**4). Link spoofing attack or IP spoofing attack [3] [10]:** Spoofing offense commences its operation by announcing false links to the nearby nodes in a network, this process would essentially disturb the entire functioning of the network. Announcement of two false paths to the sender would essentially confuse the node and would end up in unnecessary transmissions. When a node is compromised by an attacker, then unnecessary dropping of packets and alteration of normal traffic routes would resemble as attacks. Sometimes numerous IP addresses would be generated by the fake node which does not actually exist in the concerned network. Again transmissions to such addresses would load the network.

## 3. INVADING THE ROUTING PROTOCOL

Various offenses disturbing the routing algorithms exist; these offenses would entirely cease the network's normal operation. Brief explanations of such offenses are given below [13] [14]:

Routing Table Overflow: Overflow of the routing table would enable the attacker to create routes that doesn't exist. The idea here is to create numerous routes to load the network excessively. There are two different types of routing algorithms in general; they are the proactive and reactive types. Proactive types would insist the user to collect the routing information prior to the process. The reactive types would specify the need for collecting the routing information only when needed. This attack would eventually cause an overflow in the routing tables. Overflows would prevent the entries of new routes.

***1). Routing Table Poisoning*:** This type of attack would make use of the compromised nodes to transmit misleading information regarding the routing table updates, or it may involve in modifying the original updates that is sent to the authenticated users. This attack would essentially result in congestions in the network or it may even turn some portions of the network inaccessible.

***2). Packet Reproduction:*** Here the useless or unwanted packets would be taken into consideration and suitable replications on those packets would be performed. These unnecessary replications would consume additional bandwidth and battery power resources creating insufficiency of the same.

***3). Route Cache Poisoning:*** As far as the routing protocols are considered, each node would maintain a separate routing table which would hold the necessary routing details about the entire network [14]. Messages regarding the addition of new routes or deletion of existing routes if any would be constantly updated in the routing table. Modification on such contents would essentially poison the routing table.

***4). Rushing offense:*** The procedure of suppressing the contents regarding the routing information during the route discovery process is found to be susceptible to such attacks [12]. Together with the actual node the compromised nodes too would receive the route request messages, immediately after receiving such request messages the compromised node would transmit packets continuously to the concerned network in view of overloading the network. At times when the nodes of a particular network receives the genuine route request message, it would then be in a position to distinguish the actual messages from the messages sent by the attacker, after which it would essentially discard the packets. Identifying the secure routes in a network that is not subjected to attacks is not an easy process.

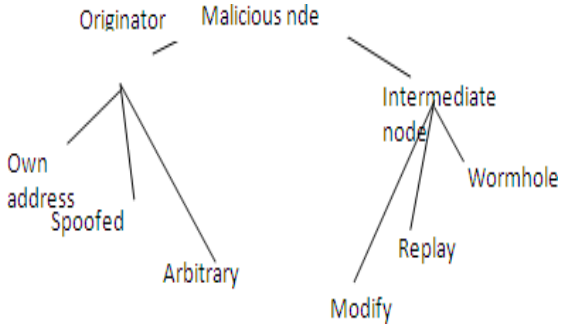


Figure 5: Representation of a malicious attack tree

## 4. VARIOUS OTHER ATTACKS ON A NETWORK

***1). Rushing offenses:*** The on demand routing protocols are responsible in carrying out this attack on the ad hoc networks, a copy of every packet that is meant to be transmitted is retained at the nodes of the network. The strategy adopted here is to transmit unwanted messages in par with the genuine messages. The genuine messages are therefore misunderstood as duplicate messages and thus discarded by the nodes. Another type of attack here is called as the spoofing attack; in this type, the compromised or malicious node would impersonate itself as the original node of the network by means of modifying its IP or MAC address.

***2). Gray hole offense:*** Gray hole attacks are more common in the ad hoc networks. This attack comprises of two different phases, in the initial phase the compromised node would send announcements stating that it has the set of valid addresses and corresponding route details relevant to the concerned destinations. In the second phase the nodes of a network would essentially involve in the task of dropping the intercepted packets with a certain probability. Gray hole attacks are quite difficult to identify when compared with that of the black hole attacks [5]. This attack expresses its fraudulent behaviors in various ways. One such expression is to continuously drop the data packets for a fixed time duration after which the compromised nodes would switch back to its usual behavior.

***3). Sinkhole offenses:*** This type of attack would enable the malicious nodes to attract the passing data packets towards itself from all the concerned neighboring nodes of a network. This attack seems to be the most important of all the other attacks as gaining illegal access to the data packets is achieved only in this type of attack. The strategy adopted by this attack is to identify the loopholes

of the routing algorithms and thereby incorporate the same for establishing themselves as the most trusted partners of the existing original nodes of the network.

***4). Location disclosure [9]:*** An attack that focuses on the privacy aspects of an ad hoc network is the location disclosure attack. The idea of this attack is to determine the location of a particular node; this can be achieved either by intruding into the network and thereby monitoring the structure and the incidents happening inside or by simply hacking the traffic patterns for in depth location details.

