IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-4 E-ISSN: 2347-2693

Efficient and Enhancement Prediction of Sybil Attacks in Online Social Networks Using Vote-Trust Method

K.Dhivya[1], S.Dhanalakshmi[2]

[1]*M.E Scholar, Department of Computer Science & Engineering, A.R.J College of Engineering & Technology, Mannargudi.*
[2] *Assistant Professor, Department of Computer Science & Engineering, A.R.J College of Engineering & Technology, Mannargudi.*

www.ijcseonline.org

Received: Mar/23/2016 Revised: Apr /03/2016 Accepted: Apr/19/2016 Published: Apr/30/2016

Abstract— A remote sensor framework comprises of numerous sensor hubs which are deployed to monitor physical or environmental conditions Also, to pass the collected information to a base station. Though remote sensor framework is subjected to have major applications in all the areas, it too has numerous security dangers Also, attacks. Among all dangers such as sinkhole, wormhole, selective forwarding, denial of service also, hub replication, Sybil assault is a major assault where a single hub has different identities. When a Sybil hub act as a sender, it can send false information to its neighbors. When it acts as receiver, it can receive the information which is originally destined for a legitimate node. The existing arrangements consume more energy. So a vitality effective calculation named Sybil secure is proposed. Experimental results appear that Sybil secure devours less vitality than existing protection mechanisms.

Keywords— Remote Sensor Network, Sybil, Group Head, Inquiry Packet.

I. INTRODUCTION

Remote sensor systems consist of as numerous numbers of hubs which can communicate with each other. Each hub comprises of a microcontroller, an electronic circuit for interfacing with sensors Also, battery, a radio transceiver Also, an external memory. Remote sensor systems are being utilized for different applications such as area monitoring, healthcare checking Also, checking the combat zone for security purposes. But due to the broadcast nature in remote correspondence Also, low physical protection of sensor nodes, an intruder can easily tend to assault the network. Different assaults on each layer are listed in the table below.

In this paper, an effective calculation against Sybil assault is proposed as it is a huge destructive assault in sensor networks. In case of Sybil attack, a sensor hub behaves as if it were a bigger number of nodes, by faking other nodes. Sybil secure is based on the querying Also, recognizing the nodes.

Table 1. Assaults on distinctive layers

Layer	Attack
Physical	Jamming, Node destruction
Data link	Denial of service
Network	Spoofing, replaying, Hello floods, Homing, Sybil
Transport	SYN flood, De synchronization attack
Application	Reprogramming attacks

II. RELATED WORK

The existing components include centralized Also, decentralized approaches. The vast implemented arrangement is trusted affirmation. This arrangement assumes that there is a exceptional trusted third party or central authority, which can verify the validity of each participant, Also, further issues a affirmation for the honest one. In reality, such affirmation can be a exceptional hardware device or a digital number. Note that essentially both of them are a series of digits, but are stored on distinctive media. Before a member joins a peer-to-peer system, provides votes, or obtains services from the system, first his personality must be verified. This strategy gets its limitation when it is applied for bigger network. Another strategy works based on the resource utilized by the node. If a Sybil hub exists then it has to perform the tasks of the personalities it possess. So when it exceeds a threshold value then the Sybil hub is detected. .Secret key can too be shared but it devours more power as it involves in complex encryption Also, decryption techniques. In contrast to existing arrangements that are based on sharing encryption keys, RSSI based scheme presents a arrangement for Sybil assault based on gotten signal strength indicator (RSSI) readings of messages. Though it is said to be lightweight (i.e., only one message communication), it is time-varying, unreliable Also, radio transmission is non-isotropic. Accuracy reduces as the transmission distance increases. Recent researches in Sybil protection components are based on Social framework based plans . These plans use the

trust structure embodied in the networks. They have two assumptions, 1) Sybil hubs can create arbitrarily number of personalities but relationship to non-Sybil nodes. Sybil hubs are poorly connected to non-Sybil nodes. 2) One trusted non-Sybil hub is known. Based on these suppositions different protection plans such as Sybilguard, Sybillimit, Sybilcontrol, Sybilinfer, Sumup, Gatekeeper are proposed.

