Impact of Sybil Attack and Security Threat in Mobile Adhoc Network

Ankit Gupta
P.G Scholar, M.TECH (CN)
Oriental University Indore (M.P)

Deepak Sukheja, PhD
Oriental University Indore (M.P)

Amrita Tiwari
Oriental University Indore (M.P)

ABSTRACT

Network security in mobile Adhoc network is major issue. MANET system efficiency and security is compromised to create instability, disrupt network performance reducing fault tolerance, capability and attack on confidentiality, integrity and availably of information in network .the attack on adhoc is launched mainly in network layer to reducing Trust ship of system. Open nature communication makes wireless connection prone for various security threats. This paper consist a brief review of mobile ad-hoc network along with effect and vulnerabilities into same. It also enlists and explores the challenges to derive new mechanism over security threats. Subsequently, a compressive study has performed on Sybil Attack and its effect on ad-hoc networks. Work also consider some existing solution mitigate Sybil attack.

Keywords
MANET, Sybil attack, Network Security, Node

1. INTRODUCTION

A wireless networks is a way to establish communication among nodes without having hurdles of wires. Wireless networks may be implemented in various manners like mobile ad-hoc networks (MANET), vehicular ad-hoc networks (VANET), wire-less sensor networks etc. mobile ad-hoc network is collection of various wireless mobile nodes connected by wireless links. It is an autonomous system which does not require any pre-existing infrastructure and establish for temporary purpose. Ad-hoc is a Latin word which stands “for this” also known as IEEE 802.11 standard. It is a new technology emerged for fast, in ex-pensive network establishment without having burden of other devices like hub, switches or router. Here, devices are itself capable to behave as node or router to discover a route and forward packets. In MANET, each mobile node has communication range depend upon transmission power, antenna gain and loss along with antenna height. Communication in the net-works depends upon the connection among nodes using wireless links. A node can communicate to another node either through direct link connection or passing through multi-hop routing nodes. It always depends upon radio range of node and connectivity among same. Here, intermediate nodes play the role of router help to discover route from source to destination.

MANETs may be deploys in structured or unstructured manner deploy with dynamic characteristics. Here, connections may be established through Peer-to-Peer or Dynamic mode without considering centralize infrastructure. It is shown in Figure 1 and Figure 2.

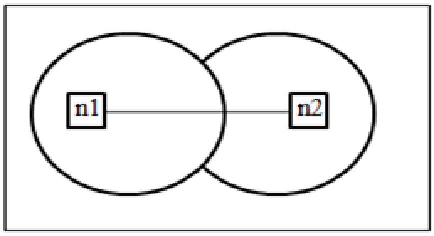

Figure 1: Peer to Peer Connection between node n1 and n2

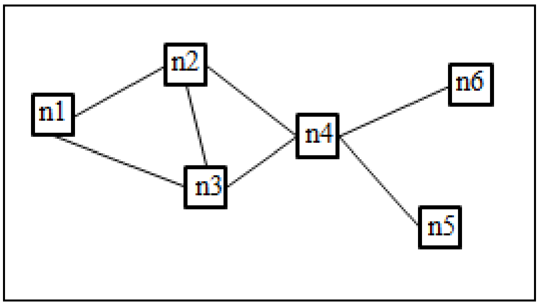

Figure 2: Dynamic Multi-hop Connection in between nodes

Due to wireless connectivity, communication becomes more vulnerable than wired networks. In wired networks a dedicated wired link provides dedicated bandwidth, unicast communication, reliable transmission, error free communication along with temper proof connection. The complete work observes that, wireless communication especially MANET is vulnerable for various security threats. This paper considers study of various resource constraints, security threats and goals of MANET. It also study and compare impact of Sybil attack and existing solution

2. MANET

Mobile adhoc network is self-configurable, infrastructure less network and dynamic multi-hop peer to peer network. Mobile Adhoc network First generation introduced in 1972 known as Packet Radio Network (PRNET), second generation is survivable adaptive radio network (SURAN) and third generation is standardized by IETF in 1990 under IEEE 802.11WLAN.

