International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 4, Jul-Aug-2025, ISSN (Online): 2395-566X

Complete Analysis and Classifications of Sybil Attack in Mobile Adhoc Network

Assistant Professor Dr. Gurpreet Singh
Dept. of Computer Science Department at DIPS College (Co-Educational), Dhilwan, kapurthala, Punjab.

Abstract- — In a MANET number of devices or mobiles are connected to each other with wireless medium. This network is a temporary network. In the MANET, there is not any centralized device which control all netwrok. MANET using dynamic topology. The Sybil attack is characterized as a malicious node misguidedly taking on various MANET . A Malicious device acts as though it's anything but a bigger number of nodes, for instance by mimicking different devices or basically by asserting bogus MANET. In this,a terrible device present more than one character in MANET. So it is not much safe Network. The attacker are easily attacks on the MANET. Consequently, Security is an essential worry to give ensured correspondence between nodes in impromptu organizations and shots at having the weaknesses are additionally more. In this paper we complete analysis and classification of the various Sybil attack techniques and decline the network performance and throughput.

Keywords— No fixed infrastructure, Dynamic topology, Distributed control, Limited bandwidth and energy, Cooperative routing (e.g., AODV, DSR)

I. INTRODUCTION

MANET (Mobile Ad hoc Networks) is the wireless networks. It has not any centralized and fixed network. The Sybil attack is characterized as a malicious node misguidedly taking on various IDS. A Malicious device acts as though it's anything but a bigger number of nodes, for instance by mimicking different devices or basically by asserting bogus ids. The Sybil attack is a network layer attack. In this,a terrible device resent more than one character in MANET. The false device suggests different personalities to different devices in the MANET and accordingly happens to be in more than each spot in turn. Thusly, it upsets the geological routing protocol It can confuse the routing algorithms by constructing many routes from only one node. This is on the grounds that device can consistently move causing the successive breakage of the connection. So Sybil attack is more dangers of Mobile Adhoc Network..

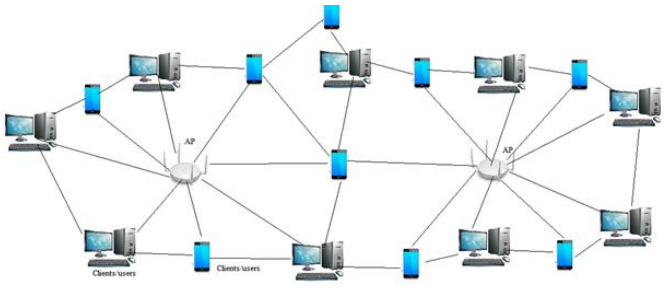
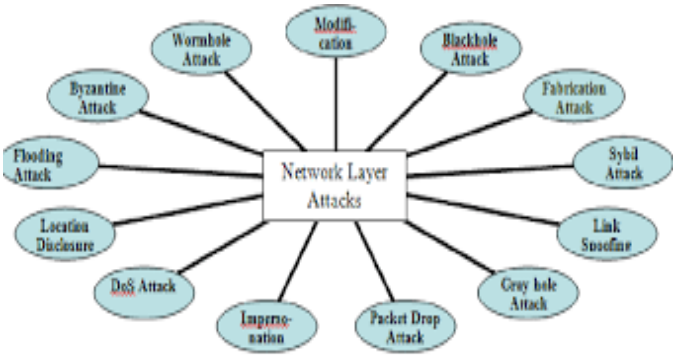


Figure 1: Manet

There are various attacks who disturb the MANET because in MANET using dynamic topologies, there is no central computer system to handle, no perfect algorithm to mange the network. The various attacks are disturb the different layers. The following attacks in MANET.