III. PROPOSED SYSTEM

The proposed arrangement is based on sending Also, responding to the inquiry sent by the group head. The Group head has a list of its sub hubs parameters. The parameters are the personalities Also, their location.

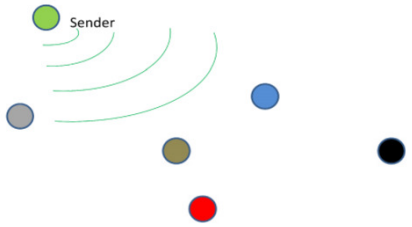

Fig.1. Framework with a Group head, 4 legitimate hubs Also, a Sybil node.

Table 2. Dataset in Group head

NODE	DATASET
	1,X
	2,Y
	3,Z
	4,A

The Group head broadcasts a inquiry bundle to all the sub hubs in such a way that it expects a answer that all the sub hubs must send their id Also, location. There are there cases in which the Sybil hub reacts.

(i) No reply:

When a inquiry bundle is gotten by all the legitimate sub hubs including Sybil node, it does not react to it. It simply gets the bundle Also, drops it. Whenever retransmission is done for different times, the Sybil hub does not react to it.

(ii) Answers with same Personality Also, distinctive coordinates:

In this case, all the legitimate sub hubs react to the group head with their personality Also, location. The Sybil hub too reacts to the group head with any one of the Sub hubs personality Also, its own location. For example, If a group head has 4 hubs say 1,2,3,4 with the area x, y, z, a respectively, Sybil hub must have any one these personality (1/2/3/4) Also, its own area d. Now the Sybil hub reacts with any one of these personalities Also, the area d. The group head already has the set of legitimate hubs personality Also, location. Conflicts arise when the legitimate hub Also, Sybil hub has same Also, distinctive location. The hub with the distinctive area is distinguished as Sybil node.

Table 3. Acknowledgements received

NODE	ID	LOCATION
	1	X
	2	Y
	3	Z
	4	A
	1/2/3/4	B

(iii) Answers with same personality Also, same coordinates:

This case will be future scope of this paper.

IV. VITALITY CALCULATION

In remote sensor framework vitality consumption is a major factor. Because when a hub runs out of battery, it becomes a major problem in network. A dead hub will affect entire communication. So the vitality devoured by the framework to distinguish a Sybil hub is calculated. Based on the formulae from , the vitality values are calculated. Equations (1) Also, (2) appear the vitality for group head Also, a hub respectively.

$$E_N(ij) = b\,V_{sup}\,I_{sense}\,T_{sense} + b\,V_{sup}\,(I_{write}T_{write} + I_{read}\,T_{read}) + b\,E_{elec} + Bd^n_{ij}\,E_{amp} + T_A\,V_{sup}[C_N\,I_A + (1\text{-}C_N)I_S] \quad \ldots(1)$$

$$ECH(j) = h_3\,b\,V_{sup}\,I_{sense}\,T_{sense} + h_4\,V_{sup}\,(I_{write}T_{write} + I_{read}\,T_{read}) + h_1\,b_1\,N_{CYC}\,C_{avg}\,V^2_{SUP}\,(n_j+1) + h_1\,b_1\,V_{sup}\,(I_0\,e^{(V_{sup}/N_P\,VT)})\,(N_{CYC}/f)\,(n_j+1) + h_2\,b_1\,E_{elec}\,(n_j) + h_2\,b_2\,(1+\gamma)\,d^n_j\,E_{amp} + h_2\,\gamma\,b_2\,E_{elec} + T_{CH}\,V_{sup}\,[C_{CH}\,I_A + (1\text{-}C_{Ch})I_S] + E_{actu}\,N_{act} \quad \ldots(2)$$

Consider a framework which has a group head Also, four nodes. The tables underneath appear the vitality devoured by group head Also, sensor node.