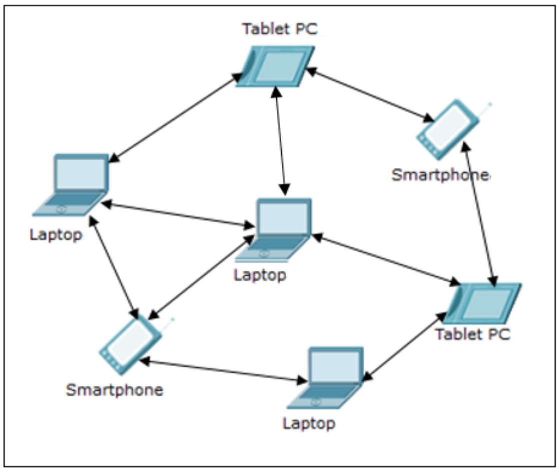

Figure 3: Mobile Adhoc Network Topology

2.1 MANET Characteristics

2.1.1 Self-organized – Mobile adhoc network provide high network agility they are self-organized and infrastructure less and quick deploy network, each node (device) in network act as relay agent and router perform packet forwarding and provide different network applications and services.

2.1.2 Dynamic topology – In MANET nodes can join or leave network anytime so topology of network is completely unpredictable, route change are also frequent because if some node leave network it required to calculate another path for network topology.

2.1.3 Scalability – MANET provide great flexibility for users, due to wireless transmission medium it is very effective to cover remote sites and geographical distance areas.

2.1.4 Multihop – MANET network node can communication only if there are in common radio cover range in MANET there are number of device present between sender and receiver and node are moving continuously message are forwarded from relay agent in network.

2.1.5 Device heterogeneity – MANET consist devices such as PDA, Smart Phones. Laptops, thin client wearable devices can connect via wireless and create adhoc network.

2.1.6 Cooperating – MANET are required coordination between node form packet forwarding to application and service delivery.in MANET each node act as client and server, node act as master or slave and each node have equal priority and service availability

2.2 MANET Application

2.2.1 Tactical networks - In military and battle field operations required adhoc network for communication with solders, vehicle, headquarter or check post and base camp.

2.2.2 Emergency services – Establish network for Search and rescue operations in Disaster recovery.

2.2.3 *Transport and avian industry* – vehicle are communicated with advance sensors in drives self-drive cars and Airplane and fighter jet communicated via adhoc network to detect and avoid collisions.

2.2.4 Entertainment – Adhoc network used in playing multi-user game via wireless point to point network and outdoor access points

2.2.5 Sensor networks **-** Remote area monitoring, Field sensing and data gathering required a quick deployable network and Coverage extension of network.

2.2.6 SOHO environment – In small office home office environment application like file sharing, data transfer, connecting printers, internet access

2.3 Limitation

2.3.1 Energy constraint **-** *l*imited Energy in mobile devices they are power by batteries which have limited capacity small size of battery and heavy consumption make it more important constraint to think before we make any changes in existing solution. It is high priority requirement to make energy consumption as low as possible to increase node as well network life.

2.3.2 Decentralized **-** MANET there is no central authority to monitor and coordinating network, so it is difficult to detect and prevent fault and issue in network

2.3.3 Routing overhead **-** Adhoc network node perform packet routing and routing lookup, due to dynamic nature of network node are moving so there is path breaks and frequent route lookup

2.3.4 Limited Resources **-** Adhoc network used shared wireless medium there is limited bandwidth available for users in network

2.3.5 Environment impact - Wireless communication affect by following issues such as noise, frequency interference, signal attenuation, line-of-sight issue, radio signal path loss, multipath fading, diffraction and diffraction of radio wave

2.3.6 Security - Wireless nature of communication links make this network more susceptible and vulnerable for security threats like eavesdropping and traffic analysis. Limited resources make it an opportunity for attacker to target and degrade the expected performance. For example, DDOS attack or flooding attacks are used to increase bandwidth and battery consumption. It leads to degrade node life and delay in packet delivery.

