# A Survey on Types of Attacks and Security in Mobile Ad hoc Network

**Priyanka Patware[1], Prof. S. R. Yadav[2]**

*[1]PG Scholar, CSE, [2]Associate Prof. & Head, P.G. CSE*

*Millennium Institute of Technology and Science, Bhopal, India*

***Abstract -— A Mobile ad hoc network is self-configuring infrastructure having less network of mobile device (laptops, smart-phones, sensors, etc.) connected by wireless link. This type of network is separate network. Security is a primary issue in order to provide secure communication in aggressive environment. There are still some challenges associated with MANETS that needs to be overcome. These challenges includes routing, short battery life, limited capacity, dynamically changed topology etc. In this work the fundamental challenging issues, Security challenges and different types of Attacks associated with MANET has been presented. Survey has been carried out on work done on Sybil attack and other attacks that generate fake identification in network. The property of this attack is to presents the two different identities in network. The proposed existing security scheme will detect the attack identification in network and block their whole misbehaviour activity as mentioned in this paper. The attacker degrades the whole network performance and this survey represents the different attacks malicious behaviour and the security aspects against attack in MANET.***

***Keywords: - MANET, Router, Sybil Attack, Security, Topology Misbehaviour activity, malicious.***

## I. INTRODUCTION

Mobile Ad hoc Network (MANET) [1] is a mobile network without having any fixed infrastructure. Each mobile node in an ad hoc network moves randomly and acts as both a router and a host. A Mobile ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and random basis. Nodes inside each other's radio range communicate directly via mobile nodes links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and obtain signals at the same frequency band. However, due to their natural characteristics of dynamic topology and lack of centralized management security, MANET is susceptible to various kinds of attacks.

A fixed behind structure limits the adaptability of wireless system. In infrastructure wireless networks, a user directly communicate with an access point or base station but on the other hand MANET, never rely on a fixed infrastructure for its procedure, a MANET is a self-configuring infrastructure less network of mobile devices connected by wireless.

## II. SYSTEM MODEL

Figure 1 represents communication between the nodes in MANET environment. The nature of ubiquitous devices makes wireless networks the easiest solution for their interconnection and, as a consequence, the wireless area has been experiencing exponential growth in the past decade. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves.

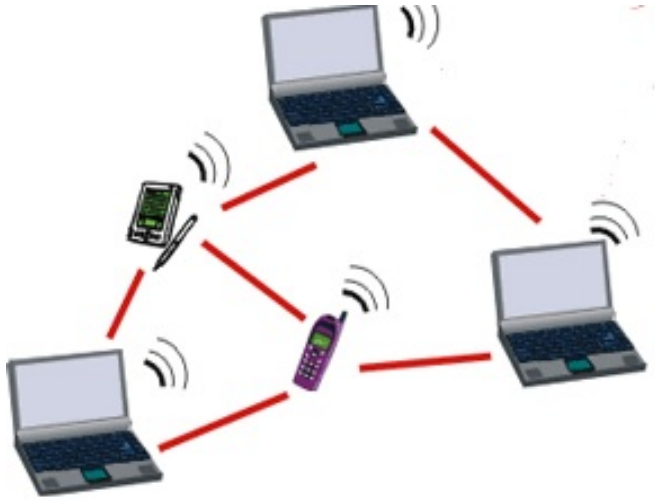

Fig. 1 Mobile Ad hoc Network

The mobile devices or the nodes of the MANTES are free to move, enter and leave eventually, node also can act as a router that can forward packets due to lack of infrastructure support. Ad hoc network also allows to device to maintain connection to the network as well as without difficulty removal and add up of devices. Due to this node mobility feature the topology of the network changes animatedly, hence the network is decentralized. Due to mobility of nodes MANETS are more susceptible than wired networks in many scenarios.

## III. ROUTING IN MANET

Routing is essential service for end-to-end communication in MANET, attacks on routing protocol disrupt the reliability and performance of MANET. It can be divided into two categories, first is routing disruption attack which the attacker trying to change the course of packets. Second resource consumption attack, the attacker inserts packet into the network to consume resources [2]. According to how the information is acquired, the routing protocols can be classified into proactive, reactive and hybrid routing [3, 4].

