CBNST: An enhanced Sybil Attack resilient mechanism for Restricting Sybil Attacks in Peer to peer E-commerce.

Urvashi Tripathi[1] Professor.S.R.Yadav[2]
Department of CSE, RGPV University
BHOPAL, (M.P) INDIA

[1]Tripathi.ushi@gmail.com
Techmillenniumk.yadav@gmail.com

Abstract- *Peer to peer e-commerce applications provide an enhanced and flexible mechanism to access content of the ecommerce vendor. But these applications are vulnerable to various security risks and cyber attacks. Sybil attack is an attack which is generally performed over such applications to get unauthorized acceded of the resources. Multiple fake identities are created by the malicious user to perform Sybil attack. A NST (Neighbour Similarity Trust) based scheme provides enhanced functionality to detect Sybil attack. But that technique uses a time consuming and complex procedure to detect such attacks. A new CBNST (Cluster Based Neighbour similarity trust) is proposed in this paper to provide an efficient mechanism to detect Sybil attack in peer to peer e-commerce. A performance comparison of the existing and proposed technique is govern in section IV which shows proposed technique provides enhanced functionality to detect Sybil attack in Peer to peer networks.*

Keywords: Peer to peer E-commerce, Sybil Attack, Neighbour Similarity Trust, and E-commerce.

I INTRODUCTION

E-commerce (electronic commerce or EC) is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the Internet. These business transactions occur either business-to-business, business-to-consumer, consumer-to-consumer or consumer-to-business. The terms e-commerce and e-business are often used interchangeably. The term e-tail is also sometimes used in reference to transactional process around online retail. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems.

Peer to peer network is a network where two or more computers are connected to share information without using any server. In peer to peer e-commerce, peer to peer applications are used to register content of the e-commerce into the peer to peer application. A manager of the ecommerce vendor can allow to search or add content to the shopping mall or to the ecommerce Network. That allows user to access that content as per their use. By the file sharing system peer to peer Networks provide an enhanced file retrieval or uploading functionality to the user.

(EDI), inventory management systems, and automated data collection systems.

Peer to peer network is a network where two or more computers are connected to share information without using any server. In peer to peer e-commerce, peer to peer applications are used to register content of the e-commerce into the peer to peer application. A manager of the ecommerce vendor can allow to search or add content to the shopping mall or to the ecommerce network. That allows user to access that content as per their use. By the file sharing system peer to peer networks provide an enhanced file retrieval or uploading functionality to the user.
But is such systems there are various types of attacks are performed by the malicious user or intruders to get unauthorized access to the content of the ecommerce network. Sybil attack is an active attack which used to perform to get unauthorized access of the e-commerce system. In Sybil attack a user creates multiple Ids to perform malicious activity in the network. Due to these attacks confidential information of the consumers and vendors are compromised. Thus a mechanism to detect such attacks is required. A neighbour similarity trust based technique is presented in [1] to provide a Sybil attack detection mechanism. But that technique is inefficient to provide better performance in continuously changing networks where multiple users are added in each second.

A CBNST (Cluster Based Neighbour Similarity Trust) technique is proposed in this paper to provide an efficient mechanism to detect Sybil attack.
A brief description over the various Sybil attack detection mechanism is given in section II Related Work. Section III provides a brief incite of the proposed technique, a performance comparison of the existing and proposed technique is presented in the section IV. V. Conclusion.

II RELATED WORK

Peer to peer network applications provides an enhanced and easy way to do transactions and online