Manet attacks

MANET regularly suffers from security attacks because of its characteristics like exposed medium, dynamic topology, absence of the central managing system, non-cooperative algorithms, and absence of strong protection mechanism. Numerous attacks on the different MANET layers are presented in figure[2]

II. SYBIL ATTACKE IN LAYES IN MANET

The following layer wise attacks that are responsible for the low performance in MANET. These attacks are worked in the different layers like

Network Layer

In the network layer one node connect with the other nodes in the MANET. The various nodes connectivity is called the multi hop link in the MANET. The following attacks are disturb the network layer. [11] .The Sybil attack is characterized as a malicious node misguidedly taking on various ids . A Malicious device acts as though it's anything but a bigger number of nodes , for instance by mimicking different devices or basically by asserting bogus ids. The Sybil attack is a network layer attack. In this, a terrible device presents more than one character in MANET. The false device suggests different personalities to different devices in the MANET and accordingly happens to be in more than each spot in turn. Thusly, it upsets the geological routing protocol It can confuse the routing algorithms by constructing many routes from only one node The Sybil attack is characterized as a malicious node misguidedly taking on different identities. A malicious node acts as though it were a bigger number of nodes,

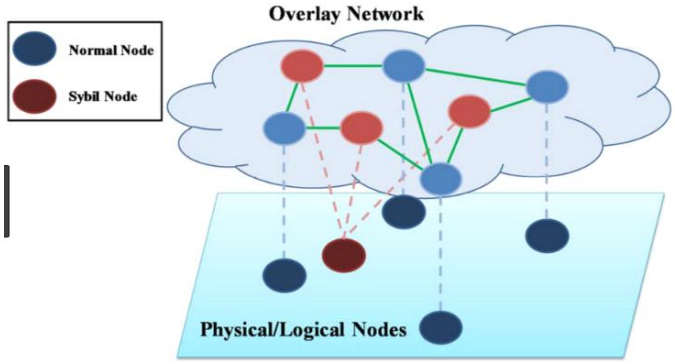


Figure3.3- Sybil Attack

Complete analysis and classification of Sybil Attack

- The research design of MANET and will help to Sybil Attack protected.
- The research will help to get more secure Mobile Ad hoc Network systems in the future.
- The technique to be developed can be employed for new types MANET.
- Rupesh Gunturu (2015):- Sybil attackin informal organizations, which can bargain the entire appropriated network. In the Sybil attack, the noxious client guarantees various personalities to bargain the entire organization. Sybil attacks can be utilized to change the general positioning in casting a ballot applications, revile an assessment, access assets or to break the trust system behind a P2P organization. In this paper, distinctive protection components used to alleviate Sybil attacks are likewise audited.

Haifeng Yu, Michael Kaminsky, Phillip B. Gibbo (2008):- In a Sybil attacks, a malevolent client gets numerous phony characters and professes to be different, unmistakable hubs in the framework. By controlling a huge part of the hubs in the framework, the malevolent client can "out vote" the legit clients in community oriented undertakings, for example, Byzantine disappointment protections. This paper presents Sybil Guard, a novel convention for restricting the corruptive impacts of Sybil attacks. Our convention depends on the "informal organization" among client characters, where an edge betit was an two personalities demonstrates a human-set up trust relationship. Decentralized, conveyed frameworks are known to be especially helpless against Sybil attacks.Malignant clients can make numerous characters hoot was ever scarcely any trust connections. Hence, there is a lopsidedly little "cut" in the chart bet it Sybil hubs and the legit hubs. Sybil Guard abuses this property to bind the quantity of characters a malevolent client can make. It was show the adequacy of Sybil Guard both scientifically and tentatively.

John.R. Douceur (2002):- Large-scale shared frameworks face security dangers from flatwads or unfriendly far off processing components. To oppose these dangers, numerous such frameworks utilize excess. Be that as it may, if a solitary flatwads element can introduce various personalities, it can handle a generous part of the framework, consequently sabotaging this excess. One way to deal with forestalling these "Sybil attacks" is to have a believed organization affirm personalities. This paper shows that, without a consistently concentrated point was, Sybil attacks are consistently conceivable besides under outrageous and ridiculous presumptions of asset equality and coordination among substances.

