Review on social security attacks on online social networking for Rumors Blocking

Mrs.Shita.M.Mohod **Dr.Swati S. Sherekar** **Dr.V.M.Thakare** **Dr. N.B.Raut**

***Abstract*- An online social media is a big platform to share thoughts, ideas and knowledge. Now a days the day life strees with social platform and end on it as well this will become big media of communication. This media will share the good as well as bad thoughts.In this rumor gets spread with the speed of light. So it is necessary to block or filter the media to spreading the rumors, for that the activities done due to rumors can be stop. People from different geometric locations to talk, share photos, ideas and interests, or make new friends as a virtual community is a website on the internet that serves as an ultimate location for. Online social network increase in security treats and rumors with the rapid increase in popularity. By exploiting user's privacy, identity and confidentiality the intruders and attackers are able to outsmart the security measures by using several techniques. In social networking sites users may be unaware of the existence of these rumors. In this paper we proposed different types of attacks to fight against rumors on social network. In this paper we study an overview and classification of Sybil, Malware, Distributed Denial-of-service(DDOS) and Spam attacks.**

***Keywords*- Attacks, OSN, DDOS, Social Security Network, Rumor Blocking**

I. INTRODUCTION

With the rapid increase in online Internet users, an online social network such as Twitter, Facebook and Whatsapps. Due to this with more terrible effects rumors can spread faster. In real world situation, Rumors exist in almost every domain of society. We study different types of attacks to fight against rumours on social network.OSN services handle user's information and manage all user;s activities in the social network. For the correct functioning of services and maintaining a profitable business model OSN's are responsible. OSN's may be translate into reputation damage Service due to following attacks. We classify the four types of attacks those are Sybil,DDoS,Spam and Malware. we also discuss merits and demerits with suitable protocols, techniques, Layers and varient parameters.

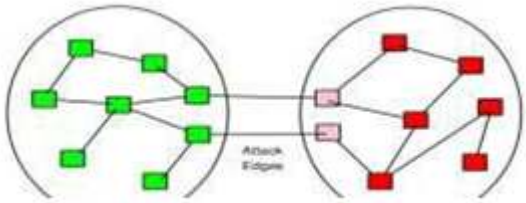

Figure 1: Sybil Attacks

In the Sybil attack, the malicious user claims multiple identities to compromise the whole network. Sybil attacks can be used to access resources or to break the trust mechanism behind a P2P network. The assumption that a P2P network is built on each entity in the network which holds a single identity. With a single entity or with no entity, Sybil attack occurs due to many bogus identities at all. Using Sybil identities, an adversary may provide false opinions for his evil benefits, limit the amount of resources reaching each node, break the trust mechanism in a P2P network and may even cause a Denial-of Service attack(DDoS)[1].digital signatures and digital analyzers were used to mitigate the Sybil attacks[2]. Much effort has gone into the study of trust relationships in social networks [1][2][3][5] and community based schemes to reduce the influences of Sybil attacks [6][7].

2. TYPES OF ATTACKS

2.1Classification of Sybil attacks

(i) Direct vs. In-Direct communication

The attacker must consider the type of communication between honest nodes and Sybil nodes [2][5]. If the communication between honest node and Sybil node is direct, i.e. if the attacker can directly communicate with the honest node using fake identities, it is a case of direct communication. However, if the attacker has to use his rightful or genuine identity to communicate with the honest node, and then divert the Sybil data to the honest node via the valid node, it is the case of indirect

communication.In direct communication, attacker has easy task to instigate Sybil attacks and it is also more difficult to detect such attacks.

(ii) Busy vs. Idle: In a P2P network, normally, only few Sybil identities participate in the network while the others remain idle [2]. The power of the Sybil attacker comes from the number of identities he or she holds. If an attacker could afford to get fake identities easily, he or she can make the identities appear more realistic by making them leave and join the network multiple times pretending as an honest node [5].

(iii)Simultaneous vs. Non Simultaneous A simultaneous attack can be performed by involving all the Sybil identities simultaneously or a single physical node can change its identities in regular time slots to appear like all the identities are involved simultaneously. In non-simultaneous attack, an attacker may bring all his identities into the network slowly over a period of time involving only few identities each time. This can be done by pretending that one identity is leaving the network while the other identity is joining the network. As honest identities generally tend to leave and join the network number of times, the malicious node won't be suspected if they pretend to leave or join the network now and then using different identities[8].

