International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Cluster Based Sybil Attack Detection in MANET By Using RSS

Omar Badeea Baban[1]

[1] *Department of Computer Engineering*
Sinhgad College of Engineering, Pune-41, Pune, (India)

ABSTRACT

Security is the most important service for all kind of network communications. MANET should provide security that increases people's confidence on MANET. Due to the broadcast nature of wireless channel, MANET has many security issues. Especially, Sybil Attack is a very serious threat to the MANET as it creates multiple virtual fake identities per entity, there by affecting the routing table. The multiple virtual identities are obtained by spoofing the victim's node or by creating an arbitrary node as there is no restriction to create an arbitrary node in MANET. Therefore, the Sybil attacks have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect Sybil attacks and eliminate them from the network. Received Signal Strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc networks. However, the traditional technique requires Geographical Positioning System (GPS) and hardware like antennas, so the cost of the initial setup is very high. This proposed scheme describes differentiation of legitimate user and illegitimate user or Sybil attacker even in the high mobility because, now a days the QOS is necessary in the network.

In particular, this scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities, this system works considering the RSS as one parameter and the Certification Authority as the other parameter. The RSS 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 neighbor's entry and exit behavior, 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.

Keywords Mobile Ad hoc Network, Received Signal Strength, Cluster Authority, Certification Head, Certificate Revocation list, Certificate Trust List, False Positive Rate, True Positive Rate, Sybil Attack.

I. INTRODUCTION

1.1 Motivation

MOBILE ad hoc network (MANETs) is an autonomous collection of mobile devices connected in a peer to-peer or multi-hop fashion without use of any centralized base station or access point. In this, each and every mobile devices acts as a router to forward the packets when the source and destination are within the radio range. If the source and the destination are in the same radio range, then they can communicate with each other without the use of any other nodes and temporary ad hoc network topologies. The mobile ad hoc networks are useful where no pre-existing infrastructure exists, for example disaster recovery environments, military combat

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

applications and Wireless Personal Area Networks, The unique characteristics of MANETs, dynamic topology and resource constraint devices, pose a number of nontrivial challenges for efficient and lightweight security protocol design. Due to the lack of centralized identity management in MANETs, it is more vulnerable to several types of attacks such as Sybil attack which will create multiple virtual identities. For example, communications in wireless networks are usually based on a unique identifier that represents a network entity. Node's identities are used as an address to communicate with a network entity. This forms a one-to-one mapping between an identity and an entity. Usually, the identity is assumed either implicitly or explicitly by many protocol mechanisms; hence two identities imply two distinct nodes. Unfortunately malicious nodes can illegitimately claim multiple identities and violate this one-to-one mapping. Douceur [4] termed this as a Sybil attack, in which an attacker manages to create and control more than one identity on a single physical device.

A Sybil attacker can cause damage to the ad hoc networks in several ways [13]. For example, a Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or paths. In reputation and trust based misbehavior detection schemes, a Sybil node can disrupt the accuracy by increasing its reputation or trust and decreasing others' reputation or trust by exploiting its virtual identities. In wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic.

The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. On the other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc networks. However, the traditional technique requires Geographical positioning system and Hardware like antennas, so the cost of the initial setup is very high. This paper describes, differentiation of legitimate user and illegitimate user or Sybil attacker even in the high mobility because, now a days the QOS is necessary in the network. This proposed scheme detects Sybil identities and legitimate identity even in high mobility. In particular, proposed scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities. First, we demonstrate the entry and exit behavior of legitimate user and Sybil user using simulation and real world test bed experimentation. Second, the threshold is defined to distinguish between the legitimate node and the Sybil node based on nodes' entry and exit behavior. Third, the threshold is detected by the getting average of all the nodes received signal strength values.

1.2 Definitions of MANET

A Mobile Ad-hoc Network (MANET) is a collection of several electronic devices equipped with wireless communication and networking capabilities. These types of networks do not possess any permanent infrastructure or physical backbone. The mobile nodes in the network dynamically set up paths among themselves to transmit packets to the destination. Due to the mobility of the nodes MANETs should have some characteristics which make them distinguishable from conventional wired and wireless network. MANETs are self-organizing and adaptive in nature which means that the nodes are spontaneously forming and deforming the

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

network and updating the routing table associated to each node. In MANET communication starts between the nodes within each other's wireless transmission ranges by broadcasting control messages between themselves directly. However, nodes beyond each other's range have to rely on some other nodes to relay messages. Control message can carry node address, global position information etc. The mobile nodes frequently change their positions inside MANET causing frequent topology change. This change in topology should be incorporated so as to keep the routing table updated in each node inside MANET to avoid communication error like link failure etc.

Moreover, due to the flexibility of MANET, new nodes can enter into the network as well as the existing node may leave the network any time which also causes changes in network topology and routing table and hence requires link modification. [14]

Mobile ad hoc networks (MANETs) are shown in figure1.1, with four nodes in the wireless coverage area. It is a type of wireless networks that are self-organized and dynamically reconfigurable with no infrastructure or no fixed base stations. MANETs are characterized by dynamic topologies, bandwidth-constrained, variable capacity links and energy constrained operation. [1]

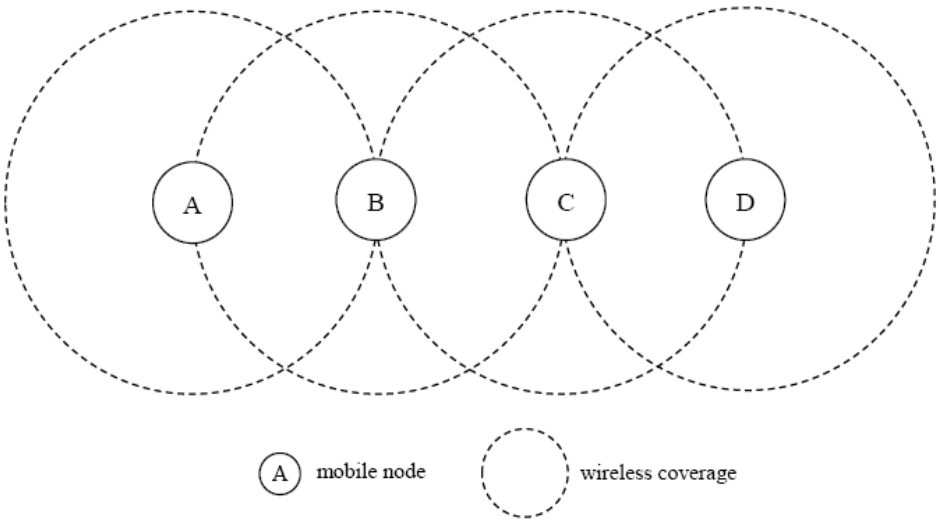

Fig.1.1 Mobile Ad-hoc Networks [1].

Link-Clustered Architecture scheme is provided in figure 1.2, it is characterized by:

- Reduces interference in multiple-access broadcast environment.
- Distinct clusters are formed to schedule transmissions in a contention-free way.
- Each cluster has a cluster head, one or more gateways and zero or more ordinary nodes.
- Cluster head schedules transmission and allocates resources within its cluster.
- Gateways connect adjacent clusters.

To establish link-clustered control structure:

1. Discover neighbors.
2. Select cluster head to form clusters.
3. Decide on gateways between clusters.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

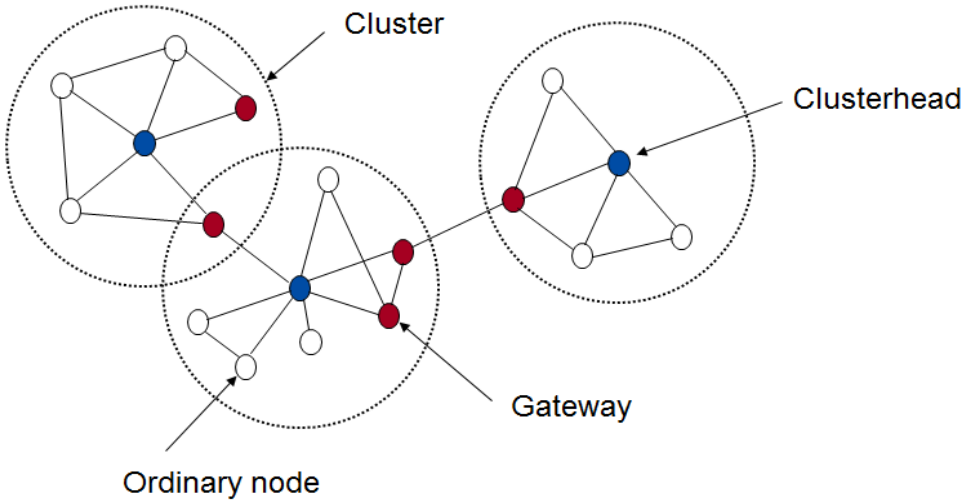

Fig.1.2 Link-Clustered Architecture [3].