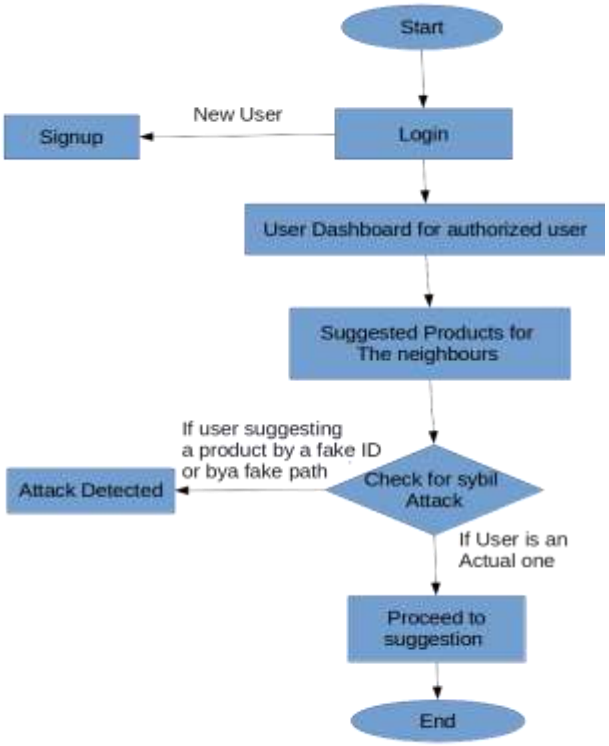
purchasing. But these applications are vulnerable to various types of attacks. Sybil attack is one of the attack which used to perform to get unauthorized access for user's data to perform any malicious activity. A neighbours similarity trust based technique is presented in [1], for restricting such attacks. In Sybil attack attacker having multiple fake Ids to perform their transactions. These attacks causes serious economic damage for the legitimate user. Trust evaluation [8] can efficiently improve the network performance by detecting malicious nodes in the network. This can be restricts various types of attacks to provide a secure access for the network. Gatekeeper [7] a Sybil attack resilient system which restricts various Sybil attacks. This system enhances the security of the whole network to provide an improve performance to communicate among the network. A Sybil attack detection mechanism for detecting Sybil attack in VANET is presented in [6]. This system uses no. of messages rather than no. of nodes to detect Sybil attacks in VANET. That improves the performance of the whole technique to provide a secure communication among the nodes in the networks.

But all these technique are not able to provide suitable and efficient solution to detect Sybil attack, a CBNST (Clustering Based Neighbour Similarity Trust) technique is proposed in this section to provide enhanced performance to detect Sybil attack.

III PROPOSED WORK

Peer to peer e-commerce applications are used to perform various online transactions and purchasing goods. Peer to peer applications improve their performance of the ecommerce by providing a flexible mechanism to access networks. Security is one of the biggest concern in ecommerce scenario, in existing technique a (Neighbour Similarity Trust) NST based mechanism is used to provide a secure access for the network. In this technique, neighbour similarity relation among the various user is used to detect Sybil nodes because each have knowledge about the neighbour node, by using that knowledge Sybil node can be detected. Sybil node is a node which performs malicious action in the network by creating fake identities.

But that technique having drawback, that it consume a lot of time to getting knowledge from the various nodes in the network. A new technique called CBNST (Cluster Based Neighbour Similarity Trust) is proposed. This technique uses a cluster of the homogeneous nodes to share information among the network. That enhances the time taken to build neighbour similarity trust in peer to peer system.



A flow diagram for the proposed technique is shown in Figure 1. First user need to login into the network by using login ID and password. Then a user dashboard is provided to the user by the use of that dashboard user can perform operations like selection of the products, online transactions etc. a check for the Sybil nodes is performed to detect Sybil attack in the network. That enhances the security of the network and restrict attacks in the peer to peer networks.

IV RESULT ANALYSIS

A comparative analysis of the results is presented in this section. Computation time is used to evaluate the performance of the techniques.

Statistical Comparison

A statistical comparison of the time taken by both the technique is given in Table 1. That comparative analysis shows proposed technique takes less amount of time as compare to the existing technique.

Table 1: Statistical comparison over Computation time.

Techniques	Computati
NST	31
CBNST	16

Graphical Comparison

A graphical comparison for the existing and proposed technique is shown in Figure 2. This shows proposed technique provides better performance as compare to the existing technique. CBNST takes ample span of time to build a neighbour similarity trust among the nodes in the network.

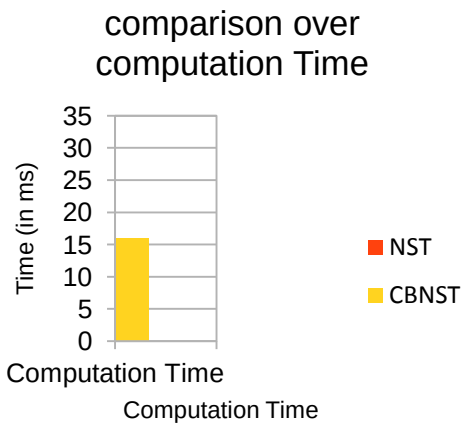


Figure 2: Graphical comparison over computation time.

V CONCLUSION

A technique called CBNST (Cluster Based Neighbour Similarity Trust) is presented in this paper. In existing technique a complex and time consuming mechanism is used to build a neighbour similarity trust among the nodes in the peer to peer networks. Proposed technique uses a clustering mechanism to provide enhanced functionality to build neighbour similarity trust among the nodes in the network. A comparative analysis of the computation time of existing and proposed technique is presented in Result Analysis section. That comparative analysis shows proposed technique provides better performances compare to the existing technique.

