DETECTING ONLINE SOCIAL NETWORK CHAT MEASUREMENT, ANALYSIS AND AUTOMATED CLASSIFICATION

C. SHEEBA JAYA PRIYA*, K.KARTHIKA**
* II ME,CSE,EASA college of engineering and technology, Anna university, Chennai.
** Assistant professor, CSE,EASA college of engineering and technology, Anna university, Chennai.

ABSTRACT:

Tweets are publicly visible by default, but senders can restrict message delivery to just their followers. Users can tweet via the Twitter website, compatible external applications (such as for smartphones), or by Short Message Service (SMS) available in certain countries. While the service is free, accessing it through SMS may incur phone service provider fees.The popularity and open structure of Twitter have attracted a large number of automated programs, known as bots, which appear to be a double-edged sword to Twitter. Legitimate bots generate a large amount of benign tweets delivering news and updating feeds, while malicious bots spread spam or malicious contents. More broadly, the full term "cybernetic organism" is used to describe larger networks of communication and control. For example, cities, networks of roads, networks of software, corporations, markets, governments, and the collection of these things together. Chatterbots are used in automated online assistants by organizations as a way of interacting with consumers and users of services. This can avail for enterprises to reduce their operating and training cost. To assist human users in identifying who they are interacting with, this paper focuses on the classification of human, bot, and cyborg accounts on Twitter.The entropy component uses tweeting interval as a measure of behavior complexity, and detects the periodic and regular timing that is an indicator of automation.The spam detection component uses tweet content to check whether text patterns contain spam or not3.The account properties component employs useful account properties, such as tweeting device makeup, URL ration, to detect deviations from normal.The decision maker is based on Random Forest, and it uses the combination of the features generated by the above three components to categorize an unknown user as human, bot, or cyborg.

Keywords*– *Twitter, bot , cyborg, social network.

1.INTRODUCTION

1.1 Dependable and secure computing

Dependability is first introduced as a global concept that subsumes the usual attributes of reliability, availability, safety, integrity, maintainability, etc. The consideration of security brings in concerns for confidentiality, in addition to availability and integrity. The basic definitions are then commented upon, and supplemented by additional definitions. Boldface characters are used when a term is defined, while italic characters are an invitation to focus the reader's attention.

1.1.1 The Basic Concepts

In this section we present a basic set of definitions that will be used throughout the entire discussion of the taxonomy of dependable & secure computing. The definitions are general enough to cover the entire range of computing and communication systems, from individual

logic gates to networks of computers with human operators and users. In what follows we focus mainly on computing and communications systems, but our definitions are also intended in large part to be of relevance to computer-based systems, i.e., systems which also encompass the humans and organizations that provide the immediate environment of the computing and communication systems of interest.

1.1.2 System Function, Behavior, Structure, and Service

A system in our taxonomy is an entity that interacts with other entities, i.e., other systems, including hardware, software, humans, and the physical world with its natural phenomena. The function of such a system is what the system is intended to do and is described by the functional specification in terms of functionality and performance. The behavior of a system is what the system does to implement its function and is described by a sequence of states. The structure of a system is what enables it to generate the behavior. From a structural viewpoint, a system is composed of a set of components bound together in order to interact, where each component is another system, etc.

1.1.3 The Threats to Dependability and Security: Failures, Errors, Faults

Correct service is delivered when the service implements the system function. A service failure, often abbreviated here to failure, is an event that occurs when the delivered service deviates from correct service. A service fails either because it does not comply with the functional specification, or because this specification did not adequately describe the system function. A service failure is a transition from correct service to incorrect service, i.e., to not implementing the system function. For this reason the definition of an error is: the part of the total state of the system that may lead to its subsequent service failure. It is important to note that many errors do not reach the system's external state and cause a failure. A fault is active when it causes an error, otherwise it is dormant.

1.1.4 Dependability, Security, and their Attributes

The original definition of **dependability** is: the ability to deliver service that can justifiably be trusted. This definition stresses the need for justification of trust. The alternate definition, that provides the criterion for deciding if the service is dependable, is: the **dependability** of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable.**Security** is a composite of the attributes of confidentiality, integrity and availability, requiring the concurrent existence of a) availability for authorized actions only, b) confidentiality, and c) integrity with 'improper' meaning 'unauthorized'.

1.1.5 The Means to Attain Dependability and Security

Over the course of the past fifty years many means have been developed to attain the various attributes of dependability and security. Fault prevention and fault tolerance aim to provide the ability to deliver a service that can be trusted, while fault removal and fault forecasting aim to reach confidence in that ability by justifying that the functional and the dependability & security specifications are adequate and that the system is likely to meet them.

