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*

Detecting Sybil Attack During Data Transmission Using Concealed Data Sharing Algorithm in Manet

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

As the mobile users are increasing sharply, the wireless or mobile ad hoc network data transmission is on the rise and gaining lot of attention from the research communities. The most important issue that has to be handled is the detecting the Sybil attack and increase the reliability and confidentiality of the data transmission. The foremost aim of this paper is to develop a mechanism to detect the Sybil attack early and evade the data loss and privacy to ensure credibility to the users. The proposed algorithm employs a concealed data sharing plan during the route discovery phase and detects and alleviates the attack to guarantee attack free data transmission in the MANET. The data sharing plan allows only the nodes that are trustworthy and permit the data to be transmitted across them, thereby evading the malicious nodes during the route discovery process and curtails the wastage of time and energy of the nodes.

Keywords: Manet, wireless, Sybil attack, concealed data sharing algorithm, CDS algorithm.

INTRODUCTION

The advent of the cell phones and mobiles especially the smart phones has changed the data transmission and data availability to the ordinary users a lot and quite a lot of data and applications can be accessed using the mobile phones. When a cluster or group of mobiles is interconnected together they are called mobile ad hoc network or MANET. The major disadvantage is that the nodes present in the network can move out of the network coverage area and hence it is called infrastructure less network. Each and every node present in the network can act as a receiver, transmitter and router to facilitate the data transfer. The most important and worrisome concern is the security and privacy of the MANET. The MANET does not have any central control administration and more importantly the network topology tends to change every now and then. This feature of the MANET is responsible for many security attacks and this paper is focusing in solving one such attack named Sybil attack.

The main criteria that are responsible for the security lapse are,

1. The MANET is infrastructure less network.
2. The MANET employs multi-hop technique to transfer data.
3. The MANET has power constraint and energy constraint.
4. The MANET has limited memory.
5. The MANET is amorphous.
6. Lack of genuine authentication schemes.
7. Inability to gauge the malicious nodes.

Let us consider a source node S1 which tries to transmit data to a particular node named D1 also called as the destination a shown in the figure1. The node S1 will follow a particular route to reach the destination D1 but if a node or nodes present in its route are in out of range or switched off due to lack of power, the source S1 will discover a new route as shown in the figure 1.

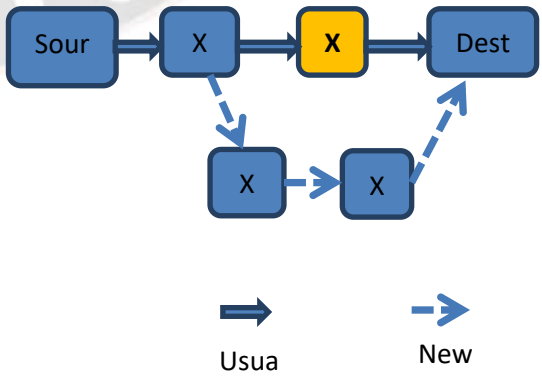

Figure 1: Route discovery model

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*

The S1 sends a RREQ message to the nearest node X1 and if receives a reply RREP from the nearest node X1, it will be updated and considered that the node X1 is active. The node X1 will send RREQ to node X2 and here in the figure 1, the RREP is not received from the node X2 and hence the next neighbor node X3 is selected and the request RREQ is sent and here the node X1 receives the RREP from the node X3 and a new route table is updated.

Here each and every node will receive a secret code from the neighbor node to authenticate the neighbor node during the route discovery phase and these concealed data are stored in local archives of each and every node. The main purpose of the Sybil attack is to generate malicious node instead of genuine nodes and then acts as a genuine node and pilfer the data which are transmitted [1]. To avoid this many research works are carried out and here in the proposed work, a secret code or a concealed code that is known only to a particular node and its neighbor is shared to authenticate the node whether it is a genuine node or not.

RELATED WORKS

The Sybil attack on the MANET can produce extreme damage and harm to two layers present in the network namely, Application and networking layer. When the Sybil attack penetrates into the network layer, the malicious nodes will multiply than the genuine nodes and cause more damage to the network [2]. Since the MANET is infrastructure less network and doesn't have any topology and often changes its topology, it is fragile and the possibility to employ a third party trust system to secure the network is a question mark [3]. The author in [4] employed a different technique by introducing ratio based mechanism to improve the efficiency of the overall data transfer and to reduce the loss of packets incurred during the transmission of the data inside the network. A typical Sybil attacker could upset the discovery of routes when a multipath or geographic directing method is utilized, by appearing to a few spots are produced routes influence the aftereffects of information conglomeration [5] by adding to the course of accumulation a few time dodge discovery while acting malevolently by spreading the activities he executes over the fashioned personalities and forestall the network.

