International Journal of Advanced Trends in Computer Applications
www.ijatca.com

A COMPREHENSIVE SURVEY ON SYBIL ATTACKS MITIGATION TECHNIQUES

Sakshi Gupta[1], Taranjit Singh Aulakh[2]
[1]Deptt. Of CSE, Bgiet
Sangur, Punjab, India.
sakshibgiet@gmail.com
[2]Assistant Professor
Deptt. Of CSE, Bgiet
Sangrur, Punjab, India.
taranaulakh@gmail.com

ABSTRACT:- *Mobile ad-hoc network (MANET) is a self-governing network that comprises of several nodes and also these specific nodes utilizes wireless links to interconnect through each former network. The structureless characterstics of MANET makes it vulnerable to various attacks. Any decentralized distributed network is particularly vulnerable to the Sybil attack wherein a malicious node masquerades as several variety of nodes, entitled as Sybil nodes, instantaneously in an endeavor to disrupt the proper functioning of the system. Such type of attacks may become reason for the impairment on an honestly large scale especially since they are difficult to detect and there has been no universally accepted scheme to counter them as yet. Defending against Sybil attacks is reasonably stimulating. In this paper, we discuss the different previous existing techniques to detect Sybil attacks.*

Keywords: *Security, Sybil attack, MANETs, Ad-hoc network.*

I. INTRODUCTION TO MANET

MANET stands for Mobile Ad-hoc Networks. It is a self-constructing structureless system. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these systems. Consequently, we talk about a wireless ad-hoc network with mobile nodes as a Mobile Ad Hoc Network. In MANET, all the devices are connected by wireless associations [8]. Each and every single device present in a MANET is quite open to travel independently in all the ways. It could probably modify the aforementioned links to several other devices frequently. Nodes are randomly connected with each other using random topology. They can also perform by way of both type routers as well as hosts. The primary challenge in building a MANET is equipping each device to continuously maintain the information which is necessary to properly route the traffic [9]. More frequent connection tearing and re-associations place an energy constraint on the portable nodes. As per MANETs are exemplified through restricted bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes. Mobile adhoc system is the kind of system where communication happens in remote medium utilizing an access point. Then again different systems like WSN are the systems in which communication happens through physical medium. It is a self-designing system where number of switches are associated through remote connections. All hubs are free of one another. All the hubs that are associated are allowed to move and are sorted out arbitrarily [10].

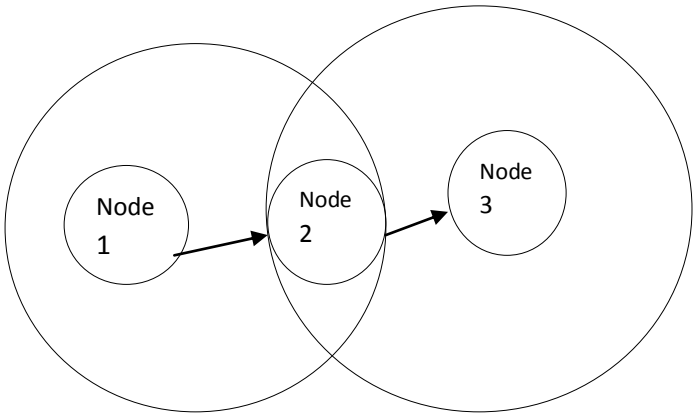

Figure MANET Block Diagram

Restricted to the framework remote systems where every client straightforwardly corresponds with an access point or base station, a mobile specially appointed arrangement, otherwise MANET is a category of wireless ad-hoc network. It is a self-arranging system of mobile routers joined by remote connections with no access point. Each mobile device in a system is self-governing. The mobile devices are allowed to move freely and compose themselves subjectively [11].

As it were, adhoc network don't depend on any fixed infrastructure (i.e. the mobile adhoc specially MANET. The Communication in MANET is occur by utilizing multi-jump ways. Hubs in the MANET offer the remote medium and the topology of the system changes sporadically and alertly. In MANET, breaking of communication connection is exceptionally less, as hubs are allowed to move to anyplace. The thickness of hubs and the quantity of hubs are relies on upon the applications in which we are utilizing MANET. MANET have offered ascent to numerous applications. With numerous applications there are still some outline issues and difficulties to overcome.