### *A. Proactive (table-driven) Routing Protocol*

The proactive routing is also known as table-driven routing protocol. In this routing protocol, mobile nodes periodically broadcast their routing information to the neighbor's nodes. Each node needs to maintain their routing table of not only adjacent nodes and reachable nodes but also the number of hops. Therefore, the disadvantage is the rise of overhead due to increase in network size, a significant big communication overhead within a larger network topology. However, the major advantage is of knowing the network status immediately if any malicious attacker joins. The most familiar types of the proactive routing protocol are: - Destination sequenced distance vector (DSDV) routing protocol and Optimized link state routing (OLSR) protocol.

### *B. Reactive (on-demand) Routing Protocol*

The reactive routing protocol is equipped with another appellation named on-demand routing protocol. In compare to the proactive routing, the reactive routing is simply starts when nodes desire to transmit data packets. The major advantage is the reduction of the wasted bandwidth induced from the cyclically broadcast. The disadvantage of reactive routing protocol method is loss of some packet. Here we briefly describe two prevalent on-demand routing protocols which are: - Ad hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) protocol.

### *C. Hybrid Routing Protocol*

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are: - Zone routing protocol (ZRP) and Temporally-ordered routing algorithm (TORA).

## IV. PREVIOUS WORK

The attackers are degrades the network performance at different layers. In this survey we focus on the misbehaviour of sybil attack in MANET.

**Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat [6]** "Lightweight Sybil Attack Detection in MANETs" in this title we discuss a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system. Through the help of extensive simulations and real-world test bed experiments, we are able to demonstrate that our proposed scheme detects Sybil identities with good accuracy even in the presence of mobility.

**Nitish Balachandran** [7] "A Review of Techniques to Mitigate Sybil Attacks" In this title, we discuss the different kinds of Sybil attacks including those occurring in peer-to-peer reputation systems, self-organising networks and even social network systems. In addition, various methods that have been suggested over time to decrease or eliminate their risk completely are also analysed along with their modus operandi.

**Chris Piro Clay Shields Brian Neil Levine** [8] "Detecting the Sybil Attack in Mobile Ad hoc Networks" In this title, we show that mobility can be used to enhance security. Specifically, we show that nodes that passively monitor traffic in the network can detect a Sybil attacker that uses a number of network identities simultaneously. We show through simulation that this detection can be done by a single node, or that multiple trusted nodes can join to improve the accuracy of detection. We then show that although the detection mechanism will falsely identify groups of nodes travelling together as a Sybil attacker, we can extend the protocol to monitor collisions at the MAC level to differentiate between a single attacker spoofing many addresses and a group of nodes travelling in close proximity.

**Sarosh Hashmi, John Brooke,[9]** "Towards Sybil Resistant Authentication in Mobile Ad hoc Networks" In this tile we present an authentication mechanism for MANETs that utilizes hardware id of the device of each node for authentication. An authentication agent is developed that verifies the hardware id of the authenticate node. A comprehensive defense model is employed to protect the

authentication agent from various static and dynamic attacks from a potentially malicious authenticate node. Security of authenticate node is assured by involving a TTP that signs the authentication agent, verifying that it will perform only intended function and is safe to execute. With this minimal involvement of the TTP, the proposed authentication scheme offers increased resistance to the Sybil attack. The attacker is now required to either thwart agent protection mechanisms or to acquire multiple devices with different hardware ids, in order to gain multiple identities.

**Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial[10]** "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET" We present in this context a Sybil detection approach, based on received signal strength variations, allowing a node to verify the authenticity of other communicating nodes, according to their localizations. In addition, we demean estimated metric of the distinguish ability degree between two nodes, allowing to determine Sybil and malicious ones within VANET. The applicability of our contributions is validated through geometrical analysis, simulations and real measurements.

**John R. Douceur[11]** "The Sybil Attack" in this title we discuss Large-scale peer-to-peer systems face security hreats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. 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 title 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.

