CHAPTER 2

LITERATURE REVIEW

This chapter provides the background of the work carried out throughout the research work. This provides the literature survey of existing routing protocols, various routing attacks, some trust based schemes and also various routing mechanisms for mitigating routing attacks.

2.1 Introduction

The goal of this research is to develop trust based mechanism for securing MANET from different types of attacks. After developing the new protocols the performance should be compared with the existing algorithms.

To get better perspectives of different issues related to the present problem, it is of great importance to review the literatures and study the details of various routing protocols exist in literature. Also it is important to study the details of various routing attacks and their way of attacking in different layer of the network. In the literature survey, different trust schemes studied. Also we have studied different new routing mechanism developed by many researchers. The literature survey helped much in achieving my goal.

2.2 Routing Protocols in MANET

MANET is a wireless network with mobile nodes without having any prior infrastructure setup. MANET does not require any access point, router, server etc. The nodes of the MANET communicate themselves through intermediate hop nodes. Each node in MANET acts both as host and also router. This is a self-organized and self-configured network. They use wireless channels randomly for communication. MANETs have many different features as compared to infrastructure network like dynamic topology, nodes higher mobility, low bandwidth, low battery power, higher error rates etc. The nodes in MANET can be connected anywhere any time arbitrarily due to its dynamic features. Also nodes in MANET act as a router and participate in route discovery and maintenance. According to Broch *et al*. (1988) in MANET if the destination node is far away from the sender node, an appropriate multi hop routing procedure is required for setting up appropriate path between the source and destination. Due to all these features the conventional routing protocols of wired network cannot be directly used in MANET. Routing protocols in MANET can be classified as proactive or table driven and reactive or on demand based on their way of routing, maintaining routing table etc. Proactive protocols keeps route to all nodes at start up and maintain periodic update of the routing table. On the other hand reactive routing protocols are developed to reduce the overhead of proactive protocols where routes are initiated and maintained only for active nodes that is when a node wants to communicate. There are various protocols (Mishra and Nadkarni, 2003) already developed for MANET. Based on routing techniques the protocols can be classified in Proactive (Table Driven) and Reactive (On-demand) protocols.

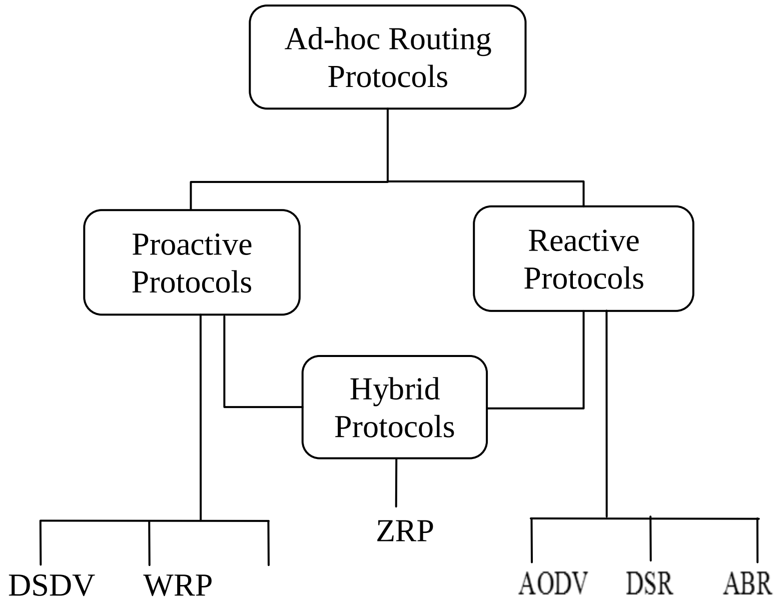

Figure 2.1: Classification of Routing Protocols

2.2.1 Table-Driven or Proactive Routing Protocols

A table-driven routing protocol store record of routing information of every node by maintaining a routing table and periodically updates the table. When the topology changes these protocols have to maintain the updated routing information in order to keep consistency of the network. Sometimes protocols have to maintain two or more tables to keep record of the updated routing information. There are various proactive routing protocols, the basic criterion for difference of these protocols are the number of tables used for keeping routing information and the methods through which the changes in the network structure are broadcast. Some of the existing proactive routing protocols are discussed below.

- **Destination-Sequenced Distance-Vector (DSDV)**

DSDV is a modification of Bellman algorithm (1957), which is loop free protocol. It uses shortest distance vector routing algorithm for selecting the single route between sources to destination. The DSDV (Perkins and Bhagwat, 1994) is proactive that is table driven routing protocol, which maintains a routing table to keep records of all possible destinations and also number of hops to each destination. Each record is given a unique sequence number which is used to identify a stale node and a new node. The mobile nodes keep additional information by maintaining an additional table which store the data sent in the incremental packet. The broadcasting routing packet contain the destination address, number of hops to reach destination, the sequence number of the received packet and new sequence number which is unique to broadcast. The route which has the latest sequence number is always used. If the two routes have the same sequence number, the route with smaller metric is taken to optimize the routing path. Routing tables update is periodically forwarded to the network for keeping the routing tables up to date. DSDV maintain two types of packet for reducing the routing overhead, full dump packet and incremental dump packet. In full dump packet all the routing information are carried whereas in incremental dump packet only the change in last full dump packet is carried. Although the incremental dump packet is sent more frequently than the full dump packet, DSDV still having large overhead because of periodic updates and is not feasible for large networks. The increase in overhead growth is still of order O (n^2).