Cluster heads

– Resemble base stations in cellular networks, but dynamic.
– Responsible for resource allocation.
– Maintains network topology.
– Acts as routers – forwards packets from one node to another.
– Aware of its cluster members.
– Aware of its one-hop neighboring cluster heads.

1.3 Why Security in MANET

The nodes in MANET have limitation in resources such as battery capacity, bandwidth, CPU capacity, storage capacity etc., which cause MANET to face some typical challenges. Moreover mobility of nodes and channel vulnerability cause problems in signal transmission, channel access, routing including packet loss, route change, increase in control traffic etc.

Limited battery power is another crucial challenge in MANET because battery technology is not progressing as fast as memory or CPU technology. In MANET wireless transmission routing, retransmission, beaconing consume more power. All these emerging challenges due to inherent characteristics of MANET are creating significant aspects of researches which include:

- Performance criteria.
- Variations in routing protocol.
- Traffic characteristics.
- Mobility models.
- Variations in capabilities and responsibilities.

Challenges of MANET lead to security issues which include:

➢ Routing security.
➢ Data forwarding security.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

- Link layer security.
- Key management.
- Intrusion detection and so on.

To maintain reliable communication in MANET five major security goals need to be considered. These are as follows:

Confidentiality: Confidentiality means that message should be kept secret and not to be exposed to any node other than the recipient. In MANET it is hard to keep message confidential because in multi hop communications there are several intermediate nodes in between which can easily snoop the message.

Availability: All the services throughout the network should be available when required so that the communication remains active. It is important in order to survive against any attack.

Authentication: It should be confirmed that all the nodes including the source and the destination nodes are legitimate ones and authenticated, otherwise a malicious node can easily take off the identity of a node and get unauthorized access to the confidential information and Consume resources of the network as well.

Integrity: Integrity means message sent by the source should reach the destination intact i.e. the transmitted message has not been modified and the order of the transmitted message remains unchanged.

Non-repudiation: The sender should not be able to deny that it has transmitted the message and receiver should not be able to deny that it has received the message. [14]

1.4 Attacks in MANET

The mobile Ad hoc Network (MANET) is vulnerable to different kinds of security attacks due to the broadcast nature of the transmission medium. In MANET security attacks can be either external or internal.

(a) External attacks: External attacks are similar to the normal attacks in the traditional wired networks in which the attacker can create congestion in the routing path or relay phony routing information or disturb nodes in providing services.

(b) Internal attacks: In case of internal attack the adversary can directly compromise an existing node and use it to conduct its malicious behaviors or impersonate itself as a new node to get access to the network.

There are several external and internal attacks in MANET which can be broadly classified into two types: Passive attack and Active attack. The figure 1.3 shows the classification of security attacks in MANET.

Passive Attacks

A passive attack does not interrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it.

Active Attacks

In contrast to passive attack an active attack goes to alter or destroy the data being exchanged in the network. It interrupts the normal functioning of the network. Active attacks, either by external means or by an internal compromised node involves actions such as impersonation, modification, fabrication and replication. Different types of attacks in MANET are simplified in table 1.1.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

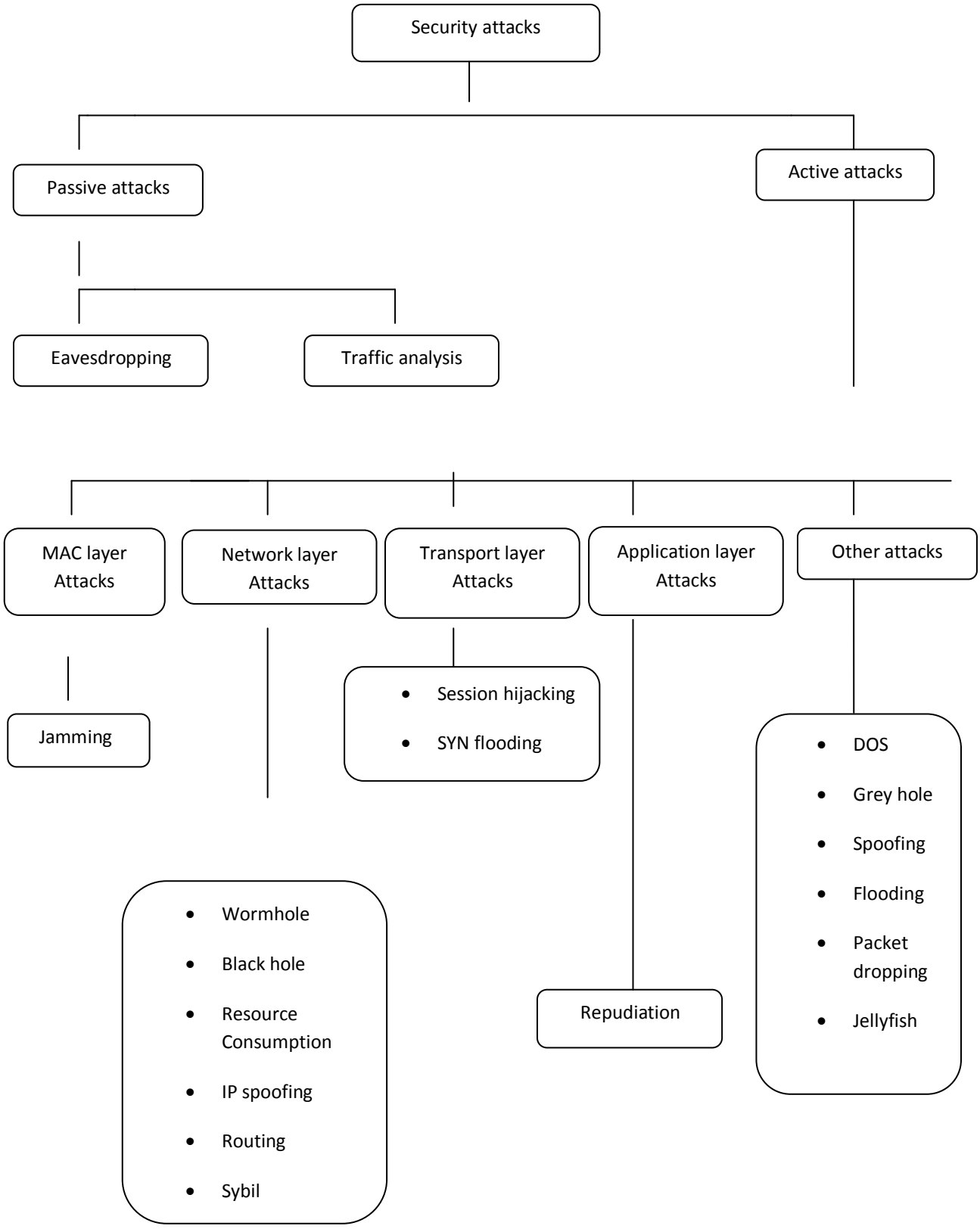

Fig. 1.3 Different types of attacks in MANET [14]

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

ATTACK NAME	ATTACK TYPE	LAYER	ACTIONS	DETECTION MECHANISMS
Black hole Attack	Active Attack	Network Layer	Listens Route Request (RREQ), When Attacker receives RREQ it makes fake route.	PCBHA (Prevention of a Co-operative Black Hole Attack).
Denial of service	Active Attack	Network Layer	Attacker acts like a busy node. So, Receiver has to wait to receive the messages.	Repudiation based incentive mechanism.
Eavesdropping	Passive Attack	Physical Layer	Intercepts and finds secret information.	Encryption mechanisms.
Rushing Attack	Active Attack	Network Layer	Whenever Attacker receives RREQ packet, it floods the packet quickly throughout the network before other nodes.	RAP (Rushing Attack Prevention).
Sinkhole Attack	Active Attack	Network Layer	Attacker sends wrong routing information and receives whole network traffic. Attacker modifies or drops packets.	SAR (Secure Aware Routing).
Sybil Attack	Active Attack	Network Layer	Attacker creates more than one identity for single node.	RSS (Received Signal Strength).
Traffic Analysis	Passive Attack	Physical Layer	Attacker monitors packet transmissions to infer important information's.	Strong Encryption mechanisms.
Wormhole Attack	Active Attack	Network Layer	Remote malicious nodes connect through high speed link and acts like a neighbor's.	Packet Leash.

1.5. Sybil Attack

MANET is a wireless mobile ad-hoc network. Due to its wireless nature it is exposed to several attacks. Among those attacks there is a Sybil attack which very badly ruins the communication among the nodes of the network. The name of the Sybil attack comes from the name of patient i.e. Sybil (Shirley ArdellMarson) who is suffering from multiple disorder personality. The name itself explains the meaning of Sybil attack. Sybil attack is an attack which uses several identities at a time and increases lot of misjudgments among the nodes of a network or it may use identity of other legitimate nodes present in the network and creates false expression of that node in the network. Thus, it disturbs the communication among the nodes of the network. To have secure communication it is necessary to eliminate the Sybil nodes from the network. Therefore, the Sybil attacks have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect Sybil attacks and eliminate them from the network. The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. On the other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc networks. However, the traditional technique requires Geographical positioning system and Hardware like antennas, so the cost of the initial setup is very high. [9]

A Sybil attacker causes damage to the ad-hoc network in several ways. For example, Sybil attacker can disrupt the multipath routing by participating in the routing. Malicious node detection is difficult in the presence of Sybil attacks. In a wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities.

