International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 11
ISSN: 2454-4248
10 –17

Spammers Detection on Twitter by Automated Multi Level Detection system

[1]G. Jhansi Mounika, [2]Y. Siva Koteswara Rao, [3]Dr. Gopisetti Guru Kesava Dasu
[1]PG Scholar, [2,3]Professor
[1,2,3]Department of Computer Science & Engineering
[1,2,3]Eluru College of Engineering and Technology, Eluru, AP.

Abstract **--** Twitter is one of the most well known micro-blogging administrations, which is commonly used to share news and updates through short messages confined to 280 characters. In any case, its open nature and huge client base are every now and again misused via robotized spammers, content polluters, and other not well expected clients to carry out different cyber violations, for example, cyber bullying, trolling, rumor dissemination, and stalking. Likewise, various methodologies have been proposed by specialists to address these issues. Nonetheless, the majority of these methodologies depend on client portrayal and totally dismissing shared communications. In this examination, we present a hybrid methodology for recognizing mechanized spammers by amalgamating network based features with other feature classifications, to be specific metadata-, content-, and association based features. The curiosity of the proposed methodology lies in the portrayal of clients dependent on their communications with their supporters given that a client can dodge features that are identified with his/her very own exercises, yet sidestepping those dependent on the devotees is troublesome. Nineteen distinct features, including six recently characterized features and two re-imagined features, are distinguished for learning three classifiers, in particular, irregular woods, choice tree, Bayesian system, and example pre-handling on a genuine dataset that involves generous clients and spammers. The separation intensity of various feature classifications is additionally broke down, and cooperation and network based features are resolved to be the best for spam identification, though metadata-based features are demonstrated to be the least compelling.

Keywords: Social network analysis, Spammer detection, Spambot detection, Social network security.

******

I. Introduction

Twitter, a micro blogging administration, is viewed as a mainstream OSN's with a huge client base and is pulling in clients from various different backgrounds and age gatherings. OSNs empower clients to stay in contact with companions, family members, relatives, and individuals with comparative interests, calling, and targets. What's more, they enable clients to connect with each other and structure networks. A client can turn into an individual from an OSN by enlisting and giving subtleties, for example, name, birthday, sex, and other contact data. Albeit countless OSNs exist on the web, Facebook and Twitter are among the most famous OSNs and are remembered for the rundown of the best 10 websites1 around the around the world.

OSN and the Social Spam Problem

Twitter, which was established in 2006, enables its clients to post their perspectives, express their considerations, and offer news and other data as tweets that are confined to 280 characters. Twitter enables the clients to pursue their preferred lawmakers, competitors, big names, and news channels, and to buy in to their substance with no prevention. Through after movement, a supporter can get notices of bought in account. Despite the fact that Twitter and different OSNs are for the most part utilized for different kindhearted purposes, their open nature, immense client base, and constant message multiplication have made them rewarding focuses for cyber crooks and social bots. OSNs have been demonstrated to be hatcheries for another type of mind boggling and complex assaults and dangers, for example, cyberbullying, falsehood dissemination, stalking, character trickery, radicalization, and other illegal exercises, notwithstanding traditional cyber assaults, for example, spamming, phishing, and drive by download [1], [2].

Throughout the years, old style assaults have developed into refined assaults to avoid identification instruments. A report2 submitted to the US Securities and Exchange Commission in August 2014 demonstrates that around 14% of Twitter accounts are really spambots and roughly 9.3% of all tweets are spam. In informal communities, spambots are otherwise called socialbots that copy human conduct to pick up trust in a system and afterward abuse it for malignant exercises [3]. Such reports and discoveries exhibit the degree of cyber wrongdoings submitted by spambots and how OSNs are demonstrating to be a paradise for these bots. Despite the fact that spammers are not exactly kindhearted clients, they are fit for influencing system structure and trust for different unlawful purposes.

 ISSN: 2454-4248
10 –17

Why Connected Users?

