Dynamic Rumour Influence Minimisation with Internet Cyber Crime

K. Maheswaran, T. Balasathuragiri
M.Tech.,Computer Science and Engineering, Prist University
Assistant Professor Faculty of Engineering and Technology
Department Of Computer Science and Engineering, Prist University
(Deemed to be University Under section 3 of UGC act 1956)
Thanjavur, Tamil Nadu, India

Abstract

Today's global scenario reflects communication is the great innovation plays an important role on day to day life of human and all creatures in the world. From once cell bacteria to 6th sense human being communicated to each other in natural way. Hence communication been exists in this world from day one where world been created. How human intelligence been played in the roll of communication? is million dollar question. Actually human making machines and nature gives SPECTRUM. Then who made spectrum? Naturally humans were not. When this research continuous and will become an end when human intelligence overcome spectrum otherwise naturally human intelligence will fail or spectrum will challenge humans. Instead of artificial intelligence we need to study natural intelligence in this modern communication systems.

The online world of cybercrime presents equally critical decisions for you to make, but there are no obvious signs like oncoming headlights. Instead, you get a silent "security warning", a link with a tempting offer, or a text message from an unknown sender. Will you choose the right option or will you get attacked? Will you "Allow" or "Deny" the cybercriminal to have their way with you? In today's online world, every click matters.

Cyber criminals are increasingly targeting victims through a text message scam called "smishing" that can infect your smartphone, laptop and let thieves steal your personal information. That means social security numbers, addresses, and even your credit card information can all be vulnerable through a simple, unassuming text message you receive.

"It may say something like, $500 was just withdrawn from your bank account, did you do it? If not, call this phone number," Pierson Clair, senior director of cyber security and investigations at Kroll, told NBC News. "There are millions of these text messages sent out every single day targeting everybody from small children to grandmothers and everybody in between." Hackers usually send the smishing messages with a link or phone number. If you call or click, they'll then be able to harvest more data.

Americans lost $1.3 billion to cyber crime in 2016, according to the FBI. That number is expected to rise as criminals get craftier and go after unsuspecting victims in new ways. "A phone or laptop is something you always have on you,". "And if you always have it on you, and you're moving quickly through life, you'll have taken your phone out and you'll say, 'Oh no!' And you'll actively respond to it. And then they've got you." There isn't a way to block scammers from sending smishing messages, so experts recommend being skeptical if you're not sure about a text.

Don't click the link or call the number. Instead, look at your bank's app independently and call a verified phone number. Finally, remember to delete suspicious texts. The bottom line, Clair said: "Trust no one. Validate everything."

“DRIMUX – Dynamic Rumour Influence Minimisation with User Experience” can be a concept of detective intelligence during national threats. The communication can be any mode but the concept of understanding may vary according to the encryption and decryption. Such encryptions may happen at level of user understanding or traditional communication like text, voice, picture and symbols. Threats can be any part like email, messaging, hackers, pornography and special intelligence also, such case how to overcome the challenge of identification of such threats and to stop such communications.

In this project we address the problem of setting thresholds to filter rules, by conceiving and implementing within FW, an Online Setup Assistant (OSA) procedure. In defining the language for FRs (FILTERING RULES) specification, we consider three main issues that, in our opinion, should affect a message filtering decision. Similar to FRs, our BL (BLOCK) rules make the wall owner able to identify users to be blocked according to their profiles as well as their relationships in the OSN. Therefore, by means of a BL rule, wall owners are for example able to ban from their walls users they do not directly know (i.e., with which they have only indirect relationships), or users that are friend of a given person as they may have a bad opinion of this person. This banning can be adopted for an undetermined time period or for a specific time window. Moreover, banning criteria may also take into account users’ behaviour in the OSN. More precisely, among possible information denoting users’ bad behaviour we have focused on two main measures. The first is related to the principle that if within a given time interval a user has been inserted into a BL for several times, say greater than a given threshold, he/she might deserve to stay in the BL for another while, as his/her behaviour is not improved.