3. NETWORK SECURITY

Network Security is protecting and maintaining confidentiality integrity availability of network information and services and resources.

3.1 Network Security Goals

3.1.1 Confidentiality – it ensure that message should be kept secret between sender and receiver. Message should protect form passive attack such as eavesdropping and traffic analysis.

3.1.2 Integrity – it ensure that message is not modified in transit in any unauthorized manner, it deals with authenticity of data. Integrity should protect form active attack such as man-in-middle attack.

3.1.3 Availability – it deals with service and resource of network to authentic members.it should protect form attack such as denial of service attack.

3.1.4 Authentication – it provide a trusted membership to users in network and verify and validate identity of user with a pre-shared secret (password) or digital certificate.

3.1.5 Authorization – it limit access level of users in network, which user can access particular services.

3.1.6 Resilience – it is survivability of network if a network segment is compromised, network should resist attack with help of mitigation technique and sustain network operation and services.

3.1.7 Timely Delivery – this term also known as data freshness, attacker can send previously capture data and repeat this data for time critical application require real time data such as data analysis ,remote site monitoring ,war field sensing this application required accurate data.

3.2 Network Security attacks

Security threats are attempts made by attacker to compromise network information or degrade performance. The vulnerabilities in ad-hoc networks make it more susceptible and prone for security threats. It may be classified into two categories-

3.2.1 Passive Attack – It is kind of where malicious node listens and observes the content of packet by eavesdropping and traffic analysis. But it does not make any fabrication and modification or drop packet.

3.2.2 Active attack - attacker may try to introduce malicious node inside the network or compromise the trusted node for Dropping of packets, denial of service attack, modification of data and sending fabricated spoofed message in network

Following table give introduction of various attack at layers in Mobile Adhoc Network.

Table 1: Various Attack in TCP/IP suit Layers

Security Threats	TCP/IP Layers	Impact of Security Threat
Jamming	Physical Layer	Disturb the communication and Jam the transmission through jam signal
DOS	Data Link Layer	Unauthorized access of resources and services.
Black-hole	Network Layer	Misguide the intermediate nodes about shortest path and towards destination and drop or fabricate packet content.
Worm-hole		Directly capture packet from source using cooperative wormhole nodes perform malicious task.
Byzantine		Compromised intermediate node(s) attempt to create collusion or routing loop
Sybil		Malicious node consist one or more fake identity and try to establish confidence among linked nodes.
Node Replication		Create replica of existing node and perform malicious task
SYN Flooding	Transport Layer	Power draining or resource engagement through incomplete synchronization.
Virus, Worm	Application Layer	Malicious code attempt to degrade the performance of applications or protocol.

4. PROBLEM STATEMENT

Sybil Attack is Named after the case study of a woman have multiple personality disorder.it is First described by Microsoft researcher John Douceur in peer to peer network. Sybil attack based upon fact that computer's in network are not able ensure and verify identity of each other in non-trusted environment. In computer network identity is internet protocol (IP) a 32bit number is allocated to each device for identity and address for communication in network and computer are known as node. Sybil attack is implemented when a malicious node claim multiple fabricated or stolen identity in network The node represent multiple fake identity and effect the network operation ,performance and fault tolerance of network. Malicious node use IP spoofing technique to implement Sybil attack. Sybil attack in effective in both Distributed and Peer to peer network, it effective on redundancy mechanisms of distributed data storage systems and effective against routing algorithms, data aggregation, voting, fair resource allocation and misbehavior detection, reputation system, torrent network, content delivery network.The attack introduce form inside or outside of network outside attack can be prevented by authentication but inside attack is not. It is important detect and mitigate Sybil attack Sybil attacks harmful for security and trust of network in peer to peer and distributed network such as torrent or anomaly network such as tor .The proposed problem may happen in MANETs.