- **Optimized Link State Routing (OLSR) Protocol**

OLSR (Clausen and Jacquet, 2003) is a table driven routing protocol basically designed for reducing flooding of packet. It is designed based on transfer of topology information, which uses multipoint relay (MPR) mechanism to limit the flooding of packet. Each node maintains the list of MPR nodes, which is called MPR selector list. The nodes which are selected as MPR, only they can forward the request. In OLSR each node selects its own MPR while trying to send RREQ. There are two types of messages used in OLSR, a Hello message and a TC (Topology Control) message. Hello message is used for MPR selection and sensing the neighbor nodes. A Hello message contains its address and the list of its one-hop neighbors. Each node in OLSR periodically sends a Hello message. From a Hello message a node can learn a topology of two hops. TC messages are used for route calculation. A TC message encloses the sender's MPR selectors. Each MPR nodes forward TC messages locally. In OLSR only MPR nodes forward the TC messages. Each node after receiving TC messages from all MPR nodes each node can create a network to every node. A MPR set is selected in such a way that it can reach all its neighbors.

- **Wireless Routing Protocol (WRP)**

WRP (Murthy and Aceves, 1996) is a proactive routing protocol which finds the path by escaping count to infinity problem. In WRP is a loop free protocol where each node checks predecessor information by its neighbors for avoiding the count to infinity protocol. In WRP each node maintains four tables: routing table, distance table, link cost table and message retransmission table. Hello messages are transferred between neighbors.

2.2.2 On Demand-Driven Reactive Protocols

On demand or reactive protocols generate route when demanded by the source nodes. When a source node wants to create a network, it starts route discovery process in the network. When it finds a route or all possible routes are checked then this process is completed. When a route is created, route maintenance phase maintain it until destination is not reachable or it is not required by the source node.

- **Ad-hoc On-Demand Distance Vector (AODV)**

AODV (Perkins and Royer, 1999) is a purely reactive routing protocol which establishes a route on demand when the communication starts and uses it until it breaks and a new path is established. It uses destination sequence number for path identification. AODV protocol has two phases (a) Route Discovery and (b) Route Maintenance. It uses Route Request (RREQ) and Route Reply (RREP) for route discovery and Route Reply (RREP) for route maintenance phase. The nodes in AODV protocols are termed as source node, intermediate nodes and destination nodes. When a particular node tries to communicate to a destination node, first it checks the routing table whether a route exist or not. If exist then it will use it, else it will broadcast RREQ to its neighbors. The RREQ will again be broadcasted by the neighboring nodes and it will continue until the destination is reached or visited all nodes but not found in the list. When the RREQ is reached at destination node a RREP message is generated and sent back to the source node. So in AODV the source nodes wait for RREP after sending the RREQ.

- **Dynamic Source Routing (DSR)**

DSR (Johnson and Maltz, 1996) is an on demand reactive unicast routing protocol which uses source routing algorithm. DSR is a reactive unicast routing protocol which carries full addresses from source to destination. DSR uses route discovery and route maintenance phase for creating and maintaining route. DSR has the advantage of route cache, which keeps multiple routes. So for a communication the DSR first checks its route cache and if it founds a valid path to destination, it does not go for route discovery phase. This is beneficial when there is low mobility in network nodes as the route will persist for long times. The DSR has also the advantage of not requiring periodic updates of routing tables; this also reduces the routing overhead. Since the DSR require carrying the full addresses of all hope to reach source to destination, so the DSR is not efficient for large network. Also as the diameter of the network increases the overhead of the routing also increases. In DSR, each packet contains complete information about routing to reach its destination. Also it contains route cache to maintain routing information. Route discovery and Route maintenance are the two phases of DSR. When source node tries to send a data packet to its destination, first it checks its route cache and if found it includes the routing information and send it. Otherwise it starts a route discovery by broadcasting RREQ packet. A RREQ packet contains a unique number for identifying RREQ packet, source node address and destination node address. After receiving the RREQ the node check its cache table, if it does not find information of destination it appends its address and rebroadcast it to its neighbors. The process continues until the destination is reached or all nodes are visited. When a destination node is reached it sends the RREP packet to the source. There may be three possible ways send a backward route. Firstly, the node may have already a route to the source. Secondly, the network may have bidirectional link and thirdly the network may have unidirectional link. In DSR, if a link failure occurs in data link layer, Route Error packet generated and sent back to the source node. The source again initiates a new route by the same process as earlier. DSR has traffic overhead because of having complete routing information in each packet.

- **Temporary-Ordered Routing Algorithm (TORA)**

TORA (Park and Scorson, 1998) is a distributed routing protocol which uses link reversal mechanism for routing. TORA is a loop free protocol which can work in a dynamic mobile environment. It uses source routing and creates multiple paths for any destination. TORA uses the concept of localization of control messages to a small set of nodes near the topological change by maintaining routing information on one hop adjacent nodes. TORA performs route creation, maintenance, and route deletion.

2.3 Performance Comparison of Proactive and Reactive Routing Protocols

MANET has various features like dynamic topology, limited power, limited bandwidth etc. Due to these features the conventional routing protocols cannot be directly used in MANET. In wired network the most common algorithms are link state algorithm and distance vector algorithm. In link state algorithm, each node keeps an up to date view of the network by periodically updating the link state costs of its neighbors using flooding technique. After receiving the update, each node updates their link state information using a shortest path algorithm. In distance vector algorithm, each node maintains a set of distances of each neighbor and selects the node which has the minimum distance. The distance table is updated by a periodical dissemination. However the routing algorithms of wired network are not feasible to MANET because of large network and other resource constraints. To overcome the problem of using wired routing protocol in MANET, many routing protocols are designed. In this section we have discussed the comparison of different proactive and reactive routing protocols, especially we have considered two protocols from each type namely, DSDV and DSR and compared the performance analysis of these protocols using some performance matrices. The justification for doing comparison is to study in different situation which protocol works more fruitfully. Routing performance matrices may include throughput, jitter, end to end delay, load, hop count, reliability and cost. Many routing protocols have been presented but a few comparisons of routing protocols have been made. B.R. *et al*. (2008) in their Monarch project made the comparison between some routing protocols. This section deals with the simulated comparison of proactive and reactive routing protocols. Here the performance of two protocols of both proactive and reactive types is compared in terms of performance matrices such as routing overhead, packet delivery fraction, end to end delay.