Numerous scientists from the scholarly world and industry are attempting to dispose of the cyber lawbreakers and malignant clients to make OSN use a charming and brilliant experience. Thus, various spam identification approaches have been proposed. Be that as it may, as approaches develop and advance, spammers are utilizing progressively refined components to sidestep location, in this way bringing about a "waiting game". Fletcher [4] thoroughly dissected various variations of spammers, beginning from regular spammers to exhibit day complex spammers, and found that such dangers present critical outcomes to various gatherings related with the Internet.

Moreover, Fletcher's paper additionally examined the legitimate provokes identified with dealing with spamming. Boshmaf et al. [5] detailed that current spamming and different vindictive conduct discovery procedures use either feature-based or chart apportioning based methodologies. In the primary case, clients are described dependent on features separated from their profiles and exercises and various classifiers are prepared to recognize generous clients and spammers [6], [7], [8]. In a feature-based technique, features, for example, number of adherents and number of tweets are commonly simple to dodge, while certain mind boggling features are hard to sidestep. Be that as it may, features are commonly founded on client exercises and in this manner, spammers can control their conduct to mirror those of typical clients. On the other hand, in diagram apportioning based systems, a client association organize is divided into sub-charts or networks utilizing diagram investigation strategies [9], [10], [11]. Despite the fact that, these systems are formal identification draws near, mechanized spammers can sidestep them by making adequate assault joins (edges) among ordinary and noxious clients. Consequently, we propose an amalgamation of network based features with other feature classes for distinguishing computerized spammers, wherein networks are recognized utilizing diagram parceling calculations.

II. Related Work

[1] M. Tsikerdekis, 2017, Identity double dealing in web based life applications has contrarily affected online networks and it is probably going to increment as the web-based social networking client populace develops. The simplicity of creating new records via web-based networking media has exacerbated the issue. Numerous past investigations have been set that centered around verbal, non-verbal, and arrange information created by clients trying to distinguish personality trickiness. Nonetheless, despite the fact that these techniques delivered a high exactness, they are principally receptive to the issue of personality duplicity. This paper proposes a proactive methodology that use interpersonal organization information and it is centered around personality duplicity aversion for online sub-networks, networks that exist inside bigger networks (e.g., Facebook gatherings or Subreddits). The technique can be applied to different sorts of internet based life applications and creates high exactness in recognizing tricky records at the hour of endeavored passage to a sub-network.

[2] T. Anwar and M. Abulaish, 2015, The developing ubiquity of online internet based life is prompting its across the board use among the online network for different purposes. In the ongoing past, it has been discovered that the web is likewise being utilized as an apparatus by radical or fanatic gatherings and clients to rehearse a few sorts of fiendish acts with disguised plans and advance belief systems in a modern way. A portion of the web gatherings are dominatingly being utilized for open discourses on basic issues impacted by radical considerations. The persuasive clients overwhelm and impact the recently joined guiltless clients through their extreme musings. This paper displays an utilization of collocation hypothesis to distinguish profoundly powerful clients in web gatherings. The profundity of a client is caught by a measure dependent on the level of match of the remarked posts with a risk list. Eleven diverse collocation measurements are detailed to recognize the relationship among clients, and they are at long last implanted in a tweaked PageRank calculation to produce a positioned rundown of fundamentally compelling clients.

[5] Y. Boshmaf, M. Ripeanu, K. Beznosov, and E. Santos-Neto, 2015, Traditional protection components for battling against robotized counterfeit records in online interpersonal organizations are injured individual freethinker. Despite the fact that casualties of phony records assume a significant job in the reasonability of consequent assaults, there is no work on using this knowledge to improve business as usual. In this position paper, we venture out propose to fuse expectations about casualties of obscure fakes into the work processes of existing barrier instruments. Specifically, we researched how such reconciliation could prompt increasingly vigorous phony record protection instruments. We likewise utilized genuine world datasets from Facebook and Tuenti to assess the practicality of anticipating casualties of phony records utilizing directed AI.