(iv) Insider vs. Outsider The impact of the Sybil attack depends on whether the attacker is inside or outside the distributed network. If the adversary is part of the network and holds at least one real identity, then the attacker is called an Insider, otherwise he or she is an outsider. An insider may introduce many fake identities, and pretend to communicate with other nodes using his fake identities. However, for an outsider, it is difficult to introduce Sybil identities into the network,

2.2 Distributed Denile-of-service:

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources such as a server, web site or other network resource. The flood of incoming messages, resource requests to the target system forces it to slow down. Exploited machines can include computers and other network resources such as IoT devices. In DDoS attack, the attacker begins by exploiting a flaws in a system that can leave it open to attack and making it the DDoS master. The flaws in a system also called vulnerability. A computer or networked device under the control of an intruder is known as a Botnet [10]. The person in control of a botnet is sometimes referred to as the botmaster (that term has also historically been used to refer to the first system "recruited" into a botnet because it is used to control the spread and activity of other systems in the botnet).Botnets can be comprised of almost any number of bots; botnets with tens or hundreds of thousands of nodes have become increasingly common, and there may not be an upper limit to their size.

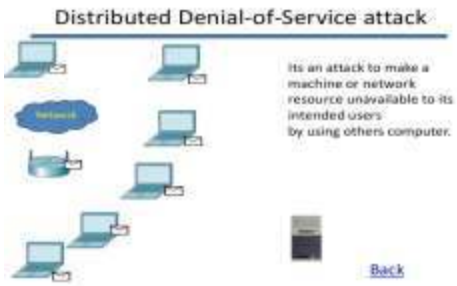

Figure2. DDOS

2.2.1 Classification of DDoS attacks:-

(i) Volume Based Attacks: The attack's goal is to saturate the bandwidth of the attacked site and Magnitude. Volume based attack include UDP floods, ICMP floods, packet floods with bandwidth. The inundation of packets at the target causes a denial of service. The internet of things (IoT) may be useful to legitimate users in some cases [9], they are even more helpful to DDoS attackers. The devices connected to IoT include any appliance into which some computing and networking capacity has been built, and, all too often, these devices are not designed with security in mind[9].For example, for attackers, devices are often shipped with hard-coded authentication credentials for system administration, to log in simply.some other cases, the authentication credentials cannot be changed. Devices also often ship without the capability to upgrade or patch device software, further exposing them to attacks that leverage well-known vulnerabilities. Internet of things bonnets are increasingly being used to wage enormous DDoS attacks[9].

2.3 Spam Attack

Spam can spread out in any information systems like emails, web, social network sites, and blogs or in review platforms. it is an endless repetition of worthless text or image, The concept of web spam was introduced in 1996 [11] and it soon become key challenges for search engine industry [12].Nowadays the major search engine companies have

identified adversarial information retrieval [13] as top priority because of multiple negative effects caused by spam, and also the appearance of new challenges in the field of research. In the first spam the quality of research spoils and prevents the genuine websites of revenue that might earn in the absence of spam. Second it weakens the trust of user in a search engine provider which is a notable issue since the user can easily continue his search form one search engine to other. In Spam to send out unrequested or unwanted messages in bulk, the electronic messaging system to be used.

Figure 3:Spam Attacks

2.3.1Classification of Spam Attack

i) Social network spam: The development of social networking site become very high in the past few years.The people communicate with their friends and chat or share multimedia contents with them. Sites like face book, twitter are constantly among top 20 most viewed websites on the internet [13].

People spent more time on social network compared with other sites. The increasing popularity of social networks allows them to collect a huge amount of personal information about the users, their friends, habits and also their wealth information. In social network a person can reach any person which is attracted by the spiteful parties.As for Twitter, [12] ran an experiment on Twitter spam. Regarding the drawbacks in Bayesian spam filter an user-friendly spam filter called Social network Aided Personalized and effective spam filter (SOAP) is used.social closeness spam filtering, social interest based spam filtering, and adaptive trust management.

ii) **Email spam:** The most common communication in the internet is using email communication. With the vast growth in email and its popularity unsolicited e-mail (spam) also emerged very quickly with almost 90% of all email messages. i.e., over 120 billion of these messages are sent each day [12]. The cost of sending these e-mails is very close to zero being easy to reach a high number of potential consumers [13]. In this context, spam consumes resources; time spent reading unwanted messages, bandwidth, CPU, disk, being also used to spread malicious content. The email system design can easily be exploited by spammers who send inaccurate information. All email on the Internet is sent via a protocol called Simple Mail Transfer Protocol ("SMTP").SMTP is designed to capture information about the route that an email message travels from its sender to its recipient. In actuality, the SMTP protocol provides no security, email is not private, it can be altered en route, and there is no way to validate the identity of the email source.

