Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e -ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

DYNAMIC PATTERN BASED VIRUS RECOGNITION USING DYNAMIC PROGRAM INVOCATION DESIGN MODEL

S Kaviarasan[1], V Kumaresh[2], T Thamban[3], A Udhayanidhi[4]
Assistant Professor[1], UG Scholars[2,3,4]
Department of Computer Science and Engineering
Panimalar Institute of Technology

ABSTRACT: *The Research focus on the dynamic invocation of code and patterns based on the existing antivirus model. This project emphasizes an artificial intelligence model in developing the code which will do the following process Invoke automatically and started executing in case of any virus files available.The virus files can be identified through the signatures.It can be identified via the type / name of files which already exists.In case, the user will train the model for the type of virus. An intelligent system will take care of future detection with those patterns.*

KEYWORDS: *Dynamic; Invocation; Patterns; Signatures; Virus.*

I. INTRODUCTION

These days one cannot open their email without seeing countless spam messages in their inbox. For the email-recipient, spam is easily recognized. However, the receiver of spam loses countless hours manually deleting the intrusive messages from their inbox. Spam filter mechanism can help mitigate this overwhelming chore. Spam filter mechanism can reduce the amount of junk mail delivered to a user's inbox.

The problem of spam or Unsolicited Bulk Email (UBE) is becoming a pressing issue. In spite of the development of many anti-spam techniques, the war against spam is far from being successful. This is partly due to several characteristics of spam that make it a difficult problem. E-MAIL communication is prevalent and indispensable nowadays. However, the threat of unsolicited junk emails, also known as spams, becomes more and more serious.The primary challenge of spam detection problem lies in the fact that spammers will always find new ways to attack spam filters owing to the economic benefits of sending spams. Note that existing filters generally perform well when dealing with clumsy spams, which have duplicate content with suspicious keywords or are sent from an identical notorious server. Therefore, the next stage of spam detection research should focus on coping with cunning spams which evolve naturally and continuously.we present an open digest technique, that we have adapted to take into account disguising attacks and illustrate its resiliency.

The content of spam email can range from the incomprehensible to the downright obscene. Spam is dangerous to both the computer and its users. Junk mail can contain viruses, key loggers, phishing attacks and more. These types of malware can comprise a user's sensitive private data by capturing bank account information, usernames and passwords. Spam blocker applications can assist a user in preventing thesetypes of PC contaminations.Reliably blocking and filtering spam is the most valuable feature of any spam filter software. The spam filter software should come equipped with multiple capabilities that prevent junk mail from contaminating the user's inbox. The best spam filtering software has both black and white lists, sensitivity settings, community-based filtering, challenge and response techniques, and quarantine settings. Additional features to evaluate are blocking by IP address, server, email address, and country code.

II. RELATED WORK

The fact that the same information is sent to many users, though spammers try to disguise it by creating a specific version of the message for each user.Reliably blocking and filtering spam is the most valuable feature of any spam filter software. The spam filter software should come equipped with multiple capabilities that prevent junk mail from contaminating the user's inbox. The best spam filtering software has both black and white lists, sensitivity settings, community-based filtering, challenge and response techniques, and quarantine settings. Additional features to evaluate are blocking by IP address, server, email address, and country code.

Previous researchers have developed variousmethods on near-duplicate spam detection; these works are stillsubject to some drawbacks. To achieve the objectives ofsmall storage size and efficient matching, prior worksmainly represent each e-mail by a succinct abstractionderived from e-mail content text. Moreover, hash-based textrepresentation is applied

extensively. One major problem ofthese abstractions is that they may be too brief and thusmay not be robust enough to withstand intentional attacks.

In this paper, we explore to devise a more sophisticated email abstraction, which can more effectively capture the near duplicate phenomenon of spams. Motivated by the fact that email users are capable of easily recognizing similar spams by observing the layouts of e-mails, we attempt to represent each e-mail based on the e-mail layout structure. Fortunately, almost all e-mails nowadays are in Multipurpose Internet Mail Extensions (MIME) format with the text/html content type. That is, HTML content is available in an e-mail and provides sufficient information about e-mail layout structure. In view of this observation, we propose the specific procedure Structure Abstraction Generation (SAG), which generates an HTML tag sequence to represent each e-mail. Different from previous works, SAG focuses on the e-mail layout structure instead of detailed content text. In this regard, each paragraph of text without any HTMLtag embedded will be transformed do a newly defined tag <my text=>.

