Improved Security Mechanism For Social Network Sybil Attack

Suchita M. Bonde[1], Prof. Chinmay Batt[2]
[1, 2] Dept of Computer Science Engineering
[1, 2] RKDF Institute of Science and Technology (RKDFIST), Bhopal (MP), India.

Abstract- *from last many years people were concerned about the security of social area network. In this social area network people create multiple bogus identities. To overcome this drawback, Sybil Defender mechanism is used along with the two ways security technique is use. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately small cut in the graph between the Sybil nodes and the honest nodes. Sybil Guard exploits this property to bound the number of identities a malicious user can create. The proposed system involves sybil identification technique along with the concept of the two way security mechanism. This two way security mechanism divide the password in two server and according to fake clustering, IP differentiation, IP log technique is used to identify where the user is sybil or genuine user. Due to this we can easily identify the sybil user. We show the effectiveness of Sybil Guard both analytically and experimentally.*

Keywords- Sybil attack, Sybil Defender, IP log.

I. INTRODUCTION

Today's era, most of the system is vulnerable to Sybil attack and there is increase in sybil attack in social network. There are various technique and concept to prevent this. Among the various algorithm and concept, the Sybil identification algorithm plays a vital role. MANET is an autonomous system consists of several nodes. These nodes communicate with each other through wireless links. Due to infrastructure less nature of MANET and as there is no central authority to maintain and control the network makes it vulnerable to various attacks. There is an attack which causes so much destruction to a network Called Sybil attack. In Sybil attack, attackers use several identities at a time or they take-off identity of some trustworthy node present in the network. This attack can create lots of false impression in the network like decrease the trust of legitimate node by using their identities, disturbs the routing of packets so that they cannot reach to its desired destination, and many more[1]. Like this it disturbs the communication among the nodes present in the network. Sybil attack is very much destructive for mobile ad-hoc network. This scheme is based on observation that whether the sybil node go through a small cut in the social graph to reach the honest region. People have failed to notice that, the sybil user can also attack using the user password. This will cause efficiency in the existing system. Therefore to overcome this drawback, the concept of two way security mechanism is use in which the password is divided on two server .With the presence of one server, the user is not able to login. Because of this, only the authenticated user can login into the system not the sybil user [2]. The existing Sybil identification Scheme is prone to the sybil Attack, due to which the security of user not ensured. The two way security can be ensured by dividing a password on two servers, Hence only the genuine user can login into the system. Due to this, even if a sybil user tries to recover the password he will not be able to retrieve the password which is stored on two server. Proposed system involves the sybil identification algorithm along with the two way security mechanism [3]. Lots of detection and prevention mechanism has been developed from such serious threat which we will discuss below. In this paper we present the literature work about black hole and Sybil attack prevention and detection together with their advantages and disadvantages [4]. This paper describes the basic scheme and the attack to which it is prone. The different sybil attack are discuss. This paper proposes the concept of sybil identification mechanism in which sybil user is identified. Due to this the attack is not able to prevent as it is not having mechanism to prevent the sybil user. The paper discusses the describes the mechanism to identify the sybil node using the random walk technique. The advantage of this paper is that it will identify the sybil node but it suffers from high sybil attackers. The paper discusses the describes the mechanism to observe the sybil user and identify the sybil user if present this will help to identify the malicious activity and bogus identities [5]. Due to this bogus identity this mechanism also fails to prevent the sybil attack. The remaining section of the paper is organized as follows:

In section II describe the Literature overview of Sybil attack and related work about detection and prevention mechanism. In Section III describe proposed detection mechanism of Sybil attack. Section IV describe Implemented algorithm and Results, Last V section gives overall conclusion of the paper.

