active members!



But unfortunately, you know unfortunately in 3 days right, my post received only 5 retweets ok. I thought you know this should not have happened because this is ultimately about a scientific you know scientific event. So, it should automatically attract researchers, students, faculties, practitioners working in social network. The fun fact was that you know that time in my lab there were around 37 students; BTech, MTech, PhD, RA's right. In fact, they also did not care about retweeting my tweets right.

(Refer Slide Time: 02:19)

Publicity is hard... 😞😞



So, you all agree that publicity is really hard ok.

(Refer Slide Time: 02:24)



40 minutes and our research

later.....



And, when it comes to you know organic publicity right, you really need a reach right, a wide reach. A reach so, that you know people can just look at your tweet and just automatically retweet it right. But, nevertheless I knew the secret because I was working on you know analyzing the collusive activities in online social network.

(Refer Slide Time: 02:54)



30 Min



And, I just applied the tricks and look what happened after you know after 30 minutes. So, within 30 minutes my tweet got boosted by 70 retweets and 10 likes ok and this happened just within 30 minutes of applying my tricks ok. So, you may wonder what is the trick?

(Refer Slide Time: 03:19)



Shortcut to become popular on





So, before that before revealing the trick and let me also tell you some other you know a news events, news articles, stories that was that were quite popular. You may have heard about you know the story right by one of the socialist in the UK, Louise Mensch. So, Louise Mensch account right got a significant number of retweets, a significant number of followers within a very short period of time. Within only 24 hours, this person got around 80k followers right, 97 percent boost and that to within 1 day.

So, of course, people start started shouting that how it happened right, people did not have response, people did not have you know justification behind it. You may have heard about some Italian professors, you know he actually had doubt about political politicians retweet, politicians tweeter and their followers.

So, they claimed so, he claimed that majority of the followers of leading politicians are essentially fraud followers, fake followers right. Fake tweets fake Twitter account for newly appointed minister received thousands of followers. So, these kind of news articles are quite prevalent across social networks right, you may have heard about such news events in the past right.

(Refer Slide Time: 04:58)

Shortcut to become popular on Social Media



BLACK MARKET

Premium Service: Provide services upon receiving payment from the customers

Freemium Service: Unpaid services that require the users to provide their Twitter login details; this in turn may involve the users unconsciously in the blackmarket activities

LIKE 4 EXP
YOU LIKE HITS 20000 POINTS
Devumi
JUST RETWEET

So, if you wonder right what actually makes all these accounts popular within such a small period of time and that too in such a way that the Twitter will not be able to identify. To detect such you know such activities right here is the solution. So, on social media there are multiple such black market services right. This black market services are open, they openly promote you know their services right.

What they do? Say, if you want to boost your boost the boost your tweet for example, boost your follower, boost your Twitter account, if you want to boost your YouTube video, if you want to boost your Facebook profile right; you just contact this black market services and they will give you the service right.

So, services like there are multiple such black market services publicly available. Like 4 Like, Just Retweet, You Like Hits, Devumi; these are all different type of different types of black market services which provide you with retweets, follows, you know views, likes and what not ok.

So, if you look at the way they operate right, there are two modes of operations. The first one is called premium service. So, the default is premium service. So, premium service is very simple. You go you basically approach them and you tell them you know your desire, your event right, they will charge you lump sum ok and this is really lump sum ok.

I mean I have tried it for my research. So, you can also try it out, although it is not recommended as such. They charge lump sum. But, if you do not have money, you still can opt for this for their services right by opting for this freemium service. Now, what does it mean? So, freemium services are essentially unpaid services right.

Say for example, you want to boost your tweet right, you contact them and what they would do, they would you know they would take control of your account of your Twitter account. So, your Twitter account will be compromised for a certain period of time right. And, your Twitter account will be used by them to do all such crap activities, followers, retweets, following, following others, retweeting others tweets and so on.

And, through these activities your account will gain virtual credits right and then you can use these virtual credits to promote your own event right. So, your account will be compromised for a certain duration, for say 3 days, 4 days of duration. When you get significant coins, significant virtual credits you can then use this to and then your again account you will get control of your account. And, you can use your this virtual credits to boost your post right.


So, the interesting part about the freemium services is that the normal customer like us right, they become you know the part of the black market services at a particular time period right. So, in general since we are normal customers, our behaviors our behavior is quite organic right. But, for a limited period of time our behavior becomes inorganic, when our account is controlled by the black market services right.