**James Newsome, Elaine Shi, Dawn Song, Adrian Perrig,[12]** "The Sybil Attack in Sensor Networks: Analysis & Defenses" This title systematically analyzes the threat posed by the Sybil attack to wireless sensor networks. We demonstrate that the attack can be exceedingly detrimental to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, etc. We establish a classification of different types of the Sybil attack, which enables us to better understand the threats posed by each type, and better design countermeasures against each type. We then propose several novel techniques to defend against the Sybil attack,

and analyze their electiveness quantitatively.

**Bin Xiao, Bo Yu, Chuanshan Gao,[13]** "Detection and Localization of Sybil Nodes in VANETs" In this title we present a lightweight security scheme for detecting and localizing Sybil nodes in VANETs, based on statistic analysis of signal strength distribution. Our scheme is a distributed and localized approach, in which each vehicle on a road can perform the detection of potential Sybil vehicles nearby by verifying their claimed positions. We first introduce a basic signal-strength-based position verification scheme. However, the basic scheme proves to be inaccurate and vulnerable to spoof attacks. In order to compensate for the weaknesses of the basic scheme, we propose a technique to prevent Sybil nodes from covering up for each other. In this technique, traffic patterns and support from roadside base stations are used to our advantage. We, then, propose two statistic algorithms to enhance the accuracy of position verification. The algorithms can detect potential Sybil attacks by observing the signal strength distribution of a suspect node over a period of time. The statistic nature of our algorithms significantly reduces the verification error rate. Finally, we conduct simulations to explore the feasibility of our scheme.

**N. Marchang, R. Datta [14]** "Light-weight trust-based routing protocol for mobile ad hoc networks" in this title we discuss a light-weight trust-based routing protocol. It is light-weight in the sense that the intrusion detection system (IDS) used for estimating the trust that one node has for another, consumes limited computational resource. Moreover, it uses only local information thereby ensuring scalability. Our light-weight IDS takes care of two kinds of attacks, namely, the black hole attack and the grey hole attack. Whereas our proposed approach can be incorporated in any routing protocol, the authors have used AODV as the base routing protocol to evaluate our proposed approach and give a performance analysis.

**Muhammad Nawaz Khan, Muhammad Ilyas Khatak, Muhammad Faisal** [15] "Intrusion Detection System for Ad hoc Mobile Networks" In this title we analysis distributed-ID, a smart agent in each mobile node analyzes the routing packets and also checks the overall network behavior of MANETs. It works like a Client-Server model using Markov process. The proposed local distributed- IDS shows a balance between false positive and false negative rate.

**Liang Xiao, Student Member, IEEE, Larry J. Greenstein, Life Fellow, IEEE, Narayan B. Mandayam, Fellow, IEEE,**[16] "Channel-Based Detection of Sybil Attacks in Wireless Networks" We analysis enhanced physical-layer authentication scheme to detect Sybil attacks,

exploiting the spatial variability of radio channels in environments with rich scattering, as is typical in indoor and urban environments. We build a hypothesis test to detect Sybil clients for both wideband and narrowband wireless systems, such as WiFi and WiMax systems. Based on the existing channel estimation mechanisms, our method can be easily implemented with low overhead, either independently or combined with other physical-layer security methods, e.g., spoofing attack detection.

**Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty [17]** "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks" In this title, we analysis a lightweight and scalable protocol to detect Sybil attacks. In this protocol, a malicious user pretending to be multiple (other) vehicles can be detected in a distributed manner through passive overhearing by s set of fixed nodes called road-side boxes (RSBs). The detection of Sybil attacks in this manner does not require any vehicle in the network to disclose its identity; hence privacy is preserved at all times. Simulation results are presented for a realistic test case to highlight the overhead for a centralized authority such as the DMV, the false alarm rate, and the detection latency.

In this section author should discuss about related research has been done in the same domain or related domains with the name of the researcher and should be mentioned in the references.