Problem 1- all system in network have one to one mapping between physical and logical identity of node, but malicious node violate this and introduce fake logical identify in network.

Problem 2- In Large network nodes are not able to validate and verify identity of other nodes in network

Problem 3- Malicious node effect routing of network and create false path in network and disrupt network operation.

Problem 4- Sybil node gain disproportional amount of resource in network using multiple identity.

Problem 5 – Sybil node hide identity of other malicious node so it is difficult to trace attacker.

5. SYBIL ATTACK

A Sybil attack is kind of attack in which malicious node carries fake identities of existing or non-existing legitimate node to control a part of network. A Sybil attack may apply due to poor authentication on network layer .it is an attack which creates repudiation of large fake identities a single physical node to gain disproportional large influence .this attack aims to degrade network services or availability of resources when co-operation is required. The Sybil attack occur in network when it runs without central authority.

A Sybil attack is an approach in which a malicious node illegitimately fakes multiple identities by compromised node or clamming same from external source Sybil attack is also capable of disturbing routing mechanism in MANET multipath routing and secure routing may affected by this attack. In multipath routing fake identities may be the part of one or various routes in different position. To compromise communication and degrade network performance.

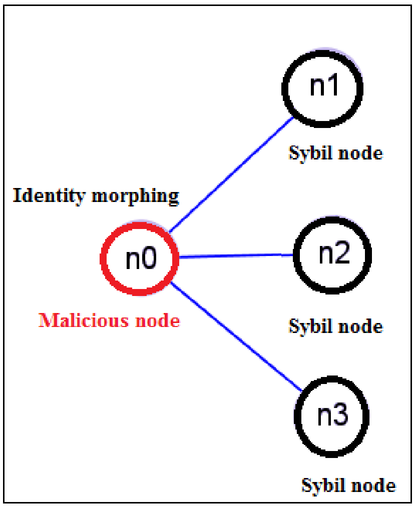

Figure 4: Sybil attack

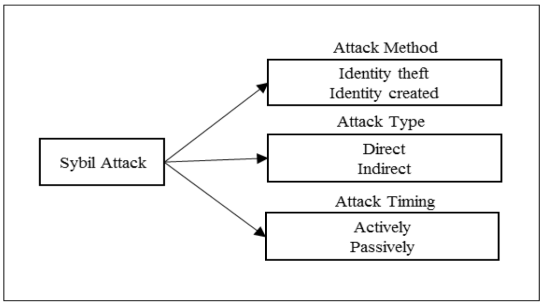

Figure 5: Sybil Attack Taxonomy

5.1 Sybil attack taxonomy

5.1.1 Dimension I Communication Type - Direct or Indirect Communication Sybil node perform attack through directly communicate with legitimate node, it can directly send message to node, and Sybil node may be next hop to genuine node. Indirect Communication Sybil node have some hop distance to legitimate node or done communication via other malicious node.

5.1.2 Dimension II Identity Method - Fabricated Identity or Stolen Identity. Sybil node required identity to communicate in network, malicious node can get identity by two ways -Sybil node Create a new identity in network, if only there is no restricted identity then it generate random identity and used it for sending messages. Sybil node spoofed identity of legitimate node, it is identity replication where an identity of node is theft and copied used in network for communication. Sybil node may use identity of remove or idle nodes.

5.1.3 Dimension III Timing - Simultaneous or Non-simultaneous. Sybil node attack network actively, it participate in network with all spoofed identity and used them one by one for sending message. Sybil node attack network passively, it perform attack randomly with spoofed and fake identity within a time range.

5.1.4 Dimension IV Node Behavior - Malicious or selfish. Selfish or greedy Sybil node is used reply attack and send fake messages with spoofed identity, this node Use greedily network resource such as bandwidth of other legitimate node by using their identity .Malicious Sybil node affect network performance and they target reputation systems in network .they also affect routing of network.

