e-ISSN : 2349-9745
p-ISSN : 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

An Enhanced Sybil Attacks In Manets

V.Sowmya Devi[1], M.Reshma[2]
[1]*Associate Professor (Dept. of CSE),GITAM University, Hyderabad*
[2]*Department of CSE, GITAM University, Hyderabad*

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

I. INTRODUCTION TO MANET'S:

Mobile applications present additional challenges for mesh networks as changes to the network topology are swift and widespread. Such scenarios require the use of Mobile Ad hoc Networking (MANET) technology to ensure communication routes are updated quickly and accurately. MANETs are self-forming, self-maintained, and self-healing, allowing for extreme network flexibility. While MANETs can be completely self contained, they can also be tied to an IP-based global or local network (e.g. Internet or private networks).[1] These are referred to as Hybrid MANETs .A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced disasters, military conflicts, emergency medical situations etc. The mobile hosts dynamically establish paths among one another in order to communicate.

History of MANETs:

The earliest MANETs were called "packet radio" networks, and were sponsored by DARPA in the early 1970s. BBN Technologies and SRI International designed, built, and experimented with these earliest systems. Experimenters included Jerry Burchfiel, Robert Kahn,and Ray Tomlinson of later TENEX, Internet and email fame. It is interesting to note that these early packet radio systems predated the Internet, and indeed were part of the motivation of the original Internet Protocol suite. Later DARPA experiments included the Survivable Radio Network (SURAN) project, which took place in the 1980s. Another third wave of academic activity started in the mid 1990s with the advent of inexpensive 802.11 radio cards for personalcomputer. Current MANETs are designed primary for military utility; examples include JTRS and NTDR.

@IJMTER-2014, All rights Reserved

II. SYSTEM ANALYSIS:

Existing System:

In existing system, in this paper, we will present our scheme that detects Sybil identities. In particular, our scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities.[5] First, we demonstrate the entry and exit behavior of legitimate nodes and Sybil nodes using simulation and test bed experimentation. Second, we define a threshold that Distinguish between the legitimate and Sybil identities based on nodes' entry and exit behavior.

- Static network: nodes are immobile after initial deployment
- We assume an initial set of nodes that are trustworthy
- New nodes are introduced to network (some may be sybil)

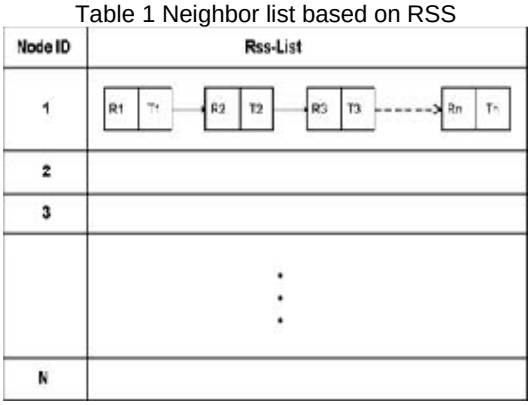
Drawback In Existing System:

1 Existing solutions for Sybil attack prevention are too costly for the resource-poor sensor platforms
2 Excessive communication burden on nodes are not acceptable since they drain the battery power quickly
3 Each entity in the network is bound to a single identity certificate. However, trusted certification suffers from Costly initial setup, lack of scalability and a single point of attack or failure.

III. PROPOSED WORK:

We proposed this paper We implement a Sybil attack detection technique based on using ratios of RSSIs from multiple nodes The technique was first introduced as a localization solution byZhong ET. al., but this is the first time it is implemented in WSNThe simulation results showed that our scheme works better even in mobile environments and can detect both join-and-leave and simultaneous Sybil attackers with a high degree of accuracy. [3] A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch

Table 1 Neighbor list based on RSS



identities in order to weaken the detection process, thereby promoting lack of accountability in the network

Advantages of Proposed System:

1. Flexibility and computational traceability.
2. Time managements.

IV. SECURITY ATTACKS:

Securing wireless adhoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information.[4]Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

@IJMTER-2014, All rights Reserved

Passive Attacks:

Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected.

Active Attacks:

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. Active attacks can be internal or external.

1. External attacks are carried out by nodes that do not belong to the network.
2. Internal attacks are from compromised nodes that are part of the network.

Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication.

