Chapter – 2

LITERATURE SURVEY

CHAPTER -2

Chapter - 2. Literature survey

CHAPTER -2

LITERATURE SURVEY

This chapter discusses the current state of the new paradigm MANET as presented by the MANET working group, namely Internet Engineering Task Force (IETF). The routing protocols will be having the draft specifications on the IETF website and they will support MANETs with examples to provide an outline as to what is available at present. In particular, the routing protocol Ad hoc On-demand Distance Vector (AODV) is presented in detail along with a review of its earlier research implementations. Finally, several proposals that have been developed to architect a secure routing protocol for the MANET paradigm are discussed.

2.1. INTRODUCTION

Because of the improvements made in the wireless communications, low cost and authoritative wireless transceivers are used in mobile applications to a great extent. Because of the enhanced flexibility and decreased costs the mobile networks have gained a lot of interest among the public during recent past. Mobile networks have their own unique characteristics when compared with the traditional wired counterparts. The node mobility in mobile networks causes the topology to change dynamically in contrast to the stable topologies of wired networks. Moreover, wireless channel capacities in mobile networks continuously vary due to the impacts of fading receiver, transmission power, sensitivity, noise, and interference as compared to a steady link capacity of the regular wired networks. In addition to

these limitations, the mobile networks also suffer from the power constraints, bandwidth restrictions and high error rates.

MANETs are originated from SURAN project and the Packet Radio Network (PRNet) of DARPA and are completely free from the pre-established infrastructure. The ease of deployment and rapidity, cheaper costs, and its enhanced flexibility are the key features of MANETs. This class of mobile networks is very much suitable for the mobile applications in hostile environments where no infrastructure exists or the temporary applications where the cost is crucial.

The active research of the MANET is mainly taking place in the areas of security, resource management, power and medium access control. As routing is the significant part in MANETs, hence several routing protocols during the recent past have been proposed for MANETs so that routing issues can be handled. There are a few challenges that make the routing protocol design a tough task in MANETs. The foremost thing to be mentioned in this aspect is the node mobility that causes the topology to change as well as the network to part frequently in the MANETs. Secondly, the loss of data packets happens so often due to the volatile and changing capacity of the open access wireless channels. Further, the inherited broadcast nature of wireless links also leads to the consequences like the hidden and exposed terminal problems. Finally, the constrained battery power, computing and bandwidth limitations of mobile nodes also require efficient routing approaches in MANETs.

The field of MANETs is thus successful in attracting the research community as a gifted network class in the upcoming mobile application. The survey made in this chapter will give us the state of the art appraisal for the prominent routing protocols of MANETs. This survey covers classical unicast and multicast routing, broadcast routing and also the popular classification methods of the MANET.

2.2. BOUNDARIES OF CONVENTIONAL ROUTING PROTOCOLS

In any type of network the routing is the most basic issue to be dealt with. Keeping the eye on it, many routing protocols have been designed to work with wired networks and some of them are being used quite extensively. In wired networks the dynamic routing schemes are also commonly used. The usual routing protocols such as link state protocols, and distance vector protocols used in these hardwired networks, cannot be applied directly in the MANETs due to the following reasons.

- There will be a single directional path between nodes.
- There exists more than one entitled path between any pair of communicating nodes.
- The periodic updating of routing information results in huge consumption of the battery power and bandwidth.
- This convergence of routing fabric is very gradual in contrast to the quick changes in topology.

The link state routing and distance vector routing are the most important and commonly used dynamic routing algorithms for wired networks.

❖ **Link State Routing Algorithm**

In this routing approach, each router updates the present status of its links periodically to all other routers in the network. Immediately after a change in link states, the corresponding notifications will be broadcasted throughout the network using the principle of flooding. Upon the receipt of these notifications, all the routers re-compute their routes as per the information specified by the new topology. In this way, the router comes to know at least how a fractional picture of the complete network is in use. In link state routing diverse metrics such as traffic congestion, number of hops and link speed are used. The Dijkstra's algorithm is used to find the shortest of the available paths. The popular example of this class of routing is Open Shortest Path First (OSPF) [13].