2.3.1 Simulation Environment

The NS2.29 simulator is used to for simulating the behavior of the protocols. We design a network scenario file which describes the feature of each node and their packet sending, receiving notion and time. After running the NS2 program by taking the scenario as input, a trace file has been generated. We have run the program 10 times and 10 trace files i.e., .tr files are generated. The .tr files of each run are stored in disk storage and finally analyzed the trace files using awk scripts for different parameters. We have taken average of 10 runs to find the results as the simulation result of every run differ from one another. Finally we have imported the data to origin graph plotter and find the graphs.

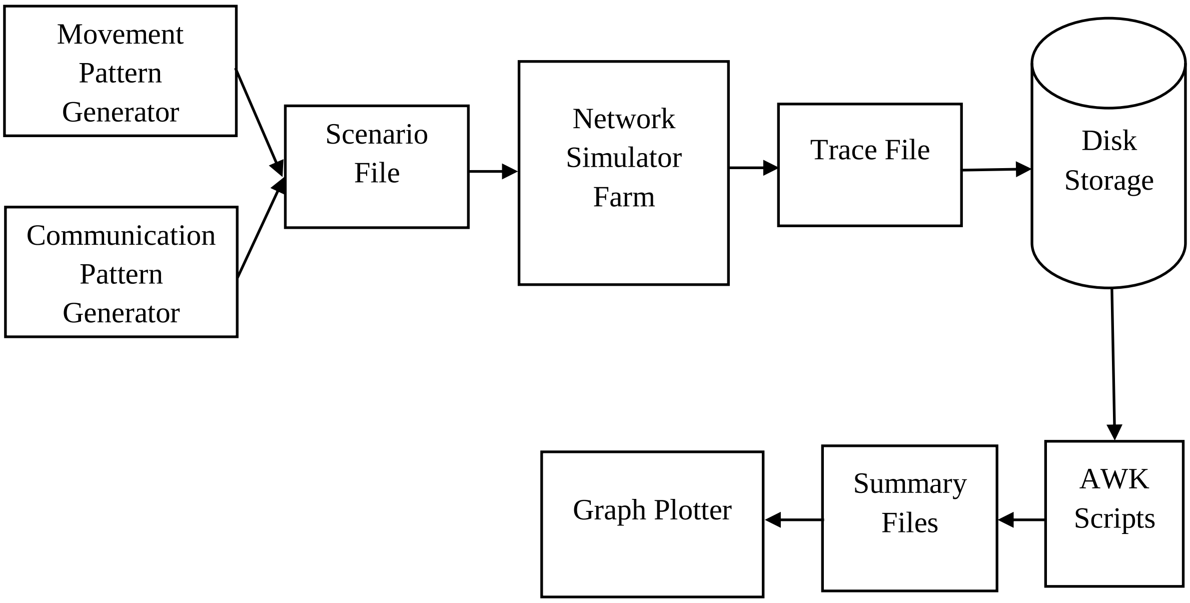

Figure 2.2: Simulation Steps

The parameters used in the simulation process are presented in the table 2.1 for a quick view. The simulations were carried out under a bit rate of 2 mbps. The packet size was fixed to 512 bytes. Communication rate was 4 packets per second. The mobility of nodes position is random. Each packet can start from random location to a random destination.

Table 2.1: Simulation Parameter

Protocols	DSDV, DSR
Number of mobile nodes	30
Simulation area size	800 m × 500 m
Simulation duration	800 seconds
Mobility model	Random way point
Traffic type	Constant bit rate (CBR)
Packet size	512 bytes
Max speed	20 m/sec
Connection rate	4 packets/sec
Pause time	0, 50, 100, 150, 200, 250,300, 350, 400
Number of sources	9

2.3.2 Performance Metrics

We have primarily selected the following three QoS parameters Clausen *et al.* (2002) in order to study the performance comparison of DSDV and DSR.

Packet Delivery Fraction (PDF): PDF is defined as the ratio between total number of packet delivered and packet generated by CBR traffic sources.

Average End-to-End delay: This is defined as the ratio between the sum of the total time difference of packets sending time and receiving time by all nodes. This includes all types of delays such as route discovery, queuing delay, transfer and propagation time etc.

Normalized routing load: This is defined as the total number of packets transmitted per data packet at the destination.

2.3.3 Results and Comparative Analysis

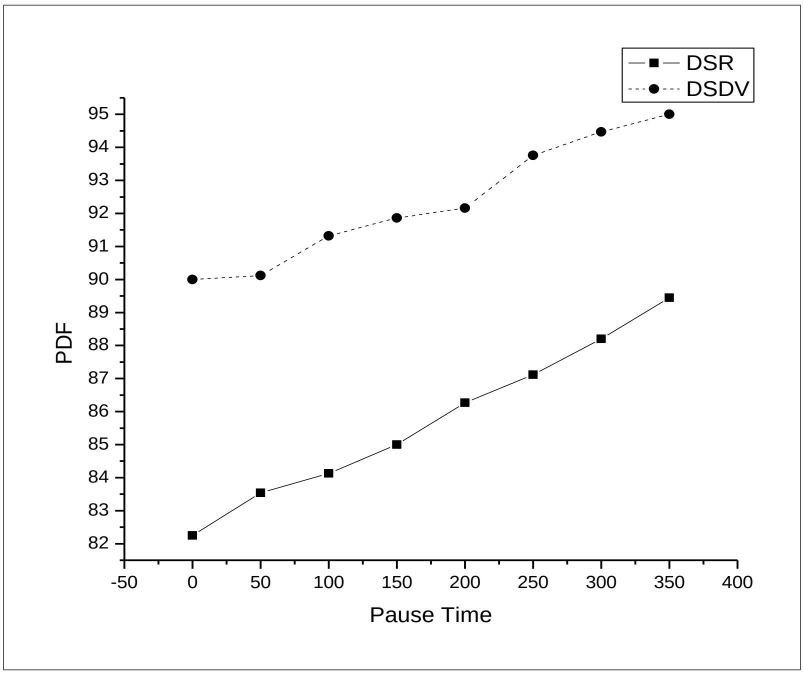

Figure 2.3: Packet Delivery Fraction Vs. Pause Time (in sec) for 9 sources, 30 wireless nodes

Figure 2.3 presents the Packet delivery fraction of DSDV and DSR obtained from our simulation experiment. The packet delivery fraction of both DSDV and DSR are obtained by doing simulation from 9 sources by varying the pause time. The graph shows that the PDF of DSDV is higher at low mobility than the DSR, because at low mobility the change in the position of the nodes is very low so the pre-established route already exist and does not require to discover and create new routes as DSDV has the proactive nature. But in DSR, since it is source initiated a substantial time will be required for initial route setup. At the time of route setup of DSR there will be no packet transfer. But when there is high mobility and when the size of the network increases, the DSDV is not well suited because of the proactive nature. In higher mobility DSR works better because of its on demand feature. Since the DSR maintain route cache, even for some link breakage the alternative link may exist in the route cache, so there may not be always necessary to establish new route.

