Chapter 2

Literature Review and General Discussion

2.1 Introduction to MANETs

2.1.1 Characteristics

Mobile ad hoc network (MANETs) is a collection of mobile nodes in which all the nodes are connected via wireless link. These are self configured networks. MANETs contains several characteristics. Because of these intrinsic properties, MANETs becomes special amongst the users. Nodes in MANETs perform in open media that permits the network to work without preinstalled infrastructure.

Figure 2.1 MANETs characteristics
Autonomous nodes of MANETs can play as host as well as router at the same time[144]. Figure 2.1 gives the idea of MANETs. These are not depended on central administration. So, network control and management is distributed amongst the nodes. Nodes must collaborate amongst themselves to avail the features of network [2].

Nodes in MANETs are free to move arbitrarily in any direction in different speeds. This leads to a dynamic network topology i.e. topology may change randomly at any moment in unpredictable fashion [144]. Thus it exhibits flexible network architecture to work with limited wireless connectivity and resources [3][6]. Network must comply with unstable node conditions including traffic and propagation condition as well as mobility pattern of the nodes. So it exhibits seamless interaction and ubiquitous mobile computing environment.

Neighbor discovery in MANETs is another intrinsic property of MANETs [3]. When a new node joins the network, immediately it is identified by the neighbor nodes and starts routing with it. Each node in the network works as intelligent node. Every node must work as DTE (Data Terminal Equipment) and DCE (Data Communication Equipment) [4].

Nodes in MANETs may rely on battery or on any exhaustible power device; So, computation and other activities of MANETs are always concerned with energy conservation [3][5][6].

The channels, over which nodes communicate, are shared by several sessions and hence subject to noise, fading, network interference. The path between any pair of nodes is a heterogeneous path and thus packets follow multiple wireless links to reach destination [2].

Another characteristic of MANETs is computational decentralization, which include independent computations, switching and computation capabilities of nodes [3]. Moreover it can support diversified digital devices such as iPods, PCs, palm handheld computers, smart phones, smart labels, smart sensors, automobile embedded systems etc.
2.1.2 Routing in MANETs

Nodes in MANETs exchange data dynamically within themselves without depending on base station. Routing is done by the routing protocol available for MANETs. Routing is the process through which user traffic is directed and transported from source to destination. Routing is the most crucial part of implementation of MANETs. Usually, packets are routed to destination from source via routers as shown in Figure 2.2.

Figure 2.2 Routing in MANETs

Figure 2.2, there is no specific device named as router; all the nodes connected to network are worked as host as well as router at the same time. To complete the routing function effectively, a good routing protocol is required. Routing in MANETs is signified as dynamic optimization task, which includes shortest path routing, optimum bandwidth utilization, and minimum delay in delivering packets. It also complies with minimum battery power and limited capacity of wireless link. Ad hoc network can enhance its performance parameters by utilizing all its nodes by allowing them to participate in packet forwarding as well routing [50][51]. Routing protocol in MANETs must be self organized and manageable. Routing must follow a loop free path while it transmits packets through multi hop path. In spite of dynamic topology change with rapid convergence, it must provide its service. It should be scalable to large network. As shown in the Figure 2.2, to send packets from source to destination,
Routing algorithm follows multi-hop routing path, at the same time it should look forward the shortest path out of several paths. Ultimate aim of routing in MANETs is to discover a path from source to destination, maintain the path in case of sudden link failure; in such cases it may alter its existing path.

Sometimes routing also provides periodic information to the nodes in MANETs. For routing in MANETs, several routing algorithm had been proposed. Task wise routing can be divided into four different segments such as,

a. Path discovery: When a node has to establish communication to destination, it will have to discover the shortest path through which data can be sent.

b. Path selection: During path discovery, if it discovers more than one path, in that case it will have to select the appropriate path based on some criteria provided in the network.

c. Data forwarding: After selection of path, routing must take the responsibility to forward packets to destination.

d. Path maintenance: Path maintenance helps to maintain the continuous flow of data in case of link failure that occurs in the network.

Routing in MANETs is limited by several characteristics that include MANET’s security, traffic pattern, routing functionality etc. In addition to these, routing in MANETs is also affected by a series of parameters such as multiple route selection, fast route establishment, bandwidth limitation, battery power constraints etc. According to different routing state, such as static, dynamic and quasi static, functionality of routing may vary. Node mobility is another important characteristic which must be considered for routing [49].

Routing in MANETs can be divided into two parts:

a. Proactive routing or table driven routing, here each node maintains one or more routing table keeping the information of entire network topology. These are updated regularly to keep up to date routing information of the network.

b. For this topology information needs to be exchanged between the nodes on
regular basis. In this routing, routes are available on request.

c. Reactive routing or on demand routing: It creates a route on demand when a packet to be sent from source to destination. For highly dynamic ad hoc network, this routing is desirable as it doesn’t require periodic updating of routing information as well as topology information.

Apart from these, MANETs has certain characteristics through which it decides the short-hop routing as it gains several benefits including energy saving as well as to reduce higher signal-to-interference ratios [48].

2.1.3 Routing Protocols

MANET Protocol

- Proactive protocol
  - DSDV
  - WRP
  - GSR
  - FSR
  - STAR
  - DREAM
  - MMWN
  - CGSR
  - HSR
  - OLSR
  - TBRPF

- Reactive Protocol
  - AODV
  - DSR
  - ROAM
  - LMR
  - TORA
  - ABR
  - SSA
  - RDMAR
  - LAR
  - ARA
  - FORP
  - CBRP

- Hybrid Protocol
  - ZRP
  - ZHLS
  - SLURP
  - DST
  - DDR

Figure 2.3 MANETs routing protocols

MANETs is a multi hops wireless network where all nodes are responsible for carrying packets from source to destination. To perform routing smoothly, it needs a set of instructions and algorithms. Accordingly, different set of routing protocols are
generated. Basic functions of such protocols are to find a route and deliver the packets to correct destination [52]. Basic properties of routing protocol include distributed nature, quality of service support, efficient bandwidth support, resource management, optimization of network performance matrices. Free from loop and strong security support [55]. The limited resource in MANETs forces the researchers to design an efficient and secure routing strategy to get reliable service [57].

Routing protocols in MANETs are classified into three different categories as shown in Figure 2.3 based on protocol discussed in the literature [52][53][54][55]. Out of these all, *Ad hoc on Demand Distance Vector (AODV)*, reactive protocol of MANETs, is discussed elaborately because AODV protocol has been taken as base protocol for implementation of proposed methodologies to detect PDA in MANETs in the thesis.

**Ad hoc on Demand Distance Vector (AODV)**

As shown in Figure 2.3, *AODV* is a reactive protocol in which routing tables are dynamically created when needed. When source node wants to send data to destination, it tries to establish the path through several ways by sending some RREQ packets. When it gets RREP packet containing shortest path, the source sends packets through this shortest path.

![Figure 2.4 Working of AODV](image)

Basic conception of AODV is based on DSR and DSDV protocol [59][60]. So, it copes with on demand route discovery and route maintenance concept of DSR, while from DSDV, it adopts the properties of hop-by-hop routing and maintenance of node sequence numbers. As a result, AODV becomes stronger enough to work in limited
bandwidth and node mobility of ad hoc network [59]. Each node in the network maintains routing table with routing details entries of its neighbor nodes with two counters namely sequence number and a broadcast id. Figure 2.4 shows the basic functionality of AODV. When a node wants to communicate with any other node in the network, it sends RREQ packets containing different fields like source address, source sequence number, destination address, destination sequence number and hop-count. A RREQ can be uniquely identified by observing the pair (source address, broadcast-id).

It establishes the reverse path back from all the nodes through which RREQ traverse. For any intermediate node, having route entry for destination in its routing table, it compares the destination sequence number in its routing table with that in the RREQ. If the destination sequence number in its routing table is less than that in the RREQ, it rebroadcasts the RREQ to its neighbors. Otherwise, it uncast a route reply packets to its neighbor.

### 2.1.4 Mobility Models

![Mobility models in MANETs](image)

Figure 2.5 Mobility models in MANETs
A mobility model in MANETs is a kind of model which mimics the movement of actual mobile nodes [61]. So, it explains the movement pattern of nodes in MANETs [53]. Mobility model is designed to understand the movement pattern of mobile users in terms of location, velocity and acceleration [64]. In real network, nodes change their direction as well as speed at any time anywhere. The performance of routing protocol is based on duration of interconnection between any two nodes taking part in communication [62]. The mobility of nodes affects the connectivity amongst the nodes. It then affects the performance of routing protocol.