V. ACTIVE ATTACKS:

1 Black hole Attack:

In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it.[9] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packet that it receive instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

2 Wormhole Attack:

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunnelled.This tunnel between two colluding attacks is known as a wormhole .In DSR,AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network

3 Byzantine attack:

A compromised with set of intermediate,or intermediate nodes that working alone within network carry out attacks such as creating routing loops ,forwarding packets through non -optimal paths or selectively dropping packets which results in disruption or degradation of routing services within the network.

4 Rushing attack:

Two collided attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne [14].

5 Replay attack:

An attacker that performs a replay attack are retransmitted the valid data repeatedly
to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions [8].

Location disclosure attack:

An attacker discover the Location of a node or structure of entire networks and disclose the privacy requirement of network through the use of traffic analysis techniques [10], or with simpler probing and monitoring approaches [14]. Adversaries try to figure out the identities of communication parties

@IJMTER-2014, All rights Reserved

and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security.

Flooding:

Malicious nodes may also inject false packets into the network, or create ghost packets which loop around due to false routing information, effectively using up the bandwidth and processing resources along the way. This has especially serious effects on adhoc networks, since the nodes of these usually possess only limited resources in terms of battery and computational power. Traffic may also be a monetary factor, depending on the services provided, so any flooding which blows up the traffic statistics of the network or a certain node can lead to considerable damage cost.

6 Sinkhole:

In a sinkhole attack, a compromised node tries to attract the data to itself from all neighboring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighboring 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.

7 Spoofing Attack:

In spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be
launched, which could seriously cripple the network. This type of attack can be launched by any malicious node that has enough information of the network to forge a false ID of one its member nodes and utilizing that ID and a lucrative incentive, the node can misguide other nodes to establish routes towards itself rather than towards the original node.

8 RERR Generation:

Malicious nodes can prevent communications between any two nodes by sending RERR messages to some node along the path. The RERR messages when flooded into the network, may cause the breakdown of multiple paths between various nodes of the network, hence causing a no. of link failures.

9 Jamming:

In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

10 Replay Attack:

The attacker collects data as well as routing packets and replays them at a later moment in time. This can result in a falsely detected network topology or help to impersonate a different node identity. It can be used to gain access to data which was demanded by replayed packet.

11 Sybil attack:

The Sybil attack especially aims at distributed system environments. The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods. Since ad
hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from source to destination. A consequence of this is that attackers have a harder time to destroy the integrity of information

12 Sinkhole attack:

The attacking node tries to offer a very attractive link e.g. to a gateway. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack.

@IJMTER-2014, All rights Reserved

13 De-synchronization attack:
In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence these messages are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information. This will cause a considerable drainage of energy of legitimate nodes in network in an end-less synchronization-recovery protocol.

14 Denial of service attack:
Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.

15 Gray-hole attack:
This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops interceptedpackets with a certain probability.

16 Selfish Nodes:
In this a node is not serving as a relay to other nodes which are participating in the network. This malicious node which is not participating in network operations, use the network for its advantage to save its own resources such as power.

17 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 neighbor can no longer be contacted [5].

VI. PASSIVE ATTACKS:

1 Traffic Monitoring:
It can be developed to identify the communication parties and functionality which could provide information to launch further attacks .It is not specific to MANET, other wireless network such as cellular, satellite and WLAN also suffer from these potential vulnerabilities.

2 Eavesdropping:
The term eavesdrops implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of message by unintended receiver take place. Mobile host in mobile ad-hoc network shares a wireless medium.
Majorities of wireless communication use RF spectrum and broadcast by nature. Message transmitted can be eavesdropped and fake message can be injected into network.

3 Traffic Analysis:
Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

4 Syn flooding:
This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate
nodes.
Attacks can occur in different layers of the network protocol stack.

@IJMTER-2014, All rights Reserved

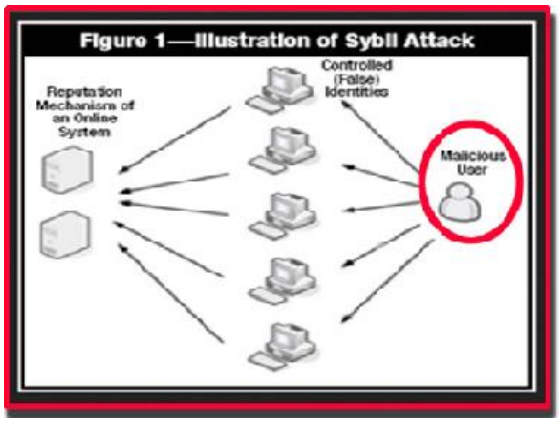
Table 2: Attacks on the Protocol Stack

Layer	Types of Attacks
Application	Malicious code, Data corruption, viruses and worms
Transport	Syn Flooding attack, session hijacking
Network	Black hole, Wormhole, Sinkhole, Replay attacks, Sybil attacks
Data link	Selfish nodes, Traffic analysis
Physical	Jamming,Eaves Dropping