5.2 Sybil node attacks

5.2.1 Smurf attack – Sybil node send ICMP echo message to broadcast address of network with spoofed IP address of legitimate node then ICMP echo-reply message from all host in network is designated to legitimate node which create flooding traffic for legitimate node

5.2.2 Fraggle attack – Sybil node broadcast UDP echo packet to network with spoofed identity of legitimate node and legitimate node flooded with reply traffic from network.

5.2.3 ARP-poisoning attack - Sybil node send reply message of arp request with spoofed IP address of gateway so it become gateway for node and perform active or passive attack on packet which send by nodes.

5.2.4 Routing loop – Sybil node send RREQ packet in network then nodes send RREP to Sybil node but the RREQ source not listed in network so RREP packet propagate in hole network until ttl value of IP packet is expired

5.2.5 TTL expiry attack - Sybil node decrement the TTL value to zero of IP packet which it received to forward ,then Sybil node send ICMP time exceeded with spoofed identity of legitimated node.so source node assume there is routing issue with particular node and remove node form its routing table.

5.3 Sybil attack effect

5.3.1 Resource allocation

Sybil attack create influence in resource distribution in network. In network there is limited shared resource such as bandwidth here Sybil node behave like greedy node, use identity of legitimate user and use network resources behalf of them. For example channel bandwidth is assigned to each node per time slot basis .Sybil node gain disproportional amount of resources and create resource availability issue for other node in network. Many network system used traffic quota system which limit data to send in particular time period.

Example node n5 use identity of n0, n1, and n2 and send resource request ticket to n2.n4 is legitimate user

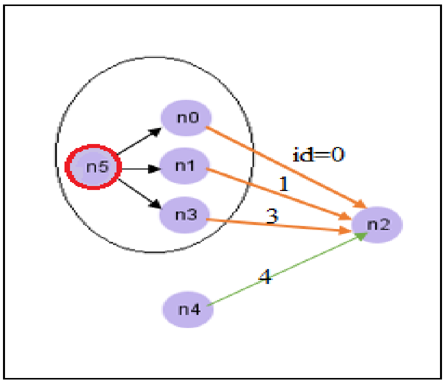

Figure 6: Sybil Attack in Resource Allocation

5.3.2 Voting

Sybil node have multiple identity ,in voting Sybil node behave as selfish node and actively participat2e in voting such as cluster head selection ,reporting malicious node(IDS) .Sybil node send vote with spoofed identity and impact on voting process . It impact voting but also give explore to malicious node to behave and control sink hole /cluster head.

It will not only lead for wrong election but will also compromise performance of complete segment in network.

Sybil node n3 use identity of n0, n1 and voted with x value to n4

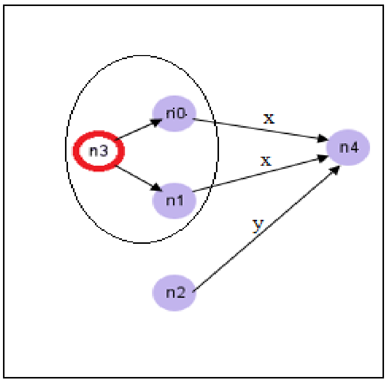

Figure 7: Sybil attack effect on Voting

5.3.3 Distributed Storage

Distributed system required redundancy of data .network node need to write process data to multiple location for redundancy and distribution of data .Sybil node claim multiple identity in distributed system and other node write data to Sybil node assuming writing it at different location.

Example process id p0, p1 of node n4 and n5 respectively need to write data at n1, n2, n3 storage location. Sybil node n0

Claim fake identity and data stored only at n0 .so data is located at false location and no redundancy is implemented

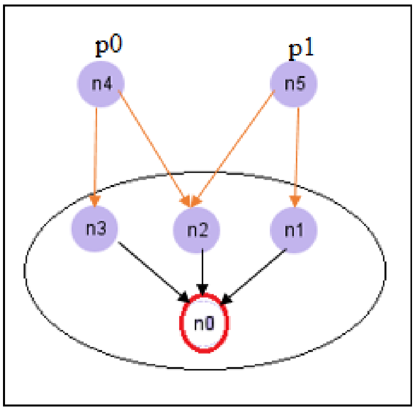

Figure 8: Sybil attack effect on Distributed Storage

5.3.4 Data aggregation

In special purpose application collection of data required from different sources (node) in network...application required periodic update data from sensors and monitoring system. Sybil node can send data with clamming identities and create false data sets.