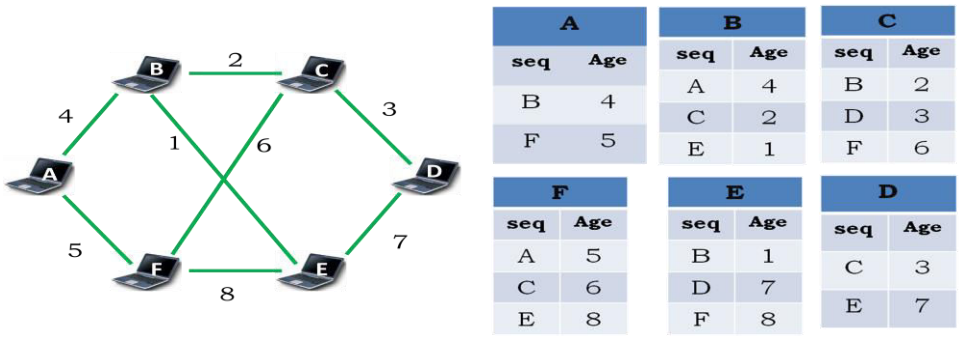

Fig 2.1: Illustration of link state routing

❖ **Distance Vector Routing Algorithms:**

These routing approaches are designed based on the Bellman Ford Algorithm. In this routing scheme, a router needs to maintain a routing table that stores the information corresponding to the distances of all the accessible destinations. To update its routing tables every router eventually exchanges the routing information with

its neighbors. Finally the metrics such as delay, queue length or number of hops are used to calculate the distances. If multiple paths are available, then the shortest path among the available paths is chosen.

The main disadvantage of this routing approach is the intentional convergence that leads to "count-to-infinity" problem. That is some routers intentionally increase its hop count to the particular routers. The popular example of this routing approach is the Routing Information Protocol (RIP) (14).

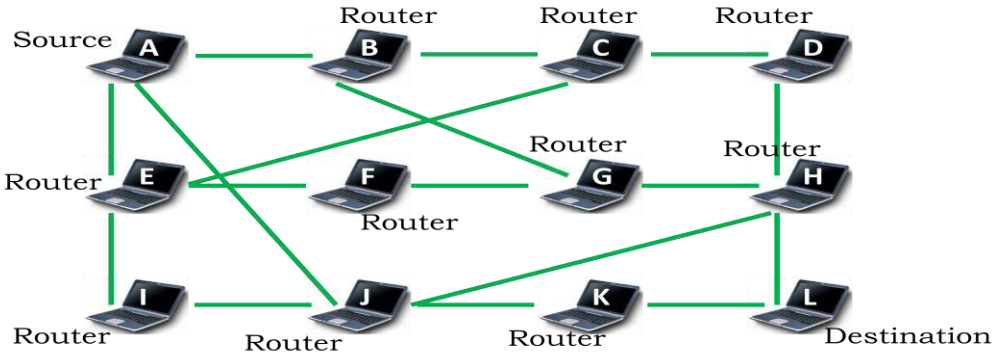

Fig 2.2: Illustration of distance vector routing

In the traditional wired networks, both the link state and distance vector routing approaches work well due to its features such as expected network topology and static link quality. But the most volatile properties of MANETs completely weaken their performance. In frequent topology changes of MANETs, while using a link state or distance vector based routing protocols that are designed exclusively for the wired counterparts, results in an increased control overhead. The additional overhead consumes the limited available bandwidth of MANETs without any remedy. In addition to that, these two routing

approaches cause routing loops and routing information inconsistency when they are used with dynamic networks like MANETs.

2.3. APPRAISAL SCHEMES OF AD HOC ROUTING PROTOCOLS

There exists no “one for all” method that is suitable for all Ad hoc network scenarios with different traffic loads, mobility patterns and network sizes even though many routing protocols have been designed for MANETs. Furthermore, all these existing protocols are designed based on different philosophies and are anticipated to meet the particular necessity from diverse application areas. Hence dramatically changes occur in the performance of ad hoc routing protocols with the variations in traffic overload and network status. So it has become a very complex task to have a broad performance comparison of diverse routing protocols due to the volatile performance nature of MANETs.