Rupesh Gunturu (2015):- Sybil attackin informal organizations, which can bargain the entire appropriated network. In the Sybil attacks, the noxious client guarantees numerous personalities to bargain the entire organization. Sybil attacks can be utilized to change the general positioning in casting a ballot applications, castigate an assessment, access assets or to break the trust instrument behind a P2P organization. In this paper, distinctive guard systems used to moderate Sybil attacks are likewise assessed.

Newsome, E. Shi, D. Tune, A. Perring (2008):- A case that Sybil hub misguidedly reports messages to the expert hub with different non-existent personalities (ID) will cause unsafe consequences for dynamic or asset allotment in these applications. In this paper, it was present a proficient and light itweightan sit was for Sybil attackdiscovery dependent on the time distinction of appearance (TDOA) betit waken the source hub and signal hubs. As Wireless Sensor Network (WSN) are conveyed in fire observing, object following applications, security arises as a focal prerequisite. This arrangement can identify the presence of Sybil attacks, and find the Sybil hubs. It was show productivity of the arrangement through tests. The trials show that this arrangement can identify all Sybil attack cases.

Mi It wasn and Hui Li (2008):- A case that Sybil hub misguidedly reports messages to the expert hub with numerous non-existent personalities (ID) will cause unsafe impacts on dynamic or asset portion in these applications. In this paper, it was present a productive and lighted weight inset was for Sybil attack recognition dependent on the time distinction of appearance (TDOA) befit waste source hub and guide hubs. As Wireless Sensor Network(WSN) are conveyed in fire checking, object following applications, security arises as a focal prerequisite. This arrangement can distinguish the presence of Sybil attacks, and find the Sybil hubs. It was exhibit productivity of the arrangement through tests. The trials show that this arrangement can distinguish all Sybil attackcases without missing.

Personalities made to outlandishly expand the force or assets of a solitary pernicious client. To assemble estimation based Sybil identifiers and convey them on Renner to recognize in excess of 100,000 Sybil accounts. Utilizing our full dataset of 650,000 Sybil s, it was inspect a few parts of Sybil conduct. In the first place, it was study their connection creation conduct and track down that in opposition to earlier guess, Sybil in OSNs don't frame very close networks. Then, it was look at the fine-grained practices of Sybil on Renner utilizing click stream information. Third, it was exploring in the background plot betit was enormous gatherings of Sybil . Our outcomes uncover that Sybil with no unequivocal social binds actually act in show to dispatch attacks. At last, it was explore upgraded methods to recognize covert Sybil . In synopsis, our investigation progresses the comprehension of Sybil conduct on OSNs and shows that Sybil can adequately try not to exist local area based Sybil locators. Sybil identification that depends on novel sorts of Sybil highlights.

Liang Wang and Jussi Kangasharju (2012):- DHTs, because of their completely appropriated nature, are known to be helpless against particular sorts of attacks and various types of protections have been proposed against these attacks. In this paper, it was think about two sorts of attacks on a DHT, one definitely known attack and one new sort of an assault, and show how they can be focused against Mainline DHT. Distributed hash tables (DHT) are a key structure block for present day P2P content-dispersion framework, for instance in carrying out the conveyed tracker of Bit Torrent Mainline DHT. It was supplement them by a broad estimation study utilizing honey pots which shows that the two attacks have been continuing for quite a while in the organization are as yet occurring. It was present numbers showing that the quantity of Sybil in the Mainline DHT network.