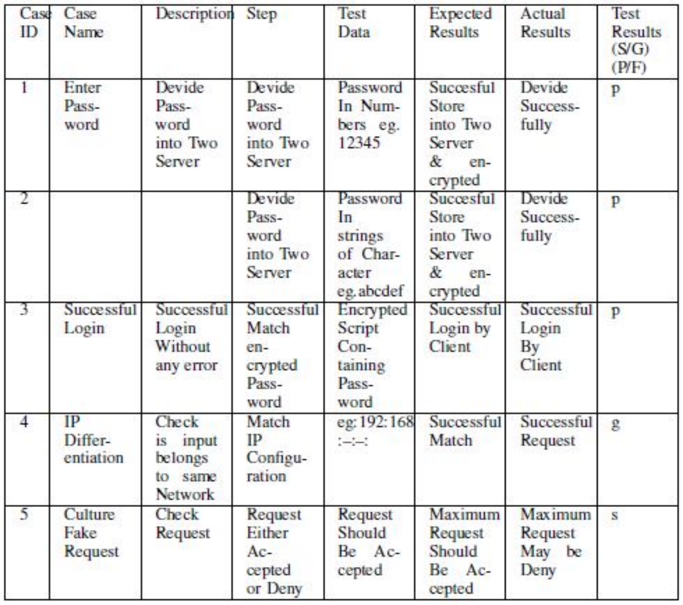
II. LITERATURE SURVEY

Literature survey plays vital role in the software development process. Different time factor, economic factor are taken into consideration. The Sybil attacks will have a serious influence on the normal process of wireless ad hoc networks. It is effectively necessary to detect Sybil attacks and remove them from the network. The traditional approach to avert Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not appropriate for mobile ad hoc networks because it usually requires inflated initial setup and incurs overhead related to maintaining and distributing cryptographic keys. But it has some Disadvantage such as first Existing approach uses extra hardware to provide security; Second Cryptographic techniques consume more resources for computation and Third Reduce the energy level of the mobile node. Lightweight Sybil Attack Detection Technique This technique is also termed as lightweight as it does not use any extra hardware or antennae for its operation. It is used to detect Sybil Attacks [15]. There are three steps in this process: 1) Types of Sybil nodes: Sybil nodes consist of two types. In the first type it simultaneously use many identities at a time either by deceiving others identities or by crafting its own identities. In the second type it uses only one identity at a time. 2) Threshold value: In this step we assume that normal nodes do not have speed greater than 10m/s. The nodes whose speed is greater than 10m/s are termed as Sybil nodes. 3) Comparison: In this step the RSS (Received Signal Strength) upper bound threshold value is calculated. The upper bound value is calculated as an average of RSS value when nodes are moving at 10m/s speed. When a new node enters in a network then its RSS value is compared with RSS upper bound value. If the value is greater or equal to upper bound RSS value then it is detected as Sybil node.

III. PROPOSED SYSTEM

The primary objective of architectural design is to develop a modular program structure and represent the control relationship between modules [7]. In addition, architectural design fields program structure and data structure, designing interface that enables data to throughout the program. Implementation plays a vital role in the project development. At this stage, the project is converted in to actual working system. Careful planning, study of existing system also plays an important role in implementation phase [6]. Implementation of the proposed system involves the environment in which the system is implemented and the overall system development. The overall development of the proposed system requires suitable environment and proper resources for its successful completion. The proposed system is developed to prevent the sybil attack.

TABLE I: Test cases for Propose system.



Case ID	Case Name	Description	Step	Test Data	Expected Results	Actual Results	Test Results (S/G) (P/F)
1	Enter Password	Devide Password into Two Server	Devide Password into Two Server	Password In Numbers eg. 12345	Succesful Store into Two Server & encrypted	Devide Successfully	p
2			Devide Password into Two Server	Password In strings of Character eg.abcdef	Succesful Store into Two Server & encrypted	Devide Successfully	p
3	Successful Login	Successful Login Without any error	Successful Match encrypted Password	Encrypted Script Containing Password	Successful Login by Client	Successful Login By Client	p
4	IP Differentiation	Check is input belongs to same Network	Match IP Configuration	eg:192:168 :–:–:	Successful Match	Successful Request	g
5	Culture Fake Request	Check Request	Request Either Accepted or Deny	Request Should Be Accepted	Maximum Request Should Be Accepted	Maximum Request May be Deny	s

1) Algorithm:

- Sybil identification: To identify the sybil user, Sybil identification algorithm is use and also determine whether the suspected node is sybil or not.
- Encryption algorithm: This encryption algorithm will encrypt the password and divide the password on two servers to provide more security to user.