INTRODUCTION

1.1 PROJECT DESCRIPTION

That recent tech innovation known as the internet has made keeping in touch with family and friends easier than ever but it might also have brought you some unwelcome attention from people you’d rather not keep up correspondence with. If you want to minimize the chances of getting contacted out of the blue, here’s what to do. We’re only going to cover some simple privacy tips here without wading into any legal issues, but if something more serious is going on, there are tools you can use to make a report: read up on the instructions for Facebook, Twitter, and Instagram.

With the soaring development and rising popularity of large-scale social networks such as Twitter, Facebook, and Chinese SinaWeibo, etc., hundreds of millions of people are able to become friends and share all kinds of information with each other. Online social network analysis has also attracted growing interest among researchers. On one hand, these online social platforms provide great convenience to the diffusion of positive information such as new ideas, innovations, and hot topics. On the other hand, however, they may become a channel for the spreading of malicious rumors or misinformation. For example, some people may post on social networks a rumour about an upcoming earthquake, which will cause chaos among the crowd and hence may hinder the normal public order. In this case, it is necessary to detect the rumour source and delete related messages, which may be enough to prevent the rumour from further spreading. However, in certain extreme circumstances such as terrorist online attack, it might be necessary to disable or block related Social Network (SN) accounts to avoid serious negative influences. For instance, in 2016, the families of three out of the forty nine victims from the Orlando nightclub shooting incident filed a lawsuit against Twitter, Facebook and Google for providing “material support” to the terrorism organization of the Islamic State of Iraq and Syria (ISIS). These companies then took measures to block related accounts, delete relevant posts and fanpages on their social network platforms to prevent the ISIS from spreading malicious information. Additionally, Facebook et al. also have issued relevant security policies and standards to claim the authority to block accounts of users when they are against rules or at risk. Undoubtedly, malicious rumors should be stopped as soon as possible once detected so that their negative influence can be minimized.

Most of the previous works studied the problem of maximizing the influence of positive information through social networks. Fast approximation methods were also proposed to influence maximization problem. In contrast, the negative influence minimization problem has gained much less attention, but still there have been consistent efforts on designing effective strategies for blocking malicious rumors and minimizing the negative influence. Budaetal. introduced the notion of a “good” campaign in a social network to counteract the negative influence of a “bad” one by convincing users to adopt the “good” one. Kimuraetal.studied the problem of minimizing the propagation of malicious rumors by blocking a limited number of links in a social network. They provided two different definitions of contamination degree and proposed corresponding optimization algorithms. Fanetal.Investigated the least cost rumour blocking problem in social networks. They introduced the concept of “protectors” and try to select a minimal number of them to limit the bad influence of rumors by triggering a protection cascade against the rumour cascade. However, there are a few limitations in those works.

The big social networks all give you a certain level of control over who can contact you, though some have more granular options than others.

Facebook’s privacy settings always seem to be in a state of flux but right now the default setting is that anyone can send anyone a message on Facebook—but messages sent by people who you aren’t friends with go into a “Message requests” folder so you can scan them without responding, or ignore them completely.

Scope of the Project:

If you have to be friends with someone for whatever reason, but don’t want any messages from them, you can use the Mute option inside the conversation in Messenger. If that’s not enough, you can block them, which means your Facebook friendship is cancelled (if it was active in the first place) and no form of direct communication is possible from either side.

The options aren’t difficult to find: you can block someone through the conversation menu in Messenger, or via the main Facebook site by clicking on the menu button (three horizontal dots) on the person’s profile.

ver on Twitter you absolutely have to be following someone before that person can send you a direct message, unless you’ve opened up DMs to all, so you can simply block messages by unfollowing the sender. As for mentions in your timeline, you can hide these by muting users (click the cog icon on any profile page), or go further and do a full block (again via the same cog icon, or the expanded menu that appears by any tweet).

You can find similar mute and block options inside individual conversation threads on Instagram (tap the “i” icon to find the block setting). Instagram lets anyone send anyone a direct message, though there’s a Facebook-style approval process if you’re not already friends with someone. If you do block someone, any mentions of your username in comments by that person won’t show up, and they won’t be able to see your feed or message you. Meanwhile you can hide your stories from certain people via the Story Setting menu under Options in the mobile app.