One can use three different approaches to evaluate and to make a performance comparison of different routing protocols in MANETs. The foremost approach is based on the analysis of parameters like communication and time complexity for evaluation of performance. Whereas the second approach uses, the results of simulation experiments for the routing performance comparison. Different network Simulators like NS2, OPNET, and OWNS [15], [16] [17] are popularly used for performing simulations. But unfortunately the simulation results vary heavily with the selection of simulation parameters and the simulator itself. Finally the routing protocol performance comparison can also be made using a third approach

that uses the real test beds. But this approach involves huge amounts, so it may not be feasible for the research scholars. In the present investigation, the second method is used to perform the comparison.

2.4. CHARACTERISTICS OF ROUTING PROTOCOLS

The suitable categorization methods are very much required to analyze and compare the routing protocols of MANETs. These categorization methods are very much helpful for the designers and researchers to have the understanding of the different characteristics of MANET routing protocols and also to discover its association with others. Primarily the characteristics of routing protocols are associated with the exploited routing information. For taking part in the routing process, the nodes have to acquire this information.

2.5. CLASSIFICATION OF MANET ROUTING PROTOCOLS

The design of effective routing protocols is the foremost challenge of MANETs, as they need to find routes dynamically among the mobile communicating nodes. The nodes in a MANET may move randomly and also the standing of the transmission channels between the nodes is a function of the different factors like the transmission power level, the location of the nodes and hindrance between the adjacent nodes. Hence, the arbitrary mobility of the nodes and variation in the status of the transmission link results in a rapid and irregular topology change in these types of wireless networks.

The design of routing protocols has consumed the most of the research effort after the invention of MANETs. Broadly the routing

protocols of MANETs are classified based on the following three approaches.

- Unicast routing approaches
- Multicast routing approaches
- Broadcast routing approaches

2.5.1. Unicast Routing Protocols

This class of routing protocols can be further categorized into two types as follows.

- ❖ Topology based routing protocols

  These are further classified into three types.

  - Proactive routing protocols
    Examples: DSDV, FSP, WRP
  - Reactive routing protocols
    Examples: AODV, DSR, TORA
  - Hybrid routing protocols
    Examples: SRP, ZRP

- ❖ Position (Geographical) Based Routing Protocols

  Examples: DRP, GLS, LAR

2.5.2. Multicast Routing Protocols

There exist two types of multicast routing protocols.

- ❖ Tree based routing protocol

  Examples: MAODV, AMIRS, AMRP

- ❖ Mesh-Based Routing Protocol

  Examples: ODMRP, NSM, PUMA

2.5.3. Broadcast Routing Protocols

Examples: MPR, SBA

Even though there exist lot many kinds of routing protocols contending for the different types of communication like multicast, unicast, as well as Broadcast communication for the MANET, it looks like that none of the existing protocol can fit with all the traffic pattern and connection pattern scenarios for different MANET applications. We concluded with this extensive survey of routing protocols that, each routing protocol has its own strength and weaknesses which aim at a particular application. Because of this reason, in MANETs, it is very likely to combine different competitive schemes for the prospective standard of routing protocols.

The categorization of different routing protocols can be illustrated in the form of a tree as shown figure 2.3 below.

