International Journal of Electrical, Electronics and Computer Engineering **6**(1): 131-138(2017)

ISSN No. (Online): 2277-2626

Exposure and Avoidance Mechanism of Sybil Attack in Mobile Ad Hoc Network: A Literature

Pallavi Sharma* and Shruti Dixit**

**Department of Electronic & Communication Engineering, SIRT, Bhopal, (Madhya Pradesh), INDIA*

***Department of Electronic & Communication Engineering, SIRT Bhopal (MP), INDIA,*

(Corresponding author: Pallavi Sharma)

(Received 27 March, 2017 Accepted 28 April, 2017)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Sybil attack is one of the security attacks of MANET which it uses multiple identities or uses the identity of another node present in the network to disrupt the communication or reduce the trust of legitimate nodes in the network. MANET is a self configuring network in which nodes can easily join or leave but it has lack of central coordination or authority and by this characteristic nodes of the network may compromise from various threats such as black hole, wormhole, byzantine attack etc. In this paper, literature about the Sybil attack detection and prevention scheme is presented.

Keywords: Authority, Black hole, MANET, Sybil attack, Wormhole

I. INTRODUCTION

MOBILE Ad hoc Networks are attacked more than wired networks because of their dynamic and versatile nature. MANET is a decentralized network there is no proper mechanism for verification of identities of nodes, so there is huge chance of malicious nodes to intrude in the network while hiding their identities and act on behalf of neighboring nodes, thus leaks important information and make information sharing between nodes harmful and risky for the network.

The mobile ad hoc network No standard specification describing how ad hoc node should auto-configure IP address and undergo DAD. For standalone MANET, there is Lack of any pre-established address or prefix allocation agency, a node may leave/join network and/or randomly change its neighborhood, protocol solutions may involve multi-hop forwarding to a node that has no established IP address and no DHCP like relay etc. Due to these characteristics mobile ad hoc network get compromised from severe types of threats

Sybil attack like other harmful attacks in MANETs may cause real damage to the network. Sybil nodes send fake information about itself to other nodes in the network, get information for other nodes and do not forward it to destination and create misunderstanding between normal nodes [1].

. Thus, Sybil attack causes real damage to the trustworthy communication of the network. In this paper we have proposed a Novel mechanism for detecting Sybil attack in MANETs. The nodes in the network perform Hash function on their MAC addresses for detecting Simultaneous Sybil attack and regular comparison of hash ensures the true identity of node in the network. In case of Join and Leave Sybil attack a Sybil node join and then leave network and then again join network with different identity than the proposed technique of Request Threshold validation mechanism ensures to remove the Join and Leave Sybil attack.

A. Security Goals

The following goals must be fulfilled by security algorithm used to detect the attack [2]:

a) Authentication

It means that each and every node, participating in communication must be genuine and legitimate node.

b) Availability

All services should be available all the time to all the nodes for the proper functioning and security of the network.

c) Integrity

It gives the assurance that the data received by the receiver will be same as the data send by the sender.

d) Confidentiality

It means that some data is only accessible by the authorized users.

e) Non-repudiation

It means sender and receiver cannot deny that they didn't send or receive the data.

B. MANET Vulnerabilities

a) Decentralized Administration

The configuration of MANET is not the centralized one. So, the detection and countering of the security attacks becomes difficult as it becomes difficult to monitor this rapidly changing nodal topology over time.

b) Scalability

Mobile ad hoc networks are highly non-scalable networks because of the mobility of the nodes. In such a network security becomes the major of concern. Security mechanism should be easily applicable to both the large and small scale ad hoc networks.

c) Cooperativeness

It is assumed by the routing algorithm of MANET that all the nodes of the network are cooperative and non-malicious. Due to which the malicious attacker can easily become part of the network and can halt the activities of the network.

d) Dynamic Topology

The topology of the MANET is highly dynamic in nature, that is, nodes of the network are free to join or leave the network. This disrupts the trust relationship among the nodes by compromising the security of the network.

e) Limited Power Supply

Nodes of ad hoc network work in a very selfish manner when there is very limited power supply. Mechanisms should be employed to security from security threats and improving the power consumption.

f) Resource availability

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism [3].

