IJCTA, 9(36), 2016, pp. 337-345

Light Weight Random Bit Hashing Technique Based Addressing Scheme Based Sybil Attack Detection for Menet

T. Sheela* and P. Muthusamy**

Abstract : The mobility nature of nodes in mobile adhoc network has great impact in producing various attacks and the network is prone for various network threats. The Sybil attack is one among them which is performed by producing multiple duplication address to read the traffic and perform various attacks. To handle the issue of Sybil attack there are number of methods has been discussed earlier and suffers to achieve the performance in detecting the Sybil attacks. We propose a novel approach in this paper, which uses random bit hashing technique to generate addresses. The method generate four bit address and assigns to the mobile nodes when the node comes into the network by the base station or a controller. The random bit hashing technique, selects a two bits to hide the network information, which consists of the node id and the number of nodes present in the network currently. At the verification phase the same is reversed to verify the address before selecting any neighbor to forward the data packet. The method performs one step verification scheme, by communicate with the base station based on the result only the data packet will be handover to the node. The method produces efficient results in mitigating the Sybil attack in mobile adhoc networks.

Keywords : Manet, Addressing Scheme, Random Bit Hashing, Sybil Attack.

1. INTRODUCTION

Mobile adhoc network is the collection of mobile nodes which are moving throughout the network and moving in different direction with different displacement speed. The mobility of the nodes makes the network topology to change in a dynamic mode at each fraction of time. The nodes of mobile adhoc network comes with a radio to perform transmission and reception, of packets. The nodes of network perform cooperative transmission and involves in routing between the nodes. Also the nodes of the network involves in source routing which routes packets by their own. Whenever a new nodes comes into the network, the base station assigns address to the new node based on which the node has been identified.

There are number of addressing schemes are presented earlier to identify the node which are located in the network. Some of the methods uses dynamic addressing and some of them uses the static addressing schemes. The method of assigning address differs according to various parameters. However the addressing scheme uses various parameters to identify the nodes of the networks. As the topology of the network changes in rapid manner, the network is more prone for various network threats. Some of the nodes declares different address to its own and gives them to the other nodes of the network. By assigning multiple addresses and using them in the network, the malicious node tries to participate in the transmission by producing the sensation that the malicious node has the direct contact with the destination.

By producing the sensation to the neighbor nodes that it has the direct contact to the destination, all the nodes sends their information through the node and it participates in almost all the transmission. By

* Professor & Head, Department of Information Technology, Sri Sairam Engineering College, Chennai – 600 44.

** Research Scholar, Department of Computer Science and Engineering, VELS University, Chennai – 600 117.

receiving the entire traffic the node can perform many threats like can perform modification, eavesdrop and many more attacks. Such traffic capturing attack is named as Sybil attack and by capturing the network traffic the node can perform various threats to degrade the performance of the network. To mitigate the Sybil attack and to detect the malicious Sybil attacks there are number of methods has been discussed earlier. The address verification schemes are available, where the source node before transmitting the packet to the neighbor node, performs the address verification by communicating to the base station or by itself according to the procedure.

Random bit hashing is the special method of computing addresses to the mobile nodes which is performed by the base station when the node enters into the network. The random hashing technique, choose a random bit to hide the network information which will be used by the base station to verify the address. The malicious node may generate duplicate address and give to the neighbor nodes but the malicious node could not identify how the address has been computed and in what basis the node has been assigned with the address.

2. RELATED WORKS

There are number of methods has been declared for the problem of Sybil attack detection and we discuss some of the methods here in this section.

Detection of Black Hole Attack Using Code Division Security Method [1], discuss that the direct communication is possible only when two nodes lie within their sensing range; otherwise communication is made through intermediate nodes till the destination is reached. Such type of networks can allow any node to join in the network or leave the network at any instant of time. So any node can act as a host or the router in the network, which results in security issues in MANETs. A well known attack in MANETs is a Black hole attack. They present a simple but effective method called Code Division Security Method (CDSM) for security in order to prevent Black hole attack in MANETs. Black hole node is a malicious node which can mislead a normal node to forward the data through it and corrupt the data so that it can degrade the performance of the network. We validate our approach using network simulator with an example.