So, it is very difficult to identify freemium activities because the customer right genuine customers like us they become part of the black market services and start doing all these inorganic activities at certain point. And, then after that they again they are free and they start doing organic activities. So, you see a mix of organic and inorganic activities exhibited by right this freemium customers.

So, our research is focused on our research completely focuses on freemium services right. In fact, the you know the topic that I am going to cover today is basically a part of our research, our labs research.

(Refer Slide Time: 09:49)

Twitter Terms of Service for fake engagements



About fake engagements on Twitter

Can I purchase or sell account interactions (e.g., Twitter followers, Retweets or likes) on Twitter?

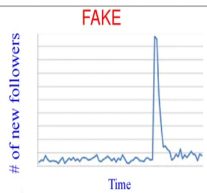
No. Twitter strictly prohibits the purchasing and selling of account interactions on our platform. When you purchase followers, Retweets and Likes, you are often purchasing bot-fake or hacked accounts. Any account caught participating in this behavior will be in violation of the Twitter Rules and may be suspended.

- If your account is found to have purchased followers, Retweets and Likes, your account may be suspended.
- If your account is promoting the selling of followers, Retweets and Likes, your account may be suspended.
- If your account is set up with the sole purpose of selling followers, Retweets and Likes, your account may be suspended.

Bookmark or share this article


[f](#) [in](#) [d](#) [R](#)

FAKE



of new followers

Time



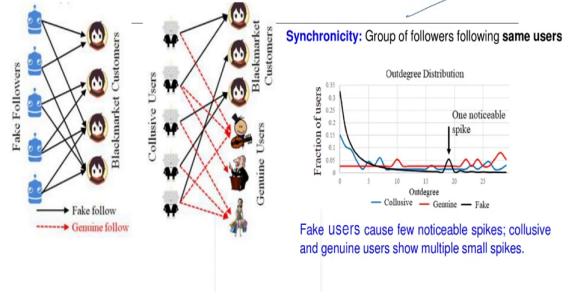
So, now this is you know totally against the terms and conditions of Twitter right because Twitter strictly said that fake see if. So, the question is can I purchase or sale account interactions right on Twitter? And, the answer is no. Twitter strictly prohibits the purchasing and selling of account interactions on our platform right.

So, this is against the terms and conditions of Twitter right. So, this is a kind of a harmful activities because, ultimately you are boosting your tweets or your events based on some inorganic activities. And, your boosted tweets would further you know influence somebody else to do some other activities right.

Now, think of this tweet that you are that you are boosting is a hate speech right, then this hate speech starts propagating right massively and people may get provoked right by this hate speech. And, then you know that may lead to communal violence and what not ok. So, if you look at the state of the art right, studies for say bot detection, fake account detection, fake activity detection.

(Refer Slide Time: 11:27)

Unlike Fake Users, Collusive Users are
“Asynchronous”



Most of the cases what people claimed that there is a synchronicity right, in terms of you know there is a synchronicity in terms of in terms of the time this activities happen right, the set of users that this fraud users follow, the you know the kind of posts that this fraud users write. So, these things are more or less same, though they tend to write similar kind of posts, they tend to follow others around the same time, they tend to follow same types of users right.

So, most of the existing studies claim that fraud activities are synchronous in nature ok but, we showed in our research that collusive activities are asynchronous and that is very obvious because there is no synchronicity between my activity and say your activity, both of us both of our accounts say have been compromised. My account has been compromised in one point; your account has been compromised by another in another time right.

But, there is no synchronicity right, there is no time synchronicity. If you think about sock puppets right, sock puppet activities are synchronous. Therefore, we consider the time duration you will hopefully you remember right, the time duration as for the signals to capture you know sock puppet activities. So, you know so, so here we claim that collusive activities are asynchronous in nature.

Therefore, we also showed empirically that state of art methods for detecting fraud activities are not useful for collusive activity detection ok. So, for that what we proposed, we proposed

a method called CoReRank, CoReRank core CoReRank right which is an unsupervised approach for collusive activity detection ok.