II. WHAT IS SYBIL ATTACK?

A Sybil attack is one in which a malicious node on a network illegitimately claims to be several different nodes simultaneously. It is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. Many distributed applications and everyday services assume each participating entity controls exactly one identity [12]. When this assumption is un-verifiable the service is subject to attack. In a large-scale peer-to-peer system, a direct connection between each pair of nodes is impossible, therefore, the nodes which are participating usually create networks, and a message is transmitted from one node to another via the relay operations of multiple intermediary nodes.

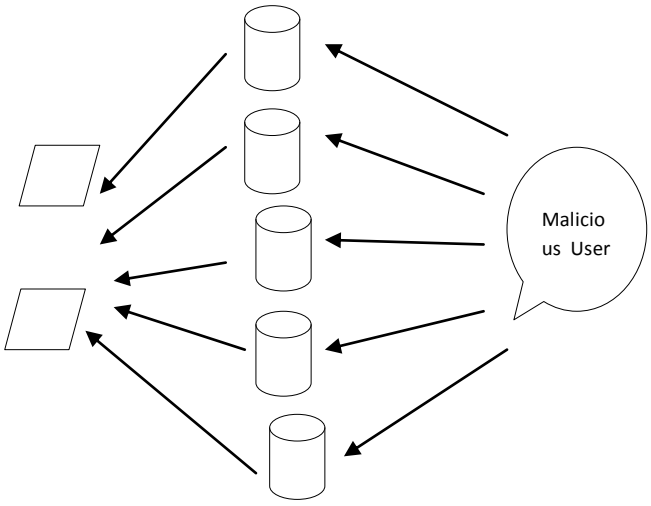

Figure 2 Sybil Attack

It belongs to direct combined attack [13]. It devours moderate battery power as matched to other attacks such as black hole, worm hole and so on. In this paper, we talked about the Sybil attack, a dangerous attack in distributed peer-to-peer networks. Almost distributed peer-to-peer systems are based on a common assumption that each participating entity controls exactly one and only identity. On the other hand, on every occasion the supposition can probably not be fulfilled, the system lead to Sybil attacks. It can maliciously introduce a considerable number of false opinions into the system, and convert it, by making decisions benefiting system itself.

III. PREVIOUS TECHNIQUES

S.no	AUTHOR NAME	TECHNIQUES USED	EXPLANATION
1.	J. R. Douceur et.al	Trusted Certification [1]	A Sybil attack depends on the way that a system of PCs can't guarantee that every processing component is an unmistakable, physical PC. Various powers have tried to set

			up the identities of PCs on a system (or hubs) by utilizing software, for example, VeriSign, utilizing IP locations to be familiar with user names, nodes, hubs, passwords and so on.
2.	James Newsome et.al	Resource Testing [2]	The Sybil Attack in Sensor Networks" talked about the Sybil attack in system C. Piro, C. Shields, and B. N. Levine additionally clarified the Sybil attack is an attack in which a single entity can control a considerable division of the system by showing different identities. DSR routing is a basic algorithm .The DSR Route Request control packet is changed by including another field that will be utilized to focus the acknowledgemen t level of accessible bandwidth. Keeping in mind the end goal to test the proposed model, a recreation model is actualized utilizing the Network Simulator (NS-2.28).
3.	B.N. Levine et.al	Recurring Fees [3]	They measured several security procedures contrary to Sybil attacks and also divided in several methods. In this method, identities are occasionally re-validated in the system. Each single one of identity that is participating is occasionally otherwise one-time have to pay a fee.
4.	J.R. Douceur et.al	Privilege Attenuation [1]	They formalize Denning's Principle of Privilege Attenuation (POPA) as a run-time assets, and also make evident that it is quite obligatory as well as sufficient condition for preventing the above form of Sybil attacks. A stationary policy analysis is at that time formulated for verifying that an FSNS is POPA compliant (and consequently Sybil free). The static examination is confirmed to be mutually sound and complete.