As per spatial and temporal dependency, different mobility models can be found in MANETs. According to spatial dependency, two nodes are moving in same direction, implies they have high spatial dependency. Temporal dependency is a measure that explains how current velocity is related to previous velocity. Nodes having same velocities have high temporal dependency.

Mobility models in MANETs can be divided into several types as shown in Figure 2.5. Mobility models are divided into several categories as per their mobility characteristics. In temporal mobility model, movement of the mobile node is affected by its movement history. In spatial dependency model, the mobile nodes tend to travel in a correlated manner. Similarly in case of geographic restriction model, the movement of nodes are guided and bounded by streets, freeways and obstacles. In case of random models, nodes move independently to a randomly chosen destination with random velocity.

2.1.4.1 Random Model

In this model, nodes move independently to a randomly chosen directions with randomly selected velocities. Mobile nodes move freely without any restriction. Random model is categorized in two types, such as random way point model and other variations. Other variations include random direction model and random walk model. Out of these all, random way point model is vastly used.
2.1.4.1.1 *Random Way Point Model*

This model was first proposed by Johnson and Maltz [64]. Because of its simplicity and wide availability, this model is used vastly. To generate the node trace of the Random Waypoint model the *setdest* tool from the CMU Monarch group may be used. This tool is included in the widely used network simulator ns-2 [64]. It is a commonly used mobility model for MANETs. It explains the movement pattern of independent nodes in a simplified way as shown in Figure 2.6. It exhibits certain properties like,

- All the nodes move along the zigzag line from the waypoint $A_i$ to $A_{i+1}$.
- Waypoints are uniformly distributed over the convex area.
- From one point to other, at the starting point, it selects a random velocity drawn from velocity distribution.
- Formally the process is defined by $(A_i; A_{i+1}); (A_{i+1}; A_{i+2}); \ldots$
- At each way point, nodes waits for a random pause time
- Random way point model is used as elementary synthetic model for Ad hoc network. These are easier to implement for process simulation with analytical results and analytical results can be used to choose the realistic values for model parameters before the actual process simulation.
2.1.4.2 *Levy Walk Model*

Commonly used mobility models in computer networking research are random way point (RWP) or random walk models. These models are simple enough to be theoretically tractable and at the same time, to be emulated in network simulators in a scalable manner. However, no empirical evidence exists to prove the accuracy of such models. Human walks are not random walks, but the patterns of human walks and Levy walks contain some statistical similarity.

The term Levy walks (LW) was first coined by Schlesinger et al to explain a typical particle diffusion not governed by Brownian motion (BM). BM characterizes the diffusion of tiny particles with a mean free path (or flight) and a mean pause time between flights [172]. The Levy Walk Mobility Model proposed in [171][172] more or less imitates the human mobility behavior in an outdoor condition. Real world human mobility traces are generated at various places that include two different campuses, a metropolitan area and a park or any other places like this by using GPS devices. The word “flight” is used to define movement of an object along a straight line without any change in the direction.

There are certain difficulties in this model. It is difficult to get a human walk flight from the traces as the human seldom walks in a straight line. Also there might not be continuity in a human walk as the person may pause for few minutes or he may change the direction or may move in a vehicle and disappear for few minutes and appear in another location or it is run out of battery service etc. To eliminate some of the errors that it may provoke, three different methods are proposed for analysis. These are

**Rectangular:** If there is no pause while moving between the two points, then the distance between any two points is considered as a flight in the rectangular model

**Angle:** In this model, the length between any two points is a perpendicular length to the point from that position. The angle model takes various flights found out from the rectangular model and combines them into a single flight provided that there is
no pause between any of the successive flights and the relative angle is less.

**Pause based methods:** The pause model also combines the flights obtained from the rectangular model. It establishes more trajectories and accordingly represents the more natural human walk.

The Levy Walk Model consists of four variables namely flight length, direction, flight time and pause time. Flight length defines the longest straight-line trip of a particle from one location to another without a directional change or pause. It is characterized by other three variables like direction, flight time and pause time [170].

### 2.1.4.3 Model with Temporal Dependency

Due to physical constraints such as acceleration, velocity, direction and other factors of mobile entities, the velocity of mobile nodes varies according to previous velocity pattern to avoid abrupt velocity change in the network [61][64]. Initially it was proposed for simulating mobility in personal communication system. Nodes having same velocity- have high temporal dependency [62]. Various mobility models are proposed based on temporal dependency as random models are unable to cope with the temporal dependency behavior. *Gauss Markov mobility* model and Smooth *random mobility* model are example of such kind of mobility model.

#### 2.1.4.3.1 Gauss Markov Mobility Model

It was first introduced by Liang and Haas [64]. Here, the velocity of mobile node is assumed to be correlated over time and modeled as a Gauss-Markov stochastic process. It was designed to work with different level of randomness via single tuning parameter. Initially each mobile node is assigned with a current speed and direction. At fixed interval of time, n, movement occurs by updating the speed and direction of each mobile node. The value of speed $S_n$ and direction $d_n$ at the nth instance is calculated using the following equation.

\[
S_n = S_{n-1} + \hat{a} r_g S \\
\]

\[
d_n = d_{n-1} + \hat{a} r_g \hat{a} \\
\]

24
Here $S_n =$New speed and $S_{n-1} =$Current speed.

d_n = New direction, d_{n-1} = Current direction

$rg =$ A random number taken from standard Gaussian distribution.

$S =$ standard deviation of speed for the Gaussian distribution.

Gauss-Markov mobility model can generate movement with smooth curve and mobile nodes are generally stayed away from the edge of simulation area. This mobility model can reduce the sudden stops and sharp turns.

2.1.4.4 Model with Spatial Dependency

The mobile node's movement can be influenced by its neighborhood. In random model, mobile nodes move independently of its neighbor or any other nodes in the network. So, it is assumed that the location, speed, movement and directions are not affected by its neighbor node. As the velocity of different nodes are correlated with the status of neighbor nodes in space, so this specific type of mobility model is call as spatial dependency model [64]. This can be categorized as Reference point model and set of correlated models.

2.1.4.4.1 Reference Point Group Model

The conception of this mobility model is that mobile nodes in MANETs tend to coordinate their movements. Accordingly a new concept of spatial mobility model i.e. reference point group mobility (RPGM) model is proposed just like a number of soldiers move together in a group or platoon. In this model, each group has a group leader. So, the group leader decides the mobility pattern of group members [64]. The members of the group follow the leader’s mobility closely, with some deviation. As shown in Figure 2.7, multiple groups can move together in the network according to different mobility pattern of respective group with their group leader in the centre. Node mobility for each node is assigned with a reference point that follows the group movement.
Node mobility for each node is assigned with a reference point that follows the group movement. Each mobile node can be placed randomly in their neighborhood upon this reference point. RPGM model is able to emulate different type of mobility behaviors such as in-place mobility model, overlap mobility model, convention mobility model.

2.1.4.5 Model with Geographic Restriction

Geographic restrictions: Most of the realistic situation regarding application of MANETs in urban areas, the movement of a mobile node may be bounded by obstacles, buildings, streets or freeways. Random waypoint model and its variants are not able to handle those situations of mobility with specific characteristics. Thus, several other mobility models like obstacle mobility model or pathway mobility model were proposed. These are defined for the objects with some geographical points. Obstacle mobility model of geographic restriction model includes the movement path through which mobile nodes can pass through. The obstacle and paths are generated with the help of a tool called tergen. This tool is restricted to creation of rectangle shaped object but by changing the coordinate position of the corner of obstacle, some advance shapes can be created.

2.1.4.5.1 Path Way Model

This is an example of a geographic model which increases the probability for the
object to travel within some specified paths. The geographic model is sometimes used for map matching. These mobility models are then used by a particle filter or a Kalman filter sequentially with the incoming position measurements. So to integrate geographic constraints with mobility model, node movement can be restricted to the pathways in the map. The map can be predefined in the simulation as city section model, city map model, obstacle mobility model.

2.1.5 Security Issues in MANETs

2.1.5.1 Introduction

Due to intrinsic properties of MANETs such as open medium, lack of central monitoring and controlling system, dynamic network topology, autonomous terminal, distributed operations, multi hop routing, easy access of network etc., security becomes a major issues in MANETs [70][71][72][73]. Due to wireless link of MANETs, the network is susceptible to some attack such as active interference. As shown in Figure 2.8, all the nodes are allowed to access the wireless link without any central monitoring system. That makes the network vulnerable to attack. Due to dynamic topology of the network, nodes can easily enter or leave the network independently. So, there is no restriction to simply discard the malicious nodes from the network. Cooperative nature of the network also makes it vulnerable to attack. MANETs does not have any clear line of defense. Attacker can enter into the system at any time from any end. There is no clear line that separate the inside network from outside world.