(Refer Slide Time: 13:35)

CoReRank: Detect Collusion in OSNs



Introduced by Chetan et al. in 2019
 A user u is said to support a tweet t if u retweets/quotes t
 Define the degree of support $S(u, t)$ as

$$S(u, t) = \begin{cases} \omega_q & \text{if } u \text{ quoted } t \\ \omega_r & \text{if } u \text{ retweeted } t \\ 0 & \text{otherwise} \end{cases}$$

Usually, $0 \leq \omega_r \leq \omega_q \leq 1$, as quoting a tweet has a higher chance of being a genuine action

A support network is a directed bipartite network $G(U, T, E)$, where

- U : set of users
- T : set of tweets supported by the users in U
- Weighted edge (u, t) denotes that user u supports tweet t
- Weight of edge (u, t) is given by $S(u, t)$



So, let us look at this CoReRank algorithm. So, this was proposed by my team right in 2019 published in WSDM conference. So, what it does? It first creates a bipartite network; user, post, bipartite network right. So, from the bipartite network, it measures two quantity. One is called the credibility of a user; other is called the merit of a tweet. I will discuss what do you mean by this. I am just trying to give you the overview of the algorithm.

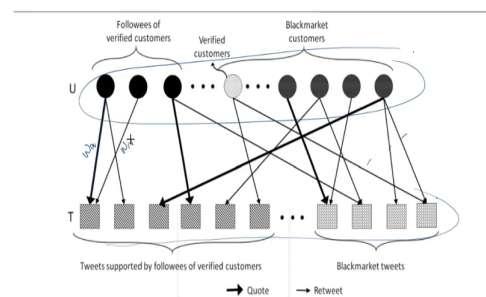
So, from the bipartite network, we measure the credibility of the user and the merit of a tweet. And, in some ways you we basically employ an iterative approach which is unsupervised. So, behavioral based iterative approach to measure the credibility and the merit right. And, then we said that ok you know so users with less credible credibility are collusive users and tweets with late less merit may merit values are basically you know fraud tweets ok.

So, we created a bipartite network right. So, in order to create the bipartite network, we basically define something called the degree of support right. So, user can support a tweet in two ways, by retweeting. So, retweeting is a direct citation of the tweet right or by quoting, quoting means you retweet with some additional text right. In this way, we basically support a tweet. Just to again reiterate, what is the problem statement here? The problem statement here is to detect collusive retweeters ok from Twitter so, right.

So, we basically define two quantities. This w_q is the amount of support due to quoting something and w_r is the amount of support due to retweeting something. So, w_q is greater than w_r , because when you quote something right, you basically add your own opinion and that is actually better than just retweeting something. So, whatever value we choose later, we need to make sure that this is satisfied. In fact, it should be like this ok. So, now we create a bipartite network.

(Refer Slide Time: 16:30)

Support Network in CoReRank: The Composition



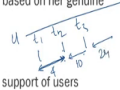
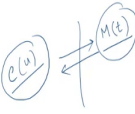
So, in a bipartite network, what are the users? So, users are some users are taken from black market; some users are normal users and so on. Now, remember this is a unsupervised method. So, the identity of a user whether the user is a part of a black market service or not, this is completely you know flagged in the in our algorithm.

So, flag the algorithm does not know which user is part of which I mean part of black market services right. So, we have some black market users, we have some normal users, we have some verified users, we have their followers, followees and so on right. And, that constitutes the user set right and the tweets that they retweeted within a particular period of time, you know when we basically script the data that constituted the tweet partition.

So, we have user partition and tweet partition and then you have basically two kinds of edges right. One is a retweeted edge, other is a quote edge. So, this bold lines are quoted edges and the thin lines are retweeted retweet edges right and we have w_q width and w_r width right.

(Refer Slide Time: 18:04)

CoReRank: Formulation



- The **credibility of a user** indicates how likely that user is to support a tweet based on her genuine appeal with the content of the tweet
- The **merit of a tweet** is a quality of the tweet to garner the genuine organic support of users
- The difference between the times of support to two consecutive support to tweets by a user u is termed as the **inter-support Time**

$C(u)$: Credibility score of a user u , $0 \leq C(u) \leq 1$

$M(t)$: Merit value of a tweet t , $0 \leq M(t) \leq 1$

$IST(u)$: Set of all inter-support times of the user u



Then, we do propose something called the credibility of a user. So, the credibility of a user u denoted by $C(u)$ is essentially the. So, we let me also tell you that we also propose something called the merit of a tweet right. So, the of the credibility of a user is determined by the number of meritorious tweets the user has retweeted so far right. How do we quantify merit? We will discuss right, where similarly merit of a tweet is determined by the number of credible users who have retweeted that tweet or quoted the tweet right.