2) Modules:

- User Registration: In user registration module, user is login in the system by filling the personal information.
- At this time the password is divided on two servers to provide security.
- Sybil Identification: This module is use to identify the sybil user and also checks the probability of the malicious activity. By observing this, the sybil user is identified and it notified admin that the user is sybil or genuine.
- Admin module: Admin will have an authority to check an individual's user whether he is sybil or genuine user. Propose system consist of following test cases shown in Table I. By considering these test cases we come to know whether the user is Sybil (s) or Genuine (G) and where the test is Pass (P) or Fail (F).

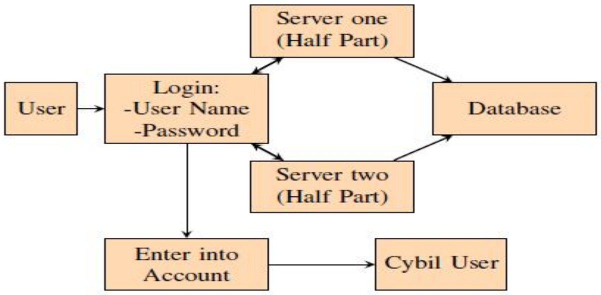


Fig. 1: Proposed System Architecture

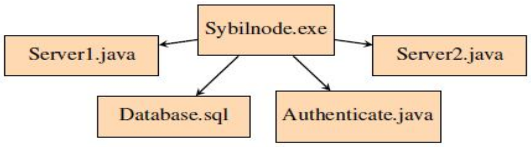


Fig. 2: Component Diagram of Sybil Defender

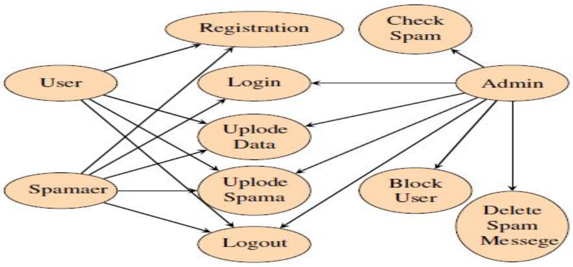


Fig. 3: Use Case Diagram of Detection for Sybil Attack

Figure 1 shows the architecture of proposed system. We propose Sybil Defender, a centralized Sybil defense mechanism. It consists of different modules and also having different methods to defense from Sybil user. Above architecture shows that user need to register for the use of social network site and User Authentication module authenticate user if multiple identities is not present. Our scheme is based on the observation that a Sybil users post which may publish in social network. After performing some detection methods on post then it will appear in social network. Hence there is no such activity which may harm to social networking site. User details and Sybil user's details stored in database and also their post details. Proposed systems have some advantages like it is helpful to and Sybil users. Also it is used to and fakes IDs. Also it is feasible limit the number of attack edges in online social networks by relationship rating. The Sybil identification mechanism is solution to the sybil attack. The sybil attack can be prevented by introducing the concept of the two way security mechanism [10]. Two way security mechanisms the password is divided on two servers. With the presence of one server, the user is not able to login. Because of this, only the authenticated user can login into the system not the sybil user. Problem Definition Secure social network is a necessity in today's era. Among the various mechanisms, sybil identification algorithm is use. But using this also the sybil user can attack the node this create adverse affect on system. Therefore, to overcome this drawback, the concept the concept of two way security mechanism is use in which the password is divided on two servers[8]. With the presence of one server, the user is not able to login. Because of this, only the authenticated user can login into the system. Sybil Defender consists of three components as shown in figure 3 a sybil Authentication Algorithm, a Sybil community detection algorithm Database and two supporting Servers approaches to limiting the number of attack edges. The three components can be used in conjunction to best mitigate sybil attacks [9]. The task of the sybil identification algorithm presented in Section III is to determine whether a suspect node is sybil or not. The proposed architecture includes activity and use cases as shown in figure 3 and 4. The user is login on the social network using username and password. The password is divided on two server half part is store on one server and another half part is on another server. When the user is login, the password from both servers is compared if they match then only user can login on the system otherwise not. The sybil user is identifies by using fake clustering, ip differentiation, ip log technique in sybil identification algorithm.

