ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Survey on Attacks in MANET

Archana.R[1], Mrs. Gracy Theresa[2]

P.G Scholar, Dept. of Computer Science & Engineering, Adhiyamaan College of Engineering, Hosur, India[1]

Assistant Professor, Dept. of Computer Science & Engineering, Adhiyamaan College of Engineering, Hosur, India[2]

Abstract: Mobile ad-hoc network is a continuously self configuring infrastructure fewer networks of mobile devices connected without wires. Each device in a MANETs is free to move independently in any direction and in therefore change its link to any other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANETs is equipping each device to continuously maintain the information required to properly route traffic and security. MANETs are usually setup in situations of emergency for temporary operations or simply if there are no resources to setup elaborate networks. As MANETs are deployed in adversarial environment there is no proper security to transmit the data securely. There are many types of attacks that causes while communication takes place between source and destination. Attacks are harmful against wireless ad-hoc network and delay tolerance network, in which a node illegitimately claims multiple identities in order to gain unfair influence. Attacks in MANETs can be classified as active and Passive Attack, Wormhole, Black hole, rushing attack etc. In this survey paper the different types of attacks in ad-hoc networks and security goals, MANET challenges, MANET security challenges and attacks in different layers have been discussed.

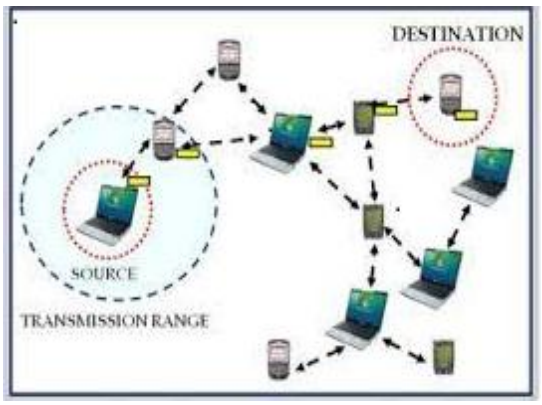
Keywords: MANETs,Adversarial, Delay Tolerance, Active Attack, Passive Attack, Wormhole, Black Hole,Rushing Security attacks.

I. INTRODUCTION

A MANET is a type of ad-hoc network that can change locations and configure itself on fly. Because MANETs are mobile they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection or another medium such as a cellular or satellite transmission. Some MANET is restricted to a local area of wireless devices while others may be connected to the internet. A Mobile ad-hoc network is generally defined as a network that has many free or autonomous nodes,often composed of mobile devices or other mobile pieces that can arrange themselves in various ways and operate without strict top-down network administration. MANET is a self-configuring network of mobile router connected by wireless links the union of which forms an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily. Thus the networks wireless topology may change rapidly and unpredictably.

These types of networks operate in the absence of any fixed infrastructure which makes it easy to deploy at the same time however due to the absence of any fixed infrastructure. It becomes difficult to make use of the existing routing technique for network services and this poses a number of challenges in ensuring the security of the communications something that is not easily done as many of the demands of network security conflict with the demands of mobile network mainly due to the nature of mobile devices.

We have surveyed the security attacks and the security goals and attacks in each layer. First section has described MANET challenges and its security challenges. Third section gives security goals required for secure routing in MANET. Fourth Section gives detailed description of various attacks on MANET. Fifth section will provide various types of attacks at each layer.



MOBILE AD-HOC NETWORK

II. MANETS CHALLENGES

Regardless of the variety of applications and the long history of mobile ad hoc network, there are still some issues and design challenges that we have to overcome [24]. This is the reason MANET is one of the elementary research field. MANET is a wireless network of mobile nodes, its a self organized network. Every device can communicate with every other device i.e. it is also multi hop network.

1) The scalability is required in MANET as it is used in military communications, because the network grows according to the need, so each mobile device must be capable to handle the intensification of network and to accomplish the task [4].
2) MANET is a infrastructure less network, there is no central administration. Each device can communicate with every other device, hence it becomes difficult to detect and manage the faults. In MANET, the mobile devices can move randomly. The use of this dynamic

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

topology results in route changes, frequent network partitions and possibly packet losses [25].