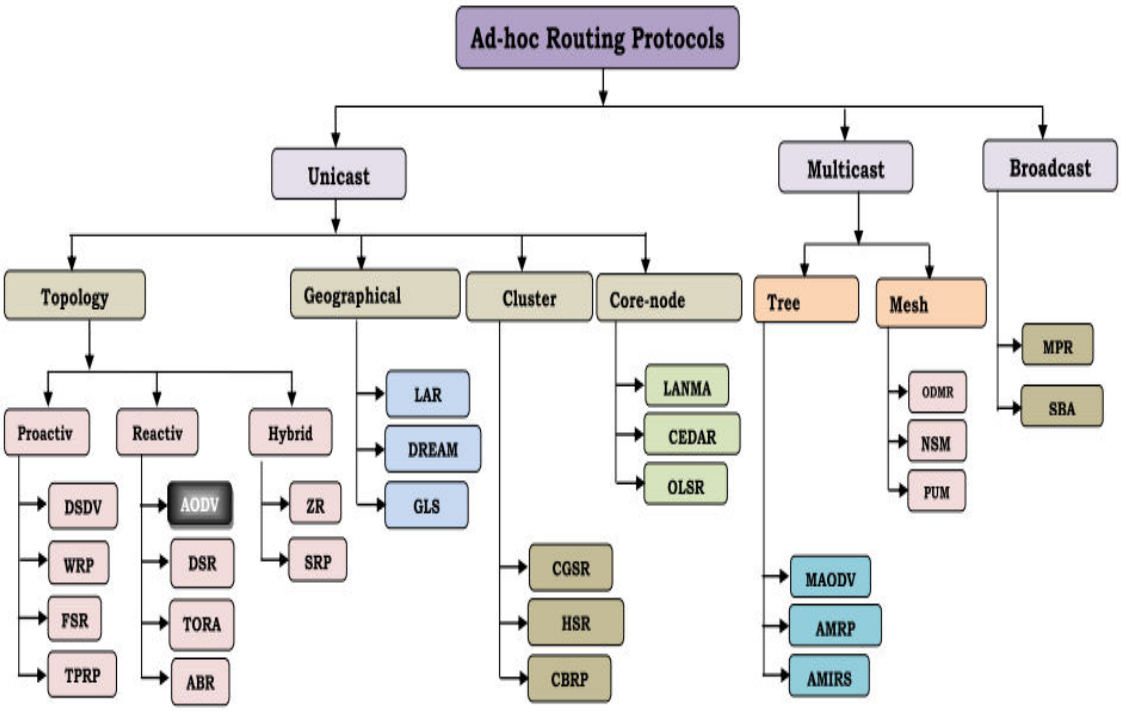

Fig 2.3: Classification of different routing Protocols

2.5.4. Illustration of Unicast Routing Protocols

The majority of the real time applications of MANET are only based on unicast communication. Hence, this type of communication is the most fundamental operation in the network layer of MANET for productively transmitting data packets from source to destination. The relaying procedure with unicast routing is quite simple. The forward node just looks into the routing table by using the destination address of the incoming data packet for the implementation of the forwarding process. If it finds that the destination address matching is very long in the routing table, then the data packet will be sent to the consequent one hop nodes. The problem that may arise here is the way the routing table is constructed in the nodes of the MANET.

In contrast to the nodes in a conventional wired network, the mobile nodes in a MANET are liberated to move randomly. Therefore, the topology of the network changes more regularly than the wired network. Numerous routing protocols have been implemented that utilize all kinds of procedures to counterbalance the brunt of mobility of MANET nodes. As discussed earlier, the unicast routing protocols can be categorized into two types. They are topology based and position based routing protocols.

2.5.4.1. Topology Based Routing Protocols

This routing protocol tries finding a route all the way from source to destination based on the metrics used for the evaluation of communication link performance of the network. The networks, which make use of topology based protocols for forwarding a data packet, are

based on the destination node address. This class of protocols can be further divided into three types, based on the means of promising the newness of the routing information. They are proactive, reactive and hybrid routing protocols.

This chapter mainly discusses the functionalities of prominent proactive and reactive routing protocols.

2.5.4.1.1. The Proactive Routing Protocols

These protocols work like conventional routing protocols that are used with internet. These protocols will always share the routing related information even if there are no particular requests to uphold the reliable and fresh routes from every node to all other nodes in a network. In order to maintain a reliable network state, the proactive protocols necessitate that every one node records a routing table in response to the network topology changes in the network by propagating up to date routing messages all the way through the network. This approach will continuously generate the control traffic, which is not optimal and should be eliminated for wireless networks. But on the other side, this scheme of implementation provides small latency route access. Existing proactive routing protocols may be different in terms of the number of necessary routing associated tables and also differentiate the other way by which network topology changes are flooded. There exist several proactive routing protocols, for instance, two of which are listed as follows.

- Destination Sequenced Distance Vector (DSDV) Routing Protocol

- Fisheye State Routing (FSR) protocol

These two routing protocols are briefly discussed before initiating the discussion on reactive routing protocols to understand their network routing mechanism, which is very much of useful for the proposed implementation.