Flexibility of operation in MANETs creates several security issues in MANETs in different layers of the network. In application layer of the network, security issues occur due to detecting and preventing viruses, malicious codes, application faults etc. In transport layer of the network, security issues occur in authenticating and securing end-to-end communication through data encryption. Issue of protecting ad hoc routing protocol in MANETs comes under network layer. Similarly link layer expects security issues in MAC sub layer. Security issues in physical layer are occurred in terms of signal jamming DoS attack [66].
Security issues in MANETs lead to some security goals such as authentication, integrity, confidentiality, availability, access control and non-repudiation [68].

Open peer-to-peer architecture of MANETs, creates security issues [73]. Since all the nodes in MANETs work as router and forward packets to next hop for destination, so presence of any vulnerable node may create security threat to the whole network. Moreover the wireless network is easily accessible to both genuine node as well as malicious node. Portable devices along with security information are vulnerable to attack. So, attacker can easily enter into the network with the help of these weaker devices as well as software.

The security solutions which are used for wired networks are ineffective and insufficient for highly dynamic network like MANETs.

### 2.1.5.2 Types of Attacks on MANETs

Mobile ad hoc network is vulnerable to different kind of attacks. Figure 2.9 shows categories of attack based on literature [74][75][76][77].
MANETs attacks
- Attack on MANETs Internet
  - Bogus Registration
  - Replay Attack
  - Forged FA
- Attacks on Mobile Ad hoc Networks
  - Passive Attacks
    - Snooping
  - Active Attacks
    - Network Layer Attacks
      - Wormhole Attack
      - Black hole Attack
      - Byzantine Attack
      - Information Disclosure
      - Resource Consumption Attack
    - Routing Attacks
      - Routing Table Overflow
      - Routing Table Poisoning
      - Packet Replication
      - Route Cache Poisoning
      - Rushing Attack
    - Transport Layer Attacks
      - Session Hijacking
    - Application Layer Attacks
      - Repudiation
    - Multi-layer Attacks
      - Denial of Service
        - SYN Flooding
        - Jamming
        - Distributed DoS Attack
      - Impersonation

Figure 2.9 Types of attack on MANETs

Attack on MANETs includes different attacks like Bogus registration, Replay attack and forged FA. In bogus registration, an attacker registers itself with bogus registration. An attacker may advertise itself as genuine node to the mobile nodes (MN) in such a way that MN starts registering the bogus node and shares its confidential information. In replay attack, valid data transmission is maliciously repeated or delayed by the malicious nodes present in the network. Forged FA is a
form of network attack in which a node advertises itself as a fraudulent FA then MN under the coverage of the forged FA may register with it. As a result, forged FA can capture the sensitive network data and may disturb the proper functioning of the network. Simply monitors the data exchanged in the network without disturbing the normal function of the network. At some point, the attacker also starts interpreting the data gathered through snooping, as a result confidentiality of network information leak out. An example of such kind of attack is snooping in which an attacker tries to access the unauthorized information from other MN.

In active attack, an attacker disrupts the normal functioning of the network by altering or destroying the original data. Again this kind of attack can be classified as external attack and internal attack. In external attack, malicious nodes are outside of the network. On the other hand internal attacks are carried out by the nodes which are part of the network. So, these are more severe kind of attack than the external attack.

Active attack may activate in different layers of the network as shown in Figure 2.9. Wormhole is a kind of network layer attack in which a malicious node tunnels the received packets from one location of the network to another location. This tunnel between two colluding attackers is referred to as a wormhole [79].

Attack on Mobile Ad hoc network includes both passive as well as active attack. Passive attack doesn’t disturb the proper operation of the network. Here, the attacker Routing in the network is severely disrupted when control packets are tunnels by this attack.

Black hole attack is a kind of network layer attack in which attacker listens to RREQ packets. Accordingly it responds to the sender by RREP, packets by showing the shortest path to the destination by altering sequence number. In response to this, when the sender sends packets through this attacker nodes, it consumes all the packets without forwarding these to destination [78][79].

In Byzantine attack, compromised intermediate nodes work together to create routing loops, forwarding packets through non-optimal path, selectively dropping packets as
well as maliciously dropping packets. As a result, network performance parameters degrade abruptly. According to information disclosure, confidential information of the network such as network topology, geographic location of nodes or optimal routes may disclose to unauthorized users by the attacker. Resource consumption attack helps the attacker to consume network resources such as battery power of MN, bandwidth, and computational power, which are limited to an ad hoc network.

Routing attack of active attack in MANETs is normally on the routing protocol of the network and disrupts the normal operations of the network. Routing table overflow is an example of such kind of attack in which attacker creates some unnecessary routes entry in the routing table, thus preventing the entry of new genuine routes in the table. Another example is the routing table poisoning. In this attack, malicious nodes present in the network, create fictitious routing updates in the table and thus mislead the sender to send packets. In case of packet replication, an attacker replicates the stale packets, thus consumes additional bandwidth of the network. In route cache poisoning, an attacker may modify the route cache to mislead the sender for forwarding packets. In rushing attack, an attacker quickly flooded the RREQ packets in to the network adversely; as a result, when the legitimate packets are flooded in the network, these are discarded by the MN by assuming these as duplicate packets. Session hijacking is an example of transport layer attack. In this attack, it gives an opportunity to the malicious node to behave as a genuine node. Since the entire authentication for the MN is done at the beginning of the session so, adversaries can take the advantage of attacking the system. Repudiation is a kind of attack which may occur in the application layer of the network. Similarly application layer attack contains repudiation attack. Multi-layer attack take place in any layer of network protocol stack. One example of such kind of attack is a kind of Denial of service attack in which attacker may prevent genuine MN from the services offered by the network. In SYN flooding attack, malicious node sends a
large number of SYN packets to victim node and then spoofing the return address. One of the severe attacks in MANETs is DDoS in which several adversaries are distributed throughout the network and they prevent the genuine nodes from accessing network services.

In impersonation attack, an adversary may become a part of network management and start changing the internal configuration of the network.

2.1.5.3 Security Goals

Security issues in MANETs lead to some security goals such as authentication, integrity, confidentiality, availability, access control and non-repudiation [68].

In authentication, it is expected that nodes in MANETs must authenticate each other to communicate amongst themselves. While communicating, it must ensure that there should not be any third party which interfere the communication. Authentication can be provided by different methodologies such as cryptographic hash function, digital signature and issuing of certificate.

Due to flexibility of MANETs, all types of MN are allowed to enter into the network. Malicious nodes may compromise with one another to mislead the genuine node and thus it may modify the original message or it may drop the packets without delivering these to destination. According to the concept of integrity, the original message must be in take. It should not be modified or dropped.

Another security goal of MANETs can be explained as confidentiality, which can be explained by the fact that any unauthorized persons are not allowed to view the message in original. It can be achieved by different encryption policies so that unauthorized persons are restricted from viewing the original messages.

Irrespective of state of the network, it must provide streamline service to the network. This fact can be explained by the concept of availability. According to non-repudiation, sender and receiver should not deny the receiving of message.

2.1.5.4 Vulnerabilities in Existing Protocol

MANETs is vulnerable to different kind of attacks due to its flexibility of uses.
Vulnerabilities in routing protocol implies the attacks against routing protocols to violet the rules of MANETs, insertion of erroneous routing information, attempting to disturb routing algorithm [82][83]. MANETs protocols are suffered from impersonation, fabrication etc. Attacks may come from any end. As mentioned in section 2.1.5.2, attacker may attack MANETs in different layer of the network such as application layer, transport layer, network layer, data link layer and physical layer.

Some of the draw backs of MANETs protocols are,

a. Lack of central monitoring system  
b. Lack of central point of entry  
c. Unable to handle high mobility of the nodes  
d. Limited resources like battery power, bandwidth  
e. Lack of clear line of defense and secure communication  
f. Easy authorization of MN  
g. Unable to handle distributed nature of attack

Due to vulnerabilities of protocol, a malicious router may inject packets with same identification information into the network by collecting source IP and sequence number of any packet [81]. So, destination accepts the invalid packets and discards the valid packets. Apart from these, different kind of attacks such as blackhole attack, wormhole attack, Byzantine attack, information disclosure attack, resource consumption attack, routing table overflow attack, routing table poison attack, packet replication attack and many other attacks are caused due to lack of security in MANETs protocol.