PROPOSED METHOD

The proposed method comprises of three stages, namely,

1. Discover the best route
2. Authentication
3. Detection

The first stage is the discovery of the best possible route for the node to transmit the data through the network and the pseudo code for this process is shown in the following figure 2.

Algorithm Route_Discovery

Begin

1. The Source S1 and destination D1 nodes are initialized.
2. Calculate the interrupt time
   T = (a. previous T) + (1- a) . current T
   Where a = small step value used in calculation.

IF(S1) search the table for destination D1

IF route_not_found in table

ADD new route with D1 in table

End IF

Else

broadcastID = broadcastID+1

transmission_RREQ (S1_ID:seq_no:0,00.endpoint_id:D1_ID,D1_seq_no:D1_seq_no, hop count:0)

End IF

If (ID) not in D1

Rebroadcast RREQ

Else

Return the RREP

Forward the RREP

End IF

If (RREP from D1 reaches the S1)

If(RREP time is less than delay time)

IGNORE RREP

Else

The route is found and formed between S1 and D1

End IF

STORE the route in table

END algorithm

The idea here is very simple the source S1 sends a request RREQ to a particular node and that node will forward a reply RREP to the S1. If the RREP arrives too early than the anticipated delay time, then the node which transmits the RREP is considered as malicious node. Since the malicious will transmit the reply without accessing the table and considering the concealed data, it will arrive quickly and assumed to be a

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*

malicious node. Even if the reply is arrived late and even if it is not the shortest path, that route will be a genuine route.

Algorithm Authenticate Node

Begin

Node discovered in the network to form the route certify themselves

A secret key K is generated based on the ID of the node

Generate certificate C based on the key K

Share the C with the neighbor nodes

D1 sends certified RREP to the neighbor nodes

Fetch all the nodes N [1 -------n]

If the certified RREP present in N and equal

Attach the certified RREP to the next node

Else

Revoke RREP

End IF

RREP reaches the source S1

S1 authenticates the certified RREP along with the route
IF (certified RREP is valid)

Data transferred through the route

Else

Announce about the malicious node to all other node in the network

End IF

End algorithm

The route is discovered in the first stage and now the data is arrived to the node where it is authenticated and checked for the malicious node presence. The secret key is generated by the individual nodes by requesting the IP address of its neighbor node and then by applying the hash function, the key is generated and stored.

HF (Message) = h(key + start padding) || h(key + end padding) || M

Where HF is the hash function, M is the message, The HF converts the message fro the neighbor node into a secret key which cannot be practically hacked or breached by the intruders.

Algorithm DetectSybil

Begin

Let S1 be the source , S2, S3,S4 …S-1 be the alternate path discovered and stored in table

Initialize Node N = 0

Consider Mp be the malicious path

For all nodes [S1, S2, S3 ------ S-1]

Select the S1 path and check whether it lies in malicious path

IF(S1 ∩ Mp==0)

Add S1 to N

If N=0

Apply Route_discovery

Else

Forward data in the route

End If

End Algorithm

The third stage of the algorithm detects the wrong or malicious nodes from the group of nodes present in the MANET. The malicious nodes that escapes from the second stage of the operation will be retained and will be informed about their malicious activities to the other nodes.

RESULT AND DISCUSSION

The proposed method to detect the Sybil attack is simulated in NS2.3 simulator and the parameters used are mentioned in the following table 1.

Table 1: Simulation parameters used

Parameter	Value
No. of Nodes	100
Area Size	1200 X 1200
Mac	802.11
Radio Range	250m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Packet rate	Five pkt/s

Initially the packet delivery ratio is computed with varying number of nodes in the simulator as shown in the table 2. The proposed algorithm is compared with random hashing technique and from the experimental results it is quite obvious that the proposed algorithm CDS outperformed the random hashing method by a large margin.