[6] N. R. Amit An Amleshwaram, S. Yadav, G. Gu, and C. Yang, 2013, Twitter, with its rising notoriety as a micro-blogging site, has definitely pulled in the consideration of spammers. Spammers utilize horde of strategies to avoid security instruments and post spam messages, which are either unwelcome ads for the person in question or draw unfortunate casualties in to clicking malignant URLs implanted in spam tweets. In this paper, we propose a few novel features fit for recognizing spam accounts from

 ISSN: 2454-4248
10 –17

authentic records. The features break down the conduct and substance entropy, snare procedures, and profile vectors describing spammers, which are then bolstered into directed learning calculations to create models for our device, CATS. Utilizing our framework on two true Twitter informational indexes, we watch a 96% identification rate with about 0.8% bogus positive rate beating best in class discovery approach. Moreover, we group the obscure spammers to recognize and comprehend the common spam battles on Twitter.

[15] C. Schafer, 2014, Seventy six percent of sent spam and phishing messages have their beginnings in botnets. They use traded off email records to send garbage mail through other SMTP servers to their goals. Normally, examine is centered around the fast identification of traded off records to ensure the honesty of different frameworks. One potential approach to do this is to filter the email substance or point of confinement the measure of messages that can be sent from an IP address or a record during a predefined timespan. An oddity is appropriately recognized if the farthest point is come to or spam messages are distinguished. The target of the exhibited research is to distinguish the irregularity with geo area and nation checking without the information on the email content. A subsequent technique, called Theoretical Geographical Traveling Speed, was created to raise the identification rate without bogus negatives. The proposed technique is multiple times quicker than the default rate constrained to the discovery of an undermined record.

[16] Computer and mehr Schäfer, Münchenbernsdorf, 2017, Fifty-four percent of the worldwide email traffic in October 2016 was spam and phishing messages. Those messages were regularly sent from bargained email accounts. Past research has basically centered around distinguishing approaching garbage mail however not privately produced spam messages. Best in class spam recognition techniques for the most part require the substance of the email to have the option to order it as either spam or a customary message. This substance isn't accessible inside scrambled messages or is restricted because of information protection. The object of the exploration displayed is to distinguish an abnormality with the Origin-Destination Delivery Notification strategy, which depends on the land inception and goal just as the Delivery Status Notification of the remote SMTP server without the information on the email content. The proposed technique recognizes a manhandled record after a couple moved messages; it is truly adaptable and can be balanced for each condition and necessity.

Problem Definition

As talked about before, most spammer location approaches depend on the features extricated from client profile and exercises in a system. Paradoxically, spammers advance themselves against these features either by abusing the escape clauses of existing location strategies or by putting resources into human or monetary assets [12]. Kind clients by and large pursue and react to demands from known clients and maintain a strategic distance from association with and correspondence from outsiders. Thusly, in the system of trust of a client, most clients display a specific degree of trust in the personality of others, which prompts the arrangement of a network like structure. A generous client might be an individual from numerous networks relying upon realworld systems and interests. On the other hand, spammers for the most part pursue irregular clients, which bring about an incredibly low response rate that structures scanty associations among devotees, and unfavorably influences connection and network based features. To avoid features from these classifications, spammers may endeavor to shape a network through shared after. Be that as it may, such endeavors will be pointless in light of the fact that it won't build their objective client base.

Implementation Methodology

In this examination, we propose a hybrid methodology for recognizing social spambots in Twitter, which uses an amalgamation of metadata, substance, cooperation, and network based features. In the examination of portraying features of existing methodologies, most system based features are not characterized utilizing client adherents and fundamental network structures [6], [7], in this way ignoring the way that the notoriety of client in a system is acquired from the devotees (instead of from the ones client is following) and network individuals. In this manner, we stress the utilization of supporters and network structures to characterize the system based features of a client.