3) Each node in the network is autonomous; hence have the equipment for radio interface with different transmission receiving capabilities these results in asymmetric links. MANET uses no router in between.
4) In network every node acts as a router and can forward packets of data to other nodes to provide information partaking among the mobile nodes. Difficult chore to implement ad-hoc addressing schemes, the MAC address of the device is used in the stand alone ad hoc network. However every application is based on TCP/IP and UDP/IP.

III. MANET SECURITY CHALLENGES

A. Dynamic topology: In MANETs node may join or leave dynamically. As node moves frequently establishing trust among nodes are very difficult [21].

B. Battery Constraints: Mobile nodes will be running with Battery. If node power utilized unnecessarily then nodemay comes to idle state [22].

C. Lack of Central Authority: In MANET there will be no centralized authority like infrastructure network. Soimplementing security without centralized authority is a challenging task.

D. Insecure Environment: Nodes may move randomly inMANET. So malicious node may attack and steal thedata.

IV. SECURITY GOALS

The following are five major security goals which require preventing from attacks [19]:

A. Access control: It is the prevention of an unauthorized use of a resource [1].

B. Authentication: Authentication ensures that the communication or transmission of data is done only by the authorized nodes. Without authentication any malicious node can pretend to be a trusted node in the network and can adversely affect the data transfer between the nodes [20]. Identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and tell other nodes in the network to add that node to their blacklists and isolate legitimate nodes from the network.

C. Availability: ensures that network resources are available all time and also ensures the ability to sustain the networking functionalities without any interruption due to security threats [3].

D. Confidentiality: Confidentiality ensures that data should be accessible only to the intended party. No other node except sender and receiver node can read the information. This is implemented through data encryption techniques [8].

E. Group Signature: Group signature scheme can provide authentications without disturbing the anonymity. Every member in a group may have a pair of group public and private keys issued by the group trust authority (i.e., group manager).The member can generate its own signature by its own private key, and such signature can be verified by other members in the group without revealing the signer's identity. Only the group trust authority can trace the signer's identity and revoke the group keys.

F. Integrity: Integrity ensures transmitted data is not being altered by any other malicious node.

G. Non-Repudiation: Non-repudiation ensures that neither a sender nor a receiver should not deny a transmitted Message [5].

V. ATTACKS IN MANET

A. CLASSIFICATION OF ATTACKS

Giving security to the Mobile Ad-hoc Network is a difficult task. In order to given better solution for security attack, First we must identify and understand about the attack because of the unavailability of centralized coordinator in MANET, the security is a challenging task in wireless communication.

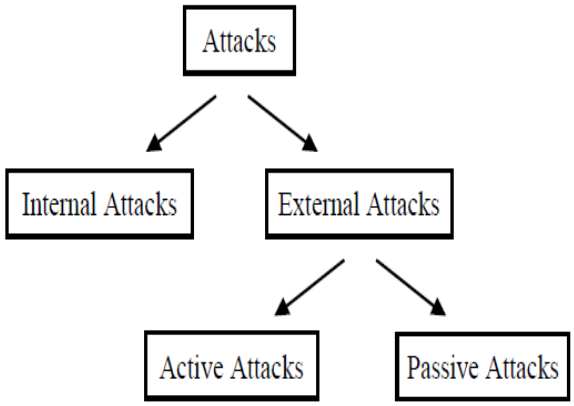


Fig 1: Classification of Attacks

The security attack classification is given below:

1) *Internal Attack:* The internal attacks are initiated from the compromised nodes in the mobile Ad-hoc network. In here the attacker node gets the unauthorized access and showing that as a normal mobile node. It analyses the data flows between the nodes in the network [2].
2) External Attack: These attacks are created by the nodes that are outside the network. It creates wrong routing information or service unavailability [11].

The External Attacks have two different classifications. They are:

- Active Attack
- Passive Attack

2.1. Active attack: In active attack the intruders can modify the packets, inject the packets, drops the packets, or it can use the various feature of the network to launch the attack. Active attacks are very dangerous.

The following are the types of active attacks over MANET and how the attacker's threat can be performed [6].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

2.1.1. Active Interference: An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications. The effects of such attacks depend on their duration, and the routing protocol in use. Attacker can change the order of messages or attempt to replay old messages. Old messages may be replayed to reintroduce out of date information [5].

2.1.2. Active insider attack: They can modify, inject, and replay genuine messages. They can also masquerade as other nodes and launch the impersonation attacks. They can create one or more phantom nodes by generating valid routing packets.