Again, as mentioned in section 2.1.5.3, security goals of MANETs can be achieved in terms of availability of service, integrity, confidentiality, authentication, non repudiation, authorization and anonymity etc. A malicious node which exhibit in the network maliciously and shows its presence in the network by packet dropping, battery drainage, bandwidth consumption, buffer overflow, stale packets, delay of
packets, link break, message tampering, fake routing, stealing information and session capturing [80].
Routing protocol in MANETs should be designed in such a way that it must meet the security goals to protect the network from attacks.

2.1.5.5 Security Mechanism

As mentioned in section 2.1.5.4, MANETs protocols are vulnerable to different kind of attacks. Adversaries compromise with network functions by attacking different layers of the network [84]. So, significant research efforts must be made to provide secure mechanism in such a way that it should increase the survivability of MANETs and protect MANETs from different attacks. It can be done either by developing secure routing protocol or by improving the robustness of MAC layer protocol [84].

![Security mechanisms in MANETs](image)

Security mechanisms in different levels are as follows:

**Link level security**: It specifies the data transfer security between two nodes. In ad hoc wireless network links are not secure. Adversaries can enter into the network at any time to intercepts the packets. So, there need a secure mechanism in this level in such a way that MN can trust each other to establish secure communication amongst them. Third party is not allowed to view information. To protect data, encryption and decryption policy of cryptography can be implemented. Certification authority is another kind of secure mechanism which can be applied as link level security in
MANETs. But certification mechanism creates network overhead and sometimes these are compromised with malicious nodes to consume confidential information from the network.

**Network level security:** Since all the nodes are worked as router in MANETs, so routing within the network is more vulnerable as adversaries are also worked as parts of network. Security mechanism in this level of the network is very challenging. Basic purpose of this security is to provide secure data transmission from source to destination. This kind of security mechanism should monitor the network in such a way that there should not be any modification or dropping of packets due to malicious node present in the network. Moreover, it should able to determine the presence of selfish node in the network. So, development of a proper intrusion detection system is an example of such kind of secure mechanism. It can be achieved by IPSec, self issuing of certificate, extending the existing routing protocol, application of multi agent system, game theoretic approach etc.

**Key management:** This is also another kind of secure mechanism, in which cryptographic keying mechanisms are used to provide security. It comprises of key generation, key distribution and key maintenance. Some key management techniques are symmetric key management such as OFT, Logical key hierarchy, asymmetric key management, mobile certification authority etc.

### 2.1.5.6 Secure Routing Protocol

Due to specific characteristics of MN of MANETs as router, mobile node that takes part in communication, have the right to work with data packets. Any intruder, which is also a part of network, may misuse the packets by its malicious activities. Most of the routing protocols are lacking behind the security. It assumes that all the nodes in MANETs are trustable. Secure routing protocols are derived as an extension of existing routing protocol. Security extensions are either cryptographic or trust based system [101]. Main security service of routing protocol is the authorization. Authorization is done by two different processes, first, when the routing updates come
from outside, router should decide whether it will make necessary change in it or not. It is named as import authorization. Another authorization known as export authorization may carry out whenever it receives a request for routing information. Authorization is related with another two terminologies such as authentication and integrity [100][102]. Routing protocol generates two kinds of messages, as data message and routing message.

Table 2.1: Security extension of some of MANETs routing protocol

<table>
<thead>
<tr>
<th>Reactive protocol</th>
<th>Proactive protocol</th>
<th>Hybrid protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension of DSR protocols:</td>
<td>Extension of DSDV:</td>
<td>Extension of ZRP:</td>
</tr>
<tr>
<td>1. SQoS Route Discovery</td>
<td>1. SEAD</td>
<td>1. SRP</td>
</tr>
<tr>
<td>2. Ariadne</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Confidant</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extension of AODV:</td>
<td>Extension of OLSR:</td>
<td></td>
</tr>
<tr>
<td>1. CORE</td>
<td>1. SLSP</td>
<td></td>
</tr>
<tr>
<td>2. SAODV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. TAODV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. SAR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. SPREAD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. ARAN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Data message can be protected by point-to-point security system as these are point-to-point in nature. But routing messages are normally processed or modified or resent by the immediate node, so immediate node must provide the power of authentication to process the routing message. Implementation of secure routing protocol is getting more challenging in MANETs to protect the network from intruders. Some examples of extension of existing protocols for secure routing are shown below in Table 1.

Data message can be protected by point-to-point security system as these are point-to-point in nature. But routing messages are normally processed or modified or resent by the immediate node, so immediate node must provide the power of authentication to process the routing message. Implementation of secure routing protocol is getting more challenging in MANETs to protect the network from intruders. Some examples of extension of existing protocols for secure routing are shown below in Table 1.
Following Table 2 shows the comparison of some of the secure routing protocols [101].

Table 2.2: Comparison of the best known secure routing protocols.

<table>
<thead>
<tr>
<th>Secure Protocol</th>
<th>Background Protocol</th>
<th>Type of Attack</th>
<th>Modification</th>
<th>Impersonation</th>
<th>Fabrication</th>
<th>Wormhole</th>
<th>Selfish</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ariadne</td>
<td>DSR</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Confidant</td>
<td>DSR</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SAODV</td>
<td>AODV</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>TAODV</td>
<td>AODV</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SAR</td>
<td>AODV</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ARAN</td>
<td>Reactive</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SEAD</td>
<td>DSDV</td>
<td>Weak</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SLS</td>
<td>OLSR</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SRP</td>
<td>ZRP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

2.1.5.6.1 SAODV

The Secure Ad hoc On-Demand Distance Vector (SAODV) routing protocol is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism by providing security features like integrity and authentication. It uses the cryptographic method to secure AODV protocol [85][86][87] [88][89][90][103][104].

Digital signature is used to authenticate non-mutable fields of the messages and hash chains to secure the hop count information, as for non-mutable information, authentication can be performed in a point-to-point manner. But for mutable information, same kind of technique cannot be used. Since router error messages are some big mutable messages. Hence, some other techniques are used [85]. SAODV can use the Simple Ad hoc Key Management (SAKM) as a key management system.

In these extension messages, there is a signature of the AODV packet with the private key of the original sender of the Routing message (not of the intermediate nodes that just forward it).

Concerning to RREQ and RREP messages there are two alternatives. In case of first one, only final destinations are allowed to reply a RREQ,
When a RREQ is sent, the sender signs the message. Intermediate nodes verify the signature before creating or updating a reverse route to that host. Reverse route is preserved only if the signature is verified and found fine.

The actual destination node signs the RREP with its private key.

Intermediate and final nodes, again verify the signature before creating or updating a route to that host, and then store the signature with the route entry.

In case of second one there is no such limitation

When a RREQ is sent, the sender signs the message. Intermediate nodes verify the signature before creating or updating and if the signature is fine they store the reverse route.

The RREQ message has a second signature that is always stored with the reverse route. This second signature is needed to be added in the RREPs of that RREQ and in regular RREPs to future RREQs that the node might reply as intermediate nodes.

An intermediate node that wants to reply a RREQ needs not only the correct route, but also the signature corresponding to that route to add it in the RREP, the 'Lifetime' and the 'Originator IP address' fields that work with that signature. If these are fine and correct, it generates the RREP.

If a node wants to reply as an intermediate node for a route to a node that has been added due to a RREQ or to a RREP, it has to store the 'RREQ Destination' or 'RREP Originator' IP address, the lifetime and the signature. And use them as the 'Signature', 'Old Lifetime', and 'Old Originator IP address' fields in the RREP-DSE message.

2.1.5.6.2 TAODV

TAODV (Trusted AODV) is a secure routing protocol which is an extension of AODV protocol. It is based on trust model. It uses trust relationship among the nodes for routing. It employs a trust model derived from subjective logic. Here signing and verification of digital signature at each routing message is not required. It consists of basic four different parts as [105][106],

38
- Basic routing protocol i.e. AODV
- Trust model that define the algorithms or rules to combine, judge, and update trust information based on subjective logic [142]
- Trusted routing protocol
- Self-organized key management mechanism that generate a \{secret, public\} key pair for each node and distribute public keys in a secure self-organized way

Modules of trusted routing protocol includes the following
- Trust recommendation
- Trust combination
- Trust judgment
- Trust update
- Signature authentication
- Trust authentication

When a node A wants to establish a route to any other node B, initially the uncertainty elements in A towards other node such as B is 0.5 or more. So, A may be in confusion whether it will believe B or not. So it will try to implement either a) cryptographic scheme as applied in SAODV or b) Any other scheme for route discovery. After consecutive communication, gradually A will try to implement the "Trust updating algorithm" for other nodes. After establishment of trust amongst the different nodes in the network, then the nodes will be relied on trusted routing protocol.