We group our arrangement of features into three general classifications, in particular, metadata, substance, and system, wherein the system class is additionally characterized into association and network based features. Metadata features are separated from accessible extra data with respect to the tweets of a client, while content-based features expect to watch the message posting conduct of a client and the nature of the content that the client utilizes in posts. System based features are removed from client collaboration arrange.

Dataset Collection

For the trial assessment of the proposed methodology, we utilize the Twitter dataset, which contains 10619 named clients. This dataset additionally contains the arrangements of devotees and followings of the named clients, alongside their profile data, for example, username, area, and userid. It likewise contains tweets and related subtleties, for example, tweet id, tweet time, and most loved check of the marked clients. Table I displays a short measurements of the dataset, where complete #users incorporates every one of the

 ISSN: 2454-4248
10 –17

supporters and followings of the named considerate clients and spammers. In this dataset, the greater part of the considerate clients doesn't have their rundown of adherents; thus estimations of their cooperation and network based features will be zero, which powers classifiers to be one-sided in spammer identification.

Feature Extraction

In the proposed robotized spammer location strategy, 19 features, including 6 new and 2 reclassified features, are distinguished. The feature set is characterized into three general classifications, to be specific, metadata-based, content-based, and arrange based features, in light of the sorts of information used to characterize a feature. System based features are additionally arranged into communication based and network based features. A concise synopsis of the features, alongside their class and source. As far as we could possibly know, features set apart as new, yet have not been utilized in the current writing for robotized spammer recognition; while features set apart as reclassified rethink existing features and references give the wellspring of existing features.

Random Forest

RF is another classification algorithm which follows ensemble classification approach. It is made up of many DTs. It was first developed in 1995 and the name was coined by Tin Kam Ho. RF combines the random selection of features and also the bagging idea of Breiman. Each decision tree which is part of RF is an individual learner. When they are combined, they become random forest. Data exploration is one of the common approaches for which RF is widely used. An example for decision tree used for RF is Classification and Regression Tree (CART). It follows a recursive, top down and greedy approach to divide the feature space into many regions.

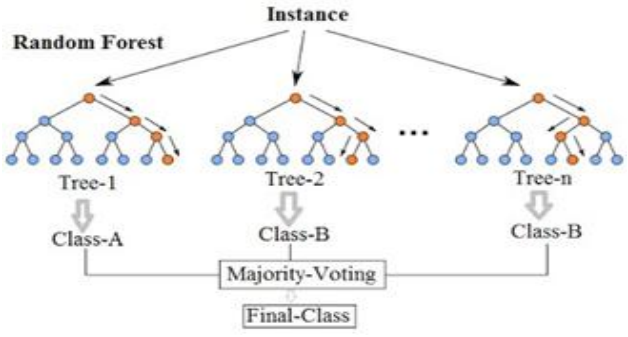

Figure 1: Random forest example

As presented in Figure 1, the RF generates multiple DTs for the given instance. Each tree corresponds to a specific class. With majority voting, the final class will be determined. From each tree, training data subset is selected. Then the stop condition is verified. It stops condition is satisfied, it ends after computing prediction error. If the stop condition is not satisfied, it builds the next split that is subjected to a series of operations namely choosing variable subset followed by an iterative process to choose the best split. There are many advantages of RF. Its accuracy is high for many datasets. It can handle large datasets efficiently. It can work with thousands of input variables and gives estimates on importance of variables. It also provides unbiased estimation of errors focuses on missing data and improves accuracy.

Decision Tree

For prediction purposes and classifications, DT is one of the popular and powerful tools. Decision rules are nothing but rules that are interpreted by humans to make well informed decisions. It returns actionable knowledge that can be used by humans. There are certain key requirements of DT. First, it needs an expressible attribute values that are clearly specified. For instance, values like code, mild, hot are specified for an attribute related to weather. Second, there needs to clearly defined target classes may be multi-class or Boolean. The learning model of DT needs sufficient training data.