Light Weight Sybil Attack Detection in Manet [3], discuss the Fully self-organized mobile ad hoc networks (MANETs) represent complex distributed systems that may also be part of a huge complex system, such as a complex system-of-systems used for crisis management operations. Due to the complex nature of MANETs and its resource constraint nodes, there has always been a need to develop lightweight security solutions. Since MANETs require a unique, distinct, and persistent identity per node in order for their security protocols to be viable, Sybil attacks pose a serious threat to such networks. A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of accountability in the network. In this research, we propose a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system. Through the help of extensive simulations and real-world testbed experiments, we are able to demonstrate that our proposed scheme detects Sybil identities with good accuracy even in the presence of mobility.

Discovering Sybil and Masquerading Attack Using Received Signal Strength of Nodes in MANET [4], discuss the requirement of novel, distinct, and protracted identity per node so as for his or her security protocols to be viable, Sybil attacks cause a heavy threat to such networks. Sybil attacker will lawlessly claim multiple identities on single node and violate one-to-one mapping. Masquerading is an active attack where one node pretends to be another and giving false impersonation. Here by using RSS (Received Signal Strength) of nodes to find Sybil and masquerading identities on network with good accuracy even in the presence of mobility. This scheme detect Sybil identities while not exploitation centralized trusty third party or any further hardware, like directional antennae or a geographical positioning system.

A Novel Algorithmic Approach for Detection of Sybil Attack in MANET [8], proposed an identity verification and resource based algorithmic approach for the detection and elimination of Sybil nodes. In proposed technique secure identity of nodes are assign to all nodes to detect the Sybil node. The Sybil node is detected with involvement of base server by verification the identity and resources node through the trustworthiness of Secure Id of all node. Here the notion of unique id using secure id is used which lead to more secure communication in network.

Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV [12], discuss that the node communicate each other, the nodes cooperatively forward data packets to other nodes in the network by using the routing protocol. However, these routing protocols are not secure hence leaving the MANET unprotected from malicious attack. Wormhole attack is a common malicious attack in MANET environment. The network consisting of 20, 60 and 100 mobile nodes uses the random model in 1000 $m \times 1000$ m flat area. The sources are spread randomly over the network and only 512 bytes data packets are used. Each packet is uniformly dispersed at 180 sec, starting its journey from a random location to a random destination the objective of this paper is to evaluate the throughput performance in AODV with the existence of wormhole and Sybil attack. The simulation result has shown that there is difference performance in throughput when there is an attack.

The most of the methods suffers with the problem of poor detection accuracy and suffers with achieving the throughput ratio in the network.