As shown in figure 1.4, C is the malicious node it creates several identities called A, B, D. Identities A, B, C, D refers to the same node but it looks like a four different nodes. [10]

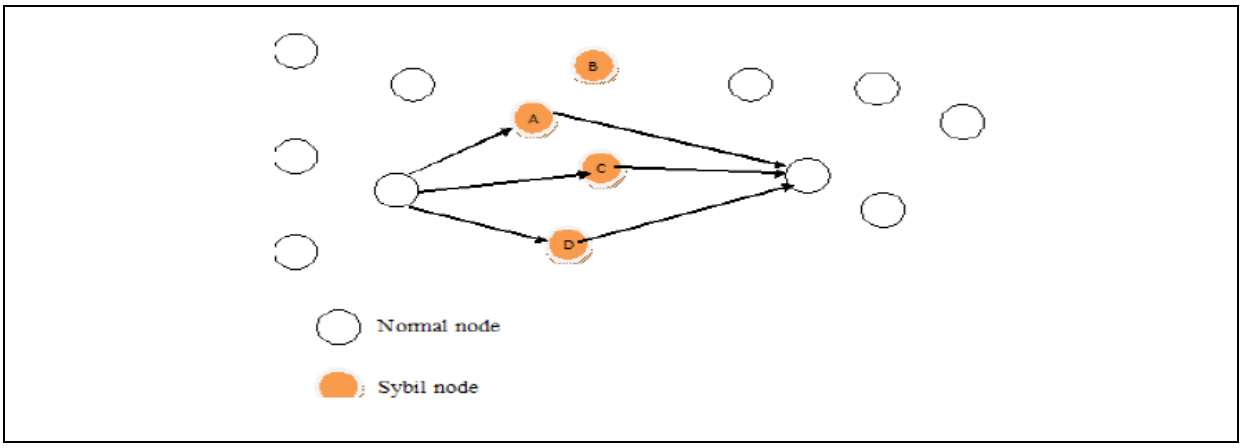

Fig.1.4 Sybil Attack [10].

II. LITERATURE REVIEW

2.1 Literature Detection methods of Sybil Attack

Still now there exists no such well accepted technique to detect the Sybil attack. A number of methods have been proposed associated with different environments. Some of them are effective to reduce the threat to a satisfactory level.

In this section different approaches proposed to prevent and mitigate the attack are discussed and their comparative study is represented (Table 2.1).

me**(i) Trusted Certification:** Trusted certification is one of the most prospective solutions to prevent Sybil attack. It requires one certification authority (CA) that validates the one to one correspondence between the corresponding entities. Douceur has proved that trusted certification has the maximum potential to eliminate Sybil attack completely. This approach may seem to be ideal for handling Sybil attack, but there are a numbers of issues related to implantation of certification authority as well as implementation of entity-identity mapping. Significant overhead and cost also restrict the use of this method. Zhaoyu Liu et al. [16] proposed a dynamic trust model for MANETs that could be used to add a significant measure of trust to the routing process. The proposed approaches do not require accurate time synchronization, complex hash chaining techniques, or authentication systems. They assign trust levels based on the type of threat being created and the reliability of the threat reports.

(ii) Testing of resources: Resource testing is one of the most widely used implemented techniques to defend Sybil attack. The idea behind this approach is the utilization of the resources by the entity. Each entity in the adhoc network has limited resources. A verifier compares the amount of resources utilized by the entity with the typical value of the resources possessed by that entity. Any discrepancy indicates the possibility of Sybil attack. Generally storage of energy, available memory space, computational capability, bandwidth and channel capacity may be considered as resources.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Radio resource testing, proposed by Newsome et al. [8], is an extension of the resource testing verification method for wireless sensor networks. The key assumptions of this approach is that any physical device has only one radio and that this radio is incapable of transmitting and receiving messages on more than one channel at any given time. Resource tests have been recommended by many researchers to detect Sybil nodes rather than to eliminate them altogether. It can also be applied generally to all types of related domains. However, this technique is based on the assumption that each node has only one channel and cannot send and receive simultaneously on more than one channel. Moreover, the testing process may consume a lot of battery power.

(iii) Recurring cost: This method is a variation of resource testing where resource tests are conducted periodically to impose a certain "cost" on the attacker that is incurred for every identity that he controls or introduces into the network. However a number of researches have certified this method and have used computational power in their resource tests.

This in itself may be inadequate in controlling the attack since a malicious user incurs only a one-time cost (for computing resources) that may be recovered via the execution of the attack itself, as pointed out by Levine et al. [7]. An attack is deemed successful only if ratio of the attacker's objective value to the cost per identity exceeds the critical value (the value that exists for a particular combination of application domain and attacker objective). They conclude that using recurring costs or fees per identity is more effective as a deterrent to Sybil attacks than a one-time resource test. The only limitation with this approach is that it requires electronic cash or significant human effort.

(iv) Privilege attenuation: Fong [6] considers a different kind of Sybil attack that aims to create pseudonymous or fake identities in a Social Network System (SNS) and get them to collude to favorably alter the existing trust relationships in the network.

These relationships are represented via a graph-theoretic relationship model that exists between the owner of a resource and a prospective user of the sa resource and is called a social graph. Such models are common in some popular Social Network Systems such as Facebook. When the fake accounts in the SNS collude, they may gain the ability to access personal, sensitive and restricted user information or perform large-scale crawls on the social graph. To counter this threat, Fong has proposed a particular version of Denning's Principle of Privilege Attenuation or POPA that is both a necessary and sufficient condition to thwart such attacks, along with a static policy analysis for verifying POPA compliance.

(v) Incentive –based detection: Margolin and Levine proposed a protocol called Informant that is based on an economic incentive policy that is not specific to any particular application domain. An entity is taken as detective to reward Sybil for revealing themselves. An identity gives the name of the target peer and a security deposit to the detective while the target peer receives the deposit and a certain reward. A Dutch auction is used to establish the minimum reward that will reveal a Sybil node.

(vi) Position verification: The method is confined to wireless ad hoc network. This is based on the fact that the same location in a network should not be occupied by two or more identities simultaneously. The method like triangulation can be used for location verification. Sybil nodes can be identified by this approach because they will appear exactly at same position as the malicious node that generates them. Tangpong et al. [15] have proposed a solution based on the above strategy. However, this technique yields false positive result (i.e. suspects a legitimate node as a Sybil node) in case of high mobility and high density of nodes.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

(vii) RSSI-based scheme: Demirbas and Song [5] proposed a method for Sybil detection based on the Received Signal Strength Indicator (RSSI) of messages. Upon receiving a message the receiver will associate the RSSI of the message with the sender identity, and later when another message with same RSSI but from a different sender is received, the receiver can detect the

Sybil attack. Sybil attacks can be detected with a completeness of 100% with few positive alerts.

However, a Sybil node can transmit message with different identities using different transmission power intensity to defeat this scheme and transmission is also non-isotropic. It also cannot deal with existing Sybil nodes in the network, location calculations are also costly. It is applicable to sensor network only.

(viii) Random key Predistribution: This technique is used in wireless sensor network to establish a secure routing for communicating with each other. A set of key are assigned randomly to a node enabling it to compute the common keys that it shares with its neighbor. Node to node privacy is ensured by using the common keys. The key ideas are the association of the identity with the key assigned to a node and the validation of the key. Validation ensures that the network is able to validate the key. There is a little probability that a forged Sybil identity will pass the key validation test as the keys associated with a random identity are not likely to have a significant intersection with the compromised key set. Another technique mostly used in modern computer communication system, proposed by Carman, Kruus and Matt is asymmetric key distribution which uses the concept of master private/public key. Here each node has one public key of its own verified by the master private key signature. During communication the key exchange procedure is deployed to set up a secure link between the nodes by using the public key and the master public key of each node. though this technique has some advantages with respect to scalability of network, node capturing, revocation of new pair of keys still it has some limitations in terms of node replication, vulnerability to DoS and dependency on cryptographic hardware and software. In pair wise key distribution technique each node shares a unique key with every other node. Again this technique suffers from poor scalability and problem of inserting new nodes. [14]

Table 2.1: Comparative analysis of the techniques to prevent and mitigate the Sybil attack and their disadvantages [14].