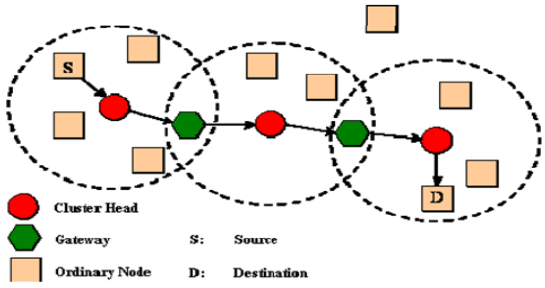

Fig. 1. Architecture of Mobile ad hoc network.

Here fig.1 shows the architecture of mobile ad hoc network which is an infrastructuless. In this paper we mainly focus the literature study about the Sybil attack in MANET.

II. ATTACKS IN MANET

Malicious and selfish nodes are the ones that fabricate attacks [28] against physical, link, network, and application layer functionality.

Current routing protocols are exposed to two types of attacks:

- Active attacks
- Passive attacks

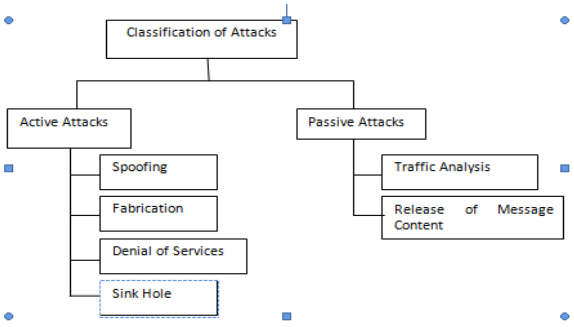

Fig. 2. Classification of Attacks in MANETs.

A. Active Attacks

Spoofing, Fabrication, Denial of Service, Sinkholes, Sybil Attack Eavesdropping, traffic analysis, monitoring Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. These attacks can be classified into further following types:

1. Spoofing: Spoofing occurs when a malicious node misrepresents its identity in order to alter the vision of the network topology that a benign node can gather [29].

2. Fabrication: The notation "fabrication" is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbour can no longer be contacted [5].

3. Denial of Service: This active attack aims at obstructing or limiting access to a certain resource. The resource can be a specific node or service or the whole network. The nature of ad-hoc networks, where several routes exist between nodes and routes are very dynamic gives ad hoc a built-in resistance to Denial of Service attacks, compared to fixed networks.

4. Sinkholes: In a sinkhole attack, a compromised node tries to attract the data to it from all neighbouring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighbouring nodes. Sinkhole attacks can also be implemented on Adhoc networks such as AODV by using flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate. The problem of sinkhole attack can be much.

B. Passive Attacks

In passive attacks the attacker does not perturb the routing protocol, instead try to extract the valuable information like node hierarchy and network topology from it. Passive attack is in nature of eavesdropping on, or monitoring of, transmission. The goal of opponent is to obtained information that is being transmitted [5]. Passive attacks are very difficult to detect because they do not involve any alteration of data.

1. Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information.

2. Release of message content: A telephonic conversation, an E-mail message or a transferred file may contain confidential data. A passive attack may monitor the contents of this transmission.

III. SYBIL ATTACK OVERVIEW

Malicious nodes in a network may not only impersonate one node, they could take up the identity of a group of nodes, and this attack is called the Sybil attack. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from point A to point B. A consequence of this is that attackers have harder time to destroy the integrity of information. However, if a single malicious node is able to represent several other nodes, the effectiveness of these measures is significantly degraded.

The attacker may get access to all the data or may alter all packets in the same transmission so that the destination node/s cannot detect the change in packets anymore. In trust-based routing environments, representing multiple identities can be used to deliver fake recommendations about the trustworthiness of a certain party, hereby attracting more traffic to it; in ideal starting point for further attacks. Amplified if, the malicious node exists within or around the centre of the network so that it hears every communication happening inside the network. However, in the case of Multipath protocols which send data redundantly, not relying on one path only, the problem of sinkholes can be reduced. Probabilistic protocols which measure the trustworthiness of a network can help detecting sinkholes within the network.