VII. SYBIL ATTACK:

Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. [10] However, if a single faulty entity can present multiple identities it can control a substantial fraction of the system, thereby undermining this redundancy. One approach to preventing these "Sybil attacks" is to have a trusted agency certify identities. This paper shows that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities.

Fig: Illustration of Sybil Attack



@IJMTER-2014, All rights Reserved

Attack Model:

There are two flavors of Sybil attacks. In the first one, an attacker creates new identity while discarding its previously created one; hence only one identity of the attacker is up at a time in the network. This is also called a join-and-leave or whitewashing attack and the motivation is to clean-out any bad history of malicious activities. This attack potentially promotes lack of accountability in the network. In the second type of Sybil attack, an attacker concurrently uses all its identities for an attack, called simultaneous Sybil attack. The motivations of this attack is to cause
disruption in the network or try to gain more resources, information, access, etc. than that of a single node deserves in a network. In our scheme, we will consider both types of Sybil attacks. The strategy of my detection mechanism is to detect every new identity created by a Sybil attacker; it does not matter if the intention of the attacker is to use that identity for whitewashing or simultaneous Sybil attack.

Resource Testing:

Resource Testing is the most commonly implemented solution to averting Sybil attacks. The basic principle is that the quantum of computing resources of each entity on the network is limited. A verifier then checks whether each identity has as many resources as the single physical device it is associated with. Any discrepancy indicates thepossibility of a compromised node. Storage, computation and communication were initially proposed as resources.However, for a system such as a wireless sensor network, an attacker might have storage and computation resources in large capacities compared to resource-starved sensor nodes. Alternatively, verification messages for verifying communication resources might flood the entire system itself. Hence, all three are inadequate choices for sensor networks. Radio resource testing, proposed by Newsome et al. in [6], is an extension of the resource testing verification method for wireless sensor networks. The key assumptions of this approach are 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 suggested by many as a minimal defence against Sybil attacks where the goal is to reduce their risk substantially rather than to eliminate it altogether.

Privilege Attenuation:

Fong considers a different kind of Sybil attack altogether – one that is distinct from others that plague peer-to-peer and reputation systems. This attack aims to create pseudonymous or fake identities in a Social Network System (SNS) and get them to collude to favourably alter the existing trust relationships in the network. These relationships are represented via a graphtheoretic relationship model that exists between the owner of a resource and a prospective accessor of the same resource and is called a social graph. Such models are common in quite a few popular Social Network Systems such as Facebook. Access control policies are as defined by the respective SNSes themselves. This concept of relationship-based access control (ReBARC) [16,17, 18] is the basis for authorization decisions in the system.

Recurring Costs:

This method is a variation of resource testing where resource tests are conducted after specific time interval 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 researchers that have endorsed this method [7, 8, 9] 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. in [5]. In [10] the authors make use of an economic model to propose a critical value that exists for a particular combination of application domain and attacker objective. An attack is deemed successful only if
ratio of the attacker’s objective value to the cost per identity exceeds this critical value.

RSSI-based scheme:

Demirbas and Song introduce a method for Sybil detection based on the Received Signal Strength Indicator (RSSI) of messages. The cooperation of one additional node (and hence one message

@IJMTER-2014, All rights Reserved

communication) is required for the proper functioning of this protocol. A localisation algorithm is used in this scheme Sybil attacks can be detected with a completeness of 100% with few false positive alerts. Despite the fact that RSSI is unreliable and that transmissions via radio are non-isotropic, the use of ratios of RSSIs from multiple receivers solves this problem.

Random Key Predistribution:

This technique enables nodes on a wireless sensor network to establish secure links for communicating with each other [15]. In random key predistribution, a set of keys are assigned at random to a node enabling it to discover or compute the common keys that it shares with its neighbouring nodes. Node-to-node secrecy is ensured by using the common keys as a shared secret session key. The main ideas are the association of the identity with the key assigned to a node and the validation of the key.