Algorithm:1 Greedy Algorithm

Different from the greedy blocking algorithm, which is a type of static blocking algorithm, we propose a dynamic rumor blocking algorithm aiming to incrementally block the selected nodes instead of blocking them at once. In that case, the blocking strategy is split into several rounds and each round can be regarded as a greedy algorithm. Thus, how to choose the number of rounds is also very important for the algorithm. In the following part, we will elaborate on the algorithm design and how we choose the specific parameters. From the probabilistic perspective, we seek to formulate the likelihood of inactive nodes becoming activated in every round of rumor blocking. Correspondingly, the likelihood function is given by

$$f(t_1|s(t_0)) = \prod_{v \in V_{N_2}} \sum_{u:t_u \leq t_0} \alpha_{uv} p_{uv}(t_1) \times \prod_{\varrho:t_\varrho \leq t_0} e^{-\alpha_{\varrho v} \int_{t_\varrho}^{t_1} p_{\varrho v}(\tau) d\tau}.$$

Correspondingly, the objective function is

$$\begin{aligned} \min_{\mathbf{A}} \quad & f(t_1|s(t_0)) \\ \text{s. t.} \quad & \alpha_{uv} \in \{0, 1\}. \end{aligned}$$

Then, the greedy algorithm is presented as below:

```
Input: Initial Edge matrix A0
Initialization: VB = 0;
for i = 1 to K do
u = arg max [f (t1|s (t0); Ai-1) - f (t1 | s (t0); Ai-1\ )]
Ai: = Ai-1\u,
VB = VB U {u}
end for
Output: VB.
```

Mathematical Model of Existing System System S as a whole can be defined with the following main components.

S= {I, O, P, s, e, U, Uf, Ad};

S=System

s=Initial State

e=Final State

U= user

Uf=Set of user friends

Ad=admin

Input {I} = {Input1, Input2}

Where,

Input1=Text

Input2=Images

Procedures {P}= {Up,Sp,Ubloack,Rdetect}

Where,

Up=upload post.

Sp=Share Post.

Ubloack= Block user who sent or shared rumor text and images.

Rdetect=Detect rumor text and images.
Output {O} = {Output1, Output2}
Where,
Output1=detecting rumor texts & images
Output2=block user who sent or shared rumor text and images
s= {initially system will be in a state where user are not enrolled, Only admin of system.}
e= {users are enrolled and successfully post or share text or images & admin detect and rumor text and images and also block user who sent or shared rumor text and images }

Result of Existing System:

Existing system Detect rumor post and text and block userwho sent rumor test or image for long time so they may quit social network. And not delete rumor post.

1.2 HOW TO STOP UNWANTED TEXT MESSAGES

How text message spam will be the death of text message marketing and written an open letter to the Mobile Marketing Association. Recently so far as to commission my own text message spam report to show the industry how big of a problem we have on our hands. The report will come out in early August and without giving too much away, our findings show that text message spam is more than a problem, it's a pandemic. Even with all of these things I've done, it seems like the majority of text message providers don't give a crap as they continue to engage in shady, borderline illegal activities without any regard to consumers, the industry or the rules put in place by the mobile phone providers.

So instead of continuing to fight, now see as a losing battle, the next best thing is to empower the consumer and teach them how to fight off text message spam individually. Here are my 6 steps on how to stop unwanted text messages

1.3 NORTON COMPANY RESEARCH REPORT

Norton cyber security, consumers are overconfident in their security prowess, leaving them vulnerable and enabling cybercriminals to up the ante this year, which has resulted in record attacks.

978 million people in 20 countries were affected by cybercrime in 2017.

44% of consumers were impacted by cybercrime in the last 12 months.

The most common cybercrimes experienced by consumers or someone they know include:

- Having a device infected by a virus or other security threat (53%)
- Experiencing debit or credit card fraud (38%)
- Having an account password compromised (34%)
- Encountering unauthorized access to or hacking of an email or social media account (34%)
- Making a purchase online that turned out to be a scam (33%)
- Clicking on a fraudulent email or providing sensitive (personal/financial) information in response to a fraudulent email (32%)

As a result, consumers who were a victims of cybercrime globally lost $172 billion – an average of $142 per victim – and nearly 24 hours globally (or almost three full work days) dealing with the aftermath.