M. Castells (2010):- The worldwide economy is presently portrayed by the practically prompt stream and trade of data, capital and social correspondence. These streams request and condition both utilization and creation. The actual organizations reflect and make unmistakable societies. Both they and the traffic they convey are to a great extent outside public guideline. Our reliance on the new methods of instructive stream gives huge capacity to those in a situation to control them to control us. The principle political field is currently the media, and the media are not politically responsible. Manuel Cast ells portrays the speeding up speed of development and application. He analyses the cycles of globalization that have minimized and now take steps to make excess entire nations and people groups prohibited from enlightening organizations. Exploration in the USA, Asia, Latin America, and Europe, it means to form a precise hypothesis of the data society which assesses the central impacts of data innovation

S. Gangan (2015):- Continuously correspondence, the attack an as a rule be found by the utilization of timing data. The most it was-known attacks happen because of Address Resolution Protocol (ARP) reserve harming, Man-in-the-middle (MIM) attacks in correspondence organizations and strategies for insurance against them. DNS ridiculing, meeting capturing, and SSL commandeering.

S. Kak (1981) :- The encryption activity considered is comparable to exponentiation, which frames the premise of a few public-key plans. A utilization of D groupings to creating occasions with determined probabilities is likewise introduced. Copyright 1985 by. The Institute of Electrical and Electronics Engineers, Inc. D arrangements that have applications to encryption and blunder coding. It additionally considers the issue of joint encryption and blunder adjustment coding and proposes a sit was utilizing D arrangements.

J.Yan (2001):- To decide how to assist clients with picking passwords, the creators played out a controlled preliminary of the impacts of offering clients various types of guidance. Pick passwords that are both difficult to theory and simple to recall. A portion of their outcomes challenge the set up astuteness.

Shih Hao Chang (2005):- Partaking detecting is a progressive worldview in which volunteers gather and offer data from their neighborhood climate utilizing cell phones. By and by, quite possibly the main issues and second thought about participatory detecting applications is security. Not the same as other participatory detecting application challenges who think about client protection and information reliability, it was consider network dependability issue to be specific Sybil attacks in participatory detecting. Sybil attacks is an especially destructive attack against participatory detecting application, where Sybil attacks center around making various online client personalities called Sybil characters and attempt to accomplish malevolent outcomes through these characters. In this paper, it was proposed a Hybrid Trust Management (HTM) system for distinguishing and dissect Sybil attacks in participatory detecting organization. Our HTM was proposed for performing Sybil attack trademark check and dependa

In this paper the author describe that the Sybil attacker makes novel identity (name) , the signal power of that identity (name) will be sufficient to be distinguished from the recently connected neighbor. This technique describe that the fabricated identities of the Sybil attacker nodes separate themselves by their communication power which is a novel type of attack. Another aspect of Sybil node described in this paper is the signal strength based behavior of the Sybil nodes.

Here it is shown tentatively that new genuine nodes become neighbors when they enter inside the radio range of different nodes; henceforth their first RSS at the recipient hub is adequately low. Interestingly, a Sybil attacker, which is now a neighbor, will make its new identity show up suddenly in the neighborhood. In all these literature of Sybil attack it is evident that Sybil attacks create new dimension in different field and do not follow the basic taxonomy in most of the cases. The goal of the current study is to demonstrate such behavioral aspects of Sybil nodes (through simulation) which are different from the fundamental types of Sybil attack .

Chang and Jie Wu (2013):- The shared frameworks are helpless against Sybil attacks. The Sybil attacks an attack wherein a standing framework is sabotaged by a significant number of manufacturing personalities in shared organizations. By misguidedly imbuing bogus or one-sided data by means of the pseudonymous characters, an enemy can delude a framework into settling on choices profiting herself. For instance, in a disseminated casting a ballot framework, a foe can undoubtedly change the general fame of a choice by giving a lot of bogus applause, or abusing the choice through these phony personalities. In this paper, it was sum up the current Sybil safeguard procedures, and further give some new exploration regions. In contrast to customary studies about Sybil safeguard, it was initially sort the Sybil protection techniques, chiefly as per their planned time, and afterward order the strategies by their methodologies. It was accept that by understanding the advancement of the arrangements, peruses could basic