Our methods will also work on disruption tolerant networks (e.g., [3]), however, just as such networks incur an extreme routing delay, there will be a corresponding large delay in successful sybil attack detection. Secured ad hoc networks can be classified into three broad groups, each of which can be susceptible to the Sybil attack.

• PKI-based protocols. Much of the initial work in ad hoc network security focuses on secure routing [4, 5, 6] A variety of protocols have been proposed to counter routing attacks, some of which require a central authority or other mechanism to distribute cryptographic material to nodes in the system prior to or during deployment. Systems involving a central authority are less flexible, and installing a central authority removes the chief advantage of ad hoc networks: the ability to form spontaneously from whatever nodes are available. Allowing nodes to join without pre-distributing keys leaves a potential Sybil attack.

• Threshold-based protocols. To avoid the untenable requirement of a PKI, other protocols use threshold cryptography. In such scheme, a group of trusted nodes distributes cryptographic material only if a subset of that group agrees on the trustworthiness of new members. Sybil attackers can additionally defeat schemes that rely on threshold cryptography because verifying the true number and independence of nodes in the network is difficult. If a Sybil attacker can generate identities to meet the threshold requirements it can effectively control the routing of the network.

• Reputation Schemes. Other security mechanisms for ad hoc networks include protocols for determining and maintaining reputation information about nodes in the group. Each node can develop trust in the other nodes that it believes are routing correctly. The Sybil attack undermines these protocols because a node can use multiple identities to falsely vouch for or otherwise support an identity that would otherwise gain a bad reputation.

A reliance on cryptographic certificates or keys does not prevent the Sybil attack in general because one entity may be in possession of multiple keys. For example, if PKI credentials are simply purchased (e.g., through VeriSign), the PKI is reduced to a resource test of each identity's wealth, which can be without bound. Unfortunately, implementing a stronger approach is problematic. This is because in practice it is untenable to create a foolproof system that can scale to a significant number of users to check identities for independence before the keys are issued. Deploying foolproof systems touches on issues including physical security and attacks involving social engineering or physical force. It would require checking a person against some set of unforgeable documents; but even government issued documents are forged regularly.

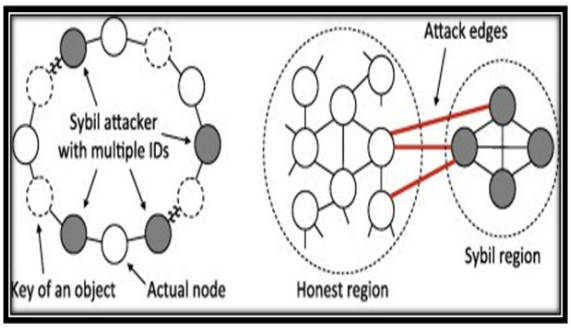

Fig. 2. Architecture of Sybil Attack in MANET.

IV. LITERATURE SURVEY

So many researchers have proposed the security mechanism against attacks. The most recent research in field of Sybil attack is discussed in this section.