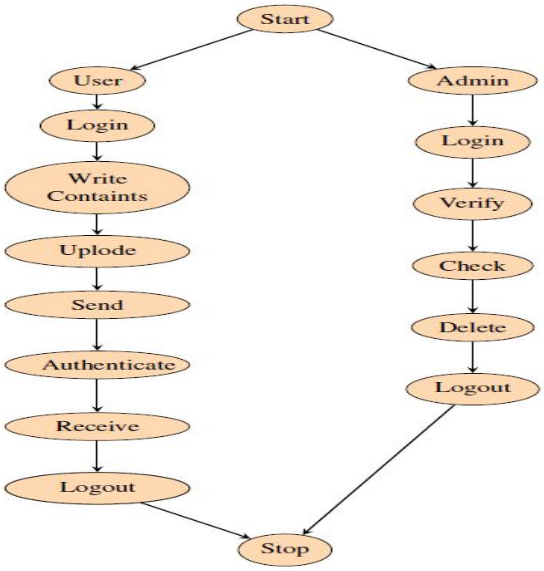


Fig. 4: Activity Diagram of Sybil Defender

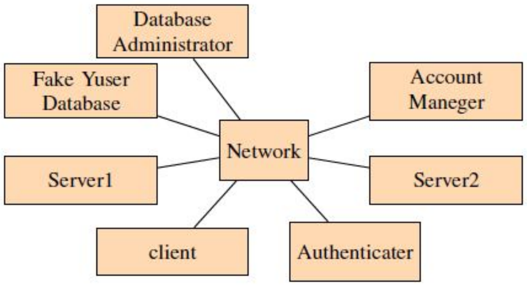
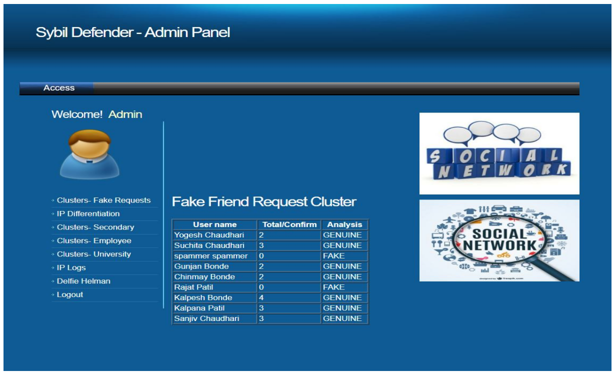


Fig. 5: Deployment Diagram of Sybil Defender

IV. IMPLEMENTATION AND RESULTS

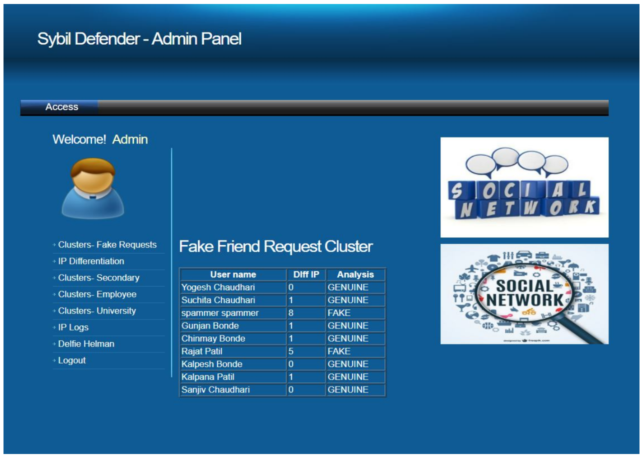
The project is Windows based hence it requires any Linux distribution. In this project, the Windows operating system is used. The implementation details include Sybil identification, Sybil Community detection and diffie helman is used to detect Sybil nodes. In this section it measure the performance of the proposed non Sybil region identification system with Sybil detection method based on the parameters like IP configuration, IP location, Gender , Falsely detected nodes between the existing and proposed Sybil and non Sybil region identification system. In this project, we implement the Sybil identification. For this implementation application and figure 5 shows deployment of sybil defender. We use Sybil identification algorithm along with Diffie Hellman algorithm. And choose the platform based on windows operating system that is implemented in java[13]. Sybil defender mechanism additionally detects the Sybil through the community based Sybil mechanism for single and numerous community based social networks which rejects the falsely detected nodes and improved identification results of the Sybil and non Sybil user. Sybil Attackers Result: Millions of node is involve in this system, however sybil user have power to launch the Sybil attack. The number of malicious node is created by sybil user to prevent this we improve the probability that user node will accept more honest node not sybil node. As the user is login on the system the password in the form of number, string, special character or a combination of these is encrypted and divided on two servers. The cluster for fake friend is determine by the formula total friend request send is divided by total confirm request using this we can determine whether the user is sybil or genuine figure 6 shows result on the basis of Fake friend requests and figure 7 shows results on the basis of Different IP address and figure 8 shows results on the basis of encrypted password on one server. The proposed system provides better reliability, integrity and security as compared to the existing system[12].