In the field of collaborative spam filtering by near-duplicate detection, a superior e-mail abstraction scheme is required to more certainly catch the evolving nature of spams. Compared to the existing methods in prior research, in this paper, we explore a more sophisticated and robust e-mail abstraction scheme, which considers e-mail layout structure to represent e-mails.

Table 1. Literature Survey

S.NO	TITLE	AUTHOR	CONCEPT	YEAR	ADVANTAGES	DISADVANTAGES
1	Understanding social behavior evolutions through agent-based modeling	M. Nemiche, V. Cavero, and R. P. Lopez	Kernel-level rootkits are a form of malicious software that compromise the integrity of the Agent-based modeling has become increasingly popular in recent years, but there is still no codified set of recommendations or practices for how to use these models within a program of empirical research. This article provides ideas and practical guidelines drawn from sociology, biology, computer science, epidemiology, and statistics. We first discuss the motivations for using agent-based models in both basic science and policy-oriented social research. We close with suggested directions for future research.	2012	Using algorithm a high precision and recall scores in several data sets is achieved.We propose a lossless pruning strategy, improve the BN evaluation time.	Fast SVM Training needs petite user intervention, in view of the fact that the user only needs to offer the attributes to be considered, their individual default probability parameter, and a similarity threshold.
2	Modeling multi-agent systems	V. T. da Silva and C. J. P. de Lucena	A rootkit is a collection of tools used by intruders to keep the legitimate users and administrators of a compromised machine unaware of their presence. Originally, root-kits mainly included modified versions of system auditing programs	2007	Memory-side accelerators carry substantial effectiveness athwart existing parsing models.	Sequential Minimal Optimization performance is hurt by the latency, due to bandwidth.

			(e.g., ps or netstat on a Unix system). However, for operating systems that support loadable kernel modules (e.g., Linux and Solaris), a new type of rootkit has recently emerged. Our technique relies on an abstract model of module behavior that is not affected by small changes in the binary image of the module. Therefore, the technique is resistant to attempts to conceal the malicious nature of a kernel module.			
3	From artificial life to artificial societies—New methods for studies of complex social systems	F.-Y. Wang and J. S. Lansing	Fundamental collective behaviors such as group formation, cultural transmission, combat, and trade are seen to "emerge" from the interaction of individual agents following a few simple rules. In their program, named Sugarscape, Epstein and Axtell begin the development of a "bottom up" social science that is capturing the attention of researchers and commentators alike. The study is part of the 2050 Project, a joint venture of the Santa Fe Institute, the World Resources Institute, and the Brookings Institution. The project is an international effort to identify conditions for a sustainable global system in the next century and to design policies to help achieve such a system. Copublished with the Brookings Institution	2004	We combine lightweight TCP/IP stack implementation and SOAP-based web service implementation.	The transparency related to SOAP message processing is very small compared to message transmission.
4	Artificial societies, computational experiments, and parallel systems	F.-Y. Wang	There are number of Anti-Spam filters that have reduced the amount of email spam in the inbox but the problem still continues as the	2004	The taxonomy presented here is clearly preliminary in	There is no information about additional SPAM filters and techniques,