2.1.3. Active outsider attack: The passive attackers avoid any attack that reveals their actions since they attempt to be invisible, but the active outside attackers do not have such restrictions. They may aim to disrupt the routing or launch a DoS attack. They can move from here to there and launch attacks randomly.

*2.1.4. Black hole Attack:*Route discovery process in AODV is vulnerable to the black hole attack [15]. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough routes, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

*2.1.5. Blackmail:*The attack incurs due to lack of authenticity and it grants provision for any node to corrupt other node's legitimate information. Nodes usually keep information of perceived malicious nodes in a blacklist. This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and tell other nodes in the network to add that node to their blacklists and isolate legitimate nodes from the network [17].

*2.1.6. 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 [11].

2.1.7. Cloning Attack: Clone attack or node replication attack is a severe attack in WSNs [16]. In this attack, an adversary captures only a few of nodes, replicates them and then deploys arbitrary number of replicas throughout the network. It is very hard to distinguish between non compromised nodes a clone node since a clone has the same security and code information of original node. Hence cloned nodes can launch a variety of other attacks. The detection of cloning attacks in a wireless sensor network is therefore a fundamental problem. Many existing protocols expose the following limitations: high performance overheads, unreasonable assumptions, necessity of central control, lack of smart attack detection etc. Few existing approaches like solved these problems. But here we present a security model to detect two more attacks along with cloning attack detection with the same communication cost and performance overhead. We used the benefit of mobile agent to reduce the communication cost. Also the proposed protocol considers Mobile Wireless Sensor Network environment.

2.1.8. Colluding misrerlay attack: In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET [14]. This attack is difficult to detect by using the conventional methods such as watchdog and path rather. Consider the case where node A1 forwards routing packets for node T. the first attacker A1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets. In the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

2.1.9. Denial of service Attack: It is a common attack. It may slow down or totally interrupt the service of a system. The attacker can use several strategies to achieve this. She might send so many bogus requests to a server that the server crashes because of the heavy load. The attacker might intercept and deletes a server response to a client .making the client to believe that the server is not responding. The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.

*2.1.10. 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

*2.1.11. Eavesdropping:*The intruder silently listens to the communication by tapping the wireless link.

2.1.12. 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 neighbour can no longer be contacted.

2.1.13. Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance [14]. For example, in AODV protocol, a malicious node can send a

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service

2.1.14. Impersanation Attack: Impersonation attacks are launched by using other node's identity, such as IP or MAC address. These attacks are sometimes are the first step for most attacks, and are used to launch furthermore sophisticated attack [7].

2.1.15. The Invisible Node Attack: Andel et al. have defined the invisible node attack and proved it to be different from the existing attacks (man in the middle, masquerading, and wormhole) and established its uniqueness. They have defined it as in any protocol that depends on identification for any functionality, any node that effectively participates in that protocol without revealing its identity is an invisible node and the action and protocol impact is termed an INA. Discussing the effects of INA on different routing protocols, they have shown it to be an unsolvable attack so far.

2.1.16. Jamming: Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication [12]. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

*2.1.17. Link spoofing attack:*In a link spoofing attack, a malicious node advertises fake links with non-neighbours to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two hop neighbours. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks.

2.1.18. Link Withholding & Link Spoofing Attacks: In link withholding attack, the malicious node does not broadcast any information about the links to specific nodes. It results in losing the links between nodes. In Link spoofing attacks, a malicious node broadcasts or advertises the fake route information to disrupt the routing operation. It results in, malicious node manipulate the data or routing traffic [12].

2.1.19. Location disclosure attack: malicious node collects the information about the node and about the route by computing and monitoring the traffic. This way malicious node may perform more attack on the network [23].

2.1.20. Malicious code Attacks: malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

2.1.21. Man-in-the-middle Attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

2.1.22. Masquerading Attack: Masquerading or spoofing happens when the attacker impersonates somebody else.

2.1.23. Modification Attack: After intercepting or accessing information the attacker modifies the information to make it beneficial to herself.

2.1.24. Node Isolation Attack: The authors in this work have introduced an attack against the OLSR protocol. As implied by the name, the goal of this attack is to isolate a given node from communicating with other nodes in the network.
The idea of this attack is that attacker(s) prevent link information of a specific node or a group of nodes from being spread to the whole network. Thus, other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes.