Now, node A will try to gather all trust information about node B from different neighbors and then calculate the trust for node B.

Node A now will utilize the trust recommendation protocol to exchange trust information about a node, B, from its neighbors, then use the trust combination algorithm to combine all the recommendation opinions together and calculate a new option towards B.

Framework for TAODV is as shown in Figure 2.11 below.
Routing Table Extension takes place in TAODV implementation; original routing table includes another three fields as [142]

- Positive events are the successful communication times between two nodes.
- Negative events are the failed communication ones
- Opinion: It is the nodes believe towards another node’s trustworthiness

Similarly routing message extension also takes place by adding new fields for trust information. These are denoted as TRREQ (trusted routing request) and TRREP (trusted routing reply).

Trust updating policy updates the trust dynamically. It consists of some steps as follows:

a. Whenever positive events occurred in A while communicating to B, immediately B’s number of successful events in A will be increased by 1.

b. Likewise each time a negative event occurs while communicating from node A to node B, immediately B’s number of failed events in A will be increased by 1.

c. Each time when the field of successful and failed events is changing, the corresponding value of opinion will be recalculated.
d. Whenever a new opinion is obtained, the corresponding number of successful or failed events will be mapped back with the help opinion space to the evidence space.

e. The positive event implies successful data or routing packets forwarding, keeping message integrity and passing cryptographic verification.

The trust recommendation protocol consists of three types of messages such as Trust Request Message (TREQ), Trust Reply Message (TREP), and Trust Warning Message (TWARN).

Trust Routing Step at a node is as shown in Figure 2.12.

![Figure 2.12 Trusted routing step at a node](image)

2.1.5.6.3 Observation-based Cooperation Enforcement in Ad hoc Networks (OCEAN)

The objective of OCEAN [173] is to avoid this trust-management machinery and see how far it can get simply by using direct first-hand observations of other nodes' behavior.

In OCEAN, a node makes routing decisions based solely on direct observations of its neighboring nodes exchanges with it. This eliminates most trust management complexity, although at a cost of less information with which to make decisions about node behavior.
OCEAN is using the same concepts deployed in the Watchdog and Pathrater but it also punishes the selfish and misbehaving nodes in order to force them to cooperate in the network.

OCEAN is a layer that resides between the network and MAC layers of the protocol stack, and it helps nodes make intelligent routing and forwarding decisions. Principle of OCEAN can be implemented in any routing protocol of MANETs [174].

OCEAN analyses the routing misbehavior according to misleading and selfish behavior. If a node takes part in routes discovery but does not forward a packet, then such kind of nodes are known as misleading nodes. On the other hand, if a node does not participate in routes finding, it is considered as a selfish node. In order to discover misleading routing behaviors, after a node forwards a packet to its neighbor, it saves the packet in its cache and monitors the neighboring node for a given period of time. It then produces a positive or negative event as its monitoring results in order to update the rating of neighboring node. If the rating is lower than faulty threshold, neighboring node is added to the list of problematic nodes and also added to RREQ as an avoid-list. As a result traffic will not use this problematic node. This node is given a specific time to return to the network because it is possible that this node is wrongly accused of misbehaving or if it is a misbehaving node, then it must improve in this time period.

OCEAN [173] is composed of five components to discover malicious nodes:

1. **Neighbor Watch**: It observes the behavior of the neighbors of a node.
2. **Route Ranker**: It holds the nodes ratings for the neighbor nodes.
3. **Rank-based Routing**: It applies the information from Neighbor Watch in the actual selection of routes.
4. **Malicious Traffic Rejection**: It performs the straightforward rejection of traffic from nodes that are considered misleading.
5. **Second Chance Mechanism**: It is intended to consider the nodes that were previously considered misleading to become useful again.
OCEAN attempts to mitigate selfish routing behavior in ad hoc networks. The general idea is to punish nodes for their selfish behavior by rejecting their traffic, in the hopes that this threat will force them to cooperate. OCEAN relies only on direct observations of interactions with neighbors to measure their performance. But OCEAN is more sensitive to some parameter settings. It doesn’t punish misbehaving node as severely as systems using full blown reputation information. OCEAN is not a guaranteed service. It doesnot guarantee whether a packet is successfully received by the destination or not [173]. Sometimes trade based system like OCEAN may suffer from deadlock problem where two nodes may not forward packets for each other for a long time. Addressing scheme for addressing this problem also consumes extra overhead. Chippoint scheme of OCEAN to detect selfish node provides a solution but decreases the network throughput [173][174].

2.2 Packet Dropping Attack in MANETs

In MANETs, node cooperation for forwarding packets from one node to another is the most essential characteristics. Initially all the nodes that participate in network communication are assumed to be trustable. All the nodes are worked as router. So, all the nodes are supposed to forward packets to their next hops in normal operation of MANETs. Instead of that, some adversaries that take part in MANETs communication are intentionally dropped packets instead of forwarding them to next hop. Such kind of attack is known as packet dropping attack. Packet dropping attack can be considered as one of the vulnerable attacks in MANETs. Malicious node in the network drops packets intentionally which are supposed to be forwarded to reach destination [107][108][109][110][113]. Routes that pass through such kind of nodes fail to establish path from source to destination [8]. As a result, network performance degrades abruptly. In ad hoc network, packets may drop due to several reasons. Some nodes are selfish nodes. Selfish nodes use system services while taking care to save some of its own resources to the extent of deviating from regular routing and forwarding some of the nodes are working as malicious node which can drop packets
intentionally in the network to reduce network performance parameters abruptly. Some packets may be dropped due unsteadiness of the medium such as network contention, congestion and corruption in the medium. Sometimes packet dropping is caused by genuineness of the node such as overflow of the transmission queue [107]. All these causes are not considered as packet dropping attack.

2.2.1 Types of Packet Dropping Attack
2.2.1.1 Selective Packet Dropping Attack

MANETs communication is a multi-hop communication and each node in the network forwards packets to its next hop for delivering packets to destination. Without the node’s cooperation, MANETs is not able to provide service. More the nodes are cooperative to transfer traffic; network becomes more powerful and reliable. Route discovery and packet forwarding by the nodes in MANETs consumes resources including local CPU time, network bandwidth, memory and most importantly energy of MN. Selfish nodes in MANETs are kind of node which wants to utilize the network resources for its own profit but not willing to provide service to other nodes [114][115][116][117][118]. As a result, any packet that comes for its own is consumed by such node, while any other packets which are supposed to be forward are dropped to maximize their benefits. They are assumed to behave rationally [119]. Nodes are strongly motivated to accept any packets which are meant for them and deny any other packets which are supposed to forward to next hop for destination [118]. Some advantages of having selfish node is that it can reduce the total rebroadcast traffic during flooding based route discovery [114]. Detected selfish nodes should be avoided from the network; thereby it helps to increase network performance parameters [116]. Selfish nodes don’t damage the other nodes in MANETs directly. But indirectly it harms the network by its non cooperative nature to forward the packets. Selfish nodes can be classified in two different categories [115].
Active selfish node: This kind of nodes participates in network communication, any packets which are meant for them are received by them, and rests of the packets are dropped by these nodes to save their resources.

Passive selfish node: These kinds of nodes don’t participate in network communication. They stay silent and they don’t contribute to any of the activities like forwarding, receiving, route discovery and network maintenance.

Selfish nodes may possibly diminish the network services and thereby decrease the whole data accessibility in the network [117]. So, the overall performance of MANETs gets affected.

2.2.1.2 Malicious Packet Dropping Attack

Malicious packet dropping attack is a kind of DoS attack in which malicious node that presents in the network, drops packets instead of forwarding these to next hop [91][92][93][95][96][97]. Such kinds of nodes disrupt the usual network services with an intention to drain other node’s resources [94].