			spammers circumvent these techniques. The problems need to be addressed from different aspects. Major problem for instance arises when these anti-spam techniques misjudge or misclassify legitimate emails as spam (false positive); or fail to deliver or block spam on the SMTP server (false negative); thus causing a staggering cost in loss of time, effort and finance. Though false positive are very harmful loss of important information for the user, false negatives defeat the purpose of the spam filtering. This paper makes an effort in proposing another aspect to address this problem. that will be subject to further research. This paper shows the decline in false negatives via results of a case study on training the Spam Bayes tool with carefully collected domain specific user preferred dataset for over a period of 12 months.		nature, and non-exhaustive.	and to address any refinements that become apparent during that process
5	Back to the future: Surrogates, mirror worlds, and parallel universes	F.-Y. Wang	EIC Fei-Yeu Wang ruminates the creation of "software surrogates" that perform our tasks for us within cyberspace—crawling beneath the Internet—gathering information, organizing our life, improving our studies, and conducting our business. Ultimately, these software surrogates will enhance our abilities and make our lives and societies safer and more effective, leading to a "smart world." This issue also presents the AI's 10 to Watch list.	2011	This type of filtering is flexible to adapt the new development of spam techniques, such as HTML tagging, image based spam, and keyword obfuscating etc. .	The obfuscated images, although still humanly readable, won't bring the expected return to the spammers, as human readers are less likely to respond to this type of images.

6	Social computing: From social informatics to social intelligence	F.-Y. Wang, K. M. Carley, D. Zeng, and W. Mao	Social computing represents a new computing paradigm and an interdisciplinary research and application field. Undoubtedly, it strongly influences system and software developments in the years to come. We expect that social computing's scope continues to expand and its applications multiply. From both theoretical and technological perspectives, social computing technologies moves beyond social information processing towards emphasizing social intelligence. As we've discussed, the move from social informatics to social intelligence is achieved by modeling and analyzing social behavior, by capturing human social dynamics, and by creating artificial social agents and generating and managing actionable social knowledge	2007	In this paper an email clustering method is proposed and implemented to efficient detect the spam mails.	In paper the BIRCH clustering, decisions made without scanning the whole data & BIRCH utilizes local information (each clustering decision is made without scanning all data points).
7	A multilevel agent-based approach for trustworthy service selection in social networks	A. Louati, J. El Haddad, and S. Pinson	The growing number of services available within social applications (viz. Social networks) raises a new and challenging search issue: selecting desired services from social networks. Traditional discovery and selection approaches, which are registry-based (e.g., UDDI, ebXML), have manifested their limitations as they often fall behind users' expectations. This is because registries fail to (i) take into consideration non functional properties such as QoS and trust and (ii) capitalize on the information resulting	2014	The proposed technique does not require the content of the mail.	The system have to be cautious about the actual performance of the proposed scheme considering that we are scoring senders instead of individual emails.

			from the previous experiences between agents recommender-based aspect such as assessing whether an agent is reliable and we can rely on its recommendations (viz. Trust in recommendation).			
8	Simulating Dynamical Features of Escape Panic	Dirk Helbing, Illes Farkas, Tamas Vicsek	One of the most disastrous forms of collective human behaviour is the kind of crowd stampede induced by panic, often leading to fatalities as people are crushed or trampled. Sometimes this behaviour is triggered in life-threatening situations such as fires in crowded buildings; at other times, stampedes can arise from the rush for seats or seemingly without causes. Yet, systematic Our results suggest practical ways of minimising the harmful consequences of such events and the existence of an optimal escape strategy, corresponding to a suitable mixture of individualistic and collective behaviour.	2000	Various security algorithm is used to protect data	Security is less and implementations of security algorithm is high
9	A 61-million-person experiment in social influence and political mobilization.	Bond RM,Fariss CJ,Jones JJ,Kramer AD,Marlow C,Settle JE,Fowler JH.	Human behaviour is thought to spread through face-to-face social networks, but it is difficult to identify social influence effects in observational studies, and it is unknown whether online social networks operate in the same way. Here we report results from a randomized controlled trial of political mobilization messages delivered to 61 million Facebook users during the 2010 US	2012	Provide an efficient algorithm to provide security	Security is low