An enhanced clustering mechanism can be used to build an enhanced neighbour similarity trust among the nodes in the peer to peer networks.

REFERENCES

[1] Guojun Wang, Felix Musau, Song Guo, and Muhammad Bashir Abdullahi "Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce" IEEE Transactions On Parallel And Distributed Systems (TPDS), December 2013.

[2] J. Douceur, "The Sybil attack," in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., 2002, pp. 251–260.

[3] A. Mohaisen, N. Hopper, and Y. Kim, "Keep your friends close: Incorporating trust into social network-based Sybil defenses," in Proc. IEEE Int. Conf. Compute. Common. 2011, pp. 1–9.

[4] K. Walsh and E. G. Sirer, "Experience with an object reputation system for peer to peer files haring," in Proc. 3rd USENIX Conf. Netw. Syst. Des. Implementation, 2006, vol. 3, pp. 1–14.

[5] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil attacks in urban vehicular networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 1103–1114, Jun. 2012.

[6] B. Yu, C. Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," J. Parallel Distrib. Compute. vol. 73, no. 3, pp. 746–756, Jun. 2013.

[7] T. Nguyen, L. Jinyang, S. Lakshminarayanan, and S. M. Chow, "Optimal Sybil-resilient peer admission control," in Proc. IEEE Int. Conf. Compute. Common. 2011, pp. 3218–3226.

[8] K. Wang, M. Wu, and S. Shen, "Secure trust-based cooperative communications in wireless multi-hop networks," in Communications and Networking J. Peng, Ed., Rijeka, Croatia: Intec, Sep. 2010 Ch. 18, pp. 360–378,.

[9] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "Sybil Limit: A near optimal social network defense against Sybil attack," IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 3–17, Jun. 2010.

[10] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "Sybil Guard: Defending against Sybil attack via social networks," IEEE/ACM Trans. Netw., vol. 16, no. 3, pp. 576–589, Jun. 2008.

[11] A. Tversky, "Features of similarity," Psychological Rev., vol. 84, no. 2, pp. 327–352, 1977.

[12] F. Musau, G. Wang, and M. B. Abdullah, "Group formation with neighbor similarity trust in P2P e-commerce," in Proc. IEEE Joint Conf. Trust, Security Privacy Compute. Common. Nov. 2011, pp. 835–840.

[13] G. Danezis and P. Mittal, "Sybil Infer: Detecting Sybil attack peers using social networks," in Proc. Netw. Distrib. Syst. Security Symp. San Diego, CA, USA, Feb. 2009, pp. 1–15.

[14] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses," in Proc. 3rd Int. Symp. Inf. Process. Sensor Netw. Apr. 2004, pp. 1–10.

[15] W. Wei, X. Feng Yuan, C. T. Chiu, and L. Qun, "Sybil Defender: Defend against Sybil attacks in large social networks," in Proc. IEEE Int. Conf. Compute. Common. 2012, pp. 1951–1959.

[16] L. Xu, S. Chain an, H. Takizawa, and H. Kobayashi, "Resisting Sybil attack by social network and network clustering," in Proc. Int. Symp. Appl., 2010, pp. 15–21.

[17] N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-resilient online content voting," in Proc. 6th USENIX Symp. Netw. Syst. Des. Implementation, 2009, pp. 15–28.

[18] I. Stoica, R. Morris, D. Karger, F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in Proc. Conf. Appl., Technol., Archit., Protocols Compute. Common, 2001, pp. 149–160.

[19] B.S. Jyothi and D. Janakiram, "SyMon: A practical approach to defend large structured P2P systems against Sybil attack," Peer-to-Peer Netw. Appl., vol. 4, pp. 289–308, 2011.

[20] E. Damiani, D. C. Di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, "A reputation-based approach for choosing reliable resources in peer-to-peer networks," in Proc. 9th ACM Conf. Compute. Common. Security, 2002, pp. 207–216.

[21] L. V. Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. 22nd Int. Conf. Theory Appl. Cryptographic Tech, 2003, pp. 294–311.

[22] A. Ramachandran and N. Feaster, "Understanding the network level behaviour of spammers," in Proc. Conf. Appl., Technol., Archit., Protocols Compute. Common. 2006, pp. 291–302.