3. LIGHT WEIGHT RANDOM BIT HASHING TECHNIQUE

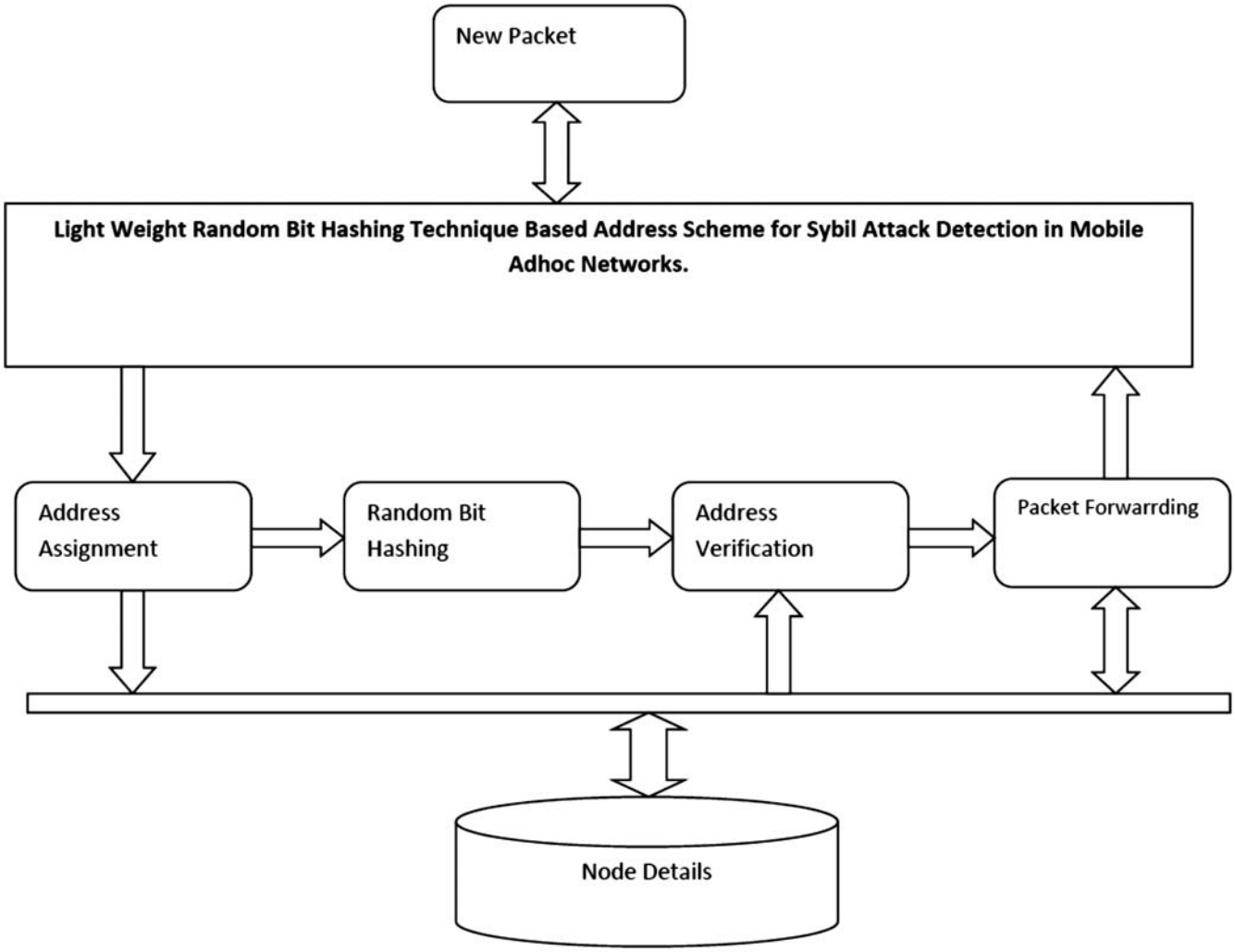

Figure 1: Architecture of proposed method

In this paper we present an Sybil attack detection approach named light weight random bit hashing based addressing. The base station assigns address for the new coming node whenever a new node arrives into the network. The base station performs address assignment according to the random bit hashing technique. Later the source node performs address verification using the same by communicate with the base station.

The entire process can be split into number of stages namely Address Assignment, Random Bit Hashing, Address Verification, Packet Forwarding. We explain each of the functional stages in detail in this section.

The Figure 1, shows the architecture of the proposed random bit hashing technique and shows the functional components in detail.

3.1. Address Assignment

The address assignment is performed whenever the new mobile node approaches the network. The base station monitors the incoming and out going nodes and when a new node approaches the base station receives the handover request and upon receiving such request, the base station computes the new address for the node using the random bit hashing technique. Generated address is sent to the mobile node which initiated the handover. The same will be broadcast into the network which will be received by the nodes of the network.

Algorithm:

Input : Address Table At, Handover Request Hr

Output : Address Table At

Start

Receive Handover Request Hr.

Read Address Table At.

Address Adr = Perform Random Bit Hashing(At).

Send to mobile node.

Generate AddressInfo Packet.

AI = { Adr, Address-Info}

Broadcast AI.

Stop.

The above discussed algorithm generates address for the incoming mobile nodes and broadcast them into the network.