			congressional elections. The results show that the messages directly influenced political self-expression, information seeking and real-world voting behaviour of millions of people. Furthermore, the messages not only influenced the users who received them but also the users' friends, and friends of friends. These results suggest that strong ties are instrumental for spreading both online and real-world behaviour in human social networks.services.			
10	Susceptible-infected-susceptible epidemics on the complete graph and the star graph: Exact analysis	Cator E, Van Mieghem P.	Since mean-field approximations for susceptible-infected-susceptible (SIS) epidemics do not always predict the correct scaling of the epidemic threshold of the SIS metastable regime, we propose two novel approaches: (a) an ε-SIS generalized model and (b) a modified SIS model that prevents the epidemic from dying out (i.e., without the complicating absorbing SIS state). Both adaptations of the SIS model feature a precisely defined steady state (that corresponds to the SIS metastable state) and allow an exact analysis in the complete and star graph consisting of a central node and N leaves.	2013	Dependence of data object in a network is reduced.	Data security is less
11	Social network analysis and mining for business applications	F. Bonchi, C. Castillo, A. Gionis, and A. Jaimes	In this article we use a business process classification framework to put the research topics in a business context and provide an overview of what we consider key problems and techniques in social network analysis	2011	It provide various security metrics	Security is less

			and mining from the perspective of business applications. In particular, we discuss data acquisition and preparation, trust, expertise, community structure, network dynamics, and information propagation. In each case we present a brief overview of the problem, describe state-of-the art approaches, discuss business application examples, and map each of the topics to a business process classification framework.			
12	Human interactive patterns in temporal networks	Yogesh Sharma, BahmanJavadi, Weisheng Si	Modern information and communication technologies provide digital traces of human interactive activities, which offer novel avenues to map and analyze temporal features of human interaction networks. This paper explores mesoscopic patterns of human interactive activities from six real-world interaction networks with temporal-topological isomorphic subgraphs, i.e., temporal motifs. Finally, we analyze temporal robustness and generalization to verify that 3-event temporal motifs are a simple yet powerful tool to capture the mesoscopic patterns of human interactive activities.	2014	Provides an efficient technic to overcome drawbacks of Networks	Required more times
13	On studying the impact of uncertainty on behavior diffusion in social networks	Y. Wang, A. V. Vasilakos, J. Ma, and N. Xiong	This paper deeply explores the pattern of gossip diffusion in social networks when uncertainty exists in users' decision making. In detail, the innovative results provided in this paper are: first, inspired by random utility theory,	2015	Data is secured based on various methods	Due to data is divided data loss is possible

			we formulate the diffusion model based on mixed logit model that allows for user's uncertainty in determining whether to adopt a specific strategy; second, the formal analysis framework characterizing the diffusion process is derived through the approximation method of mean field theory; finally, we explore the extensive applicability of our proposed analysis framework through modeling rumor diffusion in social networks as a coordination game. The obtained results perfectly comply with the philosophical saying about rumor diffusion in real social life: easy come, easy go.			
14	Formalization and verification of group behavior interactions	C. Wang, L. Cao, and C.-H. Chi	Group behavior interactions, such as multirobot teamwork and group communications in social networks, are widely seen in both natural, social, and artificial behavior-related applications. Behavior interactions in a group are often associated with varying coupling relationships, for instance, conjunction or disjunction. Such coupling relationships challenge existing behavior representation methods, because they involve multiple behaviors from different actors, constraints on the interactions, and behavior evolution. In addition, the quality of behavior interactions are not checked through verification techniquesand inter-coupled behavior aggregations (behaviors	2015	Provides more security	High level of knowledge is required

			conducted by different actors) from temporal, inferential, and party-based perspectives. OntoB converts a behavior-oriented application into a TS and temporal logic formulas for further verification and refinement.			
15	Study on cyber-enabled social movement organizations based on social computing and parallel systems	F.-Y. Wang	Social computing, as the technical foundation of future computational smart societies, has the potential to improve the effectiveness of open-source big data usage, systematically integrate a variety of elements including time, human, resources, scenarios, and organizations in the current cyber-physical-social world, and establish a novel social structure with fair information, equal rights, and a flat configuration. Meanwhile, considering the big modeling gap between the model world and the physical world, the concept of parallel intelligence is introduced. Afterwards, decisions with the expected outputs are executed in parallel in both the artificial and physical systems to interactively sense, compute, evaluate and adjust system behaviors in real-time, leading system behaviors in the physical system converging to those proven to be optimal in the artificial ones. Thus, the smart guidance and management for our society can be achieved.	2011	Trusted third parties are used	Security implementation is little costly

III. CONCLUSION

Viruses are very destructing programs, that can devasting to companies and individuals. It

consist of automatic artificial intelligence system which helps user to get rid of virus and gives the proper reporting of it.