Author/ researchers	Description
Ira Nathand and Rituparna Chaki [8]	SYBIL attack is single variety of direction finding exasperating assaults and can convey awesome harm to all groups of a MANET. Security buildups a major stand up to for these system because of their facial development of open medium, effectively changing topologies, and property without base. As an outcome, a trained calculation to notice SYBIL assault is vital. This paper proposes and assesses procedure for recognizing SYBIL assaults and create reliable and protected bury bunch steering in remote impromptu network.
Shehzad *et al.* [9]	Proposed a Novel mechanism is proposed that ensures the detection of both Simultaneous Sybil attack and Join and Leave Sybil attack in the network. The proposed mechanism in two sections Hash Function Mechanism for detecting Simultaneous Sybil attack and Request Threshold validation Mechanism for join and leave Sybil attack. The proposed hash function mechanism for the detection of Sybil attack solves the drawback of lacking central authentication in the network. Request Threshold validation mechanism do not allow nodes to compromise its identity in the network
Pareek and Sharma [10]	Implemented the Sybil Attack using MAC address to detect the Sybil nodes in the network and also prevent it. Simulation tool used for the implementation is NS2.35. The comparative analysis is done using throughput and packet delivery ratio performance metrics.
Soyoung Park [11]	In this paper author gives a timestamp series approach that defend to Sybil attack in a vehicular ad hoc network (VANET) based on RSUs. In this approach RSUs are the only components which issue the certificates neither it require dedicated vehicular public key infrastructure for individual vehicles, nor additional setup. This approach makes it an economical solution which very much suitable for the starting stage of VANET.
Sushmita Ruj [12]	In this paper author proposed the concept of Misbehavior Detection Schemes (MDS) to detect false messages and misbehaving nodes by observing their actions after sending out the messages. In the data-centric MDS, each node is to decide whether received message is correct or fake. Decisions of majority are not needed but the decision is based on the consistency of recent messages. When the attacker node is detected, fine is imposed on that node and not revoking identity of that node. By this scheme computation and communication costs have been reduced that were involved in revoking identity of attacker node.

Author/ researchers	Description
Jain and Nigoti [13]	Proposed the Sybil Detection and Prevention (SDP) against Sybil attack. The property of this attack is to reply with every neighbors through multiple recognition (MR) value of itself i.e. fake identity, fake generated specification of itself in dynamic network. The SDP is able to find routes that deviates from these compromise nodes and provides secure path in between source to designation. The SDP has detected the malicious nodes and capture the malicious information of MR value generated in MANET. The better routing performance is devalued through performance parameters such as throughput and packets drop. The proposed scheme is improves throughput, minimizes data loss and provides secure routing
Liang Xiao *et al.* [14]	Proposed Channel-Based scheme for Sybil attacks Detection in Wireless Networks. To detect Sybil attacks analysis done on enhanced physical-layer authentication method, employing the spatial instability of radio channels in environments with rich scattering, as is ordinary in indoor and urban environments. A hypothesis test is build to detect Sybil clients for both narrowband and wideband wireless systems, like Wi-Fi and WiMax systems. Based on the existing channel estimation mechanisms, this method can be easily realized with low overhead
Piro *et al.* [15]	Showed that mobility can be used to enhance security. Specifically, showed that nodes that passively monitor the traffic in the network which can detect a Sybil attacker that uses a number of network identities simultaneously. We show through simulation that this detection can be done by a single node, or that multiple trusted nodes can join to improve the accuracy of detection. They then showed that although the detection mechanism will falsely identify groups of nodes traveling together as a Sybil attacker, we can extend the protocol to monitor collisions at the MAC level to differentiate between a single attacker spoofing many addresses and a group of nodes traveling in close proximity.
Kumar *et al.* [16]	Proposed system works considering the Certification Authority as one parameter and RSSI as the other parameter. The RSSI is used to form the cluster and to elect the cluster head. The CA's responsibility is given to the CH. Whenever huge variations occur in RSSI on neighbour's entry and exit behaviour, the Certification Authority comes into play. The CA checks the certification of a node. If it is not valid, its certificate is revoked otherwise it is free to communicate in the network
Wei Wei *et al.* [17]	Proposed the approach called Sybil defender for social network. This approach is based on performing a limited number of random walks within the social graphs. Conducting the experiment of the real world topologies, researchers claimed that this strategy is the most efficient and effective in order to identify the Sybil node and Sybil communities around the Sybil node. Also this strategy is useful in limiting the attacking edges in online social networks by relationship rating

V. SYBIL ATTACK DETECTION MECHANISM

This section describes different Sybil attack detection technique:

A. Foot Printing Mechanism

This is another proposed mechanism [19] for the detection of Sybil attacks in vehicular ad hoc networks based on using the authorized event messages as vehicle trajectory by preserving the privacy of vehicles in the network. The detection mechanism is carried out by the vehicle and the road side unit which act as a conversation holder by transmitting the messages among the vehicles.