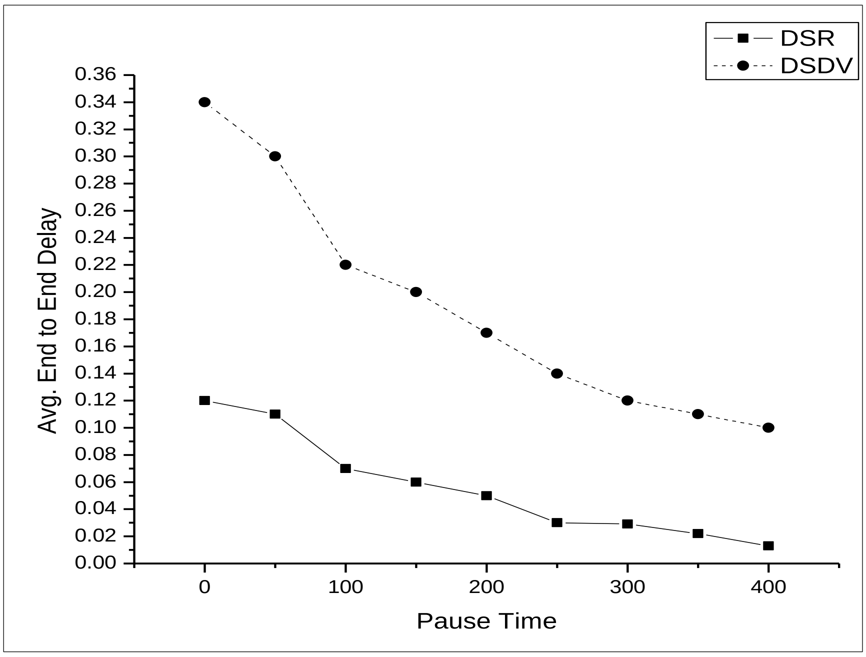

Figure 2.4: Average End to End Delay Vs. Pause Time (in sec) for 9 sources, 30 wireless nodes

Figure 2.4 shows that DSDV has less end-to-end delay than DSR since DSDV periodically update routing table, so for sending a packet to destination, it does not require to set up new path each time, hence reduces end to end delay. In DSR, for sending a packet it requires to set up a new path by discovery phase due to its reactive nature, which causes delay. Also the DSR protocols have to wait for route reply messages from all nodes which also cause delay. Also when a link failure occurs the DSR tries to find an alternate route from its cache which adds additional delay.

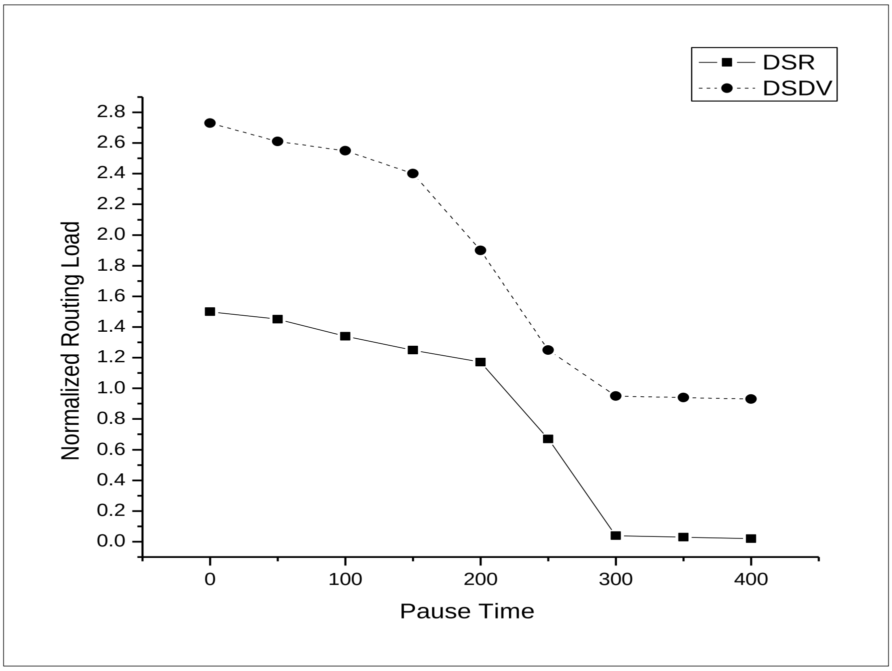

Figure 2.5: Normalized Routing Load Vs. Pause Time for 9 sources, 30 wireless nodes

Figure 2.5 shows that at lower mobility, the normalized routing load is higher in DSR because DSR is a source initiated routing protocol where every packet carries the complete routing information. Also, in route discovery process the reply comes from different nodes, this increases the control traffic. In case of DSDV, at lower mobility routing overhead is low because of stable network and need not require sending full dumps rather only incremental dumps are sent. But in higher mobility it should send full dump packets so routing overhead increases.