3.2. Random Bit Hashing Based Addressing Scheme

The random bit hashing scheme generates the address according to the bits being selected to hide the network information. First the method initialize the address with four bit and for each time window the method selects the different bits to hide the network information, which will be same for the entire time window. First the method select the random number which represent the bit, which will be used to hide the node id, the second random bit will be used to hide the number of node present in the network, the third bit is used to store the node number of generated for the mobile node. The final bit will be used to store the total number of nodes.

Algorithm :

Input : Address Table At, Node Details Nd

Output : Address Adr

Start

Initialize Four bit address Adr.

Initialize the random bit hash value Rh.

$$Rh = \int (Random\ (1, 255) + size\ (Adr)) <> 255$$

Nindex = Generate Random Number within four bits.

$$Nindex = \int Rand\ (1, 4)$$

Tindex = Generate Random number to store total number of nodes.

$$Tindex = \int Rand\ (1, 4) \cong Nindex$$

NNindex = Generate Random Number to store the node number.

$$NNIndex = \int Rand\ (1, 4) \cong (Nindex, Tindex)$$

Tindex = Identify the index to store the total number of nodes.

$$Tnindex = \int Rand\ (1, 4) \cong (Nindex, Tindex, Nnindex$$

Initialize Adr with corresponding index.

Read Address Table At.

Compute Number of nodes present in the network $Tn = \sum Nodes \in At$

Compute Node ID $Nn = Tn + 1$.

Compute Total Number of Nodes $Tnn = Tn + 1$.

Perform hashing with Rh.

Adr(Nindex) = Hash(Rh, Nn).

Adr(Tindex) = Hash(Rh,Tnn).

Adr(Nnindex) = Nn.

Adr(Tnindex) = Tnn.

Add address to address table.

Add value of Rh to Address table.

$$At = \sum (Address \in At) \cup \{Adr, Rh.\ Ti\}$$

Return Adr

Stop

The above presented algorithm generates the address for the newly incoming node and based on the values of random hashing.

3.3. Address Verification

The address verification is the process of cross checking the address given and the method verifies each process. First the method identifies the presence of address in the table. If the address present in the table then the method performs reverse hashing with the hash value present in the address table towards

the address identified. The reverse hashing result in the Node id and the total number of nodes present. If the values of node id and total number of nodes are same in the address available and given then the verification becomes successful. Otherwise the verification fails and the request being dropped.

Algorithm :

Input : Address Table At, Address Adr

Output : Boolean

Start

Identify the presence of address in the table.

Flag $f = \int_{i=1}^{size(At)} if\ (At\ (i) == Adr), 1, 0)$

If $f ==$ 1 then

Identify the Node Id Index Nindex = At(adr).Nindex

Identify the Total node index Tindex = At(adr).Tindex

Identify the nodeId index Nidindex = At(adr).Nidindex.

Identify the tnindex = At(adr).Tnindex.

Perform reverse hashing.

Node Id = Reverse-Hash(Adr(Nindex, Rh)).

Total Node = Reverse-Hash(Adr(Tindex, Rh))

Nid = Reverse-Hash(Adr(Nidindex,Rh))

Tnodes = Reverse-Hash(Adr(tnindex,Rh)).

If Node Id == Nid and Total Node == Tnodes Then

Return True

Else

Return False

End

Stop.

The above discussed algorithm verifies the address given with the address present in the address table. The reverse hashing is performed by subtracting and dividing the values.

3.4. Packet Forwarding

The mobile node receives the packet and if it has to be forwarded then the node selects the route. Before forwarding to the first neighbor the node verifies the address using one step verification with the support of base station. Based on the result from the base station the node transmits the packet to the destination. If there is a false reply from the base station then it will not be forwarded through the selected route and the node chooses the next available route to forward the data packet.

4. RESULTS AND DISCUSSION

The proposed light weight random bit hashing technique based addressing scheme has been implemented and evaluated for its performance and efficiency. The method has been validated with various simulation setup and the method has produced efficient results.