## I. PROPOSED METHODOLOGY

*Data Collection and Implementation Strategy*

For data collection and implementation we will use Network Simulator- 2 (NS-2). The description about simulation environment is as follows:

Network simulator 2 (NS2) is the result of an on-going effort of research and development that is administrated by researchers at Berkeley [18]. It is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multipath protocol. The simulator is written in C++ and a script language called OTcl2. Ns uses an Otcl interpreter towards the user. This means that the user writes an OTcl script that defines the network (number of nodes, links), the traffic in the network (sources, destinations, type of traffic) and which protocols it will use. This script is then used by ns during the simulations. The result of the simulations is an output trace file that can be used to do data processing (calculate delay, throughput etc) and to visualize the simulation with a program called Network Animator.

Our expectation is to various factors affecting the detection Accuracy improve the system. We also expecting following results:

*D.* The value of packet transmission rates.

*E.* Node density and Node speed.

*F.* Sybil attackers with a high degree of accuracy.

*G.* Improve the transmission power attacks in the network.

*H.* Properly network connections are stabilised.

## V. SIMULATION/EXPERIMENTALRESULTS

The simulation will do on the NS-2 (version ns -3.31) on the basis of some simulation parameters mentioned in table1.

### 1.10.1 Performance Evaluation

| | |
|---|---|
| Number of nodes | 30 |
| Dimension of simulated area | 800×800 |
| Routing Protocol | AODV |
| Simulation time (seconds) | 100 |
| Attack Module | Sybil Attack |
| Protection System | Cooperative Protection System |
| Transport Layer | TCP ,FTP |
| Antenna Type | Omni Antenna |
| Traffic type | CBR,FTP |
| Packet size (bytes) | 1000 |
| Number of traffic connections | 10 |
| Maximum Speed (m/s) | Random |

There are following different performance metrics have been considered to make the comparative study of these routing protocols through simulation.

**(1) Routing overhead:** This metric describes how many routing packets for route discovery and route maintenance need to be sent so as to propagate the data packets.

**(2) Average Delay:** This metric represents average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination. It is measured in seconds.

**(3) Throughput:** This metric represents the total number of bits forwarded to higher layers per second. It is measured in bps.

**(4) Packet Delivery Ratio:** The ratio between the amount of incoming data packets and actually received data packets.

## VI. CONCLUSION

Mobile ad hoc networks have the ability to set up network and provide communication in such an environment where it is really impossible to have a traditional infrastructure network. The research on MANET and its security is still in its early stage, there are lots of technical issues. Improvement in bandwidth and capacity is required which need better spectral reuse and better frequency also. Due to mobility and open media nature MANET is easily vulnerable to security than that of other wired networks. So MANET requires better security mechanism in order to provide secure communication than wired networks. Research in the field of security is still open, we can design a security mechanism by which we can minimize or can completely remove effect of Sybil attacks. The presents survey is provides the idea of the new ways of identification of malicious activities of Sybil attack in MANET.

## VII. FUTURE SCOPES

We want to detect and protect from attack all the networks , provide security to all users . By using routing methods secure the data packets.

## REFERENCES

[1] ff Macro Conti, Silvia Giordano and Ivan Stojmenovi “Mobile Ad Hoc Networks”, Stefano Basagni, IEEE press, A john Wily & Sons, INC. publication, 2003

[2] A.K. Rai, R. R. Tewari and S. K. Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication,” International Journal of Computer Science and Security, Vol. 4, No. 3, pp. 265-274, 2010.

[3] Sunil Taneja and Ashwani Kush “A Survey of Routing Protocols in Mobile Ad Hoc Networks”, International Journal of Innovation, Management and Technology, Vol. 1, No. 3, pp. 279-285, August 2010.

[4] Ipsita Panda “A Survey on Routing Protocols of MANETs by Using QoS Metrics” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp. 121-129, 2012

[5] W. Stallings, "Cryptography and Network Security", Principles and Practices, 3rd edition, Prentice Hall, 2003.

[6] 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.

[7] Nitish Balachandran “A Review of Techniques to Mitigate Sybil Attacks” Int. J. Advanced Networking and Applications 11 July 2012.

[8] Chris Piro Clay Shields Brian Neil Levine “Detecting the Sybil Attack in Mobile Ad hoc Networks” NSF grants CNS-0133055, CNS-0534618, and CNS-0087639.