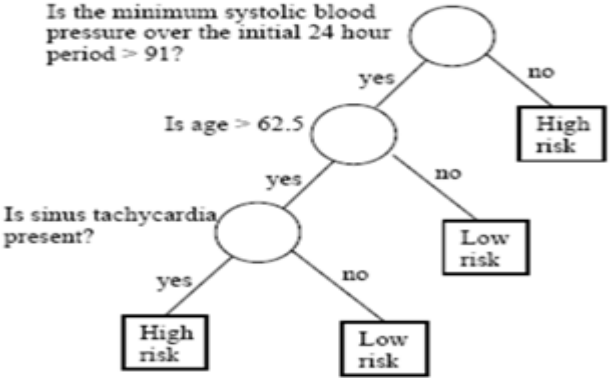

Figure 2: Shows decision tree for a healthcare dataset

There are three rules in the DT. The first rule is related to blood pressure of human. The second rule is related to age of the person while the third rule is related to the presence of sinus tachycardia. The target classes include low risk and high risk. Every condition has two possibilities like yes and no. This algorithm works effortlessly for both categorical and continuous data. The given population is divided into multiple sets. It computes entropy of every attribute. The attributes with minimum entropy and maximum information gain are used to split data for generating decisions. The entropy and gain are computed as in Eq. (1) and Eq. (2).

$$Entropy(S) = \sum_{i=0}^{n} -\text{pi} \log 2 \text{ pi} \quad (1)$$

$$Gain(\text{S}, \text{A}) = Entropy(S) - \sum_{v \in Values\ (A)} \frac{|\text{Sv}|}{|\text{S}|} Entropy(Sv) \quad (2)$$

 ISSN: 2454-4248
10 –17

At last here the inward hubs contain the attributes while the branches speak to the consequence of each test on every hub. DT is broadly utilized for grouping purposes since it needn't bother with much information in the field or setting the parameters for it to work.

Pattern Classification

Pattern acknowledgment is the study of making inductions from perceptual information, utilizing devices from insights, likelihood, computational geometry, AI, signal handling, and calculation plan. Along these lines, it is of focal significance to man-made consciousness and PC vision, and has expansive applications in building, science, prescription, and business. Specifically, propels made during the last 50 years, presently enable PCs to connect all the more adequately with people and the characteristic world (e.g., discourse acknowledgment programming). Be that as it may, the most significant issues in pattern acknowledgment are yet to be unraveled [1].

Pattern is characterized as composite of features that are normal for a person. In order, a pattern is a couple of factors {x,w} where x is an assortment of perceptions or features (feature vector) and w is the idea driving the perception (name). The nature of a feature vector is identified with its capacity to segregate models from various classes (Figure 3). Models from a similar class ought to have comparable feature esteems and keeping in mind those models from various classes having distinctive feature esteems.

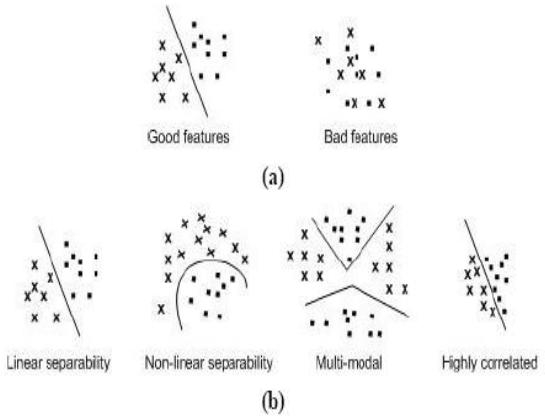

Figure 3: Characteristic (feature); a. the distinction between good and poor features, and b. feature properties.

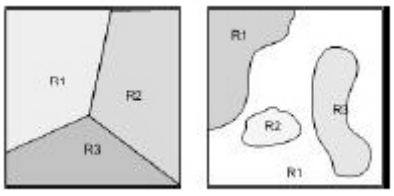

Figure 4: Classifier and decision boundaries.

