International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Evading and Averting the Sybil Attack in Manets Using Mac Hash Message Algorithm

M. Shivashankar[1], Dr. M. Prabakaran[2]
[1]Research Scholar, PG and Research Department of Computer Science, Government Arts College (Autonomous) Karur – 5
(Affiliated to Bharathidasan University, Tiruchirappalli), Tamilnadu, India
E-Mail: shivahirthik@gmail.com
[2]Research Advisor& Associate Professor, PG and Research Department of Computer Science, Government Arts College (Autonomous) Karur – 5
(Affiliated to Bharathidasan University, Tiruchirappalli), Tamilnadu, India.
E-Mail: captainprabakaran@gmail.com

Abstract

The security loopholes present in the wireless network especially MANET makes it vulnerable and weak. Most of the users are much concerned about the very security of the network and hesitate to participate actively in the transactions. Very powerful and strange attacks are pinpointed by many research scholars in the past. The Sybil attack is one of the most detrimental attacks imparted on MANETS where plethora of authentic nodes are faked and forged to enable illegal entry into a network to disrupt the very security of the MANET. The Sybil attack acts and simulates like an existing node present in the network to get unauthorized access into the network. To prevent and evade this a new algorithm using the MAC is employed in this paper. The proposed algorithm MAC Hash Message – MHM algorithm will detect, prevent and eliminate the Sybil attack completely and provides a hassle free transaction to the nodes present in the MANET.

Keywords: MANET, Sybil attack, MAC, MHM.

1. INTRODUCTION

The MANET (Mobile Ad Hoc Network) is a group of individual nodes that forms a decentralized network without depending on any centralized architecture. Each and every node present in the MANET can enter or exit the network anytime and they can wander liberally inside the network without any obstacle. The node present in the network will act as router to transmit as well as a host to receive and transmit the data within the network. The unique identifier UID is used for data communication within the network and this UID is one of the most important parameter present in the MANET to identify the node's authenticity. Usually the MANET is a self-configuring network where the topology of the network is not uniform and fixed. The nodes present in the network moves and wanders randomly to make the network unpredictable and the topology of the network changes rapidly. The nodes present in the network are fitted with receiver and transmitter (antenna) to enable two way communications. The antenna fitted in the nodes can be Omni-directional or broadcasting, single directional and peer to peer based upon the requirement.

Usually the MANET is attacked by many techniques due to lack of good security mechanism, lack of stringent monitoring system and rapid topology change [1]. It is a known fact that the communication in the MANET is occurred upon mutual trust between the nodes and there is no central vigilance to monitor the transactions or central authorization mechanism to safeguard the network [2]. This vulnerability is tapped by the intruders and attacks the network using various treats shown in the next section.

2. ATTACKS ON MANETS

The attacks on the MANET [5] can be classified into two categories as shown in the following figure 1.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

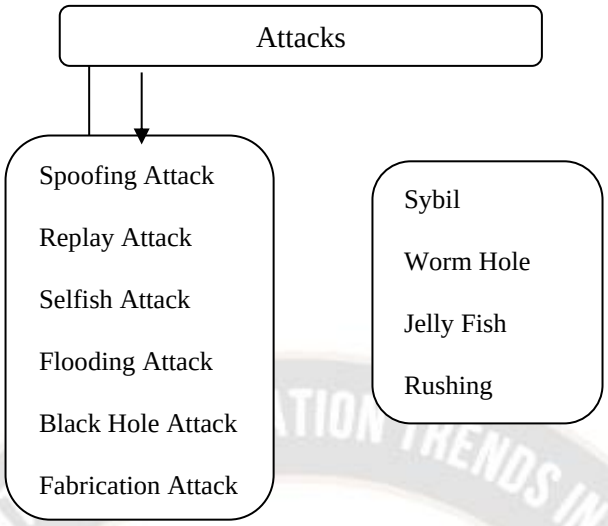

Fig.1. Various attack types in MANET

2.1. Spoofing attack – Here the RREQ and RREP are forged illegally and the network security is breached and captured.

2.2. Replay attack – The message of a valid node is recorded and played later by the attacker to gain access into the network.

2.3. Selfish attack – The attacker uses the route request RREQ or route reply RREP illegally to gain access into the network.

2.4. Flooding attack – this is a simple denial of service attack DDOS where the attacker floods the network with huge number of request RREQ.

2.5. Black hole attack – A forged RREP is used by the attacker to get into the network illegally and this type of attack is called black hole attack.

2.6. Sybil attack – The attacker will generate large number of nodes pretending as a genuine node and capture the network [4].