Table 1

Details of simulation parameters

Parameter	*Value*
Simulation Tool	Ns2
Number of Nodes	100
Transmission Range	100 meters
Simulation Area	1000/1000 meters
Simulation Time	4 minutes

The Table 1, shows the simulation parameters being used to simulate the proposed approach.

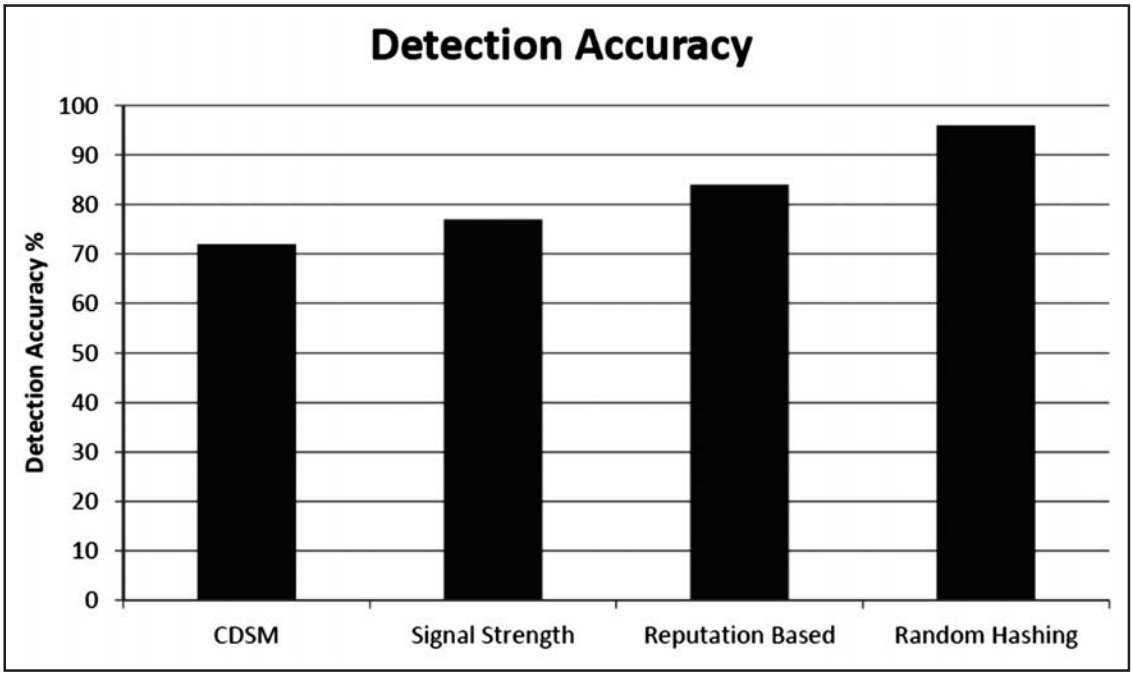

Figure 1: Comparison of detection accuracy

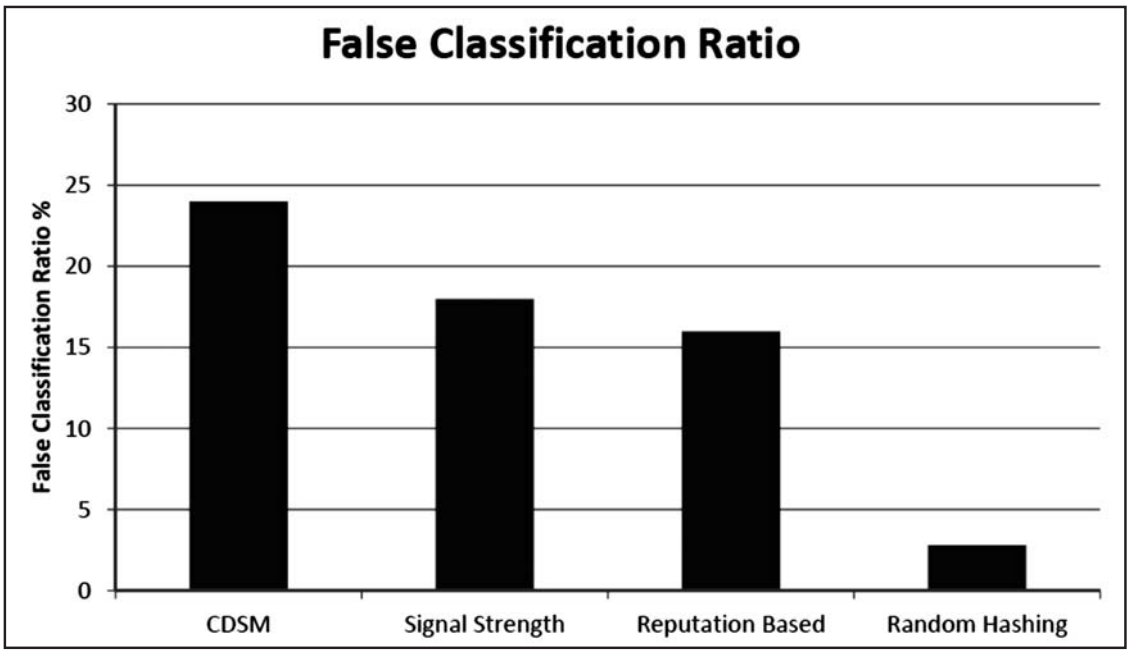

Figure 2: Comparison of false classification ratio

The Figure 2, shows the comparison of false classification ratio produced by different methods and it shows that the proposed method has produced higher false classification ratio than other methods.