5.	Margolin et.al	Economic Incentives [4]	They propose an economic approach to Sybil attack detection. In their Informant protocol, a detective offers a reward for Sybil's to disclose themselves. The detective accepts from one identity a security deposit and the name of target peer; the deposit and a reward are given to the target.
6.	Tangpong, A. et.al	Location/ Position Verification [5]	In this research, they propose a robust Sybil attack detection framework for MANETs based on cooperative monitoring of network activities. They do not require designated and honest monitors to perform the Sybil attack detection. Each mobile node in the network observes packets passing through it and periodically exchanges its observations in order to determine the presence of an attack. Malicious nodes fabricating false observations will be detected and rendered ineffective.
7.	Murat Demirbas et.al	Received Signal Strength Indicator (RSSI) – based scheme [6]	In contrast to existing solutions which are based on sharing encryption keys, we present a robust and lightweight solution for Sybil attack problem based on received signal strength indicator (RSSI) readings of messages. They show through experiments that even though RSSI is time-varying and unreliable in general and radio transmission is non-isotropic, using ratio of RSSIs from multiple receivers it is feasible to overcome these problems
8.	Wenliang Du et. al	Random Key Pre-distribution [7]	In this paper, they propose a new key pre-distribution scheme, which substantially improves the resilience of the network compared to the existing schemes. Their scheme exhibits a nice threshold property: when the number of compromised nodes is less than the threshold, the probability that any nodes other than these compromised nodes is affected is close to zero.

IV. CONCLUSION

In this paper, we talked about Sybil attack. Sybil attack is one in which a malicious node on a network illegitimately claims to be several different nodes simultaneously. It is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. In this, we presented various techniques utilized in detection of Sybil attack. From this paper, we got to know about various advantages as well as disadvantages of various existing techniques. For prevention from Sybil attack on the Adhoc network we can utilize any of existing technique in hybrid nature.

REFERENCES

1. J. R. Douceur, The Sybil attack, In Proceedings for the First International Workshop on Peer-to-Peer Systems (IPTPS'02), ser. LNCS, vol. 2429. Cambridge, MA, USA: Springer, Mar. 2002, pp. 251–260.
2. J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil attack in sensor networks: analysis & defences, In Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268, 2004.
3. B. N. Levine, C. Shields, and N. B. Margolin, A survey of solutions to the Sybil attack, University of Massachusetts Amherst, Amherst, MA, 2006.
4. Margolin, N. Boris, and Levine, Brian Neil, Informant: Detecting Sybils using incentives, In Proceedings of Financial Cryptography (FC) (February 2007) pp. 192—207.
5. Tangpong, A. , Kesidis, G. , Hung-yuan Hsu, Hurson, A., Robust Sybil Detection for MANETs, In Proceedings of 18th International Conference on Computer Communications and Networks, 2009. ICCCN 2009, pp. 1 – 6.
6. Murat Demirbas, Youngwhan Song, An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks, In Proceedings of WoWMoM 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006. 5 pp. – 570.
7. W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A pairwise key pre-distribution scheme for wireless sensor networks. In ACM CCS 2003, pages 42–51, Oct. 2003.
8. Diogo Monica, Thwarting The Sybil Attack in Wireless Ad Hoc Networks, Master's Thesis at the Universidade Tecninca de Lisboa, July 2009.
9. Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia, Nirali Mody, Sugata Sanyal, Ajith Abraham, A Distributed Security Scheme for Ad Hoc Networks, ACM Crossroads, Special Issue on Computer Security. Volume 11, No. 1, September, 2004.
10. P.W. L. Fong. Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems. In IEEE Symposium on Security & Privacy, 2011 pp. 263-278.
11. CAO, Q., SIRIVIANOS, M., YANG, X., AND PREGUEIRO, T., Aiding the detection of fake accounts in large scale social online services, In Proc. of NSDI (2012).
12. C. E. Gates, Access control requirements for Web 2.0 security and privacy, in IEEE Web 2.0 privacy and security workshop (W2SP'07), Oakland, California, USA, May 2007.
13. B. Carminati and E. Ferrari, Enforcing relationships privacy through collaborative access control in web-based social networks, In Proceedings of the 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing CollaborateCom'09), Washington DC, USA, Nov. 2009 pp. 1-9, 2009sss.