VIII. SPECIFIC TYPES OF SYBIL ATTACKS:

There are numerous malicious applications of Sybil attacks in different environments such as those including, but not limited to, the variations enlisted below.

Routing:

Sybil attacks can disrupt routing protocols in ad hoc networks, especially the multicast routing mechanism. Separate paths that initially seem disjoint may pass through the Sybil nodes of a single attacker. Another vulnerable concept is Geographical routing where malicious nodes may appear at more than one place at a time [4]. An attack in an ad hoc network and thus the availability of fake identities may further lead to a large scale attack such as distributed DoS, in addition to the inherently insecure routing protocols in such networks [12].

Tampering with Voting and Reputation Systems:

In case of any environment where there is a voting scheme in place for purposes such as reporting and identifying node misbehaviour in the system, updating reputation scores and so on, a Sybil attack may be particularly dangerous.[6] As an example, an attacker may create enough malicious identities to repeatedly report mand subsequently remove legitimate nodes from the network. Alternatively, these malicious nodes can protect themselves from ever being removed as they are in collusion.

Fair Resource Allocation:

Sybil attacks may also be used to enable the attacker to obtain an unfair and disproportionately large share of resources that were intended to be distributed amongst all nodes on the network equally. This attack denies legitimate nodes their deserved share of resources and also provides the malicious node with more avenues for other attacks.

Distributed Storage:

File storage systems in peer-to-peer and wireless sensor networks can be compromised by the Sybil attack. This is achieved by defeating the fragmentation and replication processes in the file system. A system can be tricked into storing data into the multiple Sybil identities of the same node on the network.

Data Aggregation:

Sensor network readings are computed by query protocols in a network rather than returning the reading of each individual sensor. This is done to conserve energy. Sybil identities may be able to report incorrect sensor readings thereby influencing the overall computed aggregate. A malicious user may be able to significantly alter the aggregate with enough identities.

IX. DETECTION MECHANISMS OF SYBIL ATTACK:

To defend against the Sybil attack, which is based on the assumption that each physical entity is limited in some resource. According to this approach computation, storage and communication can be used for resource testing. In [10], Newsome et al. showed that computation and storage are not suitable to ad hoc networks, because the attacker can use more computational and storage resources than the legitimate node. Instead, they suggested a scheme based on radio resource testing. This scheme assumes that

@IJMTER-2014, All rights Reserved

each node has only one radio which is not capable of sending or receiving on more than one channel, simultaneously. If a node wants to verify the presence of Sybil nodes in its neighbors, it will assign each of its neighbors a different channel to broadcast messages. The node then randomly selects a channel to listen. If the node hears the message on the channel assigned by the verifying node, then it is a legitimate node. Otherwise, the neighboring node is treated as the Sybil node. However, how a sensor node assigns the radio channels to its neighbor nodes is an unsolved problem. In addition, this testing process may consume a lots of battery power.

Tangpong et al. in [31] proposed a location-based Sybil attack detection scheme for MANETs based on path similarity. The identities that traverse the similar paths are considered Sybil nodes. Instead of selecting some trusted observer nodes as in [24], each node in the network observes and exchanges traffic observations in order to analyze the potential existence of a Sybil attack. Moreover, to prevent a malicious node from fabricating with an observation, a hop-byhop authentication protocols is being used. Ssu et al. proposed a detection scheme in which the node identities are verified simply by analyzing the neighboring node information of each node. This detection method is based on the fact that in a dense network, two different nodes cannot have the same set of neighbors. Because in a Sybil attack, all the Sybil nodes are created by the same malicious node, therefore, each of them will have same set of neighbors. This loophole of the Sybil nodes can be used to detect the presence of a Sybil attack. However, this scheme is not suitable for mobile or semi mobile Ad hoc networks.