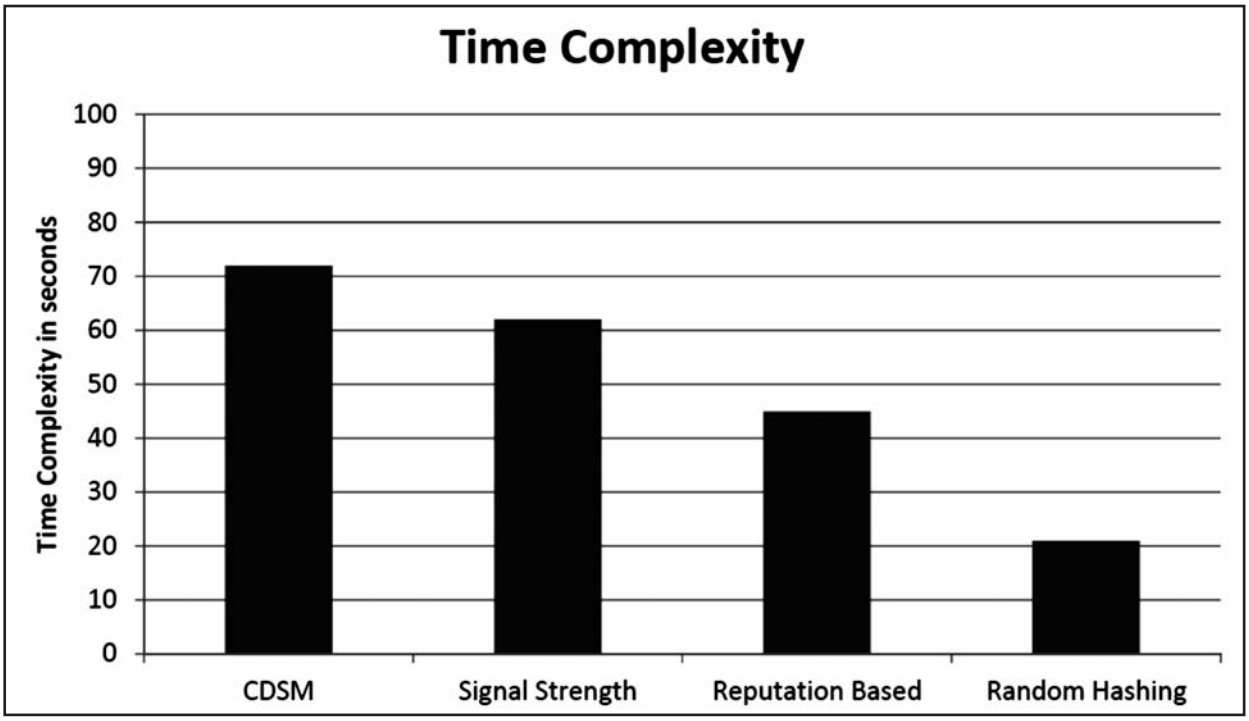

Figure 3: Comparison of time complexity

The Figure 3, shows the comparison of time complexity produced by different methods and the result shows that the proposed method has produced less time complexity than other methods.

5. CONCLUSION

In this paper, we proposed a light weight random bit hashing technique based addressing scheme and verification approach to improve the efficiency of Sybil attack detection in mobile adhoc networks. The base station generates address to the nodes and assigns them when it comes first using the random bit hashing technique. The generated address is broadcasted to the all the nodes of the network. When the mobile node has the packet and selects the route it performs address verification using the support of base station. The base station verifies the address using the reverse hashing technique and improves the performance of Sybil attack detection. The proposed method improves the performance and reduces the false classification ratio with less time complexity.

6. REFERENCES

1. Syed Jalal Ahmad , V. S. K. Reddy, A. Damodaram, P. Radha Krishna, Detection of Black Hole Attack Using Code Division Security Method, Springer, Volume 338 of the series Advances in Intelligent Systems and Computing pp 307-314,2015.
2. Anamika Pareek and Mayank Sharma. Article: Detection and Prevention of Sybil Attack in MANET using MAC Address. International Journal of Computer Applications 122(21):20-23, July 2015.
3. Abbsas S., Light Weight Sybil Attack Detection in Manet, IEEE Transaction on Systems, Vol 7, issue 2, pp:236-248, 2015.
4. Sivakumar B1 , Gracy Theresa W2, Discovering Sybil and Masquerading Attack Using Received Signal Strength of Nodes in MANET, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2015