So, you see that credibility and merit are basically interlinked ok. So, we will see how to compute credibility and merit. Then, we look at an important you know quantity which is the inter support time right. So, the inter support time for a user so, what we did for every user we have we basically noted down the tweets t_1 t_2 t_3 right. These are the tweets that this user retweeted right.

And, you also know the time, when this retweet retweets happened right. So, for every consecutive tweets, retweets we can identify the time difference right; so, t_1 t_2 t_2 t_3 and so on and so forth. And, then right so, so IST is the Inter Support Time, inter support time is basically the time duration between two consecutive retweets right. Say 4 minute right, 10 minutes, 24 minutes and so on. This is basically a set right.

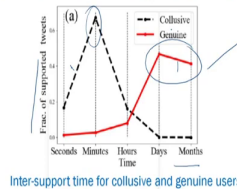
(Refer Slide Time: 20:28)

CoReRank: Formulation

□ **Axiom 1:** Collusive users have very less inter-support times compared to genuine users

□ Formally,

$$\exists u_1, u_2 \in U, C(u_1) < C(u_2) \Rightarrow \text{avg}(IST(u_1)) < \text{avg}(IST(u_2))$$



So, so then we came up with some axioms right. So, the first axiom was collusive users have very less inter support times compared to genuine users. Meaning, that collusive users basically retweets, they retweet in a very quick manner, in a very short duration right.

See, the plot here x axis is the time of retweeting, this IST inter support time and y axis is the number of such cases right. And, this black line indicates the collusive behavior and red line indicates a genuine behavior right. You see that there is a peak for a collusive user is a peak right, at the minute granularity right. It means that the average inter support time for collusive users is mostly in terms of minutes whereas, for genuine users the peak is here, days and months right. So, this was the first axiom right.

(Refer Slide Time: 21:43)

CoReRank: Formulation

- Two tweets t_1 and t_2 are said to have identically collusive support if
 - They have equal number of users supporting them
 - For every user u_1 with credibility score $C(u_1)$ supporting t_1 , there exists a user u_2 with credibility score $C(u_2)$ supporting t_2 such that $C(u_1) = C(u_2)$
- Axiom 2: Among tweets with identically collusive support, a highly meritorious tweet receives higher support
- Formally, if two tweets, t_1 and t_2 have identically collusive support, and $S(u, t_1) \geq S(u, t_2)$, such that $C(u) = C(u')$, then $M(t_1) \geq M(t_2)$
- Axiom 3: A collusive user associated with blackmarket services demonstrates immense topical diversity



Then, we also observed that if you take two tweets t_1 and t_2 , we basically quantify something called identically collusive support right. What does it mean? It means that there are two tweets t_1 and t_2 retweeted by u_1 and u_2 right, such that the credibility of u_1 and the credibility of u_2 you know u_1 and u_2 is the same. So, u_1 is the retweeter of the tweet t_1 and u_2 is the retweeter of the tweet t_2 .

So, if you know the credibility of these two retweeters, u_1 and u_2 are the same, then we say that t_1 and t_2 are supported by identically collusive users right. They are different users, but they are collusive in nature, their credibility nature is the same. So, axiom 2 is basically saying that among tweets with identically collusive support, a highly meritorious tweet receives higher support right. You see two tweets t_1 and t_2 , although they are supported by the same credible users.