iii) Image spam: Image spam have been proliferated through emails which contain the text of the spam message in a human readable image instead of the message body. The spam message into images will be embeded as email attachments. Textual content performed by spam filters, including automatic text classifiers becomes the goal for spam to circumvent the analysis of emails. Since attached images are displayed by default by most email clients, the message is directly conveyed to the user as soon as the email is opened. The simplest kind of image spam can be viewed as a screen shot of a plain text written using a standard text editor.

iv) Click spam. In click spam, the spammers generate fraud clicks and make the control function towards their websites. To achieve the goal spammers submit queries to search engine and click on the links point to the target pages [12, 13]. Online advertising is other incentive for spammers to generate fraudulent clicks [13]

V) Content spamming:In content spamming changing the logical view that the search engine has over the page contents. An example of content spamming is keyword stuffing which involves placement of keywords within the webpage to raise the keyword count.

Malware Attack

Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, Script, active content and other software[14].The code is described as computer viruses, worms, Trojan Horses, Spyware[15]. The term

malware comes from combining the two words malicious and software, and to be used to indicate any unwanted software. any code added, changed, or removed from a software system.[16].The purpose of Malware is to cause damage or penetrate users computer for the purpose of hacking personal data for illegal activity such as financial crimes. Many DoS viruses, and the Windows Explore Zip worm, are designed to

demolish files on a hard disk, or to corrupt the file system by writing void data to them.

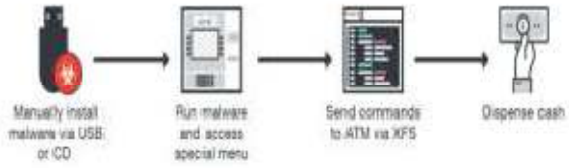

Figure 4: Malware Attacks

2.4.1 Classification of Malware Attack

Several malware classifications have been issued so far, depending on some of their characteristics. The purpose of such classifications is to facilitate the tracking of authorship, correlating information, identifying new variants [17]. However, The classification made, is to categorize the major common malware types into groups depending on the network and web usage.

i) Network-based Malware

Spyware is a kind of malware that is installed secretly on a user computer for the purpose of collecting information about users without their knowledge [17]. Even reputable vendors of software like Microsoft and Google, intentionally, collect information of their users using spywares [18].

Cookies are some information stored on user's computer by their web browsers. The main purpose of cookie is to authenticate users depending on the information stored in, storing site preferences and server-based session [17].

Trojan horse is a code that appears to be a useful program, but actually it steals information or corrupts data [17, 18].

Botnet is a collection of infected computers (contains bot software embedded in it) that have been taken over by hacker and used to perform malicious functions, without the hackers having to log into the client's computer. Botnet can make DoS attack as many clients' bots, under control of hacker bot, having a role of attack [19, 20].

ii) Ordinary Malware

Virus is any software code that has the ability to replicate itself, during infection, into any other application software or a document. Viruses can do harmful functions on a user machine; it can make destruction to the whole system from infected device to uninfected one [18, 19, 20].Worm is any software code that has the ability of self replicating on victim computer. Worms are independent; they don't need for a host program to start lifecycle [20].

Layers	Network	Transport, Application	Application	Network
Techniques	Light Weight Sybil Attack Detection	Defence techniques	Rule Based scoring system	Signature and Detection
Methods	Robust,Lightweight	Artificial Neural Network	Spammers	Pre-pending,Embedding,Post - pending
Virus Activated	Worm Rumor(Bogus	Botnet I	Worms Repetition of	Trojan Horse
Mode of Attacks	Identities)	ntruder	worthless text or image	Intrusive Code
Protocol	P 2 P	UDP,TCP/IP,HTTP, SMURF	SMTP, VOIP	UDP,HTTP,SOCKS 4/5
Merits	i)Efficient in large overhead ii)No clock synchronization	i i) Detecting and stopping a DDoS attack at the source providers. ii) minimum damage is done on legal traffic	i) In a short period of time it is essential to send as many messages as possible. ii) Transitional period is the only one service need to be maintained	**i)** Protection from Phishing Attacks. ii) Provides Robust Web Protection.

			instead of two parallel running services .	
demerits	i) reliability is lesser ii) May encourage attackers economically	i) Sources are widely distributed across the network and a single source behaves like a normal traffic due to this it become difficult to detect DDoS attack at source end. ii)The difficulty of deploying system at the source end.	i) Sending Email capacity become limitted. ii) Analyzing the messages to determine if they contain spam.	i) Security defects in software ii)Insecure design or user error.