2.5.4.1.1.1. The Destination Sequenced Distance Vector Routing Protocol

It [18] guarantees the loop-free routes and is an advanced edition of the Bellman Ford Algorithm. This routing protocol maintains complete routing tables at each node that contains all the next hop entries for all of the possible destinations. The every entry in the routing table consists of Destination Sequence Number (DSN) and number of hops to reach each destination. The DSNs are used to keep away from the formation of routing loops by facilitating or enabling the nodes to differentiate old routes from fresh ones. Periodically the updated packets are broadcasted all the way through the network to maintain up to date routing tables at the nodes. Two types of update packets are used to minimize the control overhead called incremental and full dump packets. The former packet type contains complete existing information in the routing table of every node. But on the other side, the later packet type carries the information altered only from the time the previous full dump is sent. Even though this routing mechanism decreases the control routing overload, the frequent topology changes drastically raise the quantity of incremental packets

transmitted by DSDV. In these scenarios, the update routing packets consume most of the available network bandwidth.

The advantages of DSDV

- It is convenient and beneficial to use with a MANET with a very little number of nodes.
- It solves the routing loop problem.
- The count to infinity problem is minimized.
- Instead of recording all the available paths to each destination, it maintains only the best path.

The disadvantages of DSDV:

- The DSDV protocol requires a frequent revision of its routing tables that uses the nodes with constrained battery backup and scared network bandwidth even when the network is not functioning.
- The sequence number is required whenever the network topology changes.
- DSDV is generally not optimal for exceedingly dynamic and large networks.

2.5.4.1.1.2. The Fisheye State Routing

This protocol [19] is the direct descendent of Global State Routing Protocol (GSR) [20]. GSR's update message size is reduced by FSR. It does so by updating network information for nodes which are at shorter distances than the nodes at longer distances. FSR is used in large scale MANETs with high mobility. It has got its name fish eye as it is designed from the peculiar feature of a fish. Usually the fish

can see the objects clearly with higher resolution than the objects placed at longer distances. The same method is used by the fisheye state routing protocol. Only the source has to know the direction towards the destination node which is very much far away from the source node. The nodes which exist between source and destination may correct the packet's progress during transmission. The method of FSR is as follows.

- Based on the distances (i.e., hops), the complete network is divided into networks of different capacities. For instance, if a network has nodes of hop count 2, then some of the nodes that are put in the innermost scope and the remaining nodes are put in the outer scope.
- The neighbors receive the link state updates. However, the nodes in different scopes receive the routing entries corresponding to nodes at different frequencies: the nodes in the inner scope receive routing entries at higher frequency, and then the nodes in outer scope receive at lower frequency. Hence, the nodes which are very near will take delivery of more up to date link state updates, than the nodes that are at longer distances. In MANETs, the link state updates are not flooded to discover the neighbor nodes, but are exchanged among nodes. To find the shortest path to the route towards a destination, source node uses the most recent link state information.

The advantages of FSR

- ❖ Scales well to large network sizes.

- ❖ Control traffic overhead is manageable.

The disadvantages of FSR:

- ❖ Route table size still gets larger linearly with network size.
- ❖ The routes too far away destinations become less precise with the increased mobility of the nodes.

2.5.4.1.2. Reactive Routing Protocols

Dynamic topology of the MANET regularly needs to update the global topology information stored at each node that swallows most of the available bandwidth. But, most of the times this is a waste of bandwidth, because these link state updates terminate before the route is needed between another node and itself. To keep this wastage as minimum as possible, the on demand or reactive routing approaches are anticipated.

With this approach, the phase of the routing is divided into two stages as follows.

Route discovery phase: In a conventional wired network, the source must transmit ARP request packet to the remaining nodes to get the MAC destination address earlier than it sends a packet. In a MANET, the source broadcast a route request throughout the network, if it is not having the route in its present routing table to the destination. The Intermediary nodes alongside the path relay the route discovery packet, i.e. RREQ and may generate certain data structures to find the route.

Route maintenance phase: After the establishment of the route between the source and destination, the route maintenance phase is

initiated to validate the route as the nodes along the path may collapse due to power collapse or random movement. If a failure of link is found alongside the path, then it will notify the source to make a decision to initiate the new route discovery procedure to find a completely fresh route, or initiate a local repair procedure to sidestep the failed link. The prominent protocols AODV, DSR and TORA that come under this class of routing approach are discussed in detail in the following three subsections.