On the off chance that the qualities or traits of a class are referred to, singular items may be recognized as having a place or not having a place with that class. The articles are doled out to classes by watching patterns of recognizing attributes and contrasting them with a model individual from each class. Pattern acknowledgment includes the extraction of patterns from information, their examination and, at long last, the distinguishing proof of the classification (class) every one of the pattern has a place with. A common pattern acknowledgment framework contains a sensor, a preprocessing component (division), a feature extraction instrument (manual or mechanized), a grouping or portrayal calculation, and a lot of models (preparing set) effectively characterized or depicted (post-handling) (Figure 5).

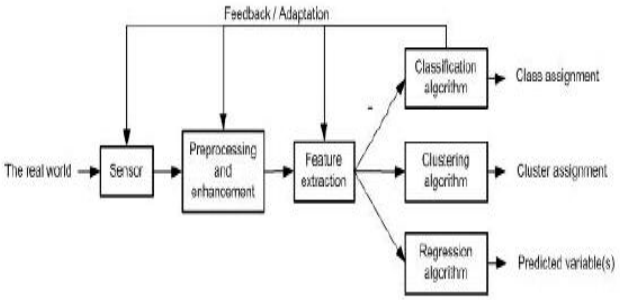

Figure 5: A pattern recognition system

Results Analysis

The proposed methodology is assessed utilizing three standard measurements, in particular, detection rate (DR), false positive rate (FPR), and F-Score. DR speaks to the division of spammers identified from the arrangement all things considered, where TP represents genuine positives and speaks to the quantity of real spammers named spammers, and FN represents bogus negatives and speaks to the quantity of real spammers misclassified as amiable clients. FPR is bogus positive rate and speaks to the division of generous clients, misclassified as spammers, where FP represents bogus positives and speaks to the quantity of kind clients misclassified as spammers and TN represents genuine negatives and speaks to the quantity of benevolent clients delegated favorable. FPR is critical parameter for assessment of classifiers, and its low worth is attractive for good classifier. At long last, F-Score is characterized as the consonant mean of accuracy and review, where exactness is characterized as the proportion of the accurately distinguished spammers to the all out number of clients recognized as spammers, and review is same as the DR. The F-Score speaks to discriminative intensity of classifier. A classifier with a high estimation of F-Score is attractive to exactly isolate the spammers and amiable clients.