IV. FUTURE WORK

Identifying and destructing the viruses which are even encrypted by crting techniques and Automatic identification and blocking of virus patterns which are not even registered.

REFERENCES:

[1] M. Nemiche, V. Cavero, and R. P. Lopez, "Understanding social behavior evolutions through agent-based modeling," in Proc. Int. Conf. Multimedia Comput. Syst. (ICMCS), Tangier, Morocco, 2012, pp. 980–986.

[2] V. T. da Silva and C. J. P. de Lucena, "Modeling multi-agent systems," Commun. ACM, vol. 50, no. 5, pp. 103–108, May 2007.

[3] F.-Y. Wang and J. S. Lansing, "From artificial life to artificial societies— New methods for studies of complex social systems," Complex Syst. Complexity Sci., vol. 1, no. 1, pp. 33–41, Jan. 2004.

[4] F.-Y. Wang, "Artificial societies, computational experiments, and parallel systems: A discussion on computational theory of complex socialeconomic systems," Complex Syst. Complexity Sci., vol. 1, no. 4, pp. 25–35, 2004.

[5] F.-Y. Wang, "Back to the future: Surrogates, mirror worlds, and parallel universes," IEEE Intell. Syst., vol. 26, no. 1, pp. 2–4, Jan./Feb. 2011.

[6] F.-Y. Wang, K. M. Carley, D. Zeng, and W. Mao, "Social computing: From social informatics to social intelligence," IEEE Intell. Syst., vol. 22, no. 2, pp. 79–83, Mar./Apr. 2007.

[7] A. Louati, J. El Haddad, and S. Pinson, "A multilevel agent-based approach for trustworthy service selection in social networks," in Proc. IEEE/WIC/ACM Int. Joint Conf. Web Intell. (WI) Intell. Agent Technol. (IAT), Warsaw, Poland, 2014, pp. 214–221.

[8] D. Helbing, I. Farkas, and T. Vicsek, "Simulating dynamical features of escape panic," Nature, vol. 407, pp. 487–490, Aug. 2000.

[9] R. M. Bond et al., "A 61-million-person experiment in social influence and political mobilization," Nature, vol. 13, no. 489, pp. 295–298, 2012.

[10] E. Cator and P. Van Mieghem, "Susceptible-infected-susceptible epidemics on the complete graph and the star graph: Exact analysis," Phys. Rev. E, vol. 87, no. 1, 2013, Art. no. 012811.

[11] F. Bonchi, C. Castillo, A. Gionis, and A. Jaimes, "Social network analysis and mining for business applications," ACM Trans. Intell. Syst. Technol., vol. 2, no. 3, Apr. 2011, Art. no. 22.

[12] Y.-Q. Zhang, X. Li, J. Xu, and A. V. Vasilakos, "Human interactive patterns in temporal networks," IEEE Trans. Syst., Man, Cybern., Syst., vol. 45, no. 2, pp. 214–222, Feb. 2015.

[13] Y. Wang, A. V. Vasilakos, J. Ma, and N. Xiong, "On studying the impact of uncertainty on behavior diffusion in social networks," IEEE Trans. Syst., Man, Cybern., Syst., vol. 45, no. 2, pp. 185–197, Feb. 2015.

[14] C. Wang, L. Cao, and C.-H. Chi, "Formalization and verification of group behavior interactions," IEEE Trans. Syst., Man, Cybern., Syst., vol. 45, no. 8, pp. 1109–1124, Aug. 2015.

[15] F.-Y. Wang, "Study on cyber-enabled social movement organizations based on social computing and parallel systems," J. Univ. Shanghai Sci. Technol., vol. 33, no. 1, pp. 8–17, 2011.