5. Cluster based Key Management Authentication in Wireless Bio Sensor Network “, ‚International Journal of pharma and bio sciences Abbas, M. Merabti, and D. Llewellyn-Jones, 2010 „Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks,‟ in Proc. WD IFIP, pp. 1–6.

6. Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, 2009 „Sybil Nodes Detection Based on Received Signal Strength Variations within VANET", International Journal of Network Security, Vol.9, No.1, PP.2233
7. Sangeeta Bhatti*, Prof Meenakshi Sharm A Novel Algorithmic Approach for Detection of Sybil Attack in MANET, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 5, issue 5, 2015.
8. Wenyu Zang "Detecting Sybil Nodes in Anonymous Communication Systems," International Conference on Information Technology and Quantitative Management, Elsevier 2013.
9. R. Vintoh kumar, "Cluster Based Enhanced Sybil Attack Detection in MANET through Integration of RSSI and CRL" International Conference on Recent Trends in Information Technology, IEEE 2014.
10. Sarosh Hashmi, John Brooke, "Towards Sybil Resistant Authentication in Mobile Ad hoc Networks," Fourth International Conference on Emerging Security Information, Systems and Technologies, IEEE 2010
11. Zolidah Kasiran and Juliza Mohamad, "Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV" in Conf. Rec. IEEE 2014.
12. Challenges and Surveys in Key Management and Authentication Scheme for Wireless Sensor Networks" in Abstract of Emerging Trends in Scientific Research 2014– 2015.
13. "Teleimersion" Research Journal of Pharmaceutical, Biological and Chemical Sciences on March – April 2016 issue.
14. Somnath Sinha, Aditi Paul, and Sarit Pal, "The Sybil Attack in Mobile Adhoc Network: Analysis And Detection" in Conf. Rec. IEEE 2013
15. Himika, "Enhanced Lightweight Sybil Attack Detection Technique," 5th International Conference- Confluence, the Next Generation Information Technology, IEEE, 2014.