2.RELATED WORK

a) Analysis of twitter:

Twitter consists of new capability so that the user can quickly view the friends. The difference between bots and human are identified using Human Interactive Proofs(HIP) such as captcha. Game bots are detected based on Human Observation Proof(HOP).

HOP consists of two advantages: first, provides continuous monitoring throughout a session. Second, HOP are non-interactive. Game bots cannot directly recognize most objects.

b) Fighting with game bots:

Distinguishing bots and humans based on human interactive proofs such as captcha consists of drawbacks. In HOP based approach, series of input traces are collected and then we characterize the game playing behavior of bots and human. Then HOP based game bot defense system analyzes user input actions with a cascade correlation neural network to distinguish bots and humans.HOP is an effective way to detect game bots.

c)Microblogging:

Microblogging is a computer-mediated chat. Twitter profile is designated as private or public. Private profiles and tweets can be viewed only to those who have permission. The flooding events in the red river valley provides conditions for examining closely what microblogging based interaction mean in a disaster. People residing in those regions have got idea about the signs, dangers and mitigation of floods.

d) Instant Messaging:

Instant messaging is very popular and malware attack takes place easily. Honey IM uses decoy accounts in users contact list as sensors to capture malware. Honey IM delivers attack info to network administrators.

3. EXISTING SYSTEM

An automated classification system consists of four major components. The entropy component uses tweeting interval as a measure of behavior complexity, and detects the periodic and regular timing that is an indicator of automation; The spam detection component uses tweet content to check whether text patterns contain spam or not3; The account properties component employs useful account properties, such as tweeting device makeup, URL ration, to detect deviations from normal; and The decision maker is based on Random Forest, and it uses the combination of the features generated by the above three components to categorize an unknown user as human, bot, or cyborg.

A classification system that includes the following four parts:

- An entropy-based component.
- A spam detection component.
- An account properties component.
- A decision maker. It uses the combination of features extracted from an unknown user to determine the likelihood of being a human, bot, or cyborg.

4. PROPOSED SYSTEM

The proposed classification system consists of two components: (1) an entropy-based classifier and (2) a Bayesian-based classifier. The two classifiers complement each other in chat bot detection. The entropy-based classifier is more accurate to detect unknown chat bots, whereas the Bayesian-based classifier is faster to detect known chat bots. Our experimental evaluation shows that the proposed

classification system is highly effective in differentiating bots from humans.

Propose classification system to accurately distinguish chat bots from humans. There are two main components in our classification system: (1) an entropy classifier and (2) a Bayesian classifier. Based on the characteristics of message time and size, the entropy classifier measures the complexity of chat flows and then classifies them as bots or humans. In contrast, the Bayesian classifier is mainly based on message content for detection. The two classifiers complement each other in chat bot detection. While the entropy classifier requires more messages for detection and, thus, is slower, it is more accurate to detect unknown chat bots. Moreover, the entropy classifier helps train the Bayesian classifier. The machine learning classifier requires less messages for detection and, thus, is faster, but cannot detect most unknown bots. By combining the entropy classifier and the Bayesian classifier, the proposed classification system is highly effective to capture chat bots, in terms of accuracy and speed. We conduct experimental tests on the classification system, and the results validate its efficacy on chat bot detection.

5. NAIVE BAYES ALGORITM:

In simple terms, a naive Bayes classifier assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature, given the class variable. For example, a fruit may be considered to be an apple if it is red, round, and about 4" in diameter. Even if these features depend on each other or upon the existence of the other features, a naive Bayes classifier considers all of these properties to independently contribute to the probability that this fruit is an apple.

Depending on the precise nature of the probability model, naive Bayes classifiers can be trained very efficiently in a supervised learning setting. In many practical applications, parameter estimation for naive Bayes models uses the method of maximum likelihood; in other words, one can work with the naive Bayes model without believing in Bayesian probability or using any Bayesian methods.

In spite of their naive design and apparently oversimplified assumptions, naive Bayes classifiers have worked quite well in many complex real-world situations. In 2004, analysis of the Bayesian classification problem has shown that there are some theoretical reasons for the apparently unreasonable efficacy of naive Bayes classifiers. Still, a comprehensive comparison with other classification methods in 2006 showed that Bayes classification is outperformed by more current approaches, such as boosted trees or random forests. An advantage of the naive Bayes classifier is that it only requires a small amount of training data to estimate the parameters (means and variances of the variables) necessary for classification. Because independent variables are assumed, only the variances of the variables for each class need to be determined and not the entire covariance matrix.