X. CONCLUSION AND FUTURE WORK:

In this paper we have tried to categorize the different types of ad hoc security attacks solely based on their characteristics to considerably reduce the mitigation period. By bringing the attacks under these two broad categories the complicacy of naming also reduces. We have also kept a close look on the existing algorithms needed to mitigate the attacks and have tried to bind the attacks into categories according to that. Some attacks have characteristics which makes them unsuitable to be categorized into these categories, so they have been kept away from this topic of discussion for the time being. Further study is in progress to find out more common characteristics of the attacks to more strongly bind them into these categories and to ably design more powerful algorithm in mitigating DATA It takes the advantage of varying the transmission power in two ways: First, it cannot be detected on the basis of same signal strengths of its Sybil nodes. Second, by decreasing the transmission power for different Sybil nodes, the message will not reach all the neighbors of the malicious node and hence cannot be detected on the basis of thefact that if a set of nodes are seen together for a long period of time by an observer node, then they are suspected to be the identities of Sybil attacker. In an impersonation based Sybil attack, a malicious can also disrupt the lowest ID based cluster algorithm by presenting multiple Sybil nodes with IDs greater than its neighboring legitimate nodes. It will target a legitimate node with lowest ID to make it clusterhead again and again, so as to drain its battery. It also utilizes its multiple Sybil nodes to communicate repeatedly with the clusterhead so as to make it busy all the time. After completely draining the battery of head node, the malicious node can impersonate its ID for one of its Sybil node to become the clusterhead. If a number of malicious nodes are spread across all over the network, the impact of the Sybil attack will be more on this clustering scheme, as most of the clusters will be under the control of these Sybil attacker nodes.

REFERENCES

[1] Mohammad Al-Shurman ,Seong-Moo Yoo , Black Hole Attack in Mobile Ad Hoc Networks , ACM-SE 42 Proceedings of the 42nd annual Southeast regional conference

[2] SongbaiLu,LingyanJia,Kwok-Yan Lam,Longxuan Li, SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack, International Conference on Computational
Intelligence and Security, 2009

@IJMTER-2014, All rights Reserved

[3] PiyushAgrawal and R. K. Ghosh: Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks www.stanford.edu/~piyushag/docs/icuimc08.pdf
[4] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in Proc. of 2002 IEEE International Conference on Network Protocols (ICNP), pp. 778-89, Nov. 12-15, 2002.
[5] B. N. Levine, C. Shields, and N. B. Margolin, A survey of solutions to the Sybil attack, University of Massachusetts Amherst, Amherst,MA, 2006.
[6] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil attack in sensor networks: analysis &defences, In Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268,
2004
[7] B. Awerbuch and C. Scheideler. Group Spreading: A Protocol for Provably Secure Distributed Name Service. In Proc. Automata, Languages and Programming (ICALP), pages 183–195, 2004
[8] P. Maniatis, D. S. H. Rosenthal, M. Roussopoulos, M. Baker, T. Giuli, and Y. Muliadi, Preserving peer replicas by ratelimited sampled voting, In Proceedings of ACM SOSP, pages 44–59, 2003
[9] P. Maniatis, M. Roussopoulos, T. J. Giuli, D. S. H. Rosenthal, and M. Baker, The locks peer-to-peer digital preservation system, ACM Transactions on Computer Systems, Vol. 23(1) pp. 2–50, 2005.
[10] Margolin, N. B. and B. N. Levine (2005) Quantifying Sybil Attacks against Network Applications, Technical Report 67, Dept. of Computer Science, University of Massachusetts Amherst.
[11] S. Basagni, I. Chlmtac, V. R. Syrotiuk and B. A. Woodward, (1998), “A Distance Routing Effect Algorithm for Mobility (DREAM)”, In Proceedings of IEEE/ACM MobiCom, pages 76-84.
[12] B. Karp and H. T. Kung, (2000), “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks”, In Proceedings of IEEE/ACM MobiCom, pages 243-254.
[13] Y. Ko and N. H. Vaidya, (1998), “Location-Aided Routing (LAR) in Mobile Ad Hoc Networks”, In Proceedings of IEEE/ACM MobiCom, pages 66-75.
[14] J. J. Garcia-Luna-Aceves, and E. L Mada-uga, (1999), “The core assisted mesh protocol”, IEEE JSAC, Vol 17, No. 8, pp. 1380-1394.
[15] S. -J. Lee, M. Gerla and C. C. Chiang, (1999), “On-demand multicast routing protocol (ODMRP)”, Proceedings of IEEE WCN’99.
[16] E. M. Royer and C. E. Perkins, (1999), “Multicast Operation of Ad Hoc On Demand Distance Vector Routing Protocol”, In Proceedings of ACM MOBICOM, pp. 207-18.
[17] S. -J. Lee and M. Gerla, (2001), “Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks”, In Proceedings of the IEEE International Conference on Communications (ICC), pp. 3201-3205, Helsinki, Finland.
[18] J. Zhao and R. Govindan, (2003), “Understanding Packet Delivery Performance in Dense Wireless Sensor Networks”, In Proc. ACM Sensys.

@IJMTER-2014, All rights Reserved