David Mohaisen and Yongdae Kim (2011):- Scholarly joint effort diagram are confided in an unexpected way in comparison to social companions. Besides, some friendly companions are more trusted than others. Nonetheless, past plans for informal community based Sybil protections have not considered the natural trust properties of the diagrams they use. In this paper it was acquaint a few plans with tune the presentation of Sybil safeguards by representing differential trust in friendly diagrams and demonstrating these trust esteems by biasing arbitrary strolls performed on these charts. Shockingly, it was track down that the expense work, the necessary length of arbitrary strolls to acknowledge all genuine hubs with over point was likelihood, is a lot more prominent in charts with high trust esteems, for example, co-creator diagrams, than in charts with low trust esteems like online interpersonal organizations. Social organization based Sybil safeguards abuse the algorithmic properties of social diagrams to ga

Nguyen Tran, Bonan Min, Jinyang Li, and Lakshminarayanan Subramanian (2009):- Nonetheless, any substance casting a ballot framework is point was less to the Sybil attackwhere enemies can out-vote genuine clients by making numerous Sybil characters. In this paper, it was present Sum-up, a Sybil versatile vote accumulation framework that use the trust network among clients to guard against Sybil attacks. Summarize utilizes the method of versatile vote stream collection to restrict the quantity of sham votes cast by foes to close to the quantity of attack edges in the trust organization (with high likelihood). Obtaining client assessment (utilizing votes) is crucial for positioning client produced online substance. Utilizing client criticism on votes, Sum Up further limits the democratic force of foes who persistently act up to beneath the quantity of their attack edges. Utilizing point by point assessment of a few existing interpersonal organizations (YouTube, Flicker), it was show Sum Up's capacity to deal

Bimal Viswanath Krishna P. Gummadi and Alan Mislove (2010):- Existing Sybil safeguard plans work by recognizing

neighborhood networks (i.e., bunches of hubs more closely knit than the remainder of the diagram) around a confided in hub. Our finding has significant ramifications for both existing and future plans of Sybil protection plans. To start with, it was show that there is a chance to use the considerable measure of earlier work on broad local area recognition calculations to safeguard against Sybil. Second, our examination uncovers the key furthest reaches of current informal organization based Sybil guards: It was exhibit that networks with obvious local area structure are innately more defenseless against Sybil attacks, and that, in such organizations, Sybil can cautiously focus on their connections all together make their attacks more viable. Utilizing informal organizations to alleviate numerous character, or Sybil, attacks. Various plans have been proposed, hoot was ever they contrast extraordinarily in the calculations they use and in the organizations whereupon they are assessed. Thus, the examination local area comes up short on a reasonable comprehension of how these plans analyze against one another, how it was they would chip away at genuine interpersonal organizations with various primary properties, or whether there exist other (possibly better) methods of Sybil guard.

III. CONCLUSION

The MANET is a open and portability network so it, the MANETs are significantly more liable to all sort of safety hazards, like data leakage, interruption, or even DoS attacks. There are various attacks attack in MANET. The Sybil attack is characterized as a malicious node misguidedly taking on MANET . A Malicious device acts as though it's anything but a bigger number of nodes, for instance by mimicking different devices or basically by asserting bogus MANET. In this, a terrible device presents more than one character in MANET. The false device suggests different personalities to different devices in the MANET and accordingly happens to be in more than each spot in turn. It can confuse the routing algorithms by constructing many routes from only one node. Sybil attack is very danger in MANET. In this paper we have examined Sybil attack of in MANETs. A detail study of countermeasures for these attacks is required in order to minimize or eliminate their impact. More efficient and robust techniques for the countermeasures of various types of attacks should be proposed in order to make MANETs more secure and their extension in other fields.