2.7. Worm hole attack – Using direct communication link between two nodes, the attacker forms a tunnel to capture the network.

2.8. Rushing attack – The attacker presents the route request RREQ faster than the original node and gain access inside the network.

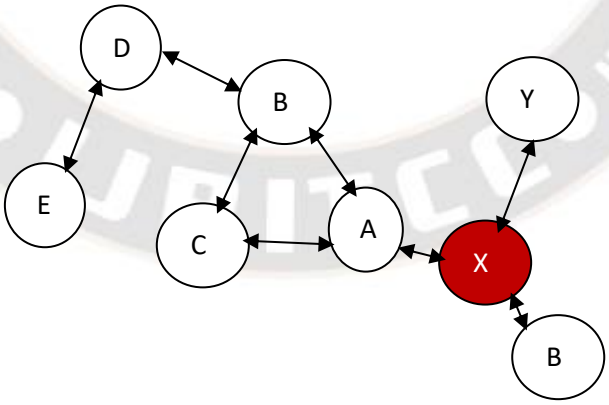

Fig.2. Typical Sybil attack with multiple ID

3. EXISTING METHOD

The Sybil attack is countered using random password generation RPG algorithm where some important information related to the nodes are stored in a table called routing table. From this routing table, the nodes that are being used to transmit the data from the sender and the receiver are present. This table is used to detect the authenticity of a particular node present in the network and this eliminates the Sybil node immediately after comparing the data present in the routing table. The algorithm creates a perfect

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

route for the data to be transmitted from the sender to the receiver using various procedures and processes. The tables are shown in the following tables,

Table 1: Node information table – NodInfo

NodeID	**N1**	**N2**	**N3**	**N4**	**N5**	**N6**	**N7**	**N8**
Time stamp	10:01	10:03	10:05	10:07	10:08	10:11	10:12	10:14
X Pos	23	35	121	12	189	87	96	110
Y Pos	117	176	56	89	67	118	138	176

Table 2: The routing table – RouteInfo

NodeID	**N2**	**N3**	**N5**	**N6**	**N8**
Time stamp	10:03	10:05	10:08	10:11	10:14
X Pos	35	121	189	87	110
Y Pos	176	56	67	118	176
Time stamp	12:02	12:04	12:05	12:08	12:10

The Sybil node present in the table is shown in the table 3 and this Sybil node pretends as an authentic node and attacks the MANET.

Table 3: Sybil node N5[N4] detected in the table

NodeID	**N2**	**N3**	**N5**	**N5[N4]**	**N6**	**N8**
Time stamp	10:03	10:05	10:08	10:18	10:11	10:14
X Pos	35	121	189	180	87	110
Y Pos	176	56	67	63	118	176
Time stamp	12:02	12:04	12:05	12:07	12:08	12:10

4. PROPOSED METHOD

Most of the existing methods detect the Sybil by matching the identities present in the node table with that of the values present in the routing table and if that value matches, it is considered as an authentic node else it was considered as Sybil node. The main goal of this paper to develop an algorithm using MAC and create a hash value to each and every node and store that value in the node table along with the existing data. The message which is sent or transmitted initially to all the node are converted into a hash value using the unique MAC id present in each and every node. This value is compared and matched with the routing table value to prove the authenticity of the node.

The base station sends a message "WELCOME" to all the nodes and this message is encrypted using a customized algorithm named "MACrypt algorithm" as given below

Algorithm MACrypt (input message, MAC address)

1. Fetch the input message from base station BS
2. Fetch the MAC address
3. MES = ϕ
4. Convert the message to ASCII→ASC_{mes}

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

5. Convert ASC_{mes} to Binary →Bin_{mes}
6. Convert the MAC to ASCII →ASC_{mac}
7. Convert the ASC_{mac} to Binary →Bin_{mac}
8. Result=[ASC_{mes}] XOR [ASC_{mac}]
9. Convert Result →Dec
10. For each pair of Decimal D in Dec
11. Convert D to ASCII → RES
12. MES = MES U RES
13. End For
14. Return MES

After executing this MACrypt algorithm, the message "WELCOME" is encrypted into various form according to the unique MAC address of each node and stored as shown in the following table 4.