Table 4. Vitality devoured by group head

Cluster head	Energy Consumed (J)
Transmit	0.00784
Transient	0.049
Sense	0.594
Data logging	0.0000385
Receive	0.00384

Table 5. Vitality devoured by each node

Sensor node	Energy consumed
Transmit	0.00088
Transient	0.012
Sense	0.54
Data logging	0.000035
Receive	0.00349

Upon simulation Sybilsecure takes about 11.327 J to distinguish a Sybil node. But when considering other social based protection plans such as Sybilguard Also, Sybillimit devours more vitality than Sybilsecure. Sybillimit devours around 8.8 J for a period of time. Sybilguard devours about 13.48 J for a single round.

V. PROPOSED METHOD

We propose Sybil Defender Vote trust concept, a centralized Sybil defense mechanism. It consists of a Sybil identification algorithm to identify the Sybil nodes. This approaches to limiting the number of attack edges in online social networks. Vote Trust first uses a Page Rank style algorithm to appropriately assign the number of votes that one can cast on another node. This process assigns few vote capacity for individual Sybil and thus prevents them from significantly vouching each other through collusion. Our scheme is based on the observation that a Sybil node must go through a small cut in the social graph to reach the honest region. Sybil would get low global acceptance rates and thus can be identified out.

Advantages:-

- It is Helpful to find Sybil Attacks.
- It is used to Find Fake User ID.
- It is feasible to limit the number of attack edges in online social networks by relationship rating.
- Provide high privacy of a user.
- To recommend to a user with guarantee.

Proposed Architecture

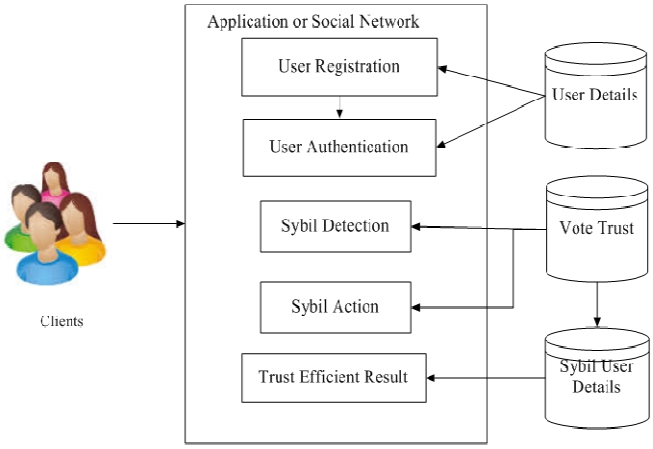

Fig 1. System Architecture

Proposed Algorithm

Item quality algorithm: Let U_k^1 and U_k^o denote the set of users who vote item I_k with 1 and 0, respectively. The trust value of user u_j is denoted by $T(u_j)$. Then, the quality of item I_k, denoted by Q(Ik), is calculated with majority voting as

$$f(x) = \begin{cases} 1 \text{ if } G(Ik) \geq B(Ik), \\ 0 \text{ if } G(Ik) < B(Ik) \end{cases}$$

Where

$$G(Ik) = \sum_{uj\ Uk1} T(uj); b(Ik) = \sum_{uj\ Uk0} T(uj)$$

In this calculation, the system utilizes the trust values as weight factors, and compare the summation of the weights of the users who vote 0 and that of the users who vote 1.

User trust algorithm: When a vote is given to item Ik by user uj , if the vote value is the same as the item quality Q(Ik) identified by item quality algorithm, this vote is considered as an honest vote. Otherwise, it is considered as a dishonest vote. For a user uj, the system calculates the number of honest votes given by this user, denoted by H(uj), and the number of dishonest votes given by this user, denoted by D(uj). The trust value of user uj is calculated with beta function.

$$T(uj) = H(uj) + 1/H(uj) + D(uj) + 2.$$

It is noted that there are many trust models. We chose beta function model because it has a solid theoretical foundation and is widely accepted in many systems. In addition, one of

the benefits of beta function is that when a user gives no vote, the trust value for him/her is 1/2.