Technique to Mitigate Sybil Attack	Disadvantages / Limitations
Trusted Certification	• In a large mobile network, the scalability problem reduces performance efficiency and increases cost in this approach. • In ad-hoc networks the local Certification Authority (CA) server may be multi-hops away from a node and may also move which makes the network complicated and creates problem in tracing a local CA server. • Multi-hop communication over the error-prone wireless channel renders the data transmission to high loss rate. This reduces the success ratio and increases the average service latency. • CA is prone to DoS attacks.
	• Depends on the total number of radio channel available to the nodes. • Testing process require lots of battery power.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Resource Testing	• Simultaneous Sender Test, Optimum Simultaneous Sender Test, and Simultaneous Receiver Test can tolerate as many as colluding nodes in the network. In contrast, Forced Collision Test cannot operate correctly in the presence of colluding nodes.
Recurring Costs	• Requires electronic cash or significant human effort that increases with the increase of total number of identities participating. • One-time fees incur only a constant cost.
Privilege Attenuation	• Incur significant run-time and storage overhead. • When phony accounts in the SNS get together; they may gain the ability to access personal, sensitive and restricted user information. Weakly configured access control policies on SNSes make them susceptible to such attacks.
Economic Incentives	• Applicable to that Sybil attacker who would like to reveal themselves on being paid.
Location/Position Verification	• Gives false positive result in case of high mobility and high density of nodes. • Vulnerable to both internal and external attacks.
Received Signal Strength Indicator (RSSI) – based scheme	• Signal strength varies with distance in the outdoor environment, but not in the indoor environment. In the open outdoor field, as the distance between the sender and the receiver increases, the strength of the signal becomes weaker. However, in the open hallway signal strength does not change with distance. • In the case of long distance, with a small RSSI, it is easy to be affected by surrounding environment, and the fluctuation becomes greater. • Obstructions affect the signal strength
Random Key Predistribution	• Pair wise keys scheme has poor scalability. • The number of keys that must be stored in each node is proportional to the total number of nodes in the network which counts a huge storage overhead. • Addition of new node is challenging. • Key establishment through a base station is not secure as base station becomes a target for compromise.

2.2 Existing methodologies

1.2.1 Lightweight Sybil attack detection in MANETs

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.

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

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

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>>.

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. 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.

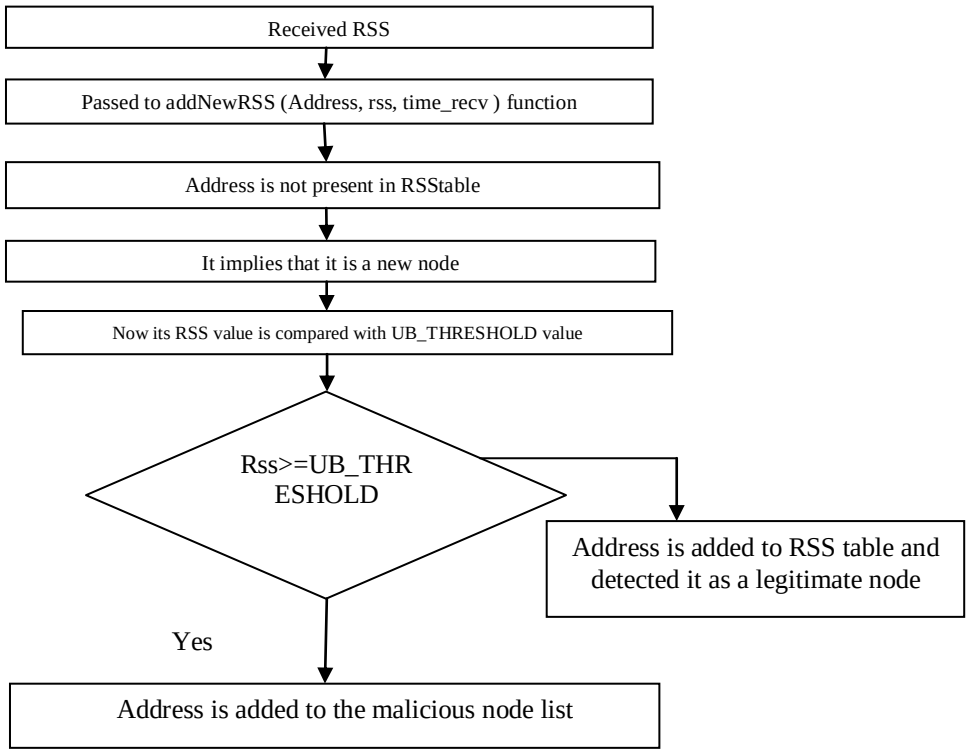

Fig.2.1 Flowchart of Lightweight Sybil Attack Detection Algorithm [11].

Explanation of figure 2.1, the received RSS value of node is passed to the addNewRSS function and then address of that node is checked if it present in RSS table or not, if it does not present in RSS table then node is considered as new node. Now RSS value of new node is compared with the upper bound threshold value, if RSS value of new node is greater or equal to upper bound threshold value then it is detected as malicious node otherwise detected as legitimate node.

2.2.2 Robust Sybil Attack Detection

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:

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

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

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:

$$\text{Sim (L1,L2)} = \left(\frac{\Sigma_{i=1}^{k} T_{bobi}}{\max(T_{obs1}, T_{obs2})}\right) * \left(\prod_{i=1}^{j} \frac{T_{coi}}{T_{bobi}}\right) \quad \text{(Eq. 1)}$$

Here L1, L2 are nodes

Tobs1= It is a duration when each node is observed.

Tbobi= 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 $\left(\frac{\Sigma_{i=1}^{k} T_{bobi}}{\max(T_{obs1}, T_{obs2})}\right)$ is used to calculate that till what time both nodes are observed commonly.

And second part of equation $\left(\prod_{i=1}^{j} \frac{T_{coi}}{T_{bobi}}\right)$ is used to determine the overlap region of the nodes.

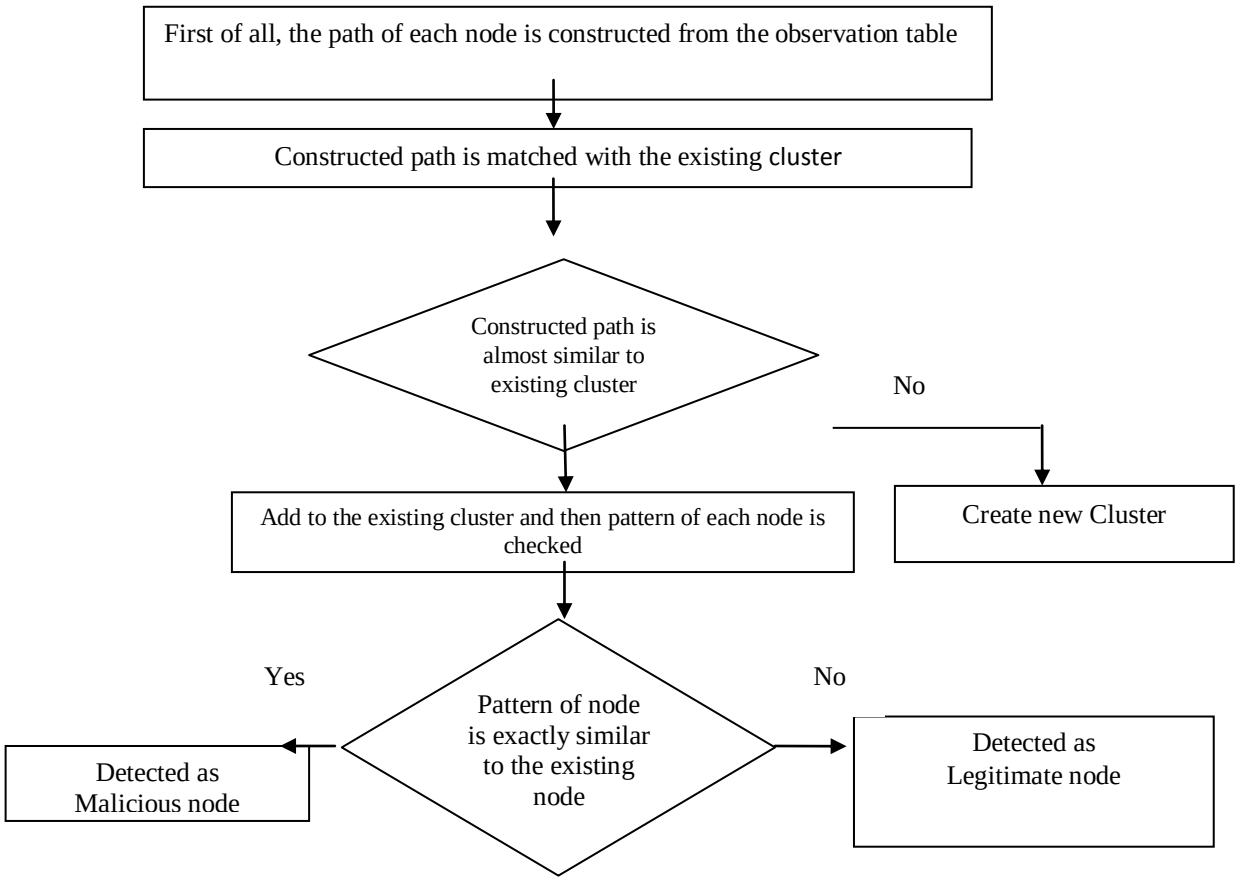

Fig 2.2 Flowchart of Robust Sybil attack detection Algorithm [11].