2.1.25. Overwhelm attack: In this attack, an attacker might overwhelm network nodes, causing network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy.

2.1.26. Replay Attacks: In MANETs, the topology is not fixed; it changes frequently due to mobility of nodes. In replay attack, a malicious node record control messages of other nodes and resends them later. This results in other nodes to record their routing table with stale routes. These replay attacks are later misused to disturb the routing operation in a MANETs

2.1.27. Repudiation attacks: Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks. For example, spyware detection software has been developed in order to monitor mission critical services.

2.1.28. 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

2.1.29. Routing Table Poisoning Attack: Different routing protocols maintain tables which hold information regarding routes of the network. In poisoning attacks, the attacker node generates and sends fictitious traffic, or mutates legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. Another possibility is to inject a RREQ packet with a high sequence number.
This causes all other legitimate RREQ packets with lower sequence numbers to be deleted. Routing table poisoning attacks can result in selection of non-optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

2.1.30. Rushing Attack: Rushing attacks are mainly against the on-demand routing protocols. These types of attacks subvert the route discovery process. On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack [12]. When compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet can react. For example, in figure the node "4" represents the rushing attack node, where "S" and "D" refers to source and destination nodes. The rushing attack of compromised node "4" quickly broadcasts the route request messages to ensure that the RREQ message from itself arrive earlier than do those from other nodes.
This result in when neighbouring node of "D" i.e. "7" and "8" when receive the actual (late) route request from source, they simply discard requests. So in the presence of such attacks "S" fails to discover any useable route or safe route without the involvement of attackers

2.1.31. Selective Forwarding Attack: The selective forwarding Attack was first described by Karl of and Wagner [18]. This attack is sometimes called Gray Hole attack. In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them. There are different forms of selective forwarding attack. In one form of the selective forwarding attack, the malicious node can selectively drops the packets coming from a particular node or a group of nodes. This behaviour causes a DoS attack for that particular node or a group of node.
They also behave like a Black-hole in which it refuses to forward every packet. The malicious node may forward the messages to the wrong path, creating unfaithful routing information in the network. Another form of selective forwarding attack is called Neglect and Greed. In this form, the subverted node arbitrarily neglecting to route some messages. It can still participate in lower level protocols and may even acknowledge reception of data to the sender but it drops messages randomly. Such a node is neglectful. When it also gives excessive priority to its own messages it is also greedy. Moreover, another variance of selective forwarding attack is to delay packets passing through them, creating the confused routing information between sensor nodes.

2.1.32. Selfish Misbehaviour of Nodes: Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of the network. It may include two important factors. Conservation of battery power Gaining unfair share of bandwidth **.**The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources. These attacks exploit the routing protocol to their own advantage. Packet dropping is one of the main attacks by selfish node which leads to congestion in network. However most of routing protocols have no mechanism to detect whether the packets being forwarded or not except DSR (dynamic source routing).

2.1.33. Session Hijacking: Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks. In Session hijacking, the malicious node tries to collect secure data (passwords, secret keys, logon names etc.) and other information from nodes. Session hijacking attacks are also known as address attack which make effect on OLSR protocol. The TCP-ACK storm problem may occur when malicious node launches a TCP session hijacking attack.

2.1.34. Sleep Deprivation: In sleep deprivation attack, the resources of the specific node/nodes of the network are consumed by constantly keeping them engaged in routing decisions [17]. The attacker node continually requests for either existing or non-existing destinations, forcing the neighbouring nodes to process and forward these packets and therefore consume batteries and network bandwidth obstructing the normal operation of the network.

2.1.35. Snare Attack: Lin et al. have proposed the snare attack, which relates to military specific applications. In a battlefield, a node could be physically compromised (say when the corresponding soldier is caught by the enemy). Afterwards, the compromised node could be used to lure a Very Important Node, (say the commander), into communicating with it. Since the adversary can easily intercept any transmission in the network through the compromised node, the adversary can identify the physical location of the VIN by tracing and analyzing some routes. After locating the VINs, the adversary will be able to launch a Decapitation Strike on those VINs as a short cut to win the battle.

2.1.36. 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

2.1.37. SYN Flooding Attack: The SYN flooding attacks are the type of Denial of Service (DoS) attacks, in which attacker creates a large number of half opened TCP connection with victim node. These half opened connection are never completes the handshake to fully open the connection.

2.1.38. 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 [11]. 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

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

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. Wormholes are dangerous because they can do damage without even knowing the network

2.2. Passive attack: In this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information [10].

This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping:

2.2.1. 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 [11].

2.2.2. Monitoring attack: Monitoring is a passive attack in which attacker can see the confidential data, but he cannot change the data or cannot modify the data.

2.2.3. Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries [12]. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information.

2.2.4. Snooping: Snooping is unauthorized access to another person's data [13]. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data transmissions. Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage. Governments may snoop on individuals to collect information and prevent crime and terrorism. Although snooping has a negative aspect in general but in computer technology snooping can refer to any program or utility that performs a monitoring function. For example, a snoop server is used to capture network traffic for analysis, and the snooping protocol monitors information on a computer bus to ensure efficient processing.

2.2.5. Jellyfish Attack: In this attack, attacker breakdown the performance of the network by introduces the delay in sending packets that it receives [9].

B. ATTACKS IN DIFFERENT LAYERS [5]

Layers	Attacks	Solutions
Physical	Jamming	Using Spread spectrum mechanisms FHSS, DHSS
	Eavesdropping	
	Active Interference	
Data Link	Selfish Misbehaviour of Nodes	Secure link layer protocol like LLSP using WPA
	Malicious Behaviour of nodes	
	DOS	
	Misdirecting Traffic	
	Attacking neighbour sensing protocols	
Network	Worm Hole Attack	Securing routing protocols like SAODV, SAR, ARAN to overcome blackhole, impersonation attacks, packet leashes, SECTOR mechanism for wormhole attack
	Black Hole Attack	
	Byzantine Attack	
	Information Disclosure	
	Resource Consumption	
	Routing Attack Routing Table Overflow Routing Table Poisoning Packet Replication Route Cache Poisoning Rushing Attack	
Transport	Session Hijacking SYN Flooding	Securing End to End communication (SSL, TLS, SET)
Application	Virus,Worms Dos, Man in the Middle Attack Impersonation	Firewalls

VI. CONCLUSION

MANETs are vulnerable to routing security attacks due to its distributed nature, so it is vital to protect them. In this paper we categorize the challenges in MANET,security goals,the types of attacks and type of attacks that occurs in each layer . MANET security composed of challenging and complex area, in which further research is still being performed and will results in finding of new threats.

REFERENCES

[1] Satyam Shrivastava, Sonali Jain "A BRIEF INTRODUCTION OF DIFFERENT TYPE OF SECURITY ATTACKS FOUND IN MOBILE AD-HOC NETWORK" International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 03 Mar 2013.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

[2] LathiesBhasker t: "A SCOPE FOR MANET ROUTING AND SECURITY THREATS" ICTACT journal on communication technology, December 2013, volume: 04, issue: 04

[3] NidhiChoudhary, Dr.LokeshTharani(associate proffesor): "A SURVEY OF ROUTING ATTACKS IN MOBILE AD-HOC NETWORK" IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 4, No.4, August 2014.

[4] B.Praveen Kumar, P.ChandraSekhar, N.Papanna, B.BharathBhushan:"A SURVEY ON MANET SECURITY CHALLENGES AND ROUTING PROTOCOLS" P Chandra Sekhar et al, Int.J.Computer Technology &Applications,Vol 4 (2),248-256 IJCTA Mar-Apr 2013 .

[5] J. Godwin Ponsam1, Dr. R.Srinivasan "A SURVEY ON MANET SECURITY CHALLENGES,ATTACKS AND ITS COUNTER MEASURES" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 1, January – February 2014 ISSN 2278-6856.

[6] J. Godwin Ponsam1, Dr. R.Srinivasan "A SURVEY ON MANET SECURITY CHALLENGES,ATTACKS AND ITS COUNTER MEASURES" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 1, January – February 2014 ISSN 2278-6856.

[7] Pankajini Panda, Khitish Ku. Gadnayak, Niranjan Panda" MANET ATTACKS AND THEIR COUNTERMEASURES " International Journal of Computer Science and Mobile Computing Vol.2 Issue. 11, November- 2013.