B. Certificate Issuing Mechanism

This way is used to detect the Sybil entities is issuing certificate to the vehicles. In this approach [18] researches propose to issue the timestamp certificate to the vehicle whenever they pass by a road side unit. This approach does not involve any use of the public key infrastructure and only road side unit are able to generate and issue the certificates. The vehicle after gaining the timestamp certificate can use this for authentication purposes and also to obtains new certificates form the next road side unit.

C. Hash Key Mechanism

Each individual node detects Sybil attackers by validating the Hash received along with message by neighbor, message can be keep alive messages, data transmissions and routing requests or replies [19].

After receiving message node gets Hash of sender and compares it with the previous Hash received in Hello message for the validation of its identity.

If Identity or Hash differs to that of Hash received along with hello message than node is nominated as Sybil and node is blocked from any communication. Thus Hash mechanism detects Simultaneous Sybil attack that tries to obtain multiple identities for incorporating storage, bandwidth or computation of network resources.

D. Lightweight Detection Mechanism

It is used to detect Sybil nodes. It does not require any extra hardware or antennae to implement it. So its cost is very less [20, 21, 22].

1. Distinct Characters of Sybil Attack: It has two characters, one is Join and Leave or Whitewashing Sybil attack and other is Simultaneous Sybil Attack. In Join and Leave or Whitewashing Attack, at a time, it uses its one identity only and discards all its earlier identities. In this, its main purpose is to remove all its previous malicious tasks performed by it. It also increases the lack of trust in the network. In Simultaneous Sybil Attack, at the same time, it uses all its identities. Its main motive is to create confusion and congestion in the network by utilizing more number of resources and make efforts to collect more information about the network.

2. Enquiry Based on Signal Strength: In this step, each node collects the information about the RSS value of neighboring nodes. On the basis of RSS value, distinction can be made between legitimate and Sybil nodes. If the RSS value of the new node which joins the network is low, then that node is considered as legitimate node otherwise it is considered as Sybil node. Each node saves RSS information about neighbor nodes in the form of

<Address, Rss-List <time, rss>>, as displayed in Table1.

3. Exposure of Sybil Nodes: In this, assumption is made that no legitimate node can have speed greater than 10m/s which is called as threshold value or threshold speed [20]. On the basis of speed, RSS value is calculated and if the RSS values of nodes are greater than or equal to threshold value than those nodes are detected as Sybil nodes otherwise as legitimate nodes.

E. Robust Sybil Attack Detection Mechanism

This is another technique used to detect the Sybil nodes. To implement this technique, some methods are required for the correct observation of traffic. These methods are discussed below [23, 24, 25]:

1. Robust Sybil Attack uses the authentication mechanism for the traffic observation. In this, each packet is signed by the sender's private key and also signed by the nodes which are traversed by it to reach the destination and in the end receiver authenticate it by its public key. So, it gives the proof that at what time and location sender sends the packet and in which direction the packet is send by the sender, so that it will reach to the destination.

2. To check the similarity of the path, it uses the novel location based Sybil attack detection mechanism. The nodes whose path is exactly similar to each other are detected as Sybil nodes.

The similarity of the node's path is checked by their overlapping components that how much they are overlapped. The similarity of the path is checked as follows [23]:

$$Sim(L_1, L_2) = \left(\frac{\sum_{i=1}^{k} T_{bobi}}{\max\left(T_{obs1}, T_{obs2}\right)}\right) * \left(\prod_{i=1}^{j} \frac{T_{coi}}{T_{bobi}}\right)$$

HereL1, L2 are nodes

T_{obs1}= It is a duration when each node is observed.

T_{bobi}= It is a duration when both nodes are observed in the observation table.

Tcoi= It is a duration when both nodes are observed at the same time and they co-exist in same area.

j= It is the number of times when both nodes are observed commonly. The first part of equation $\frac{\sum_{i=1}^{k} T_{bobi}}{\max\left(T_{obs1}, T_{obs2}\right)}$ is used to calculate that till what time both nodes are observed commonly and second part of equation $\prod_{i=1}^{j} \frac{T_{coi}}{T_{bobi}}$ is used to determine the overlap region of the nodes.