 ISSN: 2454-4248
10 –17

Figure 5: Decision Tree Performance Metrics

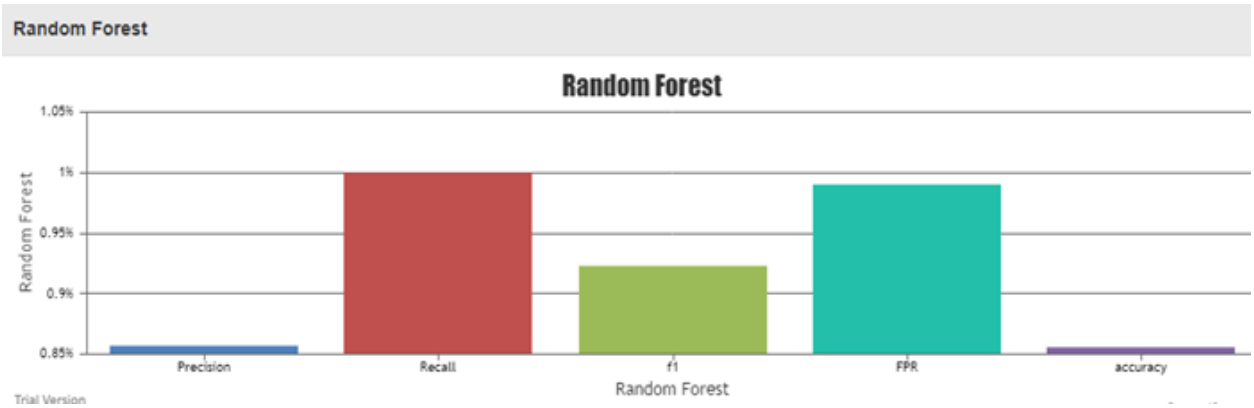

Figure 6: Random Forest Performance Metrics

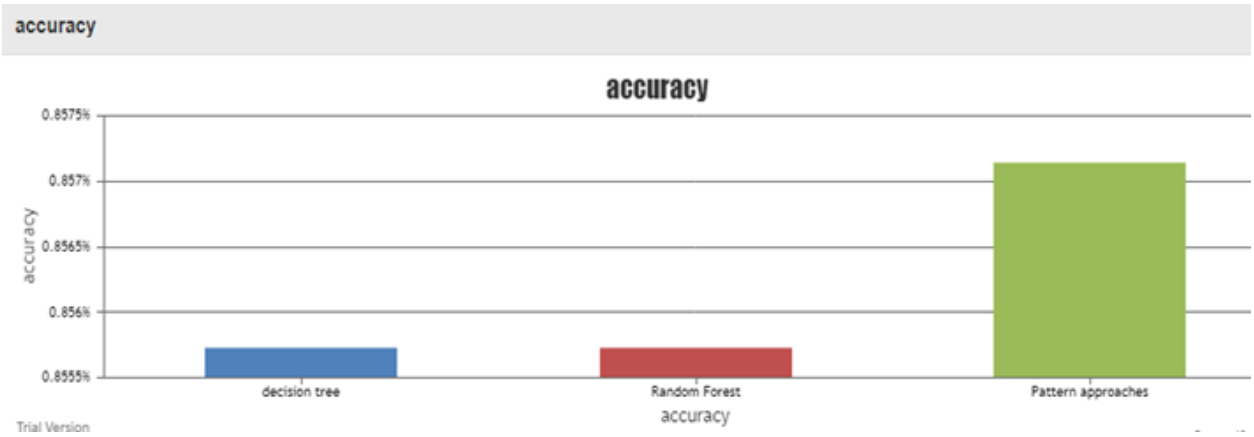

Figure 7: Accuracy of Decision Tree, Random Forest and Pattern Classification

III. Conclusion

In this paper, we have proposed a hybrid methodology misusing network based features with metadata, substance, and collaboration based features for recognizing robotized spammers in Twitter. The curiosity of the proposed methodology lies in the portrayal of a spammer dependent on its neighboring hubs (particularly, the devotees) and their cooperation arrange. This is principally because of the way that clients can sidestep features that are identified with their very own exercises, however it is hard to avoid those that depend on their devotees. On investigation, metadata-based features are seen as least viable as they can be effectively dodged by the advanced spammers by utilizing arbitrary number generator calculations.

Achieving ideal exactness in spammer's recognition is very troublesome, and as needs be any feature set can never be considered as complete and sound, as spammers continue changing their working conduct to dodge discovery instrument. Along these lines, notwithstanding profile-based portrayal, complete logs of spammers beginning from their entrance in the system to their location, should be dissected to display the developmental conduct and periods of the life-cycles of spammers. Be that as it may, for the most part spammers are recognized when they are at exceptionally

 ISSN: 2454-4248
10 –17

propelled stage, and it is hard to get their past logs information.

Future Enhancement

Investigation of spammer's system to uncover various kinds of composed spam crusades run by the spambots appears to be one of the promising future headings of research. Additionally, breaking down the worldly advancement of spammers' supporters may uncover some fascinating patterns that can be used for spammer's portrayal at various degrees of granularity.

References

[1] M. Tsikerdekis, "Identity deception prevention using common contribution network data," IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 188–199, 2017.

[2] T. Anwar and M. Abulaish, "Ranking radically influential web forum users," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1289–1298, 2015.

[3] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Design and analysis of social botnet," Computer Networks, vol. 57, no. 2, pp. 556– 578, 2013.

[4] D. Fletcher, "A brief history of spam," TIME, Tech. Rep., 2009.

[5] Y. Boshmaf, M. Ripeanu, K. Beznosov, and E. Santos-Neto, "Thwarting fake osn accounts by predicting their victims," in Proc. AISec., Denver, 2015, pp. 81–89.