1) For each user uj , initialize T(uj) as 0.5.
2) For each item Ij , update G(Ij) and B(Ij) using (2), and calculate Q(Ij) using (1).
3) For each user uj , update H(uj) and D(uj), and calculate T(uj) using (3).
4) If T(uj) for any user uj changes in step 3, go to step 2; else END.

VI. Experimental Results And, Comparisons

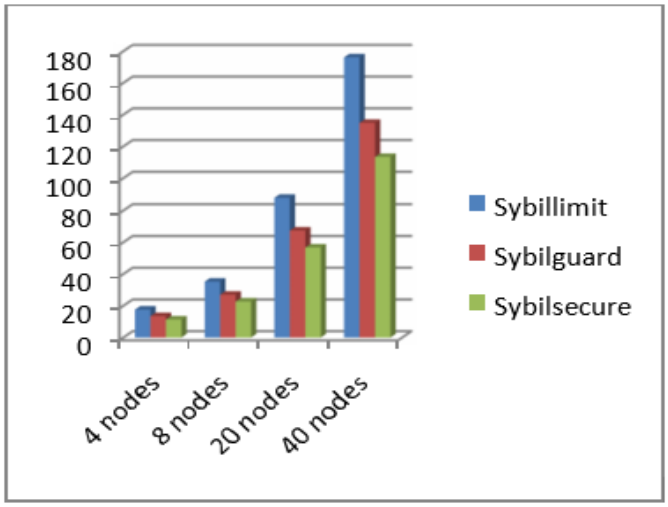

Fig 2.Vitality devoured to distinguish Sybil nodes.

VII. Conclusion

In this paper, Sybilsecure, and vitality effective calculation is proposed based on sending Also, recognizing the inquiry information packets. Social framework based plans which involved in random routes of information devoured more vitality to distinguish a Sybil node. But in Sybilsecure , a Sybil hub can be distinguished with less vitality Also, too without decreasing its efficiency.

This paper presented Sybil Guard, a novel decentralized protocol for limiting the corruptive influences of Sybil attacks, by bounding both the number and size of Sybil groups. Sybil Guard relies on properties of the users' underlying social network, namely that (i) the honest region of the network is fast mixing, and (ii) malicious users may create many nodes but relatively few attack edges. In all our simulation experiments with one million nodes based on the vote trust, Sybil Guard ensured that (i) the number and size of sybil groups are properly bounded for 99.8% of the honest users, and (ii) an honest node can accept, and be accepted by, 99.8% of all other honest nodes. Currently we are working on obtaining real social network data to further validate Sybil Guard.

Future enhancement:

In real world social network, Sybil attack be overlapped being the process of vote trust. In future may be using the Sybil attack process in the real time applications and mobile applications.

References

[1] Srdjan Krco; Mattias Johansson; Vlasios Tsiatsis; Ivica Cubic; Katarina Matusikova; Roch Glitho, "Mobile Network Supported Wireless Sensor Network Services" 2007 IEEE International Conference on Mobile Adhoc and Sensor Systems, Year: 2007, Pages: 1 – 3.

[2] Xuyuan Zhang,2009 5th International, "Model Design of Wireless Sensor Network Based on Scale-Free Network Theory" Conference on Wireless Communications, Networking and Mobile Computing, Year: 2009, Pages: 1 – 4.

[3] Xuhui Chen; Peiqiang Yu, "Research on hierarchical mobile wireless sensor network architecture with mobile sensor nodes", 2010 3rd International Conference on Biomedical Engineering and Informatics, Year: 2010, Volume: 7, Pages: 2863 – 2867.

[4] Yong-Sik Choi; Young-Jun Jeon; Sang-Hyun Park, "A study on sensor nodes attestation protocol in a Wireless Sensor Network", Advanced Communication Technology (ICACT), 2010 The 12th International Conference on, Year: 2010, Volume: 1, Pages: 574 – 579.

[5] Yang Wenguo; Guo Tiande, "Notice of Retraction The Non-uniform Property of Energy Consumption and its Solution to the Wireless Sensor Network", Education Technology and Computer Science (ETCS), 2010 Second International Workshop on, Year: 2010, Volume: 2, Pages: 186 – 192.