Text classification algorithms, such SVM, and Naïve Bayes, have been developed to build up search engines and construct spam email filters. As a simple yet powerful sample of Bayesian Theorem, Naïve Bayes shows advantages in text classification yielding satisfactory results. In this paper, a spam email detector is developed using Naïve Bayes algorithm. We use pre-classified emails (priory knowledge) to train the spam email detector. With the model generated from the training step, the detector is able to decide whether an email is a spam email or an ordinary email.

With the amount of text files on Internet increases exponentially each day,

the volume of information available online continues to expand. Text Classification, as the assignment of text files to one or more predefined categories based on information contained from text files, is an important component in information management tasks.

We focus on email classification. First, we discuss the principles of Bayes Theorem and the Naïve Bayes algorithms. Then we discuss the principles of Naïve Bayes Text Classifier by introducing the design and implementation of the spam email detector. Finally, testing results are analyzed and future work is discussed.

5.1.1 Training stages

As a supervised classification application, the spam email detector needs a training set with pairs of emails and labels indicating whether an email is a spam email. We use folders to represent the labels emails. We use spam emails and ordinary emails (ham) provided by Apache spam email assassin project.

Bayesian email filters take advantage of Bayes' theorem. Bayes' theorem is used several times in the context of spam:

- A first time, to compute the probability that the message is spam, knowing that a given word appears in this message;
- A second time, to compute the probability that the message is spam, taking into consideration all of its words (or a relevant subset of them);
- Sometimes a third time, to deal with rare words.

6. CONCLUSION

This paper first presents a large-scale measurement study on Internet chat. We collected two-month chat logs for 21 different chat rooms from one of the top Internet chat service providers. From the chat logs, we identified a total of 16 different types of chat bots and grouped them into six categories: periodic bots, random bots, responder bots, replay bots, replay-responder bots, and advanced responder bots. Through statistical analysis on inter-message delay and message size for both chat bots and humans, we found that chat bots behave very differently from human users. More specifically, chat bots exhibit certain regularities in either inter-message delay or message size. Although responder bots and replay bots employ advanced techniques to behave more human-like in some aspects, they still lack the overall sophistication of humans.

Based on the measurement study, we further proposed a chat bot classification system, which utilizes entropy-based and Bayesian-based classifiers to accurately detect chat bots. The entropy-based classifier exploits the low entropy characteristic of chat bots in either inter-message delay or message size, while the Bayesian-based classifier leverages the message content difference between humans and chat bots. The entropybased classifier is able to detect unknown bots, including human-like bots such as responder and replay bots. However, it takes a relatively long time for detection, i.e., a large number of messages are required. Compared to the entropy-based classifier, the Bayesian-based classifier is much faster, i.e., a small number of messages are required. In addition to bot detection, a major task of the entropy-based classifier is to build and maintain the bot corpus. With the help of bot corpus, the Bayesian-based classifier is trained, and consequently, is able to detect chat bots quickly and accurately. Our experimental results demonstrate that the hybrid classification system is fast in detecting known bots and is accurate in identifying previously-unknown bots.

7. REFERENCES

1. Dongwoo Kim I.-C.M., Y. Jo, and Oh.A, "Analysis of Twitter Lists as a Potential Source for Discovering Latent Characteristics of Users," Proc. CHI Workshop Microblogging: What and How Can We Learn From It?, 2010.

2. Battle of botcraft: fighting bots in online games with Human observational proofs proc.16th acm conf. Computer and comm. Security, 2009.

3. Chatter on the red: what hazards threat reveals about the social life of microblogged information kate starbird, leysia palen, amanda l. Hughes & sarah vieweg, Feb 2010.

4. Honey im: fast detection and suppressionof instant messaging malware enterprise like network. mengjun xie zhenyu wu haining wang proc. 23rd ann. computer security applications conf.,2007.

5. Zhao.D and Rosson.M.B,(2009) "How and Why People Twitter: The Role that Micro-Blogging Plays in Informal Communication at Work," Proc. ACM Int'l Conf. Supporting Group Work.

Author 1

C.Sheeba Jaya Priya, received B.E degree in 2006 from Avinashilingam Deemed University, Coimbatore,India. Currently pursuing M.E degree in Computer Science and Engineering in EASA college of Engineering and Technology.coimbatore.

Author 2

K.Karthika, Received B.E (CSE) degree in 2010 from Anna University Chennai India .Received M.E(CSE) degree in Karpagam University, India. Currently Working as Assistant Professor in EASA college of Enggineering and Technology.coimbatore.