Table 4: Encrypted message in nodeInfo

NodeID	**N1**	**N2**	**N3**	**N4**	**N5**	**N6**	**N7**	**N8**
Time stamp	10:01	10:03	10:05	10:07	10:08	10:11	10:12	10:14
X Pos	23	35	121	12	189	87	96	110
Y Pos	117	176	56	89	67	118	138	176
MES	Xb3mg Ad6Ba bagRmP 5DqUnt	Vbaq65 gHmQ1 Gkol5& Bah50O	Nas%ij aDi50K FgyT92 nH3@j	GpaK7 hYp971 FHg6& NhyP61	Haqu^k HawKm 9HqyrT1 Bae@op	@18Gao OgtY90 DfaT11 Hgaew1	GAtY18 Hyaw%7 gYpfT65 HawQB	gqRyn7 Naw*jR HayW7% nhEqpfS

From the table 4, it is quite clear that the each node is assigned unique ID, x position, y position, time stamp along with the encrypted message. The entire network is denoted by,

E = {(N1,N2,N3….Nk), base station, Admin} where k is the number of nodes present in the network.

The table 2 is presented with the source node N2 and the destination node N8 along with the routing nodes N3, N5, N6.Therefore the route discovered will be N2→N3→ N5 →N6 →N8.

In the next table 3, a Sybil node N5 is introduced which will be discovered by the proposed algorithm using the MAC hash comparison as shown in the next section.

The pseudo code of the MHM algorithm as follow:

Algorithm MHM

1. E = (N1,N2,N3,… Nk)

2. ∀ Node n ∈ E do begin

3. NodInfo=add(NodeID, Nn(X), Nn(Y), Nn(T), Nn(MES)

4. End For

5. ∀ Node n1∈ E do begin

6. ∀ Node n2∈ E do begin

7. Node n1 send request to n2

8. Node n2 accept request from n1

9. If(MES(n1) and MES(n2) present in NodInfo) do begin

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

10. Node n1 send data to n2

11. Else

12. Choose next Node

13. End For

14. End For

15. End Algorithm

5. EXPERIMENTAL RESULTS

The whole system is simulated using Network simulator NS2 with 25 nodes with a network size of 1600 X 1600. Let us assume that each and every node in the network complying with the Ad hoc on demand vector protocol. The entire 25 nodes is built with a single base station BS. The experiment is conducted by considering the node 15 as the destination node and the node 2 as the source node. The node 2 sends a REQ to the node 15, which is accepted by the node 15 and sends a RES message back to node 2. At the same time the node 10 can also sense the REQ and sends RES message back to the node 2 which is compared in the nodInfo table detected as Sybil node and that particular node is removed from the network. The proposed MHM algorithm is compared with the existing random password generation RPG algorithm with respect to throughput, delay time and packet loss and the results are show cased in the next section.

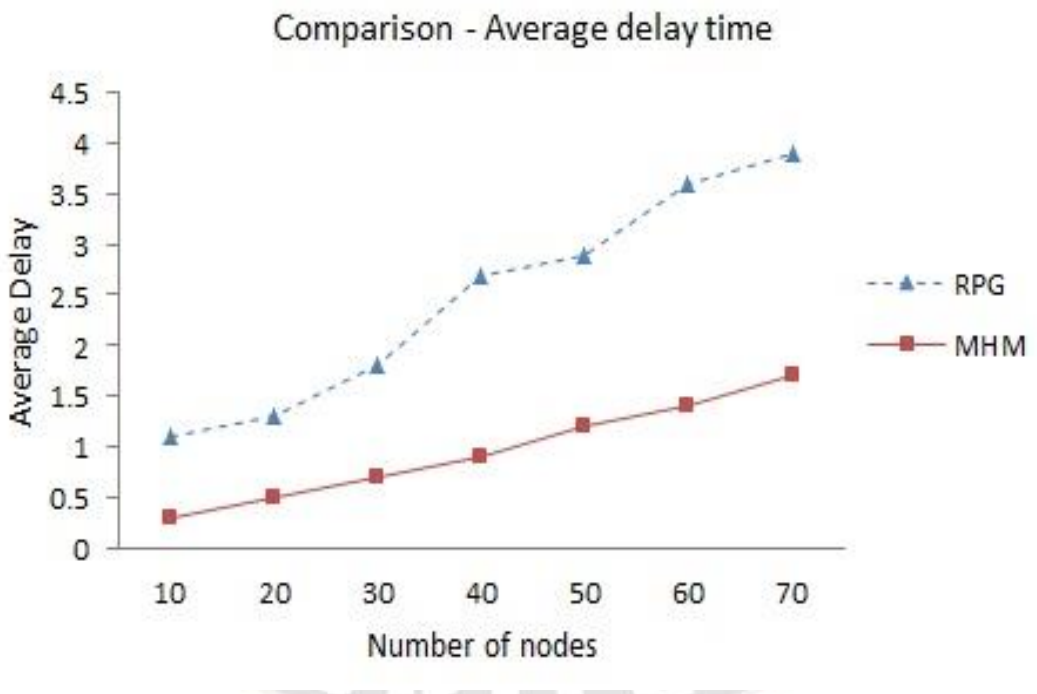

Fig.3. Comparison for average delay time

The performance of the algorithm can be gauged using the average delay time as shown in the figure 5 and from the above figure it is quite evident that the proposed MHM algorithm outscored the existing RPG algorithm.