[6] Ren Yueqing; Xu Lixin, "A study on topological characteristics of wireless sensor network based on complex network", 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), Year: 2010, Volume: 15, Pages: V15-486 - V15-489.

[7] Jing Jiang; Zifei Shan; Wenpeng Sha; Xiao Wang; Yafei Dai, "Detecting and Validating Sybil Groups in the Wild", 2012 32nd International Conference on Distributed Computing Systems Workshops, Year: 2012, Pages: 127 – 132.

[8] Kuan Zhang; Xiaohui Liang; Rongxing Lu; Xuemin Shen, "Sybil Attacks and Their Defenses

in the Internet of Things", IEEE Internet of Things Journal, Year: 2014, Volume: 1, Issue: 5, Pages: 372 – 383.

[9] Neil Zhenqiang Gong; Mario Frank; Prateek Mittal, "SybilBelief: A Semi-Supervised Learning Approach for Structure-BasedSybil Detection", IEEE Transactions on Information Forensics and Security, Year: 2014, Volume: 9, Issue: 6, Pages: 976 – 987.

[10] R. Renuga Devi; M. Hemalatha, "Sybil node identification algorithm using connectivity threshold for secured community mining in social network", Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, Year: 2013, Pages: 1 – 4.

[11] Avita Katal; Mohammad Wazid; Roshan Singh Sachan; D. P. Singh; R. H. Goudar, "Effective Clustering Technique for Selecting Cluster Heads and SuperCluster Head in MANET" Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on, Year: 2013,Pages: 1 – 6.

[12] Qiao Xuegong; Chen yan, "A control algorithm based on double cluster-head for heterogeneous wireless sensor network", Industrial and Information Systems (IIS), 2010 2nd International Conference on. Year: 2010, Volume: 1, Pages: 541 – 544.

[13] Levente Buttyan; Tamas Holczer, "Private cluster head election in wireless sensor networks", 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, Year: 2009, Pages: 1048 – 1053.

[14] Jin-Su Kim; Seong-Yong Choi; Seung-Jin Han; Jun-Hyeog Choi; Jung-Hyun Lee;Kee-Wook Rim, "Alternative Cluster Head Selection Protocol for Energy Efficiency in Wireless Sensor Networks", Future Dependable Distributed Systems, 2009 Software Technologies for, Year: 2009, Pages: 159 – 163.

[15] Xia Haiyan; Xia Haiying, "A Modified Cluster Head Selection Algorithm Based on Random Waiting", Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on, Year: 2008, Pages: 129 – 132.

[16] Yuto Takeda; Yasuo Musashi; Kenichi Sugitani; Toshiyuki Moriyama" DNS ANY Request Cannon Activity in DNS Query Packet Traffic", 2013 6th International Conference on Intelligent Networks and Intelligent Systems (ICINIS), Year: 2013, Pages: 181 – 184.

[17] Yasuo Musashi; Florent Hequet; Dennis Arturo Ludeña Romaña; Shinichiro Kubota; Kenichi Sugitani" Detection of host search activity in PTR resource record based DNS querypacket traffic", Information and Automation (ICIA), 2010 IEEE International Conference on, Year: 2010, Pages: 1284 – 1288.

[18] Chih-Chin Liu; A. L. P. Chen, "Parallel query processing in distributed object database systems by querypackets", Research Issues in Data Engineering, 1995: Distributed Object Management, Proceedings. RIDE-DOM '95. Fifth International Workshop on, Year: 1995, Pages: 26 – 31.

[19] Shailendra Kumar Pathak; Raksha Upadhyay; Uma Rathore Bhatt, "An efficient query packets forward algorithm in ZRP protocol", Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on, Year: 2014, Pages: 592 – 595.

[20] Nobuhiro Shibata; Yasuo Musashi; Dennis Arturo Ludena Romana; Shinichiro Kubota; Kenichi Sugitani, "Trends in Host Search Attack in DNS Query Request Packet Traffic", Intelligent Networks and Intelligent Systems (ICINIS), 2012 Fifth International Conference on, Year: 2012, Pages: 126 – 129.