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*

Table 2: PDR comparison for varying nodes

Packet delivery ratio PDR		
Number of NODES	**Random hash**	**CDC**
10	78.77	93.87
30	76.56	92.66
50	76.01	92.03
70	75.21	90.5
100	72.10	87.56

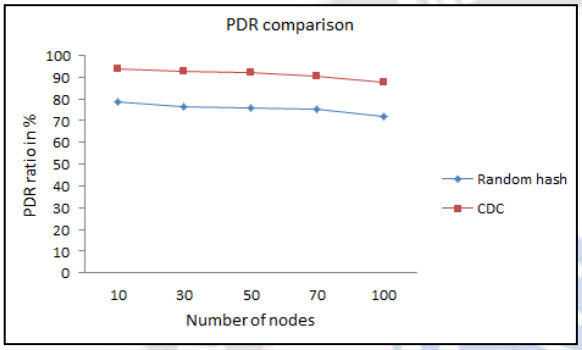

Figure 2: Graph depicting the PDR comparison

The packet delivery ratio is nothing but the amount of packet that are delivered to the destination without any loss and it is calculated using the following formula,

PD ratio = (Number of packet delivered/total packet) x 100

The next metric that is used in the paper is calculating the network lifetime and it is compared with the hashing method as shown in the table 3.

Table 3: Lifetime comparison for varying nodes

Network life time in seconds		
Number of NODES	**Random hash**	**CDC**
10	378.88	408.7
30	300.5	322.98
50	204.67	235.88
70	156.9	178.76
100	82.99	99.58

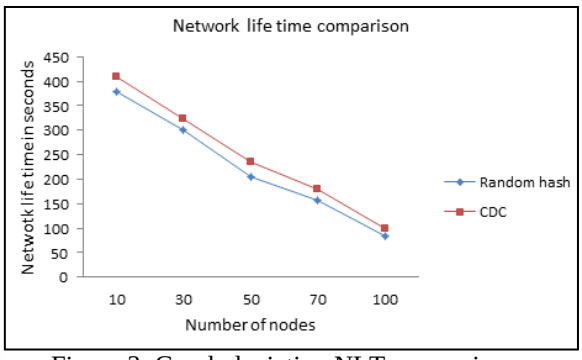

Figure 3: Graph depicting NLT comparison

From the table 3 and figure 3, it is quite clear that the proposed algorithm CDC outperformed the random hashing method and the overall network life time was definitely 20 to 25 percent more than the hashing method.

CONCLUSION

This paper focused on one of the most important attacks named Sybil attack and proposed a new method to evade and improve the overall lifetime of the network and reduces the packet loss and there by increases the PDR by a good margin. The simulation result showcased that the proposed CDC algorithm outperformed the other algorithm by a huge margin with respect to delivery ratio and life time of the network. This method ensures that no malicious node can participate in the data transmission as it employs three stage process and eliminates the malicious node before it attacks the network.

REFERENCES

[1] John R, Cherian JP & Kizhakkethottam JJ, " A survey of techniques to prevent sybil attacks", IEEE International Conference on Soft-Computing and Networks Security (ICSNS), (2015), pp.1-6.

[2] Gu P, Khatoun R, Begriche Y & Serhrouchni A, " Vehicle driving pattern based sybil attack detection", High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE 18th International Conference on, (2016), pp.1282-1288.

[3] Rashidibajgan S, "A trust structure for detection of sybil attacks in opportunistic networks", IEEE 11th International Conference for Internet Technology and Secured Transactions (ICITST), (2016), pp.347-351.

[4] Liu R & Wang Y, "A new sybil attack detection for wireless body sensor network", IEEE Tenth International Conference on Computational Intelligence and Security (CIS), (2014), pp.367-370.

[5] Triki B, Rekhis S, Chammem M & Boudriga, N, " A privacy preserving solution for the protection against sybil attacks in vehicular ad hoc networks", IEEE 6th Joint IFIP Conference on Wireless and Mobile Networking (WMNC),(2013), pp.1-8.

[6] 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)
[7] 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.
[8] Roopali Garg and Himika Sharma, "Proposed Light Weight Sybil Attack Detection Technique in MANET", IJAREEIE, Vol.3, Issue 5, May 2014.
[9] 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.
[10] 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.
[11] 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.
[12] "The Sybil Attack", John R. Douceur, Microsoft Research.
[13] 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.
[14] 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
[15] 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.
[16] Ankit Gupta et al, "Securing AODV for Defending Sybil attack in MANET", IJSER, Volume 3, October 2015, pp. 75 – 79, 2015.
[17] 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.
[18] 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.

AUTHOR PROFILES

M. Shivashankar received post graduate degree in from Government Arts College (Autonomous), Karur. He received Master of Philosophy in computer science from Government Arts College (Autonomous), Karur. He is a research student in Government Arts College (Autonomous), Karur. Currently, He is working in Guest Lecturer at Government Arts College (Autonomous), Karur. His area of research includes Network Security.

Dr. M. Prabakaran received doctoral degree in Vinayaga Mission University, Salem in the year 2011. At present, He is working as an Assistant Professor at Government Arts College (Autonomous), Karur. His research interest overs Big Data and Networking.