To obtain the overall performance of the proposed algorithm, the throughput (number of successfully delivered packets) is calculated for large number of nodes and the node number is increased from 25 to 300 as shown in the following figure 6.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

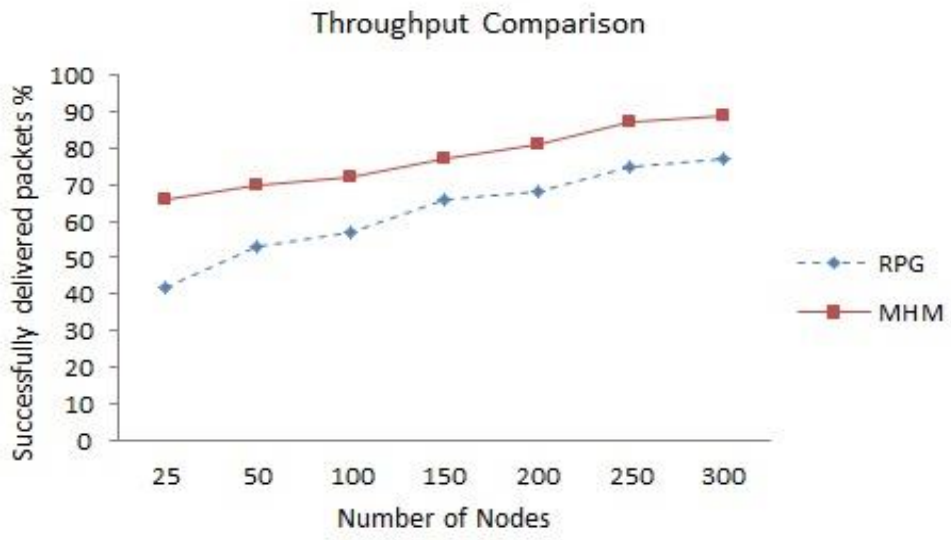

Fig.4. Comparison of throughput

The throughput values are computed for both the existing and the proposed algorithms and the throughput value of the RPG reached around 75% for 300 number of nodes whereas the throughput of the proposed MHM reached around 90% for 300 number of nodes and clearly the proposed algorithm outperformed the existing algorithm by a good margin.

The main part is the detection rate of the Sybil nodes and a detailed comparison is carried out as shown in the following figure and from the graph it is obvious that the proposed MHM outperformed the existing algorithm a detected Sybil without any false positives.