Cyber security concerns do not always seem to translate to good behaviours as many consumers put themselves at risk in their day-to-day lives. This leads us to a startling cybercrime confession: those who emphasize the importance of online security, generally contradict themselves through their actions, and as a result, are more likely to fall victim to cybercrime.

Cybercrime victims share three common traits:

Overconfident in Cybersecurity Prowess: Consumers who've fallen victim to cybercrime, emphasize the importance of online security more than non-victims, yet they're more likely to contradict their efforts through simple missteps. While 44% of consumers have personally experienced cybercrime, 39% of cybercrime victims globally report gaining trust in their ability to hold and protect their personal information and data and 33% believe they're at a low risk of becoming a cybercrime victim.

Favor Multiple Devices: Consumers who adopt the newest technologies and own the most devices are also more likely to be victims of cybercrime. More than one third (37%) own a gaming console and smart device, compared to 28% of non-victims. They're also almost twice as likely to own a connected home device than non-victims.

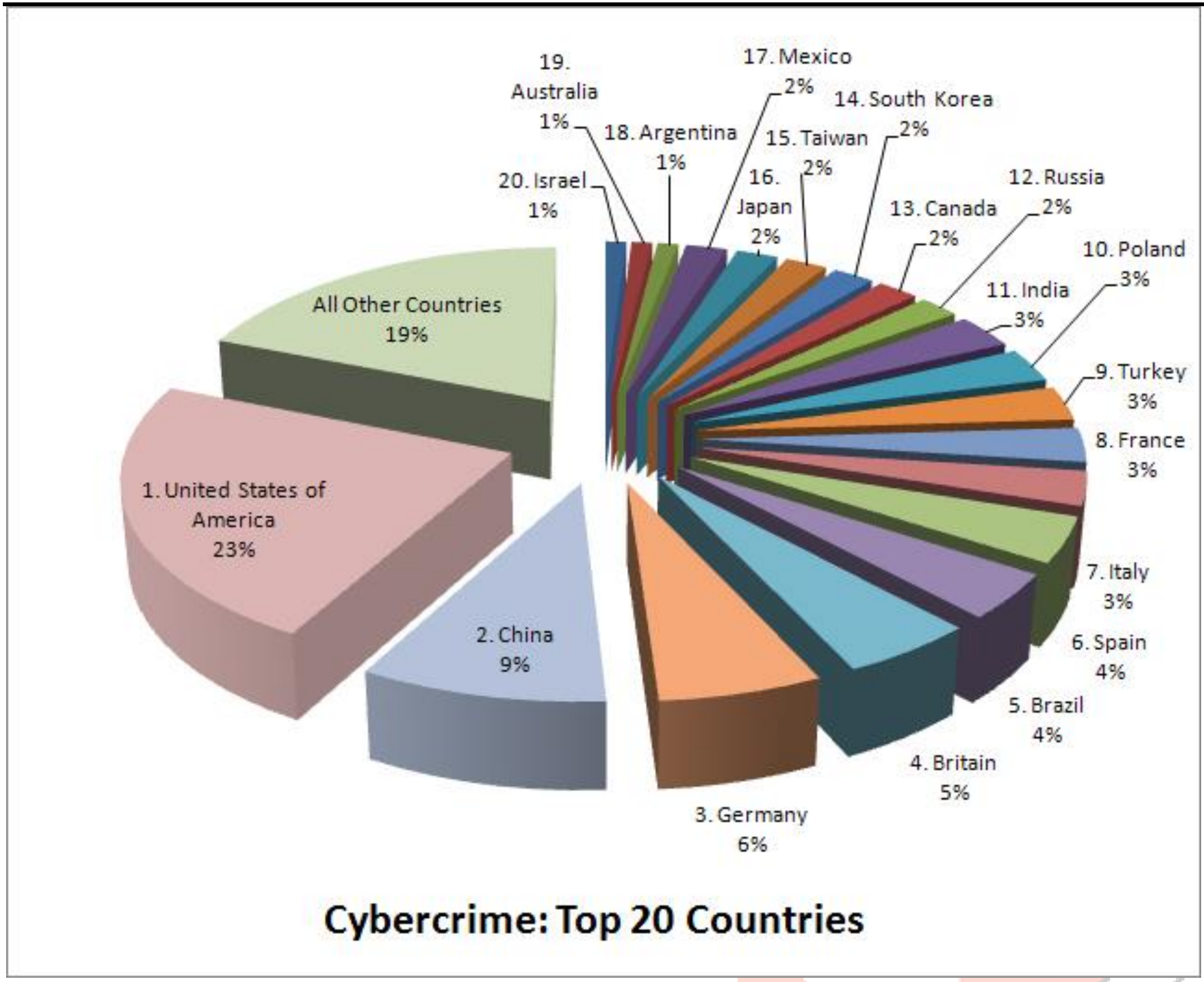
Dismiss the Basics: They practice new security techniques such as fingerprint ID (44%), facial recognition (13%), pattern matching (22%), personal VPN (16%), voice ID (10%) and two-factor authentication (13%). Yet, 20% of cybercrime victims globally use the same password across all online accounts and 58% shared at least one device or account password with others. By comparison, only 17% of non-cybercrime victims use the same password across all online accounts and 37% share their passwords with others