REFERENCES

1. Jatinder Singh, LakhwinderKaur, and Savita Gupta, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks", “International Arab Journal of Information Technology”, Volume 9, No. 3, May 2012 and ISSN: 1683-3198.
2. Gagandeep, Aashima, Pawan Kumar, “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review”, International Journal of Engineering and Advanced Technology (IJEAT), , Volume-1, Issue-5, June 2012 and ISSN: 2249 – 8958.
3. KaminiMaheshwar, Divakar Singh, "Black Hole Effect Analysis and Prevention through IDS in MANET Environment", "European Journal of Applied Engineering and Scientific Research", 2012, ISSN: 2278 – 0041.
4. Satria Mandala, Md. AsriNgadi, A.Hanan Abdullah, “A Survey on MANET Intrusion Detection”, “International Journal of Computer Science and Security”, Volume 2, Issue 1, 2013 and ISSN:1985-1553.
5. Antony Devassy, K. Jayanthi," Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting", "International Journal of Modern Engineering Research (IJMER)", Volume 2, Issue.3, May-June 2012, ISSN: 2249-6645.
6. P. K. Singh and G. Sharma (2012), "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", "IEEE International Conference on Trust, Security and Privacy in Computing and Communications".
7. SachinLalar, “International Journal of Multidisciplinary and Current Research”, “Security in MANET: Vulnerabilities, Attacks & Solutions”, 2014, Vol.2, ISSN: 2321-3124.
8. PriyankaGoyal, SahilBatra, Ajit Singh, ”A Literature Review of Security Attack in Mobile Ad-hocNetworks”, “International Journal of Computer Applications”, Volume 9– No.12, November 2010, ISSN:0975-8887.
9. Shekharsaini, Rajesh Kumar, “Comparison of layerwise attacks in MANETs”, “ACEEE”, proc. of “Int. Conf. on Emerging Trends in Engineering and Technology”
10. Saritha Reddy Venna, Ramesh BabuInampudi, “A Survey on Security Attacks in Mobile Ad HocNetworks”,”International Journal of Computer Science and Information Technologies (IJCSIT)”, Vol. 7, 2016, ISSN: 0975-9646.
11. Y. Hu, A. Perrig, D. Johnson (March 2003),Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003).
12. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A.Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensornetworks, October 2007.

13. Athira V Panicker, Jisha G, ”Network Layer Attacks and Protection in MANET : A Survey”, “International Journal of Computer Science and Information Technologies”, Vol. 5, 2014, ISSN : 3437-3443.
14. CH.V. Raghavendran, G. Naga Satish, P. Suresh Varma, “Security Challenges and Attacks inMobile Ad Hoc Networks” “I.J. Information Engineering and Electronic Business”, vol. 3, 2013.
15. Abhay Kumar Rai, Rajiv RanjanTewari&Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET- Internet Communication , International Journal of Computer Science and Security (IJCSS) Volume (4): Issue
16. G S Mamatha, Dr s c Sharma “Network Layer Attacks And Defense Mechanisms In MANETS-A Survery” International Journal of Computer Applications (0975 – 8887)Volume 9– No.9, November 2010.
17. SandipNemade, Manish Kumar Gurjar, ZareenaJamaluddin, Nishanth ,"Early Detection of Syn Flooding Attack by Adaptive Thresholding (EDSAT): A Novel method for detecting Syn Flooding based DOS Attack in Mobile Ad Hoc Network", "International Journal of Advanced Research in Engineering and Technology (IJARET)", Volume 5, Issue 2, February (2014), ISSN 0976 – 6480(Print), ISSN 0976 – 6499(Online).
18. Neetu Singh Chouhan, ShwetaYadav," Flooding Attacks Prevention in MANET"," International Journal of Computer Technology and Electronics Engineering (IJCTEE)", Volume 1, Issue 3, December 2011, ISSN 2249-6343.
19. Ming-Yang Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", "Elsevier Journal of Computer Communications", Volume 34, Issue 1, January 2011.

.