5.3.5 Routing

Routing protocol is used to discover route from source to destination, Sybil attack may give a big impact on functionality of network. Here a malicious node can present multiple fake identities which can involve into multiple path to disrupt routing procedure.

The complete phenomena will lead to wrong route selection and poor network performance.

In scenario node Sybil node n5 show identity of n1 and n6 and create ambiguous routing path in network

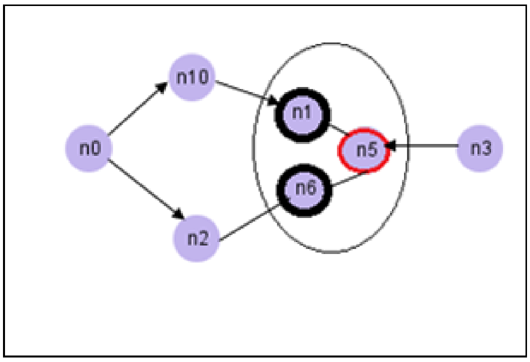

Figure 9: Sybil attack effect on Routing

5.3.6 Hidden Node

Sybil node increase its reputation, trust and creditability, so accuracy to detecting a malicious node is reduced. It create false alarm generating in (IDS/IPS) system .attack such as DOS attacker, worm, gray hole are done by other malicious node in network. Attacker is hide it identity and remain undetected. Node n5 is malicious node and node n4 is Sybil node and n4 hide original identity of n5

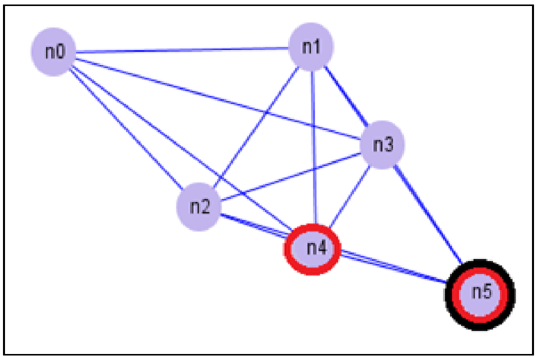

Figure 10: Sybil attack effect on misbehavior Detections

6. SYBIL ATTACK APPROACHES

6.1 RSSI Based Method

Received signal strength indication is radio signal power level measurement, each node in network have different RSSI value due to its location and distance from other node. This based upon localization algorithm it is lightweight solution for Sybil attack based upon rssi value of sender of message. Authors claims their solution is very efficient and robust and low percentage of false positive .this solution required collaboration between nodes and one protocol message exchange. Rssi Based method use multiple receiver. Detector node received protocol message

They associate sender-id and radio value and calculate location of node. When the same associate value is used by other node the node is suspected Sybil node. [10]

6.2 Trusted Authority

This method introduced trusted centralized authority in network. The authority is used to assign identity and credentials in network and one to one mapping between node and its identity. Assigned .credential use by trusted authority are cryptograph keys, digital certificate, computed checksum or hash value to verify and validate node identity.

Trusted Authority approach

6.2.1 Certificate Authority- peer to peer network a central authority used to assign ,trusted credentials to node in network such as digital certificate or validation certificate.it is similar as SSL certification assignment by CA

6.2.2 Cryptography solution – using Public key infrastructure for authentication and validity of node. a trusted node have public key of all nodes in network and send public key encrypted message for verification of nodes when node received message it decrypted it and send reply back message encrypted with private key to trusted node.