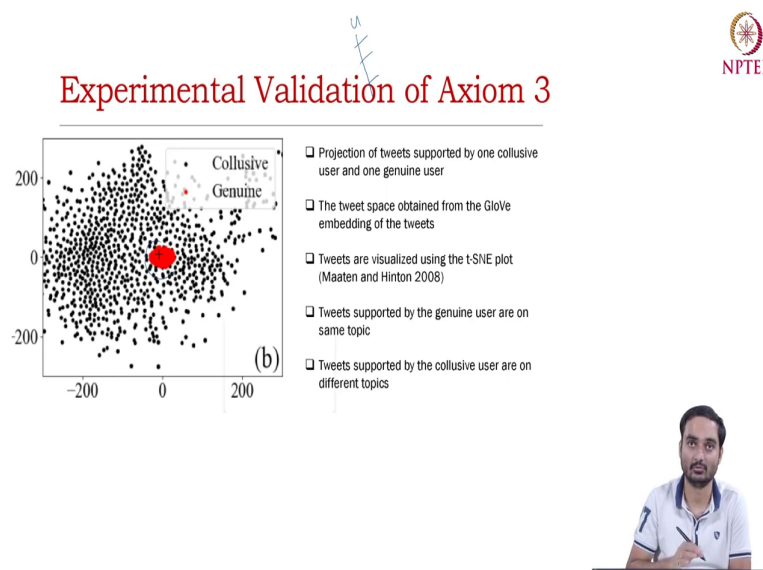
But, if t_1 has more merit than t_2 , then the support would be higher for t_1 than t_2 , it is very obvious right. The third axiom is a collusive user associated with black market services demonstrates immense topical diversity, what does it mean? So, think of a collusive user right and a collusive user is compromised by the black market services. And, the black market services basically use that account to retweet many other tweets right.

There may not be any topical similarity, it can be any type of topics right; sports, entertainment, politics right, you know some other events and anything right. Because, this account is used by somebody else, this account is not used by the actual user. But, if you

think of a genuine user like us right, our topical span is very limited. Say for example, in my case I generally retweet you know tweets of some of my favourite you know movie actor, actresses or researchers or singers.

Sometimes a few retweets you know based on some a few retweets of say you know some great politicians or philosophers and so on. So, my topical interest is very limited, it is not diverse right. But, since collusive user's accounts are compromised right, it can be I mean so, that account can be used for any purposes ok.

(Refer Slide Time: 25:31)




So, to validate this hypothesis what we did for every user right, we identified the tweets, collected the tweets and we basically used a you know a kind of topic detection method right, LDA or a simple deep learning based method right. And, then you know using the topic models, we get the topics and we basically get the representation of topics, not the actual topic. And, then we plot it in an embedding space. This is a t-SNE visualization, 2D visualization.

You see that so, this red dots are topical diversity of collusive users and black dots are genuine users. So, you see that red dots are all clustered; meaning their topic sorry I mean it is the other way around. So, the red dots are corresponding to genuine users and black dots correspond to collusive users. So, you see that for genuine users the topics are very clustered whereas, for collusive users topics are scattered all over the place ok. We will use this clues for detecting collusive users.

(Refer Slide Time: 26:53)

CoReRank: Formulation



Define the credibility $C(u)$ of user u as

$$C(u) = \frac{\sum_{t \in \text{Out}(u)} \gamma_{1u} \cdot M(t) \cdot S(u, t) + \gamma_{2u} \cdot \pi_U(u) + \gamma_{3u} \cdot \tau_U(u) + \gamma_{4u} \cdot \mu_U}{\gamma_{1u} + \gamma_{2u} + \gamma_{3u} + \gamma_{4u} + |\text{Out}(u)|}$$

- All the γ terms are constants
- These constant values are tuned using parameter sweeping
- $\pi_U(u)$: an initial anomaly score
 - Obtained using BIRDNEST algorithm proposed by Hooi et al. (2016)
- $\tau_U(u)$: topical-diversity score for a user
 - Obtained by average cosine similarity between pairs of tweets supported by the user
- μ_U : a smoothing constant to prevent bias against users with sparse connections

Handwritten notes:

$C(u) = \frac{\sum_{t \in \text{Out}(u)} \gamma_{1u} \cdot M(t) \cdot S(u, t) + \gamma_{2u} \cdot \pi_U(u) + \gamma_{3u} \cdot \tau_U(u) + \gamma_{4u} \cdot \mu_U}{\gamma_{1u} + \gamma_{2u} + \gamma_{3u} + \gamma_{4u} + |\text{Out}(u)|}$

$\pi_U = 1 - A_U$

$\tau_U = 1 - A_T$

Cold Start Problem



Let us now see how to compute the credibility and the merit ok. Remember, we already have this bipartite network right, where you have the credibility of users and merit of a tweet right and we have weights right and this course we will determine ok. So, to start with what we do? We assign some seed values to these nodes, both types of nodes right.