DoS attack may affect the network in two different ways, DoS attack on routing traffic and DoS attack on data traffic. An attacker can drop packets in the network for both kind of traffic in different ways. As for example, in case of blackhole attack, data traffic may be captured by advertising shorter distance and then drop the attracted packets. In another case, data traffic may not flow through routing paths and some of
them may drop due to network congestion. In such situation, an attacker avoids some traffic or redirects the traffic to other nodes by advertising routing update message. An attacker may mislead some of the nodes to update their routing tables with invalid paths so that if any traffic flows through such path will eventually drops packets. Malicious nodes can inject huge amount traffic into the network to clog the network, so that due to congestion in the network, genuine packets are also dropped along with malicious packets to reduce congestion. Malicious nodes join the network and compromise with genuine nodes to participate in communication; then it silently drops some or all the packets which are supposed to be forwarded. Malicious packet dropping attack is a serious threat to MANETs, which is very easy to deploy but very difficult to detect and avoid [95]. Most of the routing protocols in MANETs are vulnerable to different kind of attacks including packet dropping attack [91].

As shown in Figure 2.13, node 3 is the malicious node who replies the RREQ packet sent from source node and sends a false RREP packet by mentioning that it has the shortest route to destination. As a results source starts sending the packets via the erroneous node. It then drops the packets instead of forwarding packets to destination.

2.2.2 Mitigation of Impact of PDA in MANETs

2.2.2.1 Selfish Node Mitigation

Security is the primary concern of MANETs. Selective packet dropping attack or selfish packet dropping attack is also kind of unlawful activity in MANETs as mentioned in section 2.2.2.1. Because of this activity, normal function of MANETs gets disrupted. So, many researches are going on to mitigate such kind of attack in MANETs. Few examples are given below,

In [98], it tries to identify potential threats in MAC layer introduced by selfish nodes, mainly the “smart” attack which can cross the boundaries of existing detection and reaction system against MAC layer selfish behavior. So, they propose a Predictable Random Backoff (PRB) algorithm that is capable of mitigating the impact of these vulnerabilities. In [99], it is believed that frequent elimination of such misbehaving
nodes never allows a faster growth of MANETs. So, authors propose a mathematical model which is based on time division technique to minimize the malicious behavior of node, instead of repeated elimination of such nodes. In [119], it investigates the security mechanism which is proposed for selfish node attack, shared root node attack and control packet attack in MANETs. It is done with the help of Multicast Ad hoc On Demand Distance Vector (MAODV). Here, security solution is evaluated with the help of delivery ratio, control overhead and total overhead. In [120], authors addressed the behavior based anomaly detection technique which is inspired by biological immune system to enhance performance of MANETs in spite of presence of misbehaving node like selfish node. So, they use the intelligent learning techniques that learn and detect each node by false alarm and negative selection approach.

### 2.2.2.2 Malicious Node Mitigation

Nodes in MANETs usually cooperate and forward each other’s packets in order to carry smooth running of communication. All the nodes that work as a host are also work as router at the same time. Initially every node is trusted by every other. By taking this as an advantage, adversaries which are also represented themselves as a part of communication device, start dropping packets intentionally to disrupt the normal function of MANETs. To mitigate packet dropping attack in MANETs, several methodologies are used. These can be categorized as *Centralized methodology*, *distributed* and *game theoretic based* methodology. In *centralized methodology*, it is assumed that all data related to network communication are centrally observed. It is a static offline system. Details of this method are discussed in Chapter 3 of this thesis. In *distributed methodology*, detection of packet dropping attack is done based on cooperative participation of nodes in MANETs. Chapter 4 of this thesis contains detail discussion of this methodology. In *game theoretic based* methodology, MANETs can be formulated as coalition game in which all the genuine nodes in the network that cooperate in packet forwarding, should be in one side of the game.
Malicious nodes which will try to drop the packets invariably will be in the other side of the game. Details of this methodology are discussed in Chapter 5 of this thesis. Apart from these, several solutions are proposed for mitigating the routing attack including packet dropping attack. But most of them isolate malicious node based on binary decision taken for severity in attack. This causes additional damage to the network, so, risk mitigating technique is considered as one of the important technique [122]. In [97], authors address packet dropping attack in wireless ad hoc network by post routing detection methodology called as side channel monitoring (SCM). Basic idea behind the technology is to use the nodes which are adjacent to data communication path, to monitor the message forwarding nature of the nodes en route. These nodes constitute a directional side channel towards source which is parallel to the backward route. As and when it discovers abnormality in MANETs due to some malicious nodes, they issue an alarm packet to the source node through both the channel. Then analytical methods are used to identify number of malicious nodes and their activities. In [121], authors propose a trust based security protocol based on MAC layer approach, which attains confidentiality and authentication of packets in both routing and link layer of MANETs. First phase of the protocol contains trust based packet forwarding scheme for detecting and isolating the malicious nodes using routing layer information. They use a trust counter for each node. A node is punished or rewarded based on trust value of the counter. If the trust counter value falls below a trust threshold, then the respective node will be identified as malicious node. In [123], authors propose a security mechanism that provides message integrity, mutual authentication and two hop authentication mechanism without the help of online certification authority. This mechanism provides identity impersonation, replay attacks and enable node to regulate the behavior of its neighbors to resist active attack.

2.3 PDA Detection Methodology
Observing the severity of PDA, several methodologies have been proposed. These are broadly classified as centralized PDA detection methodology, distributed PDA detection methodology and game theoretic approach for PDA detection. In normal operation of MANETs, packets sent from source to destination must be reached in proper order. Of course sometimes due to network congestion or any other reasons except malicious activities, some of the packets may be dropped. But when an exceptional numbers of packets are dropped in the network, a PDA detection methodology must work in the network for detection and avoidance of malicious nodes so that it can continue its service. At the same time, any PDA detection methodology should not hamper the normal operation of MANETs; thereby its security goals like authentication, integrity, confidentiality, availability, access control and non-repudiation must be fulfilled as mentioned in section 2.1.5.3.

2.3.1 Categories of PDA Detection Methodology

Packet dropping attack can be addressed by following methods,

(a) Credit-based systems [175, 176, 178, 177]

(b) Reputation-based systems [181, 182, 189, 186, 180, 188, 187, 185]

(c) Acknowledgment-based systems [189, 190, 191]

Credit-Based Systems:

In this system, incentives are provided for forwarding packets. In [175][176], authors proposed a system in which nodes receive credit for each packet they forward, and spend their accumulated credit to transmit their own packets. A counter named as nuglet is used. The nuglet counter is incremented each time the node forwards a packet, and decremented each time the node transmits its own packet. The nuglet counter has some restriction like it cannot take on a negative value and cannot be arbitrarily changed by the node. To enforce this rule, the nuglet counter is implemented in a tamper-proof hardware module, called the security module. The security module is assumed to provide universal protection from both software and physical attacks.
In [177], authors proposed *Sprite*, in which nodes collect receipts for the packets that they forward to other nodes. For a packet sent from a source to a destination, each node along the path records a hash of the packet as the receipt, and forwards the packet to its next hop. When the node has a high-speed link to a Credit Clearance Service (CCS), it uploads its receipts. The CCS determines the value of the receipts and provides credit in exchange. Credit is only granted if the destination reports a receipt verifying reception of the packet and if the node was on the routing path. After verification, credit is removed from the sources account and given to each node who participated in packet forwarding. Thus nodes that transmit their own packets but do not cooperate in packet forwarding will incur a debt at the CSS. Misbehavior implies debt accumulation beyond a certain threshold is interpreted as.

A scheme has been proposed in [178], which not only rewards nodes for participating in packet forwarding with credit, but takes into account congestion. When sending a packet, the source computes a congestion price, which is a metric defined by the required power for transmission and the available bandwidth. It then compares this price to its personal willingness-to-pay parameter, which the source continually adjusts based on its personal observations. By taking into consideration bandwidth in computing the cost (credit) is required to send a message to the destination, the scheme avoids overwhelming low cost routes, as they would increase in costs as they become saturated. Power and bandwidth metrics are dynamically updated based on shared information among nodes.