From the simulated experimental result we can conclude that at higher mobility the performance of DSR is better than DSDV and at lower mobility DSDV outperforms DSR. The end- to-end delay and PDF is more in DSR than DSDV. In summary we can say that in DSR protocol- PDF, Average End-to-End delay is decreasing as packet size is increasing, routing load is also increasing with increase in packet size, and performance of DSR is high at less packet size. In DSDV, PDF, average end-to-end delay, decreases with the increase in packet size. Routing load also increases by the increase in packet size. We conclude this chapter by saying that, if there is no worry about routing delay DSR give the better performance at higher mobility in terms of PDF, throughput, normalized routing load.

Thus we can conclude that if routing delay is not major, then DSR shows better performance at higher mobility in terms of packet delivery fraction and normalized routing load in hybrid networking scenario. In less stressful scenario, DSDV can perform better in terms of these matrices.

2.4 Routing Attacks in MANET

Security is a major issue in MANET. MANET is vulnerable to different types of attack (Devi and Kannammal, 2012) due to its features like dynamic topology, limited bandwidth, battery power etc. The attackers can attack in various ways, like sending fake routing information, fake messages, flooding packets, flooding false packets etc. There are various types of attack in each layer of the network. In this thesis we will discuss only a few types of attacks which we have tried to mitigate in our research work. Some of the routing attacks are discussed below.

2.4.1 Flooding Attack

Flooding attack is a DoS (Denial of Service) attack which can affect all the reactive routing protocols. In flooding attack, the attacker node broadcasts false packets so that it can consume the resources in the network. Since the flooding of false packet consumes the resources so the throughput of the network reduced. Flooding attack can be classified as RREQ flooding and DATA flooding.

RREQ Flooding: In the RREQ flooding attack, the malicious node broadcasts fake RREQ packets. The reactive protocols like DSDV, DSR etc. use route discovery process to establish communication between two nodes. In the route discovery process the reactive protocols broadcasts RREQ packets in the network, since the priority of RREQ packet is always higher than the data packet, so malicious node takes this advantage by flooding the false RREQ packets and consume the network resources.

DATA Flooding: In data flooding the attacker node floods the network by sending bogus data. First of all they establish a path among all nodes and then forward the fake packets throughout the network. The fake data packet exhausts the network resources like battery power and bandwidth and create problems for the original users.

2.4.2 Blackhole Attack

In a blackhole attack (Tamilselvan and Sankaranarayanan, 2007), attacker node forward false routing information about fresh route to the network and the original nodes try to send packets through this fake node, the malicious node then misuse or drops the packets. In blackhole attack, the attacker node advertise as it has the optimal path to all the nodes by sending false RREP packet, the good node in reactive protocols will assume that the response has come from valid node and they will forward the packet through this node but the malicious node deprive the traffic from original one. The reactive protocols like AODV, DSR are mostly affected by this type of attack.

2.4.3 Link Spoofing Attack

In a link spoofing attack (Kannhavong *et al.*, 2007), a malicious node sends fake links to disorder routing operations. In OLSR protocol a malicious node can forward false link to its two-hop neighbors, but while selecting MPR node the source can select the attacking as MPR. The malicious node by becoming an MPR will perform various types of malicious activities like modifying or dropping packets.

2.4.4 Wormhole Attack

A wormhole attack (Cho *et al*., 2008) is a severe attack in MANET protocol, where attacker record packet from one location and by using other private network replays them at other location. This type of attacker can attack in all types of protocols even which have confidentiality and authenticity.

2.4.5 Grayhole Attack

Grayhole attack (Xiaopeng and Wei, 2007) a different form of blackhole attack (Wu *et al.,* 2006) is an active attack type which drop packets. In grayhole attack the attacker nodes accept the packets for forwarding, but without doing so it just drops it. In such attack the malicious node initially behave correctly and reply true RREP messages to nodes that forward RREQ messages. This way it takes the packets and later just drops the packets. The sender nodes thus loose the connection and again try to establish a new route, broadcasting RREQ messages. Attacker node again do the same things thus consume battery power and other network resources.

2.5 Trust in MANET

Trust (Cho *et al.*, 2009) is a very important and complex issue in social aspect. Trust may be stated as psychological cognitive process which may consists of expectations, assumptions, belief, behavior, environment and other factors. Generally in human civil society trust is used to perform certain action between two individuals. Similar things can be implemented in network for doing some actions like expectation of one node to other to provide some sort of services. Trust is a relationship between two neighbor nodes based on some criterion. The definition of trust is diverse with respect to different context. Trust (Lewis and Weigert, 1985) may be defined as quantified belief by a node to other node in terms of honesty, security, competency etc. Since in MANET network there is no centralized infrastructure, nodes communicate with each other with cooperative nature and exchange information among them depending upon the belief, so trust is an important concept in MANET. It helps mobile nodes to cope up with uncertainty and malicious behavior caused by free will of malicious nodes. Trust computation and trust management is a challenging task in MANET. An untrustworthy node in MANET can loss the network resources like battery power, data and control packets. In this section we explain different trust management scheme in MANET. In Blaze *et al.* (1996) introduced the term Trust management in MANET and treated it as a separate component of security services in network. Trust management is needed when the different nodes try to setup a network without having any previous communication history.

Many definition of trust are given in literature. The exact definition of trust cannot be given because trust is an abstract concept (Cho and Swami, 2009) which depends upon many factors like reputation, quality of services, honesty, risk, confidentiality, availability etc. The concept of trust is used in psychology, sociology, anthropology, economics, and political science and also in network (Hassan *et al.*, 2008). Each literature uses the concept of trust in different view (Shapiro, 1987). For example, Psychologists treat trust as a personal view, while sociologists see trust as a relationship in nature. In MANET Trust can be defined as follows:

a) Trust as a belief: Trust may be defined as individual belief on others words, actions and recommendations (McAllister, 1995; Olmedilla *et al*., 2005).
b) Trust as a risk factor: According to Morton Deutsch (Deutsch, 1962) when a node is bound to take an ambiguous path, which may be good or bad and the occurrence of good or bad depends upon the recommendation of other nodes, then the concept of trust arises.
c) Trust as a probability measure: Trust can be defined as a probabilistic measure which a node can expect services from others.