***5). Jamming offense:*** The MAC layer is seen as the platform over which this attack takes place. This attack is a form of the denial of service attack. Any interruption in the ongoing communication procedures in a wireless network is called so as the jamming attack. This attack encounters just by preventing the progress of the real time traffic over the network. Further it would prevent the genuine nodes from transmitting data packets to the prescribed destinations.

***6). Information Disclosure [12]:*** The aim of a secured communication is to completely protect the confidential contents from unauthorized access. Another consideration of a secured communication is to safeguard the genuine nodes from being compromised. Various other materials to be protected would include the locations of nodes, private and public keys used in the encryption and decryption process, passwords etc. Any leak in the contents of the above mentioned materials would fall into the information disclosure problem. Control data packets are sometimes more essential in the regulatory procedures, loss of those packets would again lead to the disruption of the network transmissions.

## 5. CONCLUSION

It is thus evident from this survey paper that the offenses against a mobile ad hoc network may take different forms depending on certain parameters as mentioned below: (1) the circumstances and surroundings in which a particular attack has been launched (2) targets devised by the hackers, especially the layers selected by an attacker to launch the attack (3) the ranges selected for implementing the attacks, this includes the incorporated security mechanisms of a system. Before designing an ad hoc network it is mandatory to focus on the security needs, so that improved safety mechanisms can be devised in order to protect the system and the transmission procedures. The devised security strategies must essentially consider the nature and the characteristic features of the various available offenses. MANETs are more susceptible to attacks as they do not exhibit a fixed infrastructure and that the communicating nodes move from one point to the other constantly. Hence MANETs require increased security levels than that of the conventional wired networks. New algorithms and security strategies can thus be devised keeping in mind the attacks on a mobile network.

## REFERENCES


1] Gopalakrishnan, S. (2004) “A Survey on Wireless Network Security”, International Journal of Computer Science and Mobile Computing, 3(1): 53-68.

2] Razak, S. A., Furnell, S. M. and Brooke, P. J. (2004) 'Attacks against mobile ad hoc networks routing protocol', Proceedings of the 5th annual postgraduate symposium on the convergence of telecommunications, networking and broadcasting (PgNeT), Liverpool, 28-29.

3] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication,” International Journal of Computer Science and Security (IJCSS), 4(3): 265-274.

4] Hongmei Deng, W. Li, Agrawal, D.P.(2013), “Routing security in wireless ad hoc networks”, Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, 40(10): 70- 75.

5] Ujjal Agarwal, Yadav, P.K and Upendra Tiwari, “Security Threats in Mobile Ad-Hoc Neetwork”, International Journal of Research in Science and Technology, 3(4): 53-64.

6] Jayashree. A. Patil and Nandini Sidnal, “Survey-Secure Routing Protocols of MANET”, International Journal of Applied Information Systems, 5(4):8-15.

7] Wang YT, Chen IR, Wang DC. A survey of mobile cloud computing applications: perspectives and challenges. *Wireless Personal Communications* 2015; **80**(4): 1607–1623.

8] Hu, Y.C., A. Perrig, D.B. Johnson, (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. J. Wireless Netw., 11: 21-38.

9] K. Sanzgiri, D. Laflamme, B. Dahill, B. Levine, C. Shields and E. Royer.(2005), “An Authenticated Routing for Secure Ad Hoc Networks”. Journal on Selected Areas in Communications special issue on Wireless Ad hoc Networks.

10] Roopak, M., & Reddy, B. (2013). Blackhole Attack Implementation in AODV Routing Protocol. International Journal of Scientific & Engineering Research, 4(5): 402-406.

11] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay International Journal of Computer Science and Security (IJCSS), 4(3): 265-274.

12] L. Zhou and Z. J. Haas.(1999), “Securing Ad Hoc Networks”. IEEE Network Magazine, 13(6):24-30.

13] Perkins, C.E and Royer, E.M,(1999), "Ad Hoc On-Demand Distance Vector Routing". Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, Pages 90-100.

14] Kumar, R., Verma, P., & Singh, Y. (2013). Mobile Ad Hoc Networks and It’s Routing Protocols. World Academy of Science, Engineering and Technology International Journal of Computer, Information, Systems and Control Engineering, 7(8).

15] Kumar, R., Verma, P., & Singh, Y. (2014). Review of MANET Protocols and Introduction of a New Optimized Routing Scheme using Evolutionary Algorithms and Analytical Hierarchy Process. Wireless Communication, 6(4), 161-171.

16] B. Sukla,(2008) “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks”, In proceeding of the World Congress on Engineering and Computer Science, 22-24.
17] Bing Wu, Jie Wu, Eduardo B. Fernandez, Mohammad Ilyas, Spyros Magliveras,(2007) "Secure and efficient key management in mobile ad hoc networks", Journal of Network and Computer Applications 30 (10):937-954.
18] M. Gunasekaran, P. Sampath and B. Gopalakrishnan, (2009), “AAS: An Authenticated Acknowledgement-Based Scheme for Preventing Selfish Nodes in Mobile Ad Hoc Networks”, International Journal of Recent Trends in Engineering, 1(1), : 294-298.