*6.2.3 Trusted System app*roach – this approach used a single (p2p) or group (distributed network) of administrative node in network to monitor, analysis, detection of abnormal communication pattern .if the detect threat they block node and remove from routing table of nodes in network. This approach is similar to Intrusion detection system (IDS)

6.3 Radio Resource Testing Resource testing method used single radio antenna and limit bandwidth for communication in network, it method is collaborative approach for Sybil attack defense .due to single radio antenna node acts as half-duplex communication system ,they either send or receive message at particular time. Detector node send broadcast message in network wait for replay packet .if detector node listed more than one message with same identity ,the identity is used to create Sybil attack in network.

6.4 Super node Approach

This approach protect routing from Sybil attack. A node with highest id selected as super node or cluster head. All traffic should be transit through supernode (snode).this node maintain topology table and routing table of network. Each route lookup request send to snode and snode replay with route path.

6.5 Random key Predistribution

Key distribution approach in followed in this approach.it create secure communication channel between nodes. Random key set is assigned to nodes and common key used to establish channel for communication. A set of key k assigned form key pool p and node can only communicate if they exchange shared key.

6.6 Position verification

In special type adhoc network sensor network node are located at fixed location.in sensor network a topology map is created and stored in each node. When some node failed sensor node look for other route. If node found in more than one route so it may be a Sybil node. This approach is truly based upon assumption and it is very costly in resource consumption.

Table 2 – Comparative Study of Sybil attack Approach with parameters

Technique	**Description**	**Validation node**	**Disadvantage Vulnerabilities**	**Application domain**
RSSI Based Method[10]	Radio signal strength value is used to identify Sybil node in network	Monitor node	Based upon assumption. Radio signal value is time-varying, unreliable and High false positive rate Hidden node Problem	Sensor Network adhoc network
Trusted Certificate[19]	A central trusted authority used in network to validate and verify identity of nodes	Central/head node	Required central monitor and preconfigured node. Adhoc network are decentralized. Compromise of credentials	Social network Adhoc network
Radio Resource Testing[11]	Radio channel allocation Assign each node a particular radio channel to communication with neighbor node	Neighbor node	Inefficient and required resource intensive computation Reduce performance Passive Sybil node undetected	Adhoc network Sensor network
Supernode Approach[6]	cluster head is selected to validate node identity and trusted node selection	Cluster head node	Create north-south pattern for transit traffic If node down recreate full routing table ,routing overhead Clusterhead selection may be compromised	Adhoc network
RandomKey Predistribution [13]	Radom key assigned to node for communication in each pair	Any node	If pair match is not found then request for new pair Time consuming Indirect Sybil attack is not prevent	General
Position Verification[14]	Topology table of network is used to obtain physical location of node	Neighbor	Required topology map installed in network Limited security	Sensor network
Code Attestation[15]	A secret hash value is associated with node and used as exchange value between nodes for communication	Any node	Secret value exchange each communication period. Secure code used in reply attack	General
Cryptography solutions[14]	Public key infrastructure is used encryption of decryption of data with use of public and private keys.	All nodes	Establishment of secure channel ,when communication is establish	General

7. CONCLUSION

The complete study observed that, MANET and its routing protocols are vulnerable and prone to various security threats and may open gate to take off their involvement into network. Furthermore, work also gives a deep taught on Sybil attack and its impact on MANET. Work also explore some existing solution and concludes that they all try to detect Sybil attack in ad-hoc network but limited to central authority based topology. It cannot be perform without involvement of base station or central authority. It generates a requirement to investigate and determine solution for peer to peer network without considering central authority. It also determine that, there is need to improve the node authentication approach in routing protocols to avoid fake involvement among multiple path and route selection process.

This study ends with significant identification of gap among existing solutions and techniques of implementation to Sybil attack. The complete work concludes that MANETs plays a very important role through vital range of applications. But it becomes very risky without involvement of security policy. The complete phenomena observe that Sybil attack may give a big impact to degrade network performance and compromising information. There is need to derive some mechanism to develop authentication mechanism to overcome this problem and enhance network performance.