We summarize the definition of trust as a subjective assessment of a node to other node based on accuracy and reliability of information received from it. It is the belief or confidence based on honesty, integrity, availability, ability and quality of services.

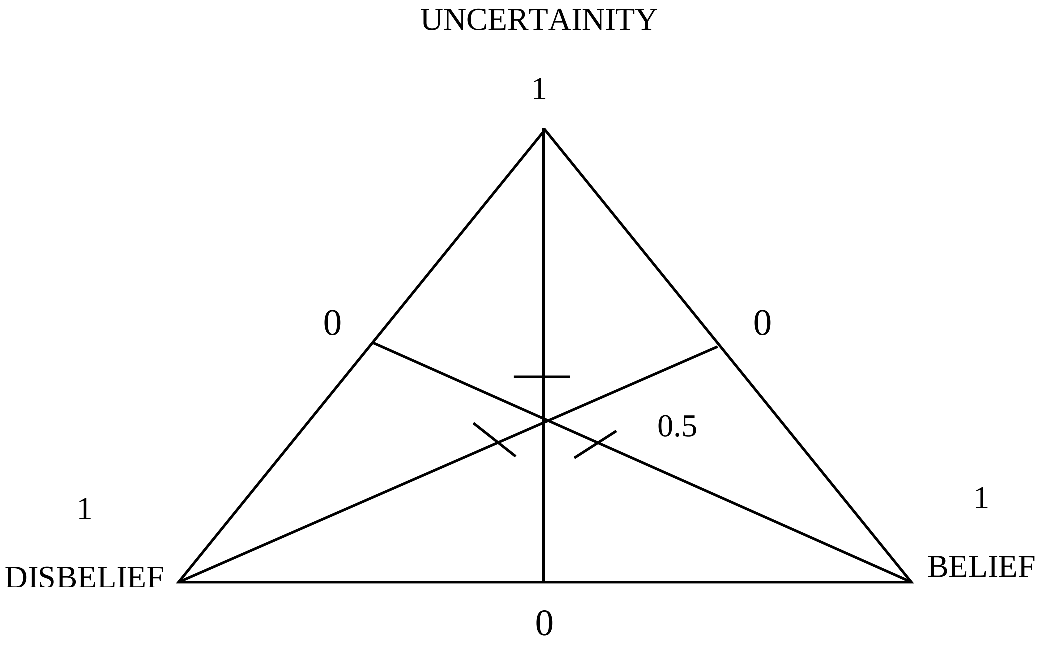

Figure 2.6 (a) Trust as Belief Function

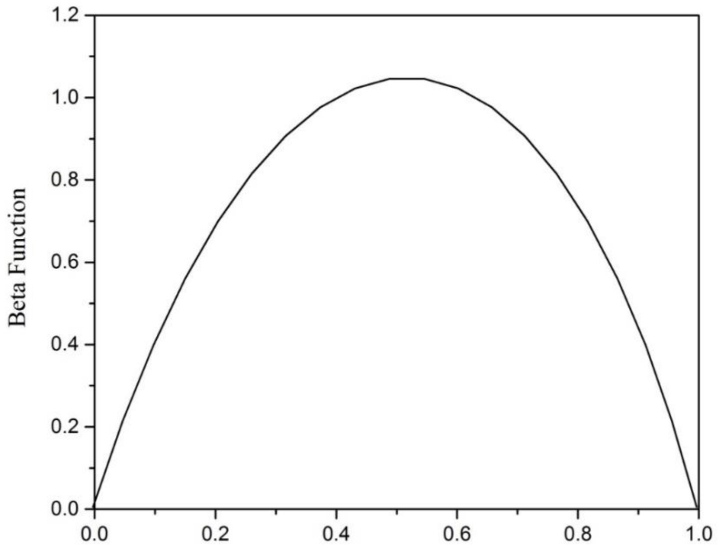

Figure 2.6 (b) Probability based Trust

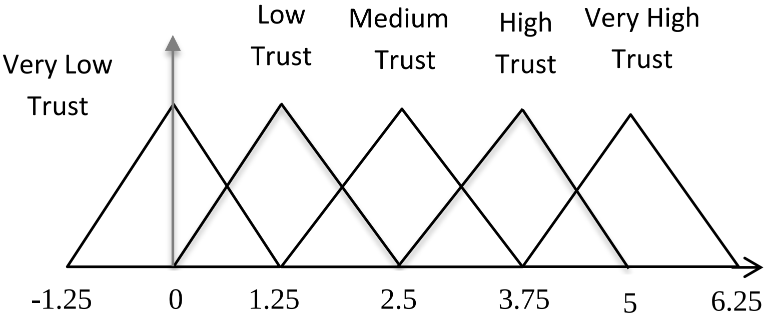

Figure 2.6 (c) Fuzzy Logic based Trust

2.6 Different Ways to Achieve Trust in MANET

There are different mechanisms for securing MANET routing protocols using trust. The different trust based security model can be classified as follows. The trust based mechanisms are classified depending upon how the trust based technique works (Dalal *et al*., 2012).