F. Authentication and Public Key Mechanism

Detecting Sybil attacks based on this approach have been a focal point of many research works. It is an understandable that using authentication mechanism and keys are the best and only approach that can fully eliminate Sybil attacks [18]. But since Public Key Infrastructure is heavy and could be complex solution, it is difficult to implement and sometimes considered unrealistic approach towards the detection of Sybil attacks n Vehicular ad hoc networks.

More time is consumed and message size is significantly increased Public key encryption or message authentication systems which intern increases the memory requirement for such approach.

G. Resource Testing

In this approach [26], various tasks are distributed to all identities of the network in order to test the resources of each node and to determine whether each independent node has sufficient resources to accomplish these tasks. These tests are carried out to check the computational ability, storage ability and network bandwidth of a node. A Sybil attack will not possess a sufficient amount of resources to perform the additional tests imposed on each Sybil identity. The drawback of this approach is that an attacker can get enough hardware resources, such as storage, memory, and network cards to accomplish these tasks.

H. Trusted Certification

It is considered to be one of a good preventive solution for Sybil attacks [27] in which a centralized authority is employed for establishing a Sybil-free domain of identities. Each entity in the network is bound to a single identity certificate. Douceur offers no method of ensuring such uniqueness, and in practice it must be performed by a manual or in-person process. This may be costly or create a performance bottleneck in large-scale systems. Moreover, to be effective, the certifying authority must ensure that lost or stolen identities are discovered and revoked. However, trusted certification suffers from costly initial setup, lack of scalability and a single point of attack or failure.

VI. CONCLUSION

MANETs is quiet not protected as well as prone to an assort attacks. One of the foremost attacks in MANET is Sybil attack which generates multiple identities to confound other nodes and lessen the trust of legal nodes in the network. Hence there is requirement of a secured protocol which can be capable to swiftly organize and also employ dynamic routing mechanism. Peer-to-peer systems play an ever-increasingly considerable role of our daily life. As, most of the network systems are vulnerable to Sybil attacks. In this paper, concerning security of the network i.e. Sybil attack has been studied. For the detection of Sybil attack in MANET different author proposed various mechanisms but some are effective and efficient to discover the malicious nodes. But in future work, need to develop such mechanism which consumes less resources, hardware, less costly and also enhances the energy level of nodes than the existing mechanism.

REFERENCES

[1]. J. R. Douceur. The Sybil Attack. In International Workshop on Peer-to Peer Systems, March 2002.

[2]. Loay Abusalah, Ashfaq Khokar, and Mohsen Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols," *IEEE Communication Surveys & Tutorials,* Vol.**10**, No.4, pp.78-93, 2008.

[3]. J. Burgess, B. Gallagher, D. Jensen, and B.N. Levine. Maxprop: Routing for vehicle-based disruption-tolerant networks”, *In Proc. IEEE INFOCOM*, April 2006.

[4]. Y. Hu and A. Perrig “A Survey of Secure Wireless Ad hoc Routing”, *IEEE Security & Privacy*, **2**(3): 28–39, May/June 2004.

[5]. Y. Hu, A. Perrig and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks. In Proc. Intl Conference on Mobile Computing and Networking, Sep. 2002.

[6]. Y. Hu, D. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks. In Proc. Workshop on Mobile Computing Systems and Applications, Jun. 2002.

[7]. Piyush Agrawal, R. K. Ghosh and Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks, 2nd International Conference on Ubiquitous Information Management and Communication, pp. 310–314, (2008).

[8]. Nath, Ira, and Dr Rituparna Chaki. "BHAPSC: A New SYBIL Attack Prevention System in Clustered MANET." *International Journal of Advanced Research in Computer Science and Software Engineering* 2.8 (2012): 113-121.

[9]. Danish Shehzad, Dr. Arif Iqbal Umar, Noor Ul Amin, and Waqar Ishaq “A Novel Mechanism for Detection of Sybil Attack in MANETs”, *International conference on Computer Science and Information Systems* (ICSIS’2014) Oct 17-18, 2014 Dubai (UAE), *In proceeding of IEEE.*

[10]. Anamika Pareek, Mayank Sharma “Detection and Prevention of Sybil Attack in MANET using MAC Address”, *International Journal of Computer Applications* (0975 – 8887) Volume **122** – No.21, July 2015.