And, the seed values are obtained from another algorithm called BIRDNEST right. So, what BIRDNEST does? BIRDNEST takes a bipartite network and with each node, we also need to provide a feature set, a vector right. It can be any vector and then BIRDNEST produces an outlier score for every node right. So, in our case for every node, for every user node we pass the inter support time right that set as a feature.

And, for every tweet we pass an embedding right of you know of the particular sentence, the particular tweet, it is a vector ok. So, what we will obtain? We will obtain seed score right, a seed anomaly score right something called say right A_U and A_T right. Now, since we are interested in the credibility which is just opposite of anomaly. So, the credibility seed score of for a user is basically π_U which is $1 - A_U$ and for tweet π_T $1 - A_T$ ok.

So, we will get this π_U this π_U is the seed value obtained from the barscore algorithm. Then, we have we also take the sum of all the merit scores of the tweets that the particular user has retweeted. So, for all the outward edges of a particular user u , you take the sum of all the merits ok and it is parameterized by this gamma ok.

So, you have $\gamma_1 u$ corresponding to this M_t component, you have $\gamma_2 u$ corresponding to the BIRDNEST score. Similarly, we also consider the topical diversity of a user. Topical diversity of a user is basically calculated by the cosine similarity of all pairs of two tweets that a particular user has retweeted right ok. So, an average cosine similarity and that is our topical diversity score, it is again parameterized ok.

And, then we have another score which is μ_U , this μ_U is a score that is useful for a to avoid cold start problem. So, what is this cold start problem? Cold start problem; so, cold start problem is a very famous you know limitation, very well known limitation in IR system, Information Retrieval system. Say for example, there is a there is a relevant web page right and there is a query and the web page is relevant to the query.


But, since the web page is new, assume that the web page is new, newly created, due to the lack of historical data; number of clicks right, number of browsing histories for the particular web page, that web page will never come to the top of the ranking. So, this is called a cold start problem. The entity does not have enough history to boost its identity ok.


So, to avoid this, here also if a user is a credible user right due to the less historical information he or she may not be you know may not be treated as a credible user. So, therefore, we use another parameter μ_U . Now, this μ_U is something that we will set empirically right and you know for this component also we have a parameter γ right.

So, this is some sort of I would say some sort of you know some sort of smoothing right. And, we normalize it by all the constants, all the parameters and the total out degree ok. So, you see here that the credibility of a user is dependent on the merit of a tweet that he has retweeted.

(Refer Slide Time: 32:16)

CoReRank: Formulation







Similarly, the merit of a tweet is the sum of all the credible sum of the credibilities of all the users who have retweeted the tweet right ok. And, remember this is multiplied by the support $S(u, t)$. Support can be with a right, sorry with r , with w_r , with w_q is the support for quote and so on ok.

And, along with this we have this BIRDNEST score, seed score and we have the parameter μ_T to address the cold start problem ok. And, this is normalized by the constants and the n degree. Remember, this is a directed graph, directed by body graph user tweet right. So, for user this would be out degree, for tweet this would be in degree ok.

(Refer Slide Time: 33:24)

CoReRank Algorithm

Algorithm 1: CoReRank Algorithm (taken from Chetan et al. (2019))

Input : $G(U, T, E), \gamma_{1u}, \gamma_{2t}, \gamma_{3t}, \gamma_{4u}, \gamma_{2u}, \gamma_{3u}, \gamma_{4u}$
Output : Credibility and merit scores for all users and tweets

