ISSN 2278-3091

Volume 5, No.4, July – August 2016

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse07542016.pdf

A Brief Review on Sybil attack and detection technique and new proposed method in MANET

Sonali Gupta
Department Computer Science
ITM Universe, Gwalior
India
Sonalimandil497@gmail.com

Arun Agrawal
Asst. Professor, Department Computer Science
ITM Universe, Gwalior
India
development_arun@rediffmail.com

***Abstract*— Wireless Network is comprises of inexpensive and simple processing procedure, called sensor node. A Wireless Network is an accumulation of dedicated transducers with a transmission framework for examining and reporting circumstances at assorted areas. Sybil attack is such type of attack where in a standing structure is subverted by an impressive amount of forged identities in disseminated networks. In this paper, we learn about Sybil attack in MANET and also no. of papers regarding Sybil attack detection.**

Keywords*—*Wireless Network; Sybil attack; MANET, etc.

1. INTRODUCTION

Distributed systems are at risk to Sybil attacks [1], [2], wherein an enemy makes numerous bogus characters, alluded to as Sybil identities, and compromises the strolling of the strategy or dirties the technique with false skill. The Sybil identities can "smother" the earnest characters in a kind of undertakings, together with online substance situating, DHT routing, report sharing. Notoriety systems, and Byzantine frustration resistances. Wireless network is turning out to be progressively prevalent because of the assortment of utilizations. It is broadly used as a part of the field of education, military, medical treatment, traffic, and has enormous potential and business esteem. In wireless network, there are a huge number of nodes sent in extreme environment to gather data, for instance, light force, weight and temperature, or distinguish peril and track of adversary. Sensor node is regularly minimal effort, battery controlled; profoundly resource obliged and as a rule collaborates with each other to finish an assignment. So it is more defenseless even with security threats than wired network [2].

The day and age Sybil attack is acquainted in [3] show an attack where the attacker (Sybil node) tries to produce different recognizing verification in a particular neighborhood. Sybil attack is uniquely convenient to take an interest in wireless network where the verbal trade medium is telecast, and identical frequency is shared amongst all nodes. By means of TV messages with more than one unmistakable bits of evidence, a Sybil node can fix the vote on group built up decisions and furthermore disrupt network middleware benefits seriously.

2.LITERATURE SURVEY

Geetha[2015] et al. In this paper proposed a TTM model to distinguish the Sybil attack in. In this technique, every last

Node in the sensor s network will keep up a perception table for putting away node id and area which is helpful to recognize the Sybil attack. The approach is simulated in a sensor network and the result shows a very good detection rate comparing with other existing algorithms [4].

Sangeeta Bhatti[2015] et al. In this paper proposed a character confirmation and asset based algorithmic methodology for the detection and elimination of Sybil nodes. In proposed strategy secure character of nodes are dole out to all nodes to recognize the Sybil node. The Sybil node is identified with inclusion of base server by check the character and resources node through the dependability of Secure Id of all nodes [5].

Rajamani Vayanaperumal[2015] et al. In this paper, an overview is done on Sybil attack and proposed a Compare and Match (CAM) Approach to confirm the Position to anticipate Sybil attacks. The leave these sorts of attacks in unit-giving a role as well as multicasting we particularly given a complete guaranteed Security for wireless network. The functional analysis of this work is done utilizing network simulator by measuring throughput, end to end delay and packet delivery ratio under different conditions [6].

T.G. Dhanalakshmi [2014] et al In this paper, a study is done on Sybil attack and projected a common RAI – Relate and Identify Tactic and LVT Location Verification procedure to keep up a key separation from these attacks. Basically a Sybil attack implies a framework which imagines its singularity like further nodes. In this situation a framework can believe the reclose framework and it begin sharing its data. Because of this movement a node's wellbeing is influenced and data is lost [7].

Imran Makhdoom [2014] In this paper we complete a detailed review and analysis of various defenses proposed against

Sybil Attack. We recognize their qualities and shortcomings and likewise propose a novel One Way Code Attestation Protocol (OWCAP) for wireless sensors networks, which is an economical and a secure code attestation scheme that protects not only against Sybil Attack but also against majority of the insider attacks [8].

A. Babu Karuppiah [2014] et al In this paper, an energy proficient incorporated IDS is proposed to identify network layer Sybil attack. Our arrangement spots out decisively and cleanses out the Sybil node which may insincerely bear on as a honest to goodness node. The exploratory results display that the crucial variable in wireless network, energy is proportioned more capably by the proposed arrangement than the current option procedures [9].

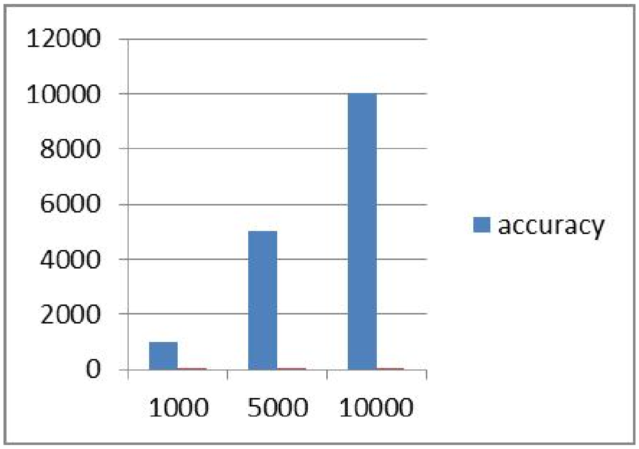
S. Sakthi Vinayagam[2014] et al this paper is focusing on location and avoidance Sybil nodes in wireless networks. Sybil is a fake-ID based malicious activity destroying the networks behavior. Here IPTTA – [IP Trace back and Token Assigner] strategy is proposed to identify and forestall Sybil attack by assigning and verifying IP address with assigned unique Token for each node in the route. IPTTA verify the node IP, Token with time stamp and fetch the contradictory node as Sybil node [[10].

Mingxi Li [2013] et al In this paper, we proposed a RSDs against Sybil attacks, which is a persuading reaction for three key issues: firstly, we address the Sybil attacks, by a RSSI-based distributed detection part; in like manner, our protocol can kept the network from a critical number of nodes dissatisfaction accomplished by Sybil attacks; Thirdly, the RSDs has been insisted can keep up a high region likelihood with low structure overhead by execute tests [11].

Siwei Peng [2012] et al. In this paper, we introduce a novel authentication plan to keep these attacks. This IMA scheme bases upon the joint identity authentication and steganography to present a secure mechanism for data aggregation in wireless networks [12].

Chia-Fen Hsieh, [2011] et al. In this paper tries to inspect how IDS about ontology and light-weight IDS are related. The supervisor develops relationship of sensor nodes on ontology to distinguish Sybil attack. Join light-weight IDS the officer technique to decrease vitality utilization and the seclusion tables abstain from identifying irregularity over and again. The proposed a lightweight ontology-based IDS, which enhances presence weaknesses of IDS on wireless network successfully [13].

3.EXISTING WORK



4.PROBLEM STATEMENT

Defenses have the big issue of network and it's a key factor for Sybil attacker node because this node takes advantage of deafness.

Every node which use radio waves check wellbeing is additionally brittle with custom radio equipment, and approval might be exorbitant as far as energy. By using radio waves position of nodes easily find out so that we get position of nodes.

In wireless network node easily add and remove the node in the network so that attack condition is enhanced.

5.PROPOSED SOLUTIONS

In our purpose, all cluster head impart to each other and whenever attack happen in network node generate out of domain address so either malicious node, which give wrong path or Sybil node reply so on the basis of first reply cluster head share info to each other and send this particular information to base station and find-out attacker node. Second approach we also consider energy of that particular attacker node if it change again and again its own identity and take data to other node to compare to remaining node its vitality level is less so on the premise of vitality we also recognize this particular node.

- **Behavior based detection and preventions**

1. RR testing ()
2. Random key distribution ()
3. Authentication ()

4. Identify place of nodes ()
5. Send data encrypted way ()

We will work on Behavior based detection and preventions, registration techniques
Types of Sybil nodes: There are two types of Sybil nodes. In first type it simultaneously use many identities at a time either By searching the identity of others at network initialize time
1) node has higher speed
2) If receive signal strength is higher than average signal strength
3) Average energy of network use for a node is higher.
4) Average frequency of network use for a node is higher.