While credit-based systems motivate selfish nodes to cooperate in packet forwarding, they provide no incentive to malicious nodes. Such nodes have no incentive to collect credit and receive no punishment for non-cooperation. Furthermore, tamper-proof hardware as mentioned in [179] is currently too expensive to integrate in every network device, while providing an unverifiable level of security. Sprite removes this requirement, at the expense of requiring the presence of a CCS. Lastly, credit-based systems lack a mechanism for identifying the misbehaving node(s), allowing them to remain within the network indefinitely.
Reputation-Based Systems: Reputation-based systems use neighborhood monitoring techniques to identify misbehaving nodes. In [180], authors proposed a scheme which relies on two modules, the watchdog and the pathrater. The watchdog module monitors the node’s behavior of their next hop node by operating their radio in promiscuous mode. Once a node forwards a packet to the next hop, the node overhears to verify that the next hop node faithfully forwarded the packet. The scheme is based on the assumption that links between nodes are bi-directional and nodes utilize omni-directional antennas. A cache is used to store packets that wait for verification. If packets remain in the cache longer than a threshold period, the watchdog makes an accusation of misbehavior. The pathrater module uses the accusations generated to chose a path that will most likely avoid misbehaving nodes. CONFIDANT, which is built upon the watchdog/pathrater model, is proposed in [181][182][183] Here, they proposed a scheme, nodes perform neighborhood monitoring using their radios in promiscuous mode while selecting paths that attempt to avoid misbehaving nodes. Whereas authors proposed using only the previous hop for monitoring, CONFIDANT requires all neighboring nodes to operate in promiscuous mode for monitoring, thus relying on a neighborhood watch. In addition, monitoring nodes notify other nodes of detected misbehavior through the broadcast of alarm messages. Instead of including a proof of the misbehavior in the alarm message, a scheme based on Pretty Good Privacy (PGP) [184] is implemented to determine the trust level of the alarm message. In [185], a reputation-based scheme is proposed which is consisting of four modules: a Monitor, an Opinion Manager, a Reputation Manager, and a Routing/Forwarding Manager. The Monitor module monitors the nodes neighbors via the watchdog model, verifying that neighboring nodes faithfully participate in packet forwarding. Based on observations from the Monitor, the Opinion Manager formulates opinions of the nodes behavior and periodically advertises them to neighboring nodes. The Reputation Manager accepts these opinions and processes them to arrive
at a trust metric for a specific node. When establishing a routing path to a destination, the Routing/Forwarding Manager uses these trust metrics to avoid including untrustworthy (misbehaving) nodes. In [186], authors present similar work on how to derive reputation rankings using beta probability functions based on feedback of behavior of neighboring node. In [187], it proposed a reputation-based scheme which also relies on first and second-hand information. However, the authors propose two different methods for nodes to acquire the second-hand information, i.e., the reputation information originating from neighboring nodes. In the first method, as soon as a node witnesses misbehavior, defined according to a threshold number of packet drops, the node immediately broadcasts the accusation. Thus the proactive transmitting of reputation information allows all nodes in the network to have up-to-date behavioral information about their neighbors. However, since the proactive broadcasting of information may require unacceptable bandwidth requirements, thus diminishing the networks functionality, nodes can also acquire second-hand information in an on demand manner. In much the same way that on demand routing protocols request route information. Another proposal in [188], proposed CORE, in which nodes create a composite reputation rating for a given node by combining the nodes subjective reputation, its indirect reputation and its functional reputation. The subjective reputation is calculated from direct observation of the nodes behavior, using a weighted average of both current and past observations. The indirect reputation is a value calculated based on second-hand observations made by other nodes in the network. A node's functional reputation is based on task-specific behavior. Thus it is computed based on its reputation in packet forwarding, routing, etc. Denial-of-service attacks based on misbehaving nodes broadcasting negative ratings for honest nodes are prevented by preventing nodes from broadcasting negative behavior. Thus when sharing reputation metrics, node are restricted to sharing only positive ratings. **Acknowledgment-Based Systems:** Acknowledgment-based systems rely on the reception of acknowledgments to verify that a message was forwarded to the next
hop. Authors proposed a scheme called TWOACK in [189], where nodes explicitly send 2-hop acknowledgment messages (TWOACK) to verify cooperation. For every packet a node receives, it sends a TWOACK along the reverse path, verifying to the node 2-hops upstream that the intermediate node faithfully cooperated in packet forwarding. Packets that have not yet been verified remain in a cache until they expire. A value is assigned to the quantity/frequency of un-verified packets to determine misbehavior.

TWOACK is improved in [190] by proposing 2ACK. Similar to TWOACK, nodes explicitly send 2-hop acknowledgments (2ACK) to verify cooperation. To reduce overhead, 2ACK allows for only a percentage of packets received to be acknowledged. It uses a one-way hash chain to allow nodes to verify the origin of packets they are acknowledging, thus preventing attacks in which a misbehaving node drops the original packet and forwards a spoofed packet.

Similarly, another method had been proposed in [191] to identify the link on which misbehavior is occurring.

Since acknowledgment-based systems are proactive, hence it incurs message overhead regardless of the presence of misbehavior. 2ACK provides a method to reduce message overhead by acknowledging only a fraction of the packets, with the tradeoff of increased delay in misbehavior detection.

### 2.3.2 Existing Detection Methodologies

Some of existing works related to distributed PDA detection as well as game theoretic approach to detect PDA are discussed below,

Distributed PDA detection approach, based on end-to-end connection is proposed in [124]. This detection and isolation mechanism of packet dropping attacks is based on three ID messages like path validation message (PVM) that enables E2E feedback loop between the source and the destination, attacker finder message (AFM) which will find the attacker node from the routing path and attacker isolation message (AIM) is used to isolate the attacker from routing path and update the black list and then
trigger to neighbors with updated information. Another cooperative PDA detection mechanism has been proposed in [125], which is based on cooperative participation of nodes in MANETs. It is a collaborative distributed protocol which involves cryptographic key distribution and intrusion detection activity for detection of malicious packet dropping attack. Key distribution requires a trust management scheme to dynamically bind the trust relationship between the key distribution servers and the clients. Initial security to intrusion detection mechanism is provided by LLCs (location limited side channels). Thereafter a dynamic trust management scheme for key distribution is provided. A reputation based approach to detect and isolate the misbehaving nodes has been proposed in [126], which can be integrated with routing protocol. It is based on sending acknowledgement packets and counting the data packets on an active path. It has basic three steps like detection of malicious group, identification of particular misbehaving node, isolation and mitigation of misbehaving node. A solution is proposed in [127] to monitor, detect and isolate misbehaving nodes that participates in packet dropping attack. It suggests a social-based approach to approve detection and isolation of malicious nodes to reduce false positive rate of detection. This methodology fails to analyze collusive dropping of packets. It has limitations to handle continuous packet dropping as well as detection of selective misbehavior. Detection is delayed because of Bayesian approach for judgment. A novel simplified IDS for detecting packet dropping attack in MANETs is proposed in [128]. Here mobility aspects are considered explicitly by means of a heuristics which considers the forwarding operation at each node. In [129], a homographic linear authentication based public auditing architecture is proposed which assist the packet dropping attack detector to detect the attack accurately by verifying the truthfulness of packet loss information reported by nodes. Game theoretic approaches to distributed PDA detection have been explored. In [130], IDS is handled by an elected leader node for a cluster of node. A unified framework has been proposed in this paper to increase the lifetime of the cluster, detect and punish the misbehaving leaders through checkers. To analyze the
hop. Authors proposed a scheme called TWOACK in [189], where nodes explicitly send 2-hop acknowledgment messages (TWOACK) to verify cooperation. For every packet a node receives, it sends a TWOACK along the reverse path, verifying to the node 2-hops upstream that the intermediate node faithfully cooperated in packet forwarding. Packets that have not yet been verified remain in a cache until they expire. A value is assigned to the quantity/frequency of un-verified packets to determine misbehavior.

TWOACK is improved in [190] by proposing 2ACK. Similar to TWOACK, nodes explicitly send 2-hop acknowledgments (2ACK) to verify cooperation. To reduce overhead, 2ACK allows for only a percentage of packets received to be acknowledged. It uses a one-way hash chain to allow nodes to verify the origin of packets they are acknowledging, thus preventing attacks in which a misbehaving node drops the original packet and forwards a spoofed packet.

Similarly, another method had been proposed in [191] to identify the link on which misbehavior is occurring.

Since acknowledgment-based systems are proactive, hence it incurs message overhead regardless of the presence of misbehavior. 2ACK provides a method to reduce message overhead by acknowledging only a fraction of the packets, with the tradeoff of increased delay in misbehavior detection.

2.3.2 Existing Detection Methodologies

Some of existing works related to distributed PDA detection as well as game theoretic approach to detect PDA are discussed below.