8. FUTURE WORK

The proposed solution is lightweight detection and prevention technique of Sybil attack in mobile adhoc network.it is based upon trusted node approach and acknowledgement based method to detect Sybil node in Network .Performance metrics for analyze the result are packet delivery ratio, end to end delay and packet loss ratio , bandwidth utilization .

9. ACKNOWLEDGEMENT

The authors wish to acknowledge oriental university for their support & motivation during this research. The Authors would also like to thank anonymous referees for their many helpful comments, which have strengthened the paper. Author also like to give thanks to Dr. Deepak Sukheja and Prof. Amrita Tiwari for discussions in specific domain.

10. REFERENCES

[1] John R. Douceur “The Sybil Attack “International workshop on Peer-To-Peer Systems” Pages 251-260 ISBN: 3-540-44179-4 Year 2002

[2] Piro, C “Detecting the Sybil Attack in Mobile Adhoc network” IEEE Securecomm and Workshops Page(s):1 – 11 E-ISBN: 1-4244-0423 Sept 2006

[3] G. Umamaheswar “Detection of Sybil Attack in Mobile Wireless Networks” International Journal of Engineering Science & Advanced Technology ISSN: 256 262 Vol.2 Issue-2 Page 256 – 262 Year 2012

[4] Security Issues and Sybil Attack in Wireless Sensor Networks International Journal of P2P Network Trends and Technology Volume3 Issue1- 2013

[5] Brian Neil Levine, Clay Shields ,N. Boris Margolin “Survey of solutions to the Sybil attack” Department of computer science, university of Massachusetts Page(s) 1-11 Year 2006

[6] Priyanka Sharma , Dr. Kamal Sharma, Surjeet Dalal “Preventing Sybil Attack In MANET Using Super Node Using Approach” International Journal of Recent Research Aspects, ISSN: 2349-7688, Vol. 1, Issue 2 pp. 25-30 Sept. 2014

[7] Anamika Pareek,Mayank Sharma “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 Page No.66-70, June 2015.

[8] Amol Vasudeva1 and Manu Sood “Sybil Attack On Lowest Id Clustering Algorithm In The Mobile Ad Hoc Network” International Journal of Network Security & Its Applications (IJNSA), ISSN: 0974 - 932 Vol.4, No.5 Pages 135-147, September 2012

[9] J. Newsome, E. Shi, D. Song, and A. Perrig “The Sybil attack in networks analysis & defences”, the 3rd International Symposium On Information Processing In Sensor NetworksPages 259-268 ISBN:1-58113-846-6 Year 2004

[10] Murat Demirbas, Youngwhan Song “An RSSI-based Scheme for Sybil Attack Detection in Wireless Networks” International Symposium on on World of Wireless, Mobile and Multimedia Networks ISBN:0-7695-2593-8 Page(s) 564-570 Year 2006

[11] Diogo Mónica “On the Use of Radio Resource Tests in Wireless ad hoc Networks” INESC-ID Page(s) 1-8 Year 2009

[12] Yue Liu “ A Defense Against Sybil Attacks in Wireless Networks Without Trusted Authorities” IEEE Transactions on Mobile Computing ISSN 1536-1233 Issue 99 Feb 2015

[13] Chunling Cheng “An Approach Based on Chain Key Predistribution against Sybil Attack in Wireless Sensor Network” International Journal of Distributed Sensor Networks Vol. 2013 (2013), Article ID 839320, Page(s) 1-8 July 2013

[14] Debapriyay Mukhopadhyay, Indranil Saha “Location Verification Based Defense AgainstSybil Attack In Sensor Networks” 8th International Conference on Distributed Computing and Networking Pages 509-521 Online ISBN 978-3-540-68140-3 2013

[15] Makhdoom “A Novel Code Attestation Scheme Against Sybil Attack” Software Engineering Conference (NSEC), 2014 National11-12 Nov. 2014 Page(s):1 – 6 ISBN:978-1-4799-6161-0