Consumers' boundaries skewed between cybercrime and "real life"

Confession: While 81% of consumers globally think a cybercrime should be treated as a criminal act, 43% believe it's acceptable to commit morally questionable online behaviours in certain instances:

Interestingly, 53 percent of cybercrime victims globally were more likely to think it was acceptable to commit morally questionable online behaviour than non-victims (32%):

Cyber Crime By Top 20 Countries:



Age distribution of people accused of a cyber-related violation against the person, by type of violation (sexual and intimidation), selected police services, 2012 – CANADA

	Sexual violations	Intimidation violations
Under 12 years	0.2	1.0
12 to 17 years	15.7	27.0
18 to 24 years	18.8	21.7
25 to 34 years	22.3	21.1
35 to 44 years	17.5	16.5
45 to 54 years	15.9	9.5
55 years and older	9.6	3.2

1.4 CONCLUSION

In this paper, we tend to investigate the rumor obstruction downside in social networks. we tend to propose the dynamic rumor influence reduction with user expertise model to formulate the matter. A dynamic rumor diffusion model incorporating each world rumor quality and individual tendency is conferred supported the Ising model. Then we tend to introduce the thought of user expertise utility and propose a changed version of utility perform to live the connection between the utility and obstruction time. After that, we tend to use the survival theory to investigate the probability of nodes obtaining activated beneath the constraint of user expertise utility. Greedy algorithmic rule and a dynamic obstruction algorithmic rule area unit projected to unravel the optimization downside supported totally different nodes choice methods. Experiments enforced on planet social networks show the efficaciousness of our methodology.

1.5 FUTURE ENHANCEMENT

After studying various scenarios of cybercrimes, we propose the dynamic rumour influence minimization with user experience model to formulate the problem not only to the social networks also to all text communications as part of firewall and security. A dynamic rumour diffusion model incorporating both global rumour popularity and individual tendency is presented based on the Ising model. Then we introduce the concept of user experience utility and propose a modified version of utility function to measure the relationship between the utility and blocking time. After that, we use the survival theory to analyze the likelihood of nodes getting activated under the constraint of user experience utility. Greedy algorithm and a dynamic blocking algorithm are proposed to solve the optimization problem based on different nodes selection strategies. Experiments implemented on real world social networks show the efficacy of our method. In our future work, we plan to design more sophisticated rumour blocking algorithms considering the connectivity of the social network topology and node properties. We intend to separate the entire social network, emails, messaging, smartphone applications with different user interests and then analyze the rumour propagation characteristics among communities. We are also interested in investigating how to prevent the rumour propagation effectively at a late stage.

1.6 REFERANCES

- 2017 Norton Cyber Security Insights Report – Global Results by Symantec
- C. Budak, D. Agrawal, and A. E. Abbadi, “Limiting the spread of misinformation in social networks,” in Proc. 20th Int. Conf. World Wide Web, 2011, pp. 665–674
- B. Wang, G. Chen, L. Fu, L. Song, and X. Wang, “Drimux: Dynamic rumor influence minimization with user experience in social networks,” in Proc. 30th AAAI Int. Conf. Artif. Intell., Feb. 2016.
- Statistica Canada - www.statcan.gc.ca
- Press release Department of Homeland Security – United states of America Booklet Cyber Crime Exposed