Distributed PDA detection approach, based on end-to-end connection is proposed in [124]. This detection and isolation mechanism of packet dropping attacks is based on three ID messages like path validation message (PVM) that enables E2E feedback loop between the source and the destination, attacker finder message (AFM) which will find the attacker node from the routing path and attacker isolation message (AIM) is used to isolate the attacker from routing path and update the black list and then
trigger to neighbors with updated information. Another cooperative PDA detection mechanism has been proposed in [125], which is based on cooperative participation of nodes in MANETs. It is a collaborative distributed protocol which involves cryptographic key distribution and intrusion detection activity for detection of malicious packet dropping attack. Key distribution requires a trust management scheme to dynamically bind the trust relationship between the key distribution servers and the clients. Initial security to intrusion detection mechanism is provided by LLCs (location limited side channels). Thereafter a dynamic trust management scheme for key distribution is provided. A reputation based approach to detect and isolate the misbehaving nodes has been proposed in [126], which can be integrated with routing protocol. It is based on sending acknowledgement packets and counting the data packets on an active path. It has basic three steps like detection of malicious group, identification of particular misbehaving node, isolation and mitigation of misbehaving node. A solution is proposed in [127] to monitor, detect and isolate misbehaving nodes that participates in packet dropping attack. It suggests a social-based approach to approve detection and isolation of malicious nodes to reduce false positive rate of detection. This methodology fails to analyze collusive dropping of packets. It has limitations to handle continuous packet dropping as well as detection of selective misbehavior. Detection is delayed because of Bayesian approach for judgment. A novel simplified IDS for detecting packet dropping attack in MANETs is proposed in [128]. Here mobility aspects are considered explicitly by means of a heuristics which considers the forwarding operation at each node. In [129], a homographic linear authentication based public auditing architecture is proposed which assist the packet dropping attack detector to detect the attack accurately by verifying the truthfulness of packet loss information reported by nodes.

Game theoretic approaches to distributed PDA detection have been explored. In [130], IDS is handled by an elected leader node for a cluster of node. A unified framework has been proposed in this paper to increase the lifetime of the cluster, detect and punish the misbehaving leaders through checkers. To analyze the
interaction of checkers, a cooperative game theoretic model has been proposed in such a way that it is able to reduce false positive rate. To maximize the probability of detection, a zero-sum non-cooperative game between the leader and intruder is formulated. It also helps the leader to use its optimal sampling strategy during intrusion detection. A throughput characteristic function is defined in [131] which is meant for maximal throughput and reliable traffic. Nodes are enforced to form coalition based on this function. It is also used to imply quantification of security function. Thus, it creates a threatening mechanism to the nodes to join the network. Shapley value is used in this method to fair payoff distribution inside the coalition. This method can be integrated with any routing protocol for wireless network. In [132], a game theoretic frame work is proposed to analyze regular as well as malicious nodes. Individual strategy of nodes in terms of cost and gain are generated based on Bayesian signaling game. Regular nodes update their belief based on the behavior of opponent while malicious nodes evaluate their risk of being caught. A Game-Theoretic Adaptive Multipath Routing (GTAMR) protocol is proposed in [134] to detect and punish malicious node as well as selfish node that drops packets. In this scheme, more than one node coordinates their misbehavior and can be used in the network in which wireless network use directional antennas. ERTFT, a game theoretic strategy, allows the nodes to promote their cooperation for detection. Security and QoS, both are considered together in Service Level Specification (SLSs) in [24]. A game theoretic approach is proposed to make the system in such a way that a service level agreement (SLA) can be established with user to establish security and QoS parameters for the user.

### 2.3.3 Desirable Properties of Detection Methodology

Desirable properties of any PDA detection methodology can be summarized as below,

1. Implementation of PDA detection methodology should not create another weakness in the MANETs.
2. The methodology should be an autonomous system and it must be transparent to the system as well as to the users.

3. It must use very less system resources to perform its goal; otherwise system overhead will be high. So, excessive communication amongst the nodes or run complex algorithm is not desirable.

4. It must be fault-tolerant so that it is able to recover itself automatically during system crashes. It should not loss any of its previous information and should work from that point onward. It must be same with its objective during life time of its work [135].

5. Apart from normal detection and isolation of malicious nodes, the system should save itself from intruder so that it should not compromise with intruder and take part in malicious activities in the network.

6. The system must generate very less false positive and false negative rate so that its accuracy remains high.

7. Implementation of such system should not degrade network performance in terms of some parameters such as throughput, packet delivery ratio etc.

8. It should interoperate with other existing systems to collaboratively detect intrusions.

9. It should isolate the malicious nodes from the system

2.4 Game Theoretic Approach

2.4.1 Introduction

Game theory can be identified as mathematical model of conflict and co-operation amongst intelligent rational decision makers [140]. Though game theory is basically a part of mathematics and it is used vastly in economics, it can also be used in other field of application. It is an interactive decision situation which is represented by mathematical model. Game theory can be modeled to MANET's nodes which are autonomous but interdependent of rational decision makers.
The work can be represented either as non-cooperative security game between attacker and detector or as model of cooperation amongst the various nodes that are involved in detecting malicious activities in MANETs. These models of cooperation can be classified as credit based model and trust model. Credit based model is based on economic incentive while trust based model is based on reputation [157]. The concept can also be explained by the fact that to encourage the nodes, two basic mechanisms are followed. One is reputation based mechanism and other is price-based mechanism. In reputation based mechanism, any node keeps a record of its neighbour’s reputation. The more cooperative a node is the better reputation it gains. In price-based mechanisms, the loss that a cooperative node makes is compensated by some kind of virtual money. The price of relaying a packet may be different for each node. Therefore, an effective price-based mechanism should be supplemented by a technique which determines these prices accurately.

Non cooperative game theory can be applied to forward decision by autonomous nodes, they also involve with cooperation aware routing [158]. A non cooperative game may contain the elements such as number of players, objective function of each player for which it tries to optimize utilities, preference, utility, actions, strategies etc [138].

Normally a game may contain the following Components:

- players
- actions
- strategies
- information
- outcomes
- payoffs
- Equilibrium concept

Goals of players are articulated by utility functions and utility is defined over outcomes. Actions and strategies can be defined as follows:

- Any plan or steps for performing some actions are known as strategy.
• In some cases, actions and strategies are taken as equivalent.
• But in some cases both actions and strategies are granted differently. In such cases strategies are recognized as primary choice of actions.
• The payoff for each player depends on the combined actions of all players.

**Characteristics of game theory**

Strategic game consists of three main basic components

- A set players \( N = \{1, 2, \ldots, n\} \text{ where } N \geq 2 \)
- A set of actions for each player ( )
- Utility function for each player ( )

### 2.4.2 Game Theoretic Approach to PDA Detection in MANETs

It can be considered as cooperative or coalition game because it considers the cooperative actions of number of players and then analyze the results accordingly. It is also a kind of strategic game, as all the players have the idea about their strategies; they make the outcome of the game based on their decision. Solution of a strategic game is either Nash equilibrium or stability. It is the point from which no other players want to deviate unilaterally.

Due to the De-centralized nature of nodes, they can independently adapting its operation based on perceived or measured statistics. Similarly, due to interactive decision makers of the nodes, decision taken by one node affects and influences the other nodes.

MANETs is very much vulnerable to attack due to decentralized nature of nodes, open topology and dependency of each node on others for packet forwarding etc. Hence to detect vulnerabilities, either we may follow centralized detection methodology or distributed detection methodology. But from several performance evaluation processes, it is observed that distributed detection methodology is found better. Game theory can be used to study the different decision made by the players (i.e. network nodes) in a distributed way to reach the goal.

MANETs components can be set as equivalent game components as follows:
Player Set: Player sets in MANETs implies different nodes that participated in communication in the network including attacker and genuine node.

Action set: Nodes may act as,
   a. Source i.e. sender
   b. Destination i.e. receiver
   c. Forwarder
   d. Packet dropper
   e. Malicious packet dropper detector etc.

Utility function
   a. Utility function is a kind of function which can be implemented to network to determine the network status at a time whether it is dominated by genuine nodes or attacker.
   b. Based on node's performance, incentives can be paid in terms of trust, it can be categorized under “Credit exchange”, “Optimal equilibrium inducing mechanisms” of game theory.
   c. To win game by genuine node, utility function’s value must be increased.

A game with complete information implies that each player knows the facts about the game such as set of players, strategies and utility functions. Of course set of complete information always doesn’t mean that these are complete information.

2.4.3 Equilibrium Concept

The concept of equilibrium in game theoretic approach can be understood by the fact that no players that participate in the game is able to earn any other extra benefit by changing their strategies. So, it is a state in which opposing forces or influences are balanced. Equilibrium selection implies identification of desired Nash equilibrium [159] or stability achieved by the system.

2.4.4 Nash Equilibrium

NASH EQUILIBRIUM is an important concept in game theory, It occurs when each