Fake Friend Request Cluster

User name	Total/Confirm	Analysis
Yogesh Chaudhari	2	GENUINE
Suchita Chaudhari	3	GENUINE
spammer spammer	0	FAKE
Gunjan Bonde	2	GENUINE
Chinmay Bonde	2	GENUINE
Rajat Patil	0	FAKE
Kalpesh Bonde	4	GENUINE
Kalpana Patil	3	GENUINE
Sanjiv Chaudhari	3	GENUINE

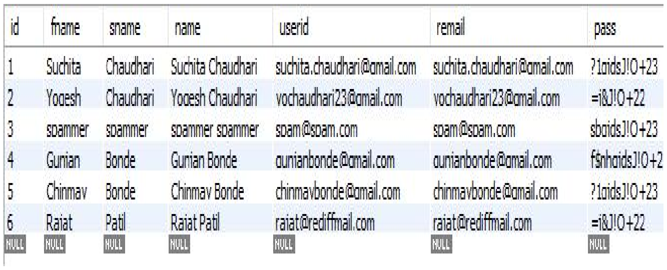
Fig. 6: Result on the basis of Total confirmation



Fake Friend Request Cluster

User name	Diff IP	Analysis
Yogesh Chaudhari	0	GENUINE
Suchita Chaudhari	1	GENUINE
spammer spammer	8	FAKE
Gunjan Bonde	1	GENUINE
Chinmay Bonde	1	GENUINE
Rajat Patil	5	FAKE
Kalpesh Bonde	0	GENUINE
Kalpana Patil	1	GENUINE
Sanjiv Chaudhari	0	GENUINE

Fig. 7: Result on the basis of Different IP Address



id	fname	sname	name	userid	remail	pass
1	Suchita	Chaudhari	Suchita Chaudhari	suchita.chaudhari@gmail.com	suchita.chaudhari@gmail.com	?1gidsJ!O+23
2	Yogesh	Chaudhari	Yogesh Chaudhari	ygchaudhari23@gmail.com	ygchaudhari23@gmail.com	=i&J!O+22
3	spammer	spammer	spammer spammer	spam@spam.com	spam@spam.com	sbgidsJ!O+23
4	Gunjan	Bonde	Gunjan Bonde	gunjanbonde@gmail.com	gunjanbonde@gmail.com	f$nhgidsJ!O+2
5	Chinmay	Bonde	Chinmay Bonde	chinmaybonde@gmail.com	chinmaybonde@gmail.com	?1gidsJ!O+23
6	Rajat	Patil	Rajat Patil	rajat@rediffmail.com	rajat@rediffmail.com	=i&J!O+22
NULL	NULL	NULL	NULL	NULL	NULL	NULL

Fig. 8: Result of encrypted password on one server.