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

In fig.2.2, firstly the path of each node is constructed from the observation table and then path of each node is matched with the existing cluster. If path of node is almost similar to the existing cluster then add that node in the existing cluster and if path of node is not matched with any cluster present in the network, then new cluster is created for that node. After this the pattern of each node is checked present in almost similar cluster, the nodes having exactly similar pattern are detected as malicious node otherwise detected as legitimate nodes.

2.2.3 MAC address Sybil Attack Detection

In the proposed Architecture for detection of Sybil attack, any node can start the detection for Sybil node. In our case sender node starts detection for Sybil node before it sends packets to the receiver node. Firstly sender node broadcast a request packet which in return wants a reply message which contain logical (IP) address and physical address (MAC).sender nodes maintain a table for that and checks if a node with same physical address reply with different logical address then the node with different logical identity is declared as a Sybil node and the sender node chooses another path for sending packets to destination.

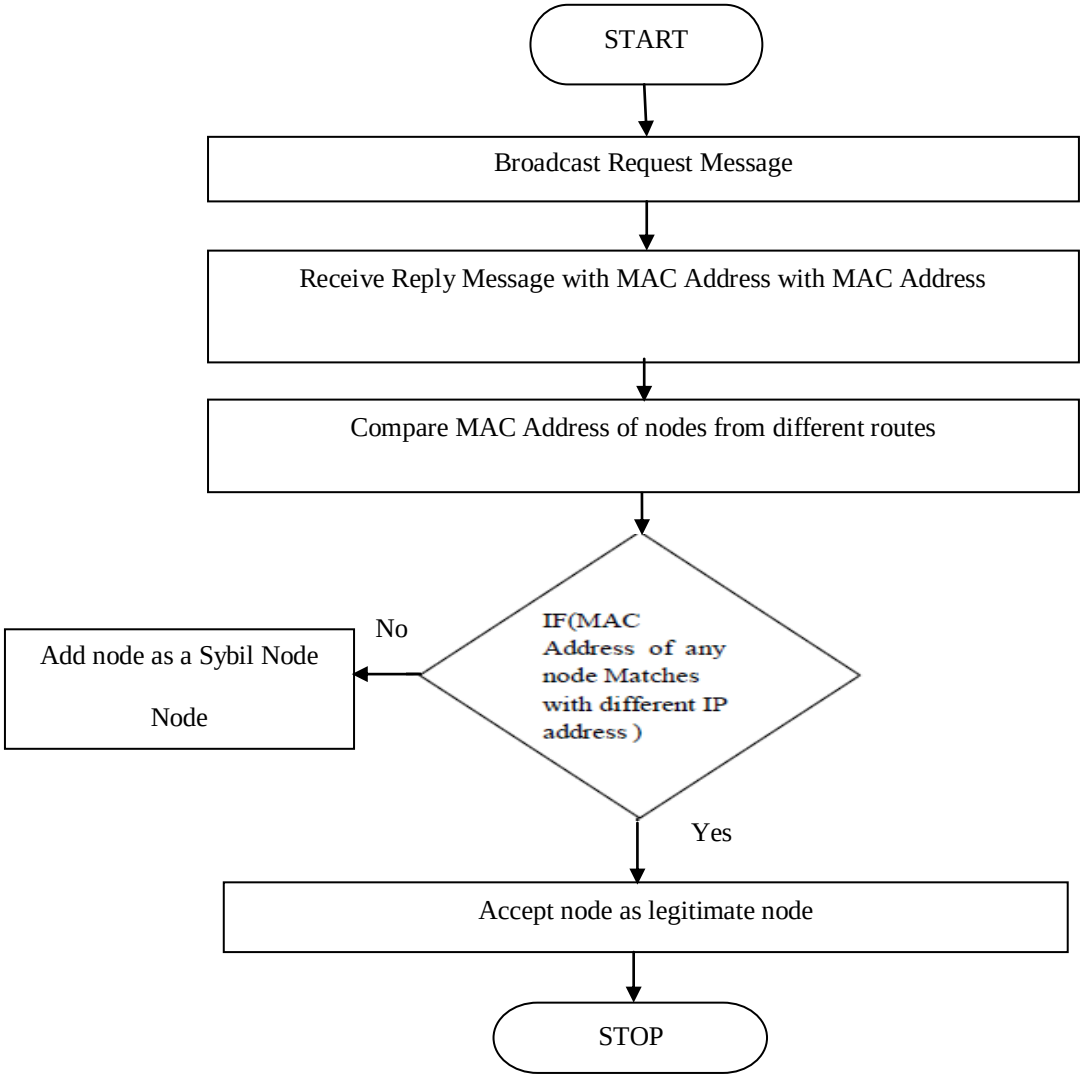

Fig 2.3 Flowchart of MAC address Sybil Attack Detection Algorithm [2].

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

2.3 Comparison of Sybil attack detection techniques

MANET is vulnerable to various attacks due to its infrastructure less or wireless nature. To have safe communication it is must be secure network. There are various attacks in MANET and there is one attack which is very dangerous called Sybil attack, 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.

In this section two techniques are discussed the Lightweight Sybil attack detection algorithm and Robust Sybil Attack Detection Algorithm and Comparison is done between these two techniques. In Robust Sybil attack detection technique; there is requirement of directional antennae to check the location of the nodes, so it is costly whereas in Lightweight Sybil attack detection technique there is no requirement of any extra hardware or directional antennae, therefore it is called as lightweight and it is also cheap in cost than robust technique. Parameters used in robust technique are time and location and parameters used in lightweight technique are RSS and speed. Robust technique, 80% detects the Sybil node as Sybil node and 20% detects the legitimate node as Sybil node whereas lightweight technique, 90% detects the Sybil node as Sybil node and 10% detects the legitimate node as Sybil node. So on the basis of comparison Lightweight Sybil attack detection technique is better than the Robust technique.

Table 2.2: Comparison of Sybil attack detection techniques: Lightweight and Robust [11].

Algorithm	Parameters	Directional Antennae	Cost	Results*	Summary
Lightweight Sybil Attack Detection Technique	Speed, RSS	Not required	Cheap	90% true positive,10% false Negative	The nodes entering in the network with RSS greater than the threshold value are detected as Sybil nodes.
Robust Sybil Attack Detection Technique	Time, Location	Requir ed	Costly	80% true positive,20% false Negative	The nodes having exactly the same path or pattern are detected as Sybil nodes

*True Positive: It detect Sybil node as Sybil node.

* False Positive: It detect legitimate node as Sybil node.

And for the third approach which is depending on the physical address, we can say that MANET is vulnerable to various attacks due to its infrastructure less or wireless nature. To have safe Communication it is must be secure network. There are various attacks in MANET and there is one attack which is very dangerous called Sybil attack, 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. An architecture to detect Sybil nodes have provided to safeguard the network which is depending on the physical address (MAC address) of the nodes, if any node send a reply message to the sender node with the same physical address but with different logical address it is considered as a Sybil node.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

III. PROPOSED METHODOLOGY

The proposed scheme describes, differentiation of legitimate user and illegitimate user or Sybil attacker even in the high mobility because, now a days the QOS is necessary in the network. It detects Sybil identities and legitimate identity even in high mobility. In particular, proposed scheme utilizes the RSS (Received Signal Strength) in order to differentiate between the legitimate and Sybil identities. First, we demonstrate the entry and exit behavior of legitimate user and Sybil user using simulation and real world test bed experimentation. Second, the threshold is defined to distinguish between the legitimate node and the Sybil node based on nodes' entry and exit behavior. Third, the threshold is detected by the getting average of all the nodes received signal strength values. The proposed simulated method shows the true positive range of 95% and false positive rate is reduced to 20% from 30% even in the high mobility than existing one.

3.1 Cluster formation

A Successful dynamic clustering algorithm achieves the stable cluster topology with minimal communication overheads and computational complexity. The efficiency of the algorithm can also be measured by the number of clusters formed.

The main goals of our clustering algorithm are as follows:

1. The algorithm minimizes the number of clusters by group mobility pattern.
2. Network-wide flooding must be avoided.
3. The algorithm must be distributed and executed asynchronously.

Before introducing Mobile D-Hop clustering we have to assume that:

1. Two nodes are connected by the bi-directional links.
2. Networks are not partitioned
3. Every node measures its received signal strength.

The periodic beaconing or hello messages are used in some routing protocols. The mobile nodes are estimates the distance to its neighbor by received signal strengths by participating direct or indirect communication with that particular node. The Transmission equation describes the received power between point to point nodes. This shows the familiar inverse square-law dependence of the received power (Pr) with distance (d). I.e. Pr α 1/d2, the Figure 3.1 illustrates the estimated distance between two nodes from the received signals strength. But it is difficult to calculate the estimated distance between two nodes in real world scenario.