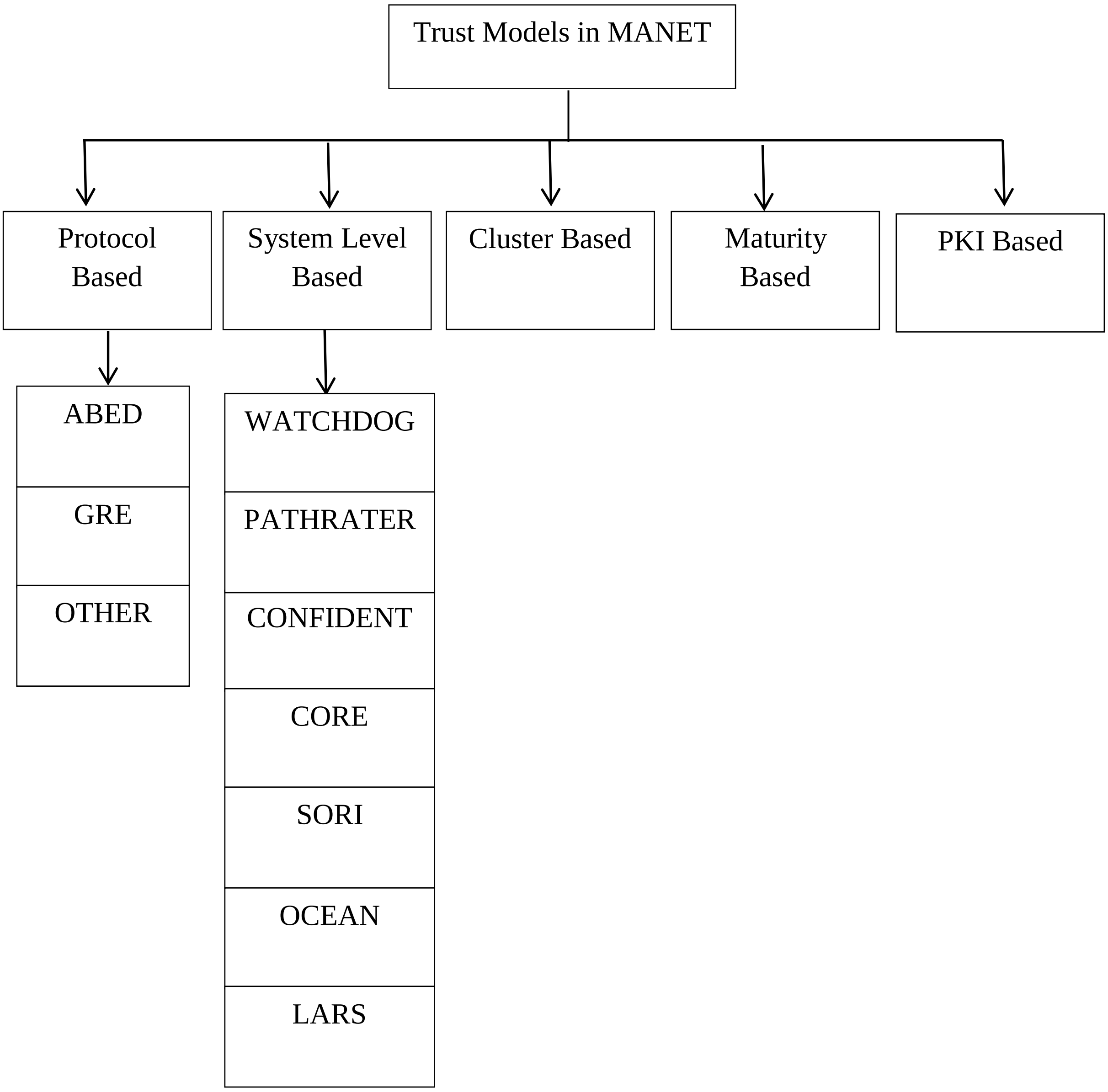

Figure 2.7: Trust based Schemes in MANET

2.6.1 Protocol based Trust Models

Protocol based trust models used security based protocol and they communicate with other nodes indirectly. Some of the protocol based trust models are listed below.

a) **Ant based Evidence Distribution scheme (ABED):** Jiang & Baras (2004) proposed ABED scheme, which uses swarm intelligence in which the nodes communicate with other nodes via agents, here termed as ants. Agents collect the information called pheromones, through which the ants find the optimal path for measuring trust. ABED is adaptable to mobility, can solve the dynamic optimization problem.

b) **Generalized Reputation Evidence (GRE):** Buckerche & Ren (2008) proposed Generalized Reputation Evidence protocol based on reputation function. GRE helps to secure the MANET from malicious node because GRE does not allowed any malicious node in the network. None of the attack is addressed in GRE scheme.

c) **Other Schemes:** Theodorakopoulos and Baras (2006) proposed another trust evaluation scheme, which solves the problem using directed graph. They used theory of semi ring where nodes as entities and link represents trust relationship for evaluating trust between two nodes. They used binary values 0 or 1 as trust values. According to them Trust is transitive.

2.6.2 System Level Trust Model

System Level Trust scheme is based on trust evidence distribution technique (Han *et al*., 2010). In this model the system either rewards the trusted node or gives punishment to the misbehaving node.

a) **Watchdog:** In Marti *et al.* (2000) proposed the watchdog mechanism which detects the malicious node by observing the mobile nodes every function. The nodes are detected as malicious in two cases: First, if the intermediate node does not forward the packet within a stipulated time, second, if the overhead packet is not same as the packet stored in buffer by the node.

b) **Pathrater:** Pathrater model works similar as watchdog mechanism, which selects the best route by calculating the path metric by observing the rating of the neighboring node. This scheme provides the shortest route. If negative value exist in the path metric this means malicious node exist in the path.

c) **Cooperation of Nodes Fairness in Dynamic Network (CONFIDENT):** In Buchegger *et al.,* (2002) proposed the Confident model which isolates the misbehaving nodes in the network. The CONFIDENT mechanism has three components: monitor reputation function, trust management and path manager. The model found the abnormal behavior of node by monitoring the behavior of nodes while transmitting packet to next nodes. If any suspicious node found in the network, an alarm message is sent to the trust manager. The trust manager calculates the trust value of every node. The path manager contains the list of all malicious nodes and has the path list to reach the destination.

d) **CORE (Collaborative Reputation):** The CORE (Michirardi *et al.,* 2002) model was proposed in 2002 by Michirardi *et al*. The CORE model differentiates malicious node and selfish node. The malicious nodes do unwanted behavior and damage the network resources, the selfish node does not cooperate with other nodes for saving their battery power, while these nodes do not harm to other nodes. This model uses three types of reputations, Subjective reputation, Functional Reputation and Indirect Reputation. In Subjective Reputation, reputation value is evaluated by giving priority to past observation of nodes and if any malicious node is found then Watchdog mechanism is used. In indirect Reputation, trust value is calculated depending upon the recommendation given by other nodes. If any nodes have negative recommendation that node will be rejected. Functional reputation is the combination of both subjective and Indirect Reputation. The weight assigned formula is used for calculating Functional reputation.