III. CONCLUSION

Social security attacks are needed to fight against rumors blocking on social network. In this paper, we study how social network security attacks occur to fight against rumors on social network and their classification with variant parameters. In Sybil attack, an intruder may introduce many unauthorised identities and to communicate with other nodes using unauthenticated identities. For an outsider it is difficult to introduce sybil identities into the network. In DDoS multiple computer systems attacks a object such as server, website or other network resources and exploiting a vulnerability in one computer system and making it the DDoS master. Using SMTP, VoIP protocols, Spam is essential to send many messages in short period of time. There is an endless repetition of worthless text, lines, videos and images. Spam can spread out in any information system like E-mails, Web, Social Network Sites.Using malware attack any code added, changed or removed from a software system by intentionally causing harm or to disturb the internal function of the system that encompasses viruses, Trojans and other intrusive code. The purpose of such classification is to facilitate the tracking of authorship, correlating information, denitrifying new varients.In future to avoid rumor blocking occurance on social network we needed social security attacks in this direction.

REFERENCES

[1] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman. Sybil Guard: Defending against Sybil attacks via social networks. In SIGCOMM, 2006.

[2] H. Yu, M. Kaminsky , P.B. Gibbons, and A. Flaxman. Sybil Limit: A near optimal social network defense against Sybil attacks. In IEEE Symposium on Security and Privacy, 2008.

[3] J. Newsome, E. Shi, D. Song, A. Perring. The Sybil Attack in Sensor Networks: Analysis & Defenses, In Proc. of ACM IPSN, 2004.

[4] W. Chang and J. Wu. A Survey of Sybil Attacks in Networks. In publications of computer and Information Sciences, Temple University, Philadelphia, 2013

[5] G.V. Rakesh, S. Rangaswamy, V. Hegde, G. Shoba. A Survey of techniques to defend against Sybil attacks in Social Networks, In IJARSCCE, 2014.

[6] W. Wei, F. Xu, C.C. Tan, Q. Li. Sybil Defender: Defend Against Sybil Attacks in Large Social Networks, In Proc of IEEE INFOCOM, 2012.

[7] L. Shi, S. Yu, W. Lou, Y. T. Hou. Sybil Shield: An agent-Aided Social Network-Based Sybil Defense among Multiple Communities, In Proc of IEEE INFOCOM, 2013

[8] Manju V C "Sybil attack prevention inWireless Sensor Network", IJCNWMC 2014.

[9] A. Harrison, "The denial-of-service aftermath," Feb. 2000, http://www.cnn.com/2000/TECH/computi ng/02/14/dos . aftermath.idg/index.html.

[10] www.academia.edu/2963956/A_Brief _Review_of_Denial-of-Service_Research_Papers

[11] Wikipedia, Spam"http://en.wikipedia.org/wiki/Spam_(electronic)

[12] https://www.ijcaonline.org/archives/v olume157/.../vairagade-2017-ijca-912633.pdf

[13]https://ieeexplore.ieee.org/abstract/document/7226077/

[14]https://ieeexplore.ieee.org/document/8 094101/ Vinod, P., et al., Survey on Malware Detection Methods. 2009

[15] McGraw, G. and G. Morrisett, Attacking Malicious Code: A Report to the Infosec Research Council. IEEE Softw., 2000. 17(5): p. 33-41.

[16] Xufang, L., P.K.K. Loh, and F. Tan.Mechanisms of Polymorphicand Metamorphic Viruses. in Intelligence and Security In

[17] Egele, M., et al., A survey on

automated dynamic malware-analysistechniques and tools. ACM Comput. Surv., 2008. 44(2): p. 1-42.

[18Idika, N. and A.P. Mathur., A Survey of Malware Detection Techniques. 2007.

[19] Nataraj, L., Karthikeyan, S., Jacob, G. and Manjunath, B.(2011) MalwareImages: Visualization and Automatic Classification. Proceedings of the 8th International Symposium on Visualization for Cyber Security, Article No. 4.

[20] Nataraj, L., Yegneswaran, V., Porras, P. and Zhang, J. (2011) A Comparative Assessment of Malware Classification Using Binary Texture Analysis and Dynamic Analysis. Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence,