THE REQUIREMENTS OF SECURITY IN ADHOC NETWORKS.

A security protocol for ad hoc wireless networks should satisfy the following requirements

J Confidentiality:

- The data sent by the sender must be comprehensible only to the intended receiver.
- Though an intruder might get hold of the data being sent, he / she must not be able to derive any useful information out of the data.
- One of the popular techniques used for ensuring confidentiality is data encryption.

J Integrity:

- The data sent by the source node should reach the destination node without being altered.
- It should not be possible for any malicious node in the network to tamper with the data during transmission.

J Availability:

- The network should remain operational all the time.
- It must be robust enough to tolerate link failures and also be capable of surviving various attacks mounted on it.
- It should be able to provide guaranteed services whether an authorized user requires them

J Non-Repudiation:

- It is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
- Digital signatures are used for this purpose.

ISSUES AND CHALLENGES IN SECURITY PROVISIONING

The security provisioning in adhoc network differs from that in infrastructure based network.

Shared broadcast radio channel :

- The radio channel used for communication in adhoc wireless networks is broadcast in nature & is shared by all nodes within its direct transmission range.
- Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network.
- This problem can be minimized to a certain extent by using directional antennas.

1. ***Limited resource availability :***

- Resources such as bandwidth, battery power, & computational power are scarce in adhoc wireless networks.
- Hence it is difficult to implement complex cryptography-based security mechanisms in

networks.

2. ***Insecure operational environment :***
   - The operating environments where adhoc wireless is used may not always be secure.
   - One important application of such networks is in battlefields.
3. ***Physical Vulnerability :***
   - Nodes in these networks are usually compact & hand-held in nature.
   - They could get damaged easily & are also vulnerable to theft.
4. ***Lack of central authority:***
   - In wired networks & infrastructure-based wireless networks, it would be possible to monitor the traffic on the network through certain important central points & implement security mechanisms at such points.
   - Since adhoc -wireless networks do not have central points, these mechanisms cannot be applied in ad hoc wireless networks.
5. ***Lack of associations:***
   - Since these networks are dynamic in nature, a node can join or leave the network at any point of time.

6. If no proper authentication mechanism is used for associating nodes in a network, an intruder would be able to join into the network quite easily & carry out his/her attacks. Limited Resource availability:

- Resources such as Bandwidth, battery power and computational power are scarce in WSN.
- Hence It is difficult to implement complex cryptography based security mechanisms in such networks.

7. **Physical Vulnerability:**
   - Nodes in these networks are usually compact and handheld in nature.
   - They could get damaged easily and are also vulnerable to theft.