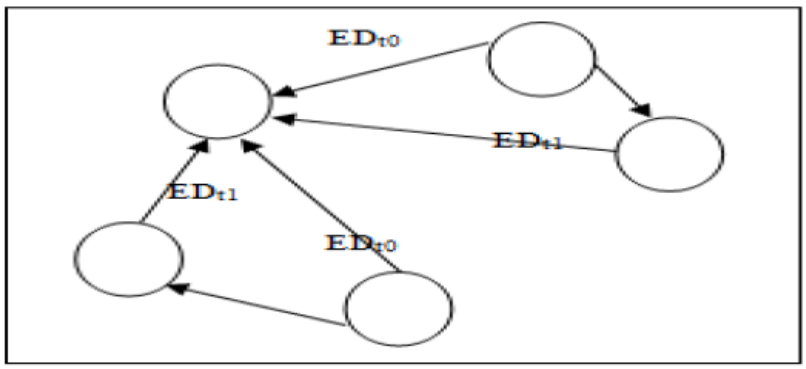

Fig. 3.1 Relative mobility of a node [9].

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

(Eq. 2) $$Pr = \frac{Pt * Gt * Gr * \lambda^2}{4 * \pi^2 * d^2}$$

Where,

Pr – Received Power

Pt – Transmission Power

Gt –Transmission Antenna Gain

Gr –Receiver Antenna Gain

λ – Wavelength

d – Distance between nodes

The proposed cluster scheme does not depend on the estimated distance. But, it depends on the variation of the estimated distance and the received signal strength. Instead we will observe the variation of the received signal strength over a time period‘t’. If the received signal strength between two nodes is high, then the nodes are very close to each other. If the received signal strength between two nodes is less, it indicates that two nodes are far away from each other. If two nodes moving together with a same speed the variation of the received signal strength is very small. So have to form it as a cluster. RSSI is used as a parameter to avoid complex calculations. Measured signal strength of the successive received packet is used to estimate the relative mobility of the node. The relative mobility is calculated by taking difference of the estimated distance with respect to time. The variation shows the relative mobility of the node. The Estimated difference between the mobile nodes are given below,

$$E[D_{pq}] = \frac{K}{\sqrt{P_r}} \quad \text{(Eq. 3)}$$

Relative mobility between two nodes at different time interval t1 and t2,

$$M_{pp} = E[D^{t2}{}_{pp}] - E[D^{t1}{}_{pp}] \quad \text{(Eq. 4)}$$

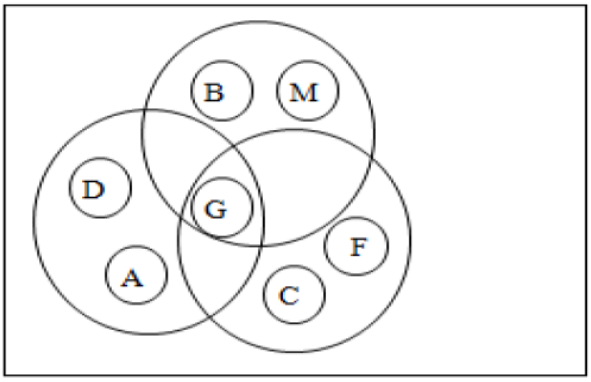

Fig.3.2 Cluster formation based on Mob D Hop [9].

Discovery stage represents the stable links between the nodes after getting received signal strength from successive packets from a particular node on a time intervals of t1 and t2.Merging stage describes the process of

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

joining the new node into the cluster. The Fig. 3.2 shows the model cluster formation. It has two scenarios' one is joining of non-clustered node and the other is the joining of gateway nodes G. The cluster maintaining stage also has two scenarios whenever the node is OFF, the node leaves the cluster and whenever the node is ON, the node joins the cluster. These two scenarios results in the dynamic topology changes in the network.

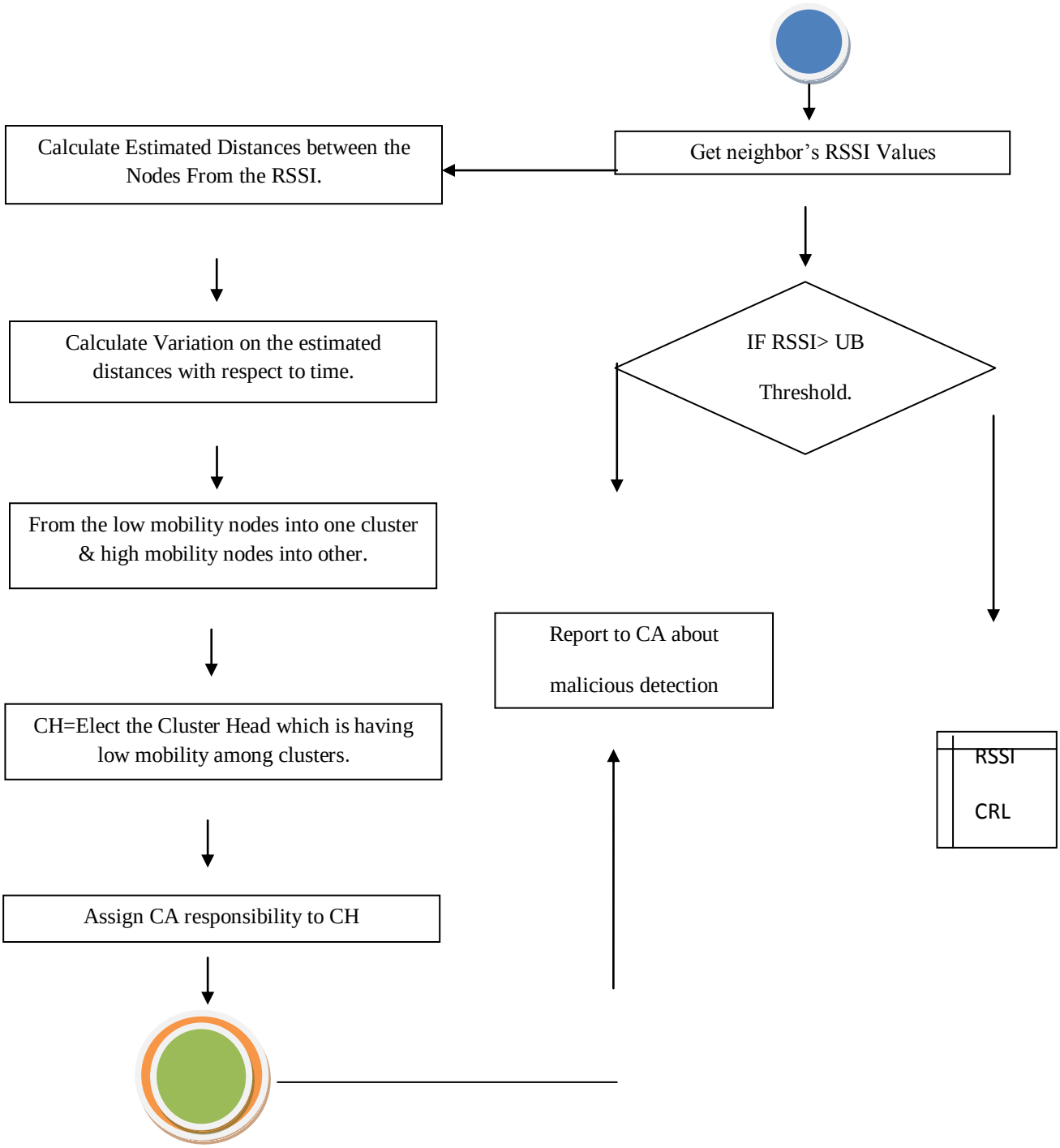

Fig.3.3 Flow chart representation of the proposed work [9].

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

3.2 Entry and Exit Behavior of Nodes

The legitimate identity and Sybil identity are differentiated by the Entry and Exit behavior of neighborhood nodes. The legitimate identity increases and decreases its RSSI values gradually (i.e.) its entry and exit behavior is identified by the neighborhood because it goes gradually going towards the neighborhood node and gradually coming away from the neighborhood node. Based on the mobility of the node, the node's radio range is divided into two sections that is 1.Grey zone, 2.White zone. So the legitimate node gives the first RSSI value as low. But in case of Sybil identity, the node changes its identity often. Its first RSSI value is high enough to be differentiated from the legitimate node. The RSSI values are affected by. 1. Transmit power 2.Mobility. So, in case of increasing transmission power the first RSSI value will be high and due to high mobility, the node is identified in White zone i.e. the first RSSI value is high, even though it is a legitimate node. Hence, consider the transmission power of the node is constant. The below algorithm works whenever the RSSI values exceed the threshold and if not received a predefined threshold time, Then CA comes into the role and checks the certification of the particular node.