[8] T. Navaneethanet al:" SECURITY ATTACKS IN MOBILE AD-HOC NETWORKS – A LITERATURE SURVEY", International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 4, April- 2014 ISSN: 2321-8363.

[9] Ashima Mittal1 and Satwinder Singh:"SURVEY ON VARIOUS SECURITY ATTACKS AND THE MITIGATION TECHNIQUES FOR MANET" International Conference on Communication, Computing & Systems (ICCCS 2014).

[10] MahaAbdelhaq, Rosilah Hassan, Mahamod Ismail, RaedAlsaqour, DaudIsraf, "DETECTING SLEEP DEPRIVATION ATTACK OVER MANET USING A DANGER THEORY –BASED ALGORITHM",International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085).

[11] PriyankaGoyal,SahilBatra , Ajit Singh, "A LITERATURE REVIEW OF SECURITY ATTACK IN MOBILE AD-HOC NETWORKS", International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.

[12] Gagandeep, Aashima, Pawan Kumar, "ANALYSIS OF DIFFERENT SECURITY ATTACKS IN MANETS ON PROTOCOL STACK A-REVIEW" ,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[13] Abhay Kumar Rai, Rajiv RanjanTewari&Saurabh Kant Upadhyay, "DIFFERENT TYPES OF ATTACKS ON INTEGRATED MANET- INTERNET COMMUNICATION" ,International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3).

[14] Rishabh Jain, CharulDewan, Meenakshi, "A SURVEY ON PROTOCOLS & ATTACKS IN MANET ROUTING", IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012 ISSN (Online): 2231 –5268.

[15] Pramod Kumar Singh, Govind Sharma, "AN EFFICIENT PREVENTION OF BLACK HOLE PROBLEM IN AODV ROUTING PROTOCOL IN MANET", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[16] D Sheela , G. Mahadevan," MOLLIFYING THE EFFECT OF CLONING, SINK HOLE AND BLACK HOLE ATTACKS IN WIRELESS SENSOR NETWORKS USING MOBILE AGENTS WITH SEVERAL BASE STATIONS", International Journal of Computer Applications (0975 – 8887) Volume 55– No.9, October 2012.

[17] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A SURVEY OF ROUTING ATTACKS AND SECURITY MEASURES IN MOBILE AD-HOC NETWORKS, JOURNAL OF COMPUTING", VOLUME 3, ISSUE 1, JANUARY 2011, ISSN 2151-9617.

[18] WazirZadaKhana, Yang Xiangb, Mohammed Y Aalsalema, QuratulainArshada "THE SELECTIVE FORWARDING ATTACK IN SENSOR NETWORKS: DETECTIONS AND COUNTERMEASURES", I.J. Wireless and Microwave Technologies, 2012, 2, 33-44 Published Online April 2012 in MECS.

[19] C.-K Toh, Ad Hoc Mobile Wireless Networks:Protocols and Systems, Prentice Hall, New Jersey, pp:34-37, 2007.

[20] J.P.Hubaux, L.Buttyan, S.Capkun, "THE QUEST FOR SECURITY IN MOBILE AD HOC NETWORKS," Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing *(MobiHOC)*, October, 2001.

[21] Hao yang, Haiyunluo, Fan ye, Songwulu, and Lixiazhang,"SECURITY IN MOBILE AD-HOC NETWORKS: CHALLENGES AND SOLUTIONS", IEEE Wireless Communications, Feb 2004.

[22] I.Chlamtac, M.Conti, and J.Liu, "MOBILE AD HOC NETWORKING: IMPERATIVES AND CHALLENGES IN AD HOC NETWORKS" vol. 1, no. 1, pp. 13-64, 2003.

[23] K.P.Manikandan, Dr.R.Satyaprasad, Dr.K.Rajasekhararao, "A SURVEY ON ATTACKS AND DEFENSE METRICS OF ROUTING MECHANISM IN MOBILE AD HOC NETWORKS", International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.

[24] C.-C. Chiang, "ROUTING IN CLUSTERED MULTIHOP MOBILE WIRELESS NETWORKS WITH FADING CHANNEL", in: Proceedings of IEEE SICON, April 1997, pp. 197–211.

[25] G. Aggelou, R. Tafazolli, "RDMAR: A BANDWIDTH-EFFICIENT ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS", ACM International Workshop on Wireless Mobile Multimedia(WoWMoM), 1999, pp. 26–33.