Algorithm:

```
1) Calculate node speed
2) Calculate receive upper bound thresh
3) Check node address
4) If node is new than address is not present
5) Probability of node to be malicious (Sybil Attacker) PS=0
6) Calculate avg energy of nodes in network
7) Calculate avg frequency of network
THEN
If node speed>= 10
{
PS=PS+ 0.1
}
If RSS (node)>= RSS UB_THRESHOLD
{
PS=PS+ 0.25
}
if node energy <=avg energy of nodes in network
{
PS=PS+ 0.2
}
if node frequency >= avg frequency of network
{
{
PS=PS+ 0.25
}
Else
{
Add node into the safe list.
}
End
```

First of all network is created which consists of nodes. Four parameters are taken i.e. Speed, energy and frequency. Threshold value of speed is set to 10m/s whereas threshold value of energy is set to average energy of network and threshold value of frequency is set to average frequency of network. On this, on the off chance that new node enters a network then its velocity, Energy and frequency value must be less than threshold value, handiest then that node is at the point seen as legitimate node generally as Sybil node. At the point. When node enters in a network, firstly it is checked whether its area is accessible in the table or not. On the off chance that it's not remunerate in the table then its velocity, Energy and frequency parameters values are checked. Then the threshold worth of pace is ready to 10m/s. The nodes relocating with pace greater than 10m/s are considered as Sybil nodes otherwise as legitimate nodes. After this RSS upper bound edge quality is figured and it is computed by taking normal of RSS estimations of nodes which are moving at rate of 10m/s. When some node enters in a network then its location is checked in the table that whether it is available in the table or not. In case it is not present in the table then its RSS value is compared against RSS upper bound value. If its RSS value is greater or equal to upper bound value then we increase possibilities that this nod is malicious otherwise as legitimate node. And if Speed, Energy and frequency parameters qualities are not as much as edge values then it is considered as legitimate node generally as Sybil node.

6.CONCLUSION

WSNs are networks with no permanent infrastructure and network capacities are done by every single accessible node, which are exceptionally mobile and have compelled power assets. In this way, WSNs has greater affectability to node mischief. Sybil Defender can effectively perceive the Sybil nodes and recognize the Sybil group over a Sybil node, despite when the measure of Sybil nodes displayed by each attack edge is near the hypothetically perceivable lower bound. In this paper, we study about Sybil attack in MANET and also no. of papers regarding Sybil attack detection.

REFERENCES

1. Wei Wei, Fengyuan Xu, Chiu C. Tanand Qun Li," SybilDefender: A Defense Mechanism for Sybil Attacks in Large Social Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 12, DECEMBER 2013, pp: 2492-2502.
2. Preeti , Poonam Chaudhary," Detection and Prevention of Sybil Attacks in Mobile WSNs", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 7, July 2015, pp: 3032-3036.
3. Murat Demirbas and Youngwhan Song," An RSSI-based Scheme for Sybil Attack Detection in WSNs", ieee 2015.
4. Geetha, M. Ramakrishnan "Detection of SYBIL Attack using Neighbour Nodes in Static WSN " International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 4 April 2015,
5. Sangeeta Bhatti*, Prof Meenakshi Sharma " A Novel Algorithmic Approach for Detection of Sybil Attack in MANET" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 5, May 2015 Udaya Suriya Rajkumar.
6. Dr. Rajamani Vayanaperumal " A Compare and Match Approach for Preventing Sybil Attacks in WSNs" International Journal of Engineering Technology Science and Research IJETSR September 2015.

7. T.G. Dhanalakshmi, Dr.N.Bharathi and M.Monisha “SAFETY CONCERNS OF SYBIL ATTACK IN WSN” International Conference on Science, Engineering and Management Research (ICSEMR 2014)978-1-4799-7613-3/14/$31.00 ©2014 IEEE

8. Imran Makhdoom, Mehreen Afzal and Imran Rashid “A Novel Code Attestation Scheme Against Sybil Attack in WSNs” 2014 National Software Engineering Conference.

9. A. Babu Karuppiah, J. Dalfiah, K. Yuvashri S. Rajaram and Al-Sakib Khan Pathan “A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in WSNs” 2014 3rd International Conference on Eco-friendly Computing and Communication Systems.

10. S. Sakthi Vinayagam, Dr V. Parthasarathy “IPTTA: Leveraging Token-Based Node IP Assignment and Verification for WSN” International Conference on Science, Engineering and Management Research (ICSEMR 2014) 978-1-4799-7613-3/14/$31.00 ©2014 IEEE

11. Mingxi Li, Yan Xiong, Xuangou Wu Xianchun Zhou, Yuhui Sun, Shenpei Chen and Xiaoya Zhu “A Regional Statistics Detection Scheme against Sybil Attacks in WSNs” 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.

12. Siwei Peng “AN ID-BASED MULTIPLE AUTHENTICATION SCHEME AGAINST ATTACKS IN WIREL ESS SENSOR NETWORKS” Proceedings of IEEE CCIS2012.

13. Chia-Fen Hsieh, Yung-Fa Huang and Rung-Ching Chen* “A Light-weight Ranger Intrusion Detection System on WSNs” 2011 Fifth International Conference on Genetic and Evolutionary Computing.