ESAD ALGORITHM

Add New RSS (Address, rssi, time_recv)
BEGIN SUB:
IF: Address is not in the table
THEN
IF: rssi>=UB_THRESHOLD
THEN: Checks the certificate of that node
IF: Certificate is not valid
THEN: Add _To_CRL (Address)
Broadcast_Detection_Update (Address)
ELSE: Add_To_CTL (Address)
END_IF
END_IF
END_IF
Create_Record (Address)
END SUB:

The ESAD (Enhanced Sybil Attack Detection) algorithm is used to differentiate the legitimate node and Sybil node even in high mobility through the certification checking. It stores the node's RSSI value in the table with respect to time if its first RSSI value is lower than the threshold, else add it to malicious list and update to its neighbors. Due to battery constraint, every mobile node maintains only 5 lists. The TTP is CH and it handles the certificate checking and revocation process. Whenever, the node reports to CA about neighbor's activity, the CA will start the certificate checking. If it is valid certificate, the node is a legitimate node otherwise will be a Sybil node. Due to fast movement of the node, it gives high RSSI values in the network. The ESAD process diagrammatical representation is given below.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

3.3 Certification Authority

The certification authority is used to authenticate the nodes within the network and also to provide the certificate whenever a new node enters into the network. Here, the CA responsibility is given to the cluster head because of low mobility and trusted node. Whenever, a new node enters hardware or MAC address of its own have to submit to get the certificate from the cluster head. Every mobile node has its own MAC address. Whenever, the abnormal RSSI value is received by any one of the nodes, it reports to the corresponding certification authority to check its certification. If certificate is not valid, its certificate will be removed and that status will be updated to its neighborhood nodes.

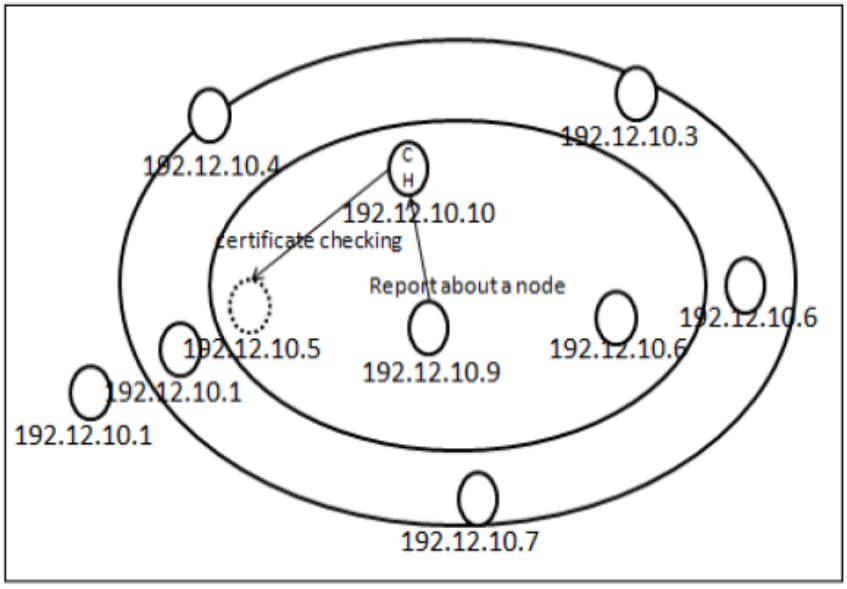

Fig.3.4: Architecture Diagram of Certification Authority [9].

The CA uses the Diffie Hellman Key exchange method; in this every node maintains a pair of private key and public keys. The public key made known to all and private key is kept secret and is known only to the corresponding node. In this scheme, the Certificate authority will maintain the Certificate Trust List (CTL) and all other nodes have the Certificate Revocation List

(CRL). The Certificate Trust List is used to store the collections of legitimate node list and the safe packet transmissions can be done through this CTL list node. It will provide a high throughput and network performance. The Diffie Hellman Key Exchange method is used only at the time of certification checking and there after adopts with the symmetric key cryptography. Due to this, the network complexity is reduced The entire certification checking process is done by three key exchanges, the user sends its certificate to the CS server, The CS server verifies its signature which is present on the certificate and sends CS server's certificate with Yc encrypted by Ku. After user verifies it, sends authentication with Yu encrypted by Kc.

3.4 Certificate Revocation List

The certificate revocation list is used to store the addresses of Sybil nodes. Every node has the CRL and this is useful to identify the Sybil identity without certification checking. So it reduces the detection time and the time complexity. The CRL is explained in the following diagram. In the below figure, M and B are the two node's radio range. C is Sybil node present in M's CRL but not in B's CRL.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

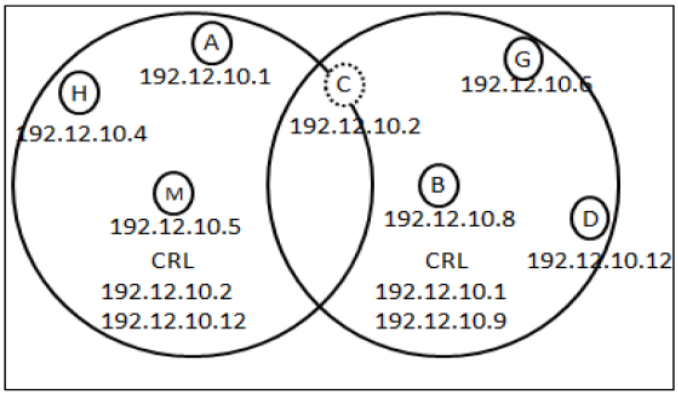

Fig. 3.5 Certificate revocation list [9].

When node C comes into the M's radio range then it will be matched and detected in M's range. Through this CRL, the Sybil node is identified without checking the certification of its node. It reduces the complexity and as well as increase the network throughput with less pocket drop ratio.

3.5 Mathematical Model

S= {I,F,O}

I = $\{i_1, i_2, \ldots, i_n\}$ = > set of inputs (Nodes).

F = $\{f_1, f_2, f_3\}$ => set of functions.

O = $\{o_1, o_2 \ldots o_n\}$ => set of output (Nodes).

Where, f1 = Accuser Node function.

f_2 = Sybil Node function.

f_3 = Revoke certificate of malicious node and restore function.

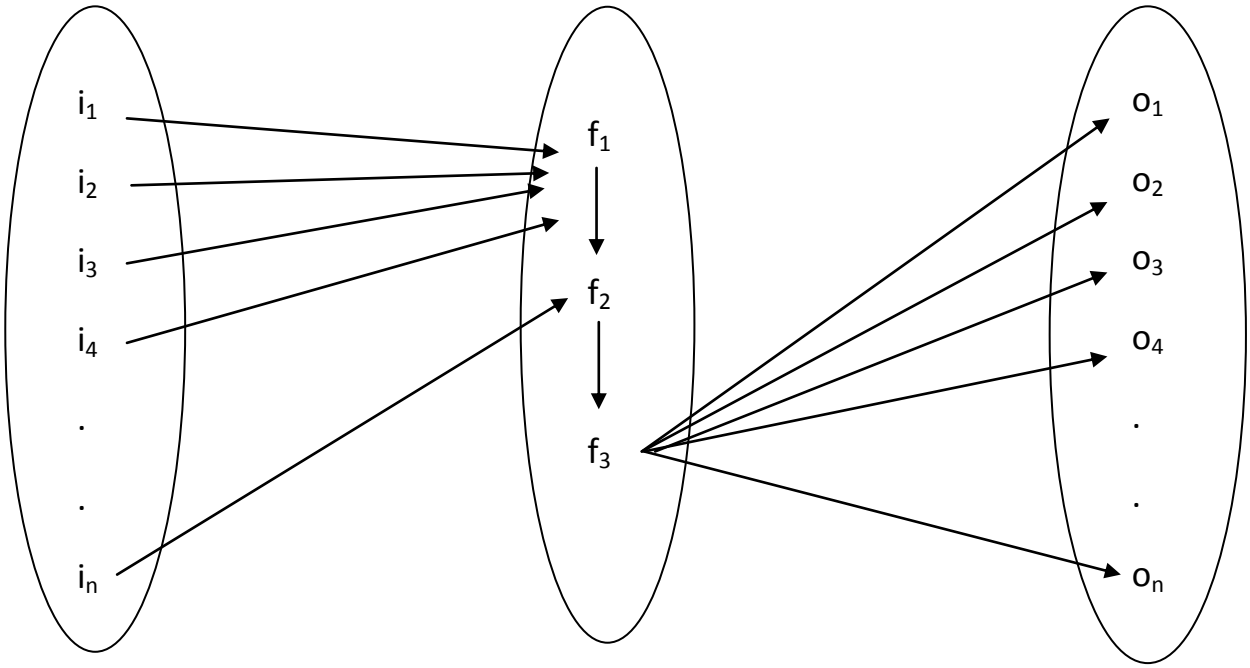

Fig. 3.6 Mathematical Model for proposed System.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

IV. RESULTS AND DISCUSSION

Table 4.1 Simulation parameters [9].

PARAMETER	LEVEL
AREA	1000 X 1000
SPEED	5 to 30m/s
PAUSE TIME	10 s
RADIO PROPOGATION MODEL	Two ray ground model
RADIO RANGE	250 m
CARRIER SENSE RANGE	550 m
NUMBER OF NODES	15 to 50
MAC	802.11
APPLICATION	CBR 10 to 40
SIMULATION TIME	150 s
MOVEMENT	Random way point model
RSSI TIME OUT	120 s
PLACEMENT	Uniform
RSSI THRESHOLD	2.0e-10 W

The figure 4.1 shows the TPR for the proposed work with various numbers of nodes like 10, 20, 30, 40 numbers of nodes.