- 1 Calculate $\pi_U(u) \forall u \in U$ and $\pi_T(t) \forall t \in T$
- 2 Initialize $C(u)^0 = \pi_U(u)$ and $M(t)^0 = \pi_T(t) \forall u \in U, \forall t \in T$
- 3 Initialize $\mu_U = \frac{\sum_{u \in U} C(u)^0}{|U|}$ and $\mu_T = \frac{\sum_{t \in T} M(t)^0}{|T|}$
- 4 $k = 0$
- 5 error = maximum possible integer value
- 6 **while** error $> \epsilon$ **do**
- 7 $k = k + 1$
- 8 $\tilde{C}^{k-1}(u) = \text{norm}(C^{k-1}(u)) \forall u \in U$ such that $\tilde{C}^{k-1}(u) \in [0, 1]$
- 9 Update the merit of tweets using Equation 6: $\forall t \in T$,
- 10 $M^k(t) = \frac{\sum_{u \in \text{In}(t)} \gamma_u \tilde{C}^{k-1}(u) S(u, t) + \gamma_{2t} \pi_T(t) + \gamma_{3t} \mu_T}{\gamma_u + \gamma_{2t} + \gamma_{3t} + |\text{In}(t)|}$
- 11 Update the credibility of users using Equation 7: $\forall u \in U$,
- 12 $C^k(u) = \frac{\sum_{t \in \text{Out}(u)} \gamma_u M^k(t) S(u, t) + \gamma_{2u} \pi_U(u) + \gamma_{3u} \gamma_u + \gamma_{4u} \mu_U}{\gamma_u + \gamma_{2u} + \gamma_{3u} + \gamma_{4u} + |\text{Out}(u)|}$
- 13 error = $\max(\max_{u \in U} |C^k(u) - C^{k-1}(u)|, \max_{t \in T} |M^k(t) - M^{k-1}(t)|)$
- 14 **end**
- 15 **return** $C^k(u) \forall u \in U$ and $M^k(t) \forall t \in T$



So, now let us look at the algorithm, the CoReRank algorithm. So, CoReRank algorithm starts with an arbitrary value of right are arbitrary initial value of this cold start value mu U and mu T right. And, you also initialize credibility and merit in some ways right and then you update keep on updating the values of merit and credibility.


Until unless, you see that the change of the values of credibility and merit in two consecutive iterations is less than the threshold some threshold right, some threshold epsilon. Now, this is user defined right and this indicates the convergence, think about it. This is completely unsupervised method ok and what you get at the end of the day?

We get the credit the credibility score of every user and the merit score of every tweet right. And, then we rank the users based on the credibility and those users who have less credibility are returned as collusive users and those tweets which have less mid scores are returned as collusive tweets ok. So, if you go through the paper, we also theoretically show that this algorithm has some beautiful properties.

For example, this algorithm you know converges within a bounded number of iterations right. And, we also you know we also showed that you know there exists right between two consecutive iterations, the difference between the scores right C u C and M, the difference between the score is again bounded right.

So, we showed we proved that C_u at iteration k minus C_u at iteration k minus 1 is basically bounded by $3/4$ to the power some constant k ok. And, we also showed empirically that you know this outperforms, this method outperforms other fraud detection methods right. And, this is kind of the first method for collusive entity detection using an unsupervised method ok.

(Refer Slide Time: 36:14)




Blackmarket-driven Collusion on Online Media: A Survey

HRIDOY SANKAR DUTTA*, IIT-Delhi, India
TANMOY CHAKRABORTY, IIT-Delhi, India

Online media platforms have enabled users to connect with individuals, organizations, and share their thoughts. Other than connectivity, these platforms also serve multiple purposes - education, promotion, updates, awareness, etc. Increasing the reputation of individuals in online media (aka Social growth) is thus essential these days, particularly for business owners and event managers who are looking to improve their publicity and sales. The natural way of gaining social growth is a tedious task, which leads to the creation of unfair ways to boost the reputation of individuals artificially. Several online blackmarket services have developed thriving ecosystem with lucrative offers to attract content promoters for publicizing their content online. These services are operated in such a way that most of their inorganic activities are being unnoticed by the media authorities, and the customers of the blackmarket services are less likely to be spotted. We refer to such unfair ways of bolstering social reputation in online media as collusion. This survey is the first attempt to provide readers a comprehensive outline of the latest studies dealing with the identification and analysis of blackmarket-driven collusion in online media. We present a broad overview of the problem, definitions of the related problems and concepts, the taxonomy of the proposed approaches, description of the publicly available datasets and online tools, and discuss the outstanding issues. We believe that collusive entity detection is a newly emerging topic in anomaly detection and cyber-security research in general and the current survey will provide readers with an easy-to-access and comprehensive list of methods, tools and resources proposed so far for detecting and analyzing collusive entities on online media.

Additional Key Words and Phrases: Collusion, blackmarket, Twitter, YouTube, social media analysis



So, if you want to know more about the collusive activity identification techniques, we also wrote a survey paper; Blackmarket-driven Collusion Online social network. This is available online. So, you can go through it and you can get to know about you know the kind of summary of all the methods that have been proposed so far for collusive entity detection ok. So, we stop here. In the next lecture, we will discuss another application of network science which is basically modeling the COVID-19 spread ok.

Thank you.