V. CONCLUSION

Security plays an important role in large social area network. In Existing system social area network people create multiple bogus identities. To overcome this drawback, Sybil Defender mechanism is used along with the two ways security mechanism is use. The proposed system consists of Sybil identification technique along with the concept of the two way security mechanism. This two way security mechanism divide the password in two server and according to fake clustering, IP differentiation, IP log technique is use to identify where the user is sybil or genuine user. The system can be further extended for the secure One more layer of password authentication to Secured a Communication in the cloud computing. In future we apply the existing system into the more real social network data among dissimilar structures and further improve the efficiency of our Sybil Identification algorithm. It will be implement in to use One more layer of password authentication to Secured a Communication in the cloud computing.

REFERENCES

[1] Suhendry Effendy and Roland H. C. Yap,“The Strong Link Graph for Enhancing Sybil Defenses”, IEEE 37th International Conference on Distributed Computing Systems, IEEE, pages 944-954, 2017.

[2] Muhammad Al-Qurishi, Atif Alamri and Sk Md Mizanur Rahman,"Sybil Defense Techniques in Online Social Networks: A Survey", IEEE ACCESS 2017,pages 1-19, 2017.

[3] Krishna N, Bhattchayrya and Dr. Narendra M. Sheokar,"At glance Sybil Detection OSN", 2015 IEEE International Symposium on Nanoelectronic and Information Systems, pages 47-52, 2015.

[4] Satyajayant Misra, Abu Saleh Md Tayeen and Wen Xu,"SybilExposer: An Effective Scheme to Detect Sybil Communities in Online Social Networks", IEEE ICC 2016 SAC Social Networking, 2016.

[5] Dimitris Mitropoulos, Panos Louridas, Michalis Polychronakis and Angelos D. Keromytis,"Defending Against Web Application Attacks: Approaches, Challenges and Implications", 1545-5971 (c) IEEE, pages 1-14, 2016.

[6] Zhi Yang, Jilong Xue, Xiaoyong Yang, Xiao Wang and Yafei
Dai,"VoteTrust: Leveraging Friend Invitation Graph to Defend against Social Network Sybils", IEEE Transactions on Dependable and Secure Computing, pages 1-14, November 2015.

[7] M.Shahira Banu, S. Lakshmi Narasimmha,"A Survey on Sybil Attacks in Social Networks", International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 4, Issue 3, pages 197-201, March 2015.

[8] Aparna Raj, Pankaj Kumar Vyas,"Detection and Prevention Mechanism of Black Hole and Sybil Attack in Mobile Ad Hoc Network: A Review", International Journal of Computer Applications (0975 8887) Volume 154 No.1,pages- 35-40, November 2016.

[9] Wei Chang and Jie Wu,"A Survey of Sybil Attacks in Networks", pages 1-12.

[10] Haifeng Yu, Michael Kaminsky and Phillip B. Gibbons,"SybilGuard: Defending Against Sybil Attacks via Social Networks", IEEE/ACM Transactions On Networking, VOL. 16, NO. 3, pages 576-589, JUNE 2008.

[11] Qiang Lu and Bo Liu and Huaping Hu,"SMCSN: A New Secure Model of Content Sharing Network by Using Multi-roles Sybil Nodes",Proceeding of Science(CENet2015),Pages 1-8, Shanghai, China, September 2015.

[12] Vrushali Kelatkar and Prof. Pravin Dere,"Prof. Pravin Dere", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 11, pg.173 180, November 2015.

[13] Xun Yi, San Ling and HuaxiongWang, " Efficient Two-Server Password-Only Authenticated Key Exchange",IEEE Transactions On Parallel And Distributed Systems, VOL. 24, NO. 9, pages 1773-1783, September 2013

[14] Wei Wei, Fengyuan Xu, Chiu C. Tan and Qun Li, " SybilDefender: A Defense Mechanism for Sybil Attacks in Large Social Networks", IEEE Transactions On Parallel And Distributed Systems, Pages 1- 11, 2013.

[15] Roopali Garg and Himika Sharma, "Comparison between Sybil Attack Detection Techniques: Lightweight and Robust" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 2, February 2014 Copyright to IJAREEIE www.ijareeie.com 7142.