The TPR is increased with the increasing number of nodes but it increases the detecting time because of certification checking often due to

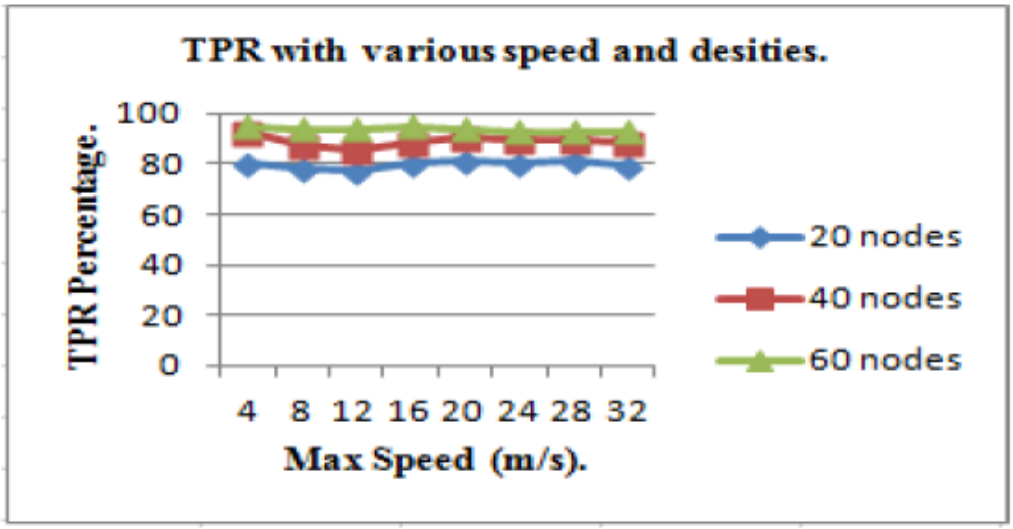

Fig. 4.1 TPR for various speed and densities [9].

The figure 4.2 shows the FPR for the proposed work with various number nodes like 10 to 40. The FPR is gradually increasing for more than 50 numbers of nodes in the network.

This is happening because of huge variation on the RSS values.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

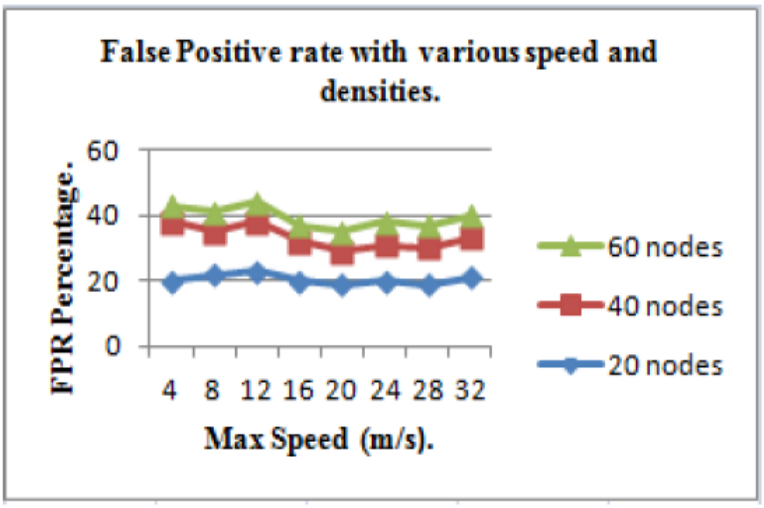

Fig. 4.2: FPR for various speed and densities [9].

$$\text{False Positive rate} = \frac{\text{Incorrectly detected good ID's}}{\text{Total good ID's}}$$

$$\text{True Positive rate} = \frac{\text{correctly detected Sybil ID's}}{\text{Total Sybil ID's}}$$

V. CONCLUSION

Received Signal Strength (RSS) based localization is considered as one of the most promising solutions for wireless ad hoc networks to detect Sybil attacks and eliminate them from the networks, Sybil attack is an active attack. This attack causes various bad effects to the network. Sybil attack is an attack which uses many false identities or single false identity at a time and creates false expression of legitimate nodes within the network.

There are various damages caused by this attack to the network. For example, internet polls can be controlled by this attack by using multiple identities or IP addresses and result can be made in their favor. Sybil attacks can also decrease the trust of legitimate nodes and increases their trust in the network which helps them to easily harm the network. Companies can also use this attack to increase the ranking of the Google page of their client. In vehicular ad hoc network, it can provide fake information about the congestion of traffic in order to change the direction of traffic. Hence, Sybil attack poses serious threats to the mobile ad hoc network. So it is very crucial to eradicate this attack from the network.

In this method of detecting the Sybil attack, there is no requirement of any extra hardware or directional antennae, therefore it is called as lightweight and it is also cheap in cost compared with other approaches. The proposed system works well and differentiating the Sybil identity and legitimate identity even in high mobility with reduced false positive rate. The proposed system works when different kind of mobile nodes are available with different transmission rate by mobile D-Hop cluster. The mobile D-Hop algorithm groups the low range nodes into one cluster and high radio range nodes into another cluster. So it works well even with the heterogeneous mobile nodes with high true positive rate.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

It avoids the link breakage and packet drops. The proposed work reduces the enlarging of routing table due to Sybil attack, thus, saving the node's battery life; it is also very useful in wireless sensor and VANET applications with good network performance. [9]

5.1 Future work

In future work new issues could be included related to increasing complexity and increasing detection time for Sybil node when more number of nodes present in the networks.

The proposed detection scheme can work as a standalone scheme, but could equally be deployed as an add-on to existing schemes, for example it could be incorporated into a reputation-based system, i.e., the detected Sybil identities from the MAC layer will be plugged into the reputation-based system on network layer.

Our proposed scheme does not use localization technique for Sybil attack detection, and hence does not need any directional antennae or any GPS equipment but they can be added it the future systems. [12]

REFERENCES

[1] A.Aranganathan, C.D.Suriyakala," Mobile Agent based Security in MANETS against Sybil Attack" 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), IEEE 2014.

[2] Anamika Pareek, Mayank Sharma, Sanghvi Institute of Management & Science, Indore, "Architecture For Detection Of Sybil Attack In MANET Using MAC Address", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Issue 6, Volume 2 (June 2015).

[3] "Clustering in Mobile Ad hoc Networks", University of Central Florida, Baker+ 1981b, D.J. Baker and A. Ephremides, IEEE Transactions on Communications.

[4] Chris Piro, Clay Shields, Brain Neil Levine, "Detection the Sybil Attack in Mobile Ad hoc Networks", in IEEE 2006..

[5] Demirbus M., Sang Y. (2000) : "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", Department of Computer Science and Engineering, Department State University of New York at Buffalo, NY 14260.

[6] Fong P.W.L.(2011): 'Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems'. In IEEE Symposium on Security & Privacy, pp. 263-278, IEEE2011.

[7] Levine B.N., Shields C., and Margolin N.B. (2006):'A survey of solutions to the Sybil attack', University of Massachusetts Amherst, Amherst, MA.

[8] Newsome J., Shi E., Song D., and Perrig. A (2004): 'The Sybil attack in sensor networks: analysis & defences', In Proceedings of the third international symposium on Information processing in sensor networks, pp. 259–268.

[9] R. Vintoh kumar, Mr. P. Ramesh, Dr. H. Abdul Rauf, India," Cluster Based Enhanced Sybil Attack Detection in MANET through Integration of RSSI and CRL", 2014 International Conference on Recent Trends in Information Technology, IEEE 2014.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[10] Rajakumar P, Prasanna venkatesan T, Pitchaikkannu A, Dept. of information technology Anna university,
RC, Coimbatore – 641047, "Security Attacks and Detection Schemes in Manet",IEEE 2014

[11] Roopali Garg, Himika Sharma " Comparison between Sybil Attack Detection Techniques: Lightweight and Robust", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 2, February 2014, IEEE 2014

[12] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat, " Lightweight Sybil Attack Detection in MANETs", IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013, IEEE 2013.

[13] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat,
"Signal Strength Based Sybil Attack Detection in Wireless Ad hoc Networks", in IEEE CONF at 2009.

[14] Somnath Sinha, Aditi Paul, and Sarit Pal," The Sybil Attack In Mobile Ad Hoc Network: Analysis And Detection', in IEEE 2013

[15] Tangpong, A., Kesidis, G., Hung-yuan Hsu, Hurson, A. (2009): 'Robust Sybil Detection for MANETs, 'In Proceedings of 18th International Conference on Computer Communications and Networks ICCCN 2009, pp. 1 – 6.

[16] Zhaoyu Liu, Anthony W. Joy, Robert A.: 'A Dynamic Trust Model for Mobile Ad Hoc Networks', Thompson Department of Software and Information Systems University of North Carolina at Charlotte Charlotte, NC 28223, USA.