[6] N. R. Amit A Amleshwaram, S. Yadav, G. Gu, and C. Yang, "Cats: Characterizing automation of twitter spammers," in Proc. COMSNETS, Banglore, 2013, pp. 1–10.

[7] K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: Social honeypots + machine learning," in Proc. SIGIR, Geneva, 2010, pp. 435–442.

[8] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in Proc. ACSAC, Austin, Texas, 2010, pp. 1–9.

[9] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: Defending against sybil attacks via social networks," IEEE/ACM Transactions on Networking, vol. 16, no. 3, pp. 576–589, 2008.

[10] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in Proc. IMC, Melbourne, 2001, pp. 35–47.

[11] W. Wei, F. Xu, and C. C. Tan, "Sybildefender: Defend against sybil attacks in large social networks," in Proc. INFOCOM, Orlando, 2012, pp. 1951–1959.

[12] C. Yang, R. C. Harkreader, and G. Gu, "Die free or live hard? Empirical evaluation and new design for fighting evolving twitter spammers," in Proc. RAID, Menlo Park, California, 2011, pp. 318–337.

[13] S. Lee and J. Kim, "Warningbird: A near real-time detection system for suspicious urls in twitter stream," IEEE Transaction on Dependable and Secure Computing, vol. 10, no. 3, pp. 183–195, 2013.

[14] M. Sahami, S. Dumais, D. Heckerman, and E. Horvitz, "A Bayesian approach to filtering junk e-mail," in Proc. of Workshop on Learning for Text Categorization, Madison, Wisconsin, 1998, pp. 98–105.

[15] C. Schafer, "Detection of compromised email accounts used by a spam botnet with country counting and theoretical geographical travelling speed extracted from metadata," in Proc. ISSRE, Naples, 2014, pp. 329–334.

[16] "Detection of compromised email accounts used for spamming in correlation with origin-destination delivery notification extracted from metadata," in Proc. ISDFS, Tirgu Mures, 2017, pp. 1–6.

[17] A. H. Wang, "Detecting spam bots in online social networking sites: A machine learning approach," in Proc. DBSec, Rome, 2010, pp. 335–342.

[18] F. Ahmed and M. Abulaish, "A generic statistical approach for spam detection in online social networks," Computer Communications, vol. 36, no. 10, pp. 1120–1129, 2013.

[19] C. Yang, R. Harkreader, and G. Gu, "Empirical evaluation and new design for fighting evolving twitter spammers," IEEE Transactions on Information Forensics and Security, vol. 8, no. 8, pp. 1280–1293, 2013.

[20] Y. Zhu, X. Wang, E. Zhong, N. N. Liu, H. Li, and Q. Yang, "Discovering spammers in social networks," in Proc. AAAI-12, Toronto, Ontario, 2012, pp. 52–58.

Authors Profiles

Gunnabathula Jhansi Mounika pg student from department of computer science & engineering, Eluru College of Engineering and Technology, affiliated to JNTUK University, ap india. Completed UG B.Tech (Computer Science & Engineering) in the year **2017** from Eluru College of Engineering and Technology, **JNTU, Kakinada.** Completed Diploma (Computer Engineering) in the year **2014** from sir C. R. R. Polytechnic, Eluru. **Sbtet, Andhra Pradesh.**

Y. Siva Koteswara Rao he is currently working as professor in faculty of Computer Science & Engineering at, Eluru College of Engineering and Technology, Eluru, Ap. Having have a total teaching experience of 10 years. Completed M.Tech in the CSE in the year **2014** from JNTUK, University.

ISSN: 2454-4248
10 –17

Dr. Gopisetti Guru Kesava Dasu professor and HOD department of Computer Science & Engineering at, Eluru College of Engineering and Technology, Eluru, Ap. he have a total teaching experience of 19 years. Completed M.E (CSE) & Ph.d(CSE).