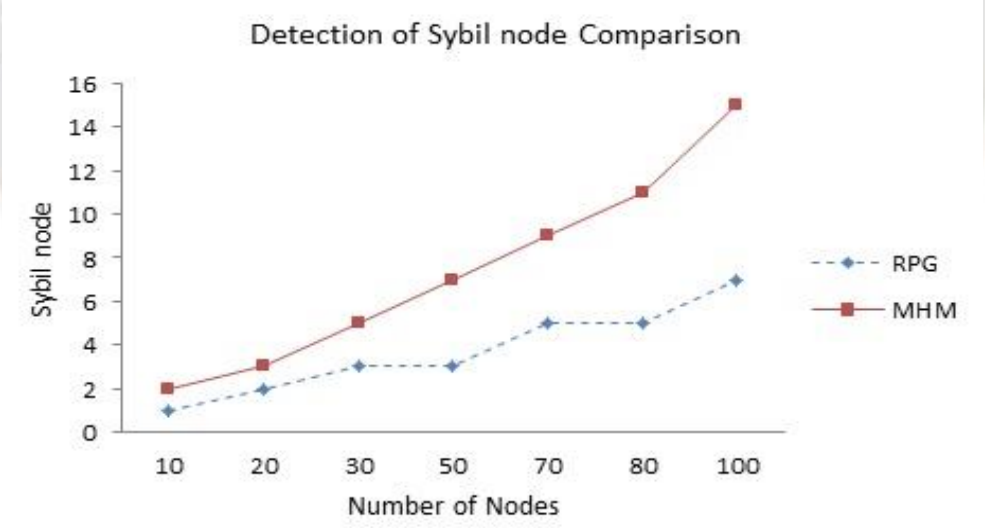

Fig.5. Sybil node detection comparison

6. CONCLUSION

In this paper a new algorithm with encryption of the message that is passed into the node for verification is employed and from the experimental results it is quite clear that the proposed MHM algorithm performed extremely well and outperformed the RPG algorithm with respect to throughput and Sybil detection. But the important drawback of the proposed method is it takes little bit of time as the message has to be encrypted and compared with the message present in the nodInfo table. In future steps has to be carried out to reduce the time consumption and improve the overall performance of the proposed MHM algorithm.

REFERENCES

[1] M. Mulla, "Efficient Analysis of Lightweight Sybil Attack Detection Scheme in Mobile Ad hoc Networks," in IEEE 2015 International Conference on Pervasive Computing, 2015.
[2] Z. Kasiran and J. Mohamad, "Throughput performance analysis of the wormhole and sybil attack in AODV," in IEEE 2014 Fourth International Conference on Digital Information and CommunicationTechnology and its Applications (DICTAP), 2014, pp. 81–84.
[3] R. Amuthavalli and R. S. Bhuvaneswaran, "Detection and prevention of sybil attack in wireless sensor network employing random password comparison method," Journal of Theoretical and Applied Information Technology,vol.67,pp.236–246, 2013.
[4]L.Xiao,L.J.Greenstein,N.B.Mandayam,andW.Trappe, "Channel-based detection of sybil attacks in wireless networks," IEEE Transactions on Information Forensics and Security,vol.4, no. 3, pp. 492–503, 2009.
[5] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," International Journal of Computer Science and Information Security,vol.4,pp.1–9,2009.
[6] Sangeetha Bhatti and Meenakshi Sharma, "A Novel Algorithmic Approach for Detection of Sybil attack in MANET", International Journal of Advanced Research in Computer Science and Sofware Engineering, Volume 5, Issue 5, May 2015, pp.1680-1685, 2015. ISSN: 2277128X
[7] Anamika Pareek and Mayank Sharma, "Detection and Prevention of Sybil Attack in MANET using MAC Address", International Journal of Computer Applications, Volume 122 – No.21, July 2015, pp.20-23.
[8] Ankit Gupta et al, "Securing AODV for Defending Sybil attack in MANET", IJSER, Volume 3, October 2015, pp. 75 – 79, 2015.
[9] Vivek Jaglan, "Innovation Approach for Resolving Sybil Attack in MANET", International Journal of Recent Research Aspects, Vol.2, Issue 1, March 2015, pp.95-99.
[10] Anamika Pareek and Mayank Sharma, "Architecture for Detection of Sybil Attack in MANET using MAC Address", IJIRAE, Issue 6, Volume 2, June 2015, pp.66-70.
[11] M. Reshma and V. Sowmiya Devi, "Detection of Sybil Attack for P2P Security in MANET", IISTE, Computer Science and Intelligent Systems, ISSN 2222-1719 (Paper), ISSN 2222-2863 (Online)
[12] Mohd Amir Siddiqui et al, "Design and Implementatin of Routing Protocol for detection of Sybil Attack in MANET", IJARSE, Vol.No. 4, Issue 08, August 2015, ISSN 2319-8354, pp. 247-254.
[13] Roopali Garg and Himika Sharma, "Proposed Light Weight Sybil Attack Detection Technique in MANET", IJAREEIE, Vol.3, Issue 5, May 2014.
[14] Somnath sinha et al, "Use of Spline Curve in Sybil Attack Detection based on Receiving Signal Power – New Approach", ACEEE Int.J. of Recent Trends in Engineering & Technology, Vol.11, June 2014, pp.602-611.
[15] R. Bhuvaneswari et al, "An Improve Performance, Discovery and Interruption of Sybil Attack in MANET", Middle-East Journal of Scientific Research 23 (7): 1346-1352, 2015, ISSN:1990-9233, pp.1346-1352.
[16] K. Vaijayanthi et al, "Detecting and Resolving The Sybil Attack in MANET Using RSS Algorithm", IJCSMC, Vol.3, Issue.11, November 2014, pg.233-241.
[17] "The Sybil Attack", John R. Douceur, Microsoft Research.
[18] Kuan Zhang et al, "Sybil attack and Their Defense in the Internet of Things", IEEE Inernet of Things Journal, Vol.1, NO. 5, October 2014.