e) **Observation Based Cooperation Enforcement in ad-hoc Network (OCEAN):** OCEAN Bansal *et al.,* (2003) proposed the OCEAN trust scheme. OCEAN scheme have five components, Neighbor Watch, Route Ranker, Rank based routing, malicious traffic rejection and second chance mechanism. The neighbor watch will observe the behavior of neighboring nodes; the Route Ranker will maintain the route rank list of the neighboring nodes. The rank based routing isolates the malicious node based on rank. The Malicious Traffic Rejection remove all the malicious traffic from the node and finally the Second chance mechanism remove the suspicious node after a stipulated duration of being inactive.

f) **Secure and Objective Reputation-based Incentive (SORI):** He *et al.,* (2004) proposed SORI in 2004. This model is based on reputation rating based on packet forwarding ratio of a node. SORI have three components: Neighbors Monitoring, Reputation Propagation, and Punishment. Neighbors monitoring collects information about neighboring nodes behavior regarding packet forwarding. Reputation Propagation share information of other nodes to its neighbors. Punishment component removes the malicious node from the network.

g) **Locally Aware Reputation System (LARS):** Hu *et al*. (2006) proposed LARS trust model. It gives reputation value to its neighbor node by direct observation.

The trust evaluator node (EN) sends warning message, if it finds any nodes reputation value is less than the threshold value.

2.6.3 Cluster based Trust Model

Aiguo *et al.,* (2008) introduced Cluster Based Trust Model in MANET for maintaining trust relationship dynamically. In this model the MANET is divided into group of clusters. The major components of this model are Direct Trust, inter Cluster trust value, Gateway, Routing. The Direct Trust value calculates the trust value between any two nodes within cluster, Inter Cluster trust value is calculated by cluster head after collecting recommendation information from other nodes. Gateway maintains interaction between clusters. Intra cluster routing and inter-cluster routing is used for routing within cluster and routing between two different clusters. They used Zone Routing protocol which is both proactive and reactive.

2.6.4 Maturity based Trust Model

Pedro *et al.* (2010) proposed maturity based Trust model (Pedro et. al, 2010). In this approach each node that has trust value will provide behavioral view of all its neighboring nodes. Trust is calculated based on past experience of the node and also the behavioral view of the neighboring trusted node. In this model as time grows up trust also grows up. Every nodes takes only direct recommendation from neighbors. As new neighbor nodes increases the trust value decreases.

2.6.5 PKI based Trust Model

The PKI Based trust model uses either self-organized public key management or distributed certification. The self-organized certificate authentication (Capkun *et al.,* 2002) mechanism uses certificates issued by mobile trusted nodes. In this scheme it is considered that all mobile nodes have equal roles and it uses simple bootstrap mechanism. The distributed certification model uses digital signatures which issue and renew certificates (Saxena *et al.,* 2007). This approach requires additional storage.

Lui and Kaiser (2008) reviewed that many researchers are trying to remove main limitations of MANET like limited computing power, low bandwidth, battery power, etc. In the literature reviewed, trust has been used in various heterogeneous networks for securing the nodes from malicious attacks. Bharghavan *et al.*, (1994) proposed a media access protocol for wireless LAN. Their protocol was based on the concept of trust. In RAWCON (1998), IEEE (1999) Trust Computing Group designed a specification for encryption, decryption, signature generation and data storage for heterogeneous network data integrity, security, device authentication and device verification. Yan *et al*. (2003) proposed a statistical trust model in MANET. They defined a trust evaluation matrix using some statistical data such as association between nodes.

Pirzada and Donald (2004) presented a trust scheme to evaluate trust of each node in MANET. They expressed the trust value between -1 and +1. Negative trust value increases because of failure of various actions like packet forwarding, packet receiving etc. They have considered only the direct communication of nodes. Nagi *et al.* (2004) proposed an authentication service against dishonest nodes in MANET, by applying Beth *et al.* (1994) trust evaluation model. Beth *et al.* (1994) presented a trust model where trust is classified as direct trust and recommendation trust. Trust value is calculated into a continuous range between 0 and 1. However, their approach is designed only for open static networks. For trust evaluation between two end nodes they have used only either direct experience or recommendation but not both at the same time.

Virendra *et al.*(2005) presented a self-evaluation based trust scheme. Here trusts are calculated by monitoring the data delivery of node in the network. Omara *et al.* (2009) proposed a distributed public key certificate management system based on trust graphs and cryptography. Authentications are done through certificate chain. Yu *et al.*(2010) presents reputation based trust model. Reputation is an important concept in trust evaluation. Reputations are obtained from the society. In their approach reputation is the collection of trust from nodes in the network. Mejia *et al*. (2011) projected a trust model based on game theory. The concept of game theory was used for estimating the cooperativeness among nodes in MANET. They used a bacterial like algorithm for learning the cooperative behavior among nodes. Bao *et al.*, (2012), Lopez *et al.,* (2010), Cho *et al.,* (2011), Patwardhan *et al.,* (2005) proposed reputation-based framework for securing the integrity of data and used Watchdog scheme for identifying worthless data and awkward nodes. Feng *et al.* (2012) presented a trust model based on fuzzy theory and Markov chain model. They make a pattern for prediction making using the Markov model. The results analysis shows that this scheme is efficient in trust prediction for ad-hoc networks up to some extent but not up to the mark.

2.7 Chapter Summary

This chapter gives a detailed background of the work. It gives an overview of different routing protocols, different security threads, and various trust models. This chapter also presents some security mechanism designed by different researchers for preventing the routing attacks in MANET. The literature survey reveals that till today, there is a huge requirement for designing an efficient security mechanism as the existing schemes are not enough for secure routing. This chapter also presents a detailed comparison about the characteristic of DSDV and DSR routing protocols. From the next chapter we discuss about modification of these protocols for better performance.