[11]. Soyoung Park, Baber Aslam, Damla Turgut and Cliff C. Zou,’ Defense Against Sybil Attack In Vehicular Ad Hoc Network Based On Roadside Unit Support, Springer Science, Business Media. 2010.

[12]. Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, “On Data-centric Misbehavior Detection in VANETs”, International journal of Network Security& its applications, 2011

[13]. Priya Jain, Rashmi Nigoti “A Novel Technique for Sybil Attack Detection and Prevention in MANET”, *International Journal of Computer Applications* (0975 – 8887) Volume **130** – No.9, November 2015.

[14]. Liang Xiao, Larry J. Greenstein, Narayan B. Mandayam, “Channel-Based Detection of Sybil Attacks in Wireless Networks” *IEEE Transactions on Information Forensics and Security*, Vol. **4**, No. 3, September 2009.

[15]. Chris Piro, Clay Shields ; Brian Neil Levine "Detecting the Sybil Attack in Mobile Ad hoc Networks", Securecomm and Workshops, Proceeding of IEEE 2006 Page(s):1 – 11.

[16]. R. Vintoh Kumar, P. Ramesh , H. Abdul Rauf "Cluster based enhanced Sybil attack detection in MANET through integration of RSSI and CRL", International Conference on Recent Trends in Information Technology (ICRTIT), 2014 Page(s):1 – 7.

[17]. Wei Wei, FengyuanXu, Chiu C. Tan and Qun Li "SybilDefender: A Defense Mechanism for Sybil Attacks in Large Social Networks" *IEEE Transaction On Parallel And Distributed Systems*, Dec. 2013. Vol. **24**, P. 2492-2502.

[18]. Nidhiya Krishna "Detection and Prevention of Sybil Attack in Networks", *International Journal of Engineering Science and Computing,* April 2016, Volume **6** Issue No. 4 ISSN 2321 3361.

[19]. K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.

[20]. Sohail Abbas, MadjidMerabti, David Llewellyn-Jones, and KasifKhifayat,``Lightweight Sybil Attack in MANETs," IEEE System Journal , Vol.7, No.2, pp.236-248, June 2013.

[21]. J. R. Douceur, "The Sybil Attack", presented at the Revised Papers from the first Int. Workshop on Peer-to-Peer Systems, 2002 pp.251-260

[22]. J. Wang, G. Yang, Y. Sun and S. Chen "Sybil Attack Detection Based on RSSI for Wireless Sensor Network ", In Proc. WiCom, Sept, 2007.

[23]. Athichart Tangpong, George Kesidis, Hung-yuan Hsu, Ali Hurson,`` Robust Sybil Detection for MANETs "In proc. Of 18th International Conference on Computer Communications and Networks: IEEE, pp.1-6, 2009.

[24]. T. Zhou, R. R. Choudhury, P. Ning and K. Chakrabarty``Privacy –Preserving detection of Sybil attacks in vehicular ad hoc networks " In Proc. MobiQuitous, Philadelphia, 2007.

[25]. C Piro, C. Shields, and B. N. Levine ``Detecting the Sybil attack in mobile ad hoc networks " In Proc. IEEE/ACM Secure Comm, August, 2006.

[26]. H. Liming, L. Xiehua, Y. Shutang, and L. Songnian, "Fast authentication public key infrastructure for mobile ad hoc networks based on trusted computing," in Proc. Int. Conf. WiCOM, 2006, pp. 1–4.

[27]. Brian Neil Levine, Clay Shields, N. Boris Margolin," A Survey of Solutions to the Sybil Attack," Dept. of Computer Science, Univ. of Massachusetts, Amherst Dept. of Computer Science, Georgetown University.

[28]. "TEMPORALLY-ORDERED ROUTING

[29]. ALGORITHM"http://en.wikipedia.org/wiki/Temporallyordered_routing_algorithm.

[30]. Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2010.