2.5.4.1.2.1. The Ad hoc On-demand Distance Vector (AODV) Routing Protocol

The AODV [21] uses an on demand or reactive routing approach, with route discovery and route maintenance procedures as follows

Route discovery phase: If the source is not having the route to the respective destination in its present routing table, then it initiates a route request procedure by broadcasting RREQ packets to all of its one hop neighbors in the network. On receipt of a RREQ, the intermediary nodes to create an entry to reverse route to the source of the RREQ and is used to forward the route replies (RREP) soon after. Then the intermediary node or destination, that has a legitimate route towards the destination, responds with a unicast RREP packet. After the receipt of RREP, the reverse routing entry to the source of RREP is also formed in the same way as that of RREQ process. The ancestor list that is connected with each routing entry is generated at the same

time. The complete detail of upstream nodes towards the same destination is included in the ancestor list.

Route maintenance: After the route is established between the source and destination, the route maintenance phase is initiated to validate the route as the nodes along the path may shut down due to power collapse or move randomly. Each node along the live route occasionally transmits HELLO messages to its on hop neighbors. If the particular node fails to receive a data packet or a HELLO message from a one hop neighbor for quite some time, the link is assumed to be broken to that neighbor. If the destination to this neighbor is believed not to be far away, the local repair mechanism may be once again initiated to reconstruct the route to the destination else inform all the neighbors towards the originator in the ancestor list of the related route entries by sending route error packets.

The sequence number forwarded along with both RREQ and RREP and recorded in the routing table. The larger value of the sequence number indicates the newness of the route information.

The advantages of AODV protocol:

- Routes are created
- Sequence numbers are used to stay away from the routing loops.
- The route setup delay is smaller.

The disadvantages of AODV protocol:

- The Intermediary nodes may lead to conflicting routes if it has the very old source sequence number.

- ❖ The unnecessary bandwidth consumption due to periodic updates.

2.5.4.2.1. The Dynamic Source Routing (DSR) Protocol

It [22] is first and foremost on demand or reactive routing approach, which aims at the MANET that consists of mobile nodes up to two hundred. In contrast, to the other unicast protocols, the DSR uses the option of source routing in data packets, hence it does not require maintaining the routing tables. Instead, it utilizes the mechanism of a route cache to save the full IP addresses list of each node alongside the route that leads to the destination. The basic working principle of DSR is as follows.

Route discovery process: If the source does not have the route entry towards the destination in the route cache, then a RREQ packet is transmitted to all one hop nodes all the way through the MANET until it finds the destination. The intermediary node augments its own IP address in an inventory of the RREQ before it forwards the packet. Immediately after the receipt of packet by the destination, the RREQ packet accumulates the route from source to destination, if the underlying MAC layer supports unidirectional links, subsequently the destination executes another route discovery process to discover the path towards the source; or else, it just reverses the source path which is saved in the route request packet. In other words, a RREP packet is sent back to the source which contains the route from source to destination. After the route is detected, both the source and destination will have the path towards each other.

Route maintenance: No periodic HELLO message is initiated in DSR, unlike the routing protocol AODV as mentioned earlier. In DSR every node is responsible for the legitimacy of the downstream channel along the path connecting itself and the next hop in the source path, which could be found by DSR specific software acknowledgement or MAC layer. If the established link is collapsed then the originator of the path will be informed with a special control packet called a Route Error packet. Then the source will re-initiate a new route discovery process.

In DSR, the Route cache mechanism adopts to a greater extent. For instance, the intermediary nodes cache the path that leads to the destination and delivers back to the source. In addition, the header of the data packet contains the source path; the nodes that respond can cache the path in its routing cache.

The mechanism of route cache reduces the routing overload as illustrated below.

(1) All the way through the route discovery process the intermediary nodes answer the RREP packet, if their routing cache has the path that leads to the destination.

(2) As DSR supports multiple paths, the source may use an alternate path stored in the route cache instead of initiating a new path to save the overhead of the route discovery if it receives a route error packet.

(3) While the intermediary node is forwarding a data packet, and if it detects the downstream link breakage, but it has another

path in its routing cache that leads to the same destination, then it will relay the packets alongside the alternate route, which we call the packet salvaging.

The advantages of DSR:

- The route is established only on demand; hence it avoids the necessity to find paths to all other nodes.
- A route cache mechanism is so much of helpfulness for the intermediary nodes to minimize the control overload.

The disadvantages of DSR:

- The broken link cannot be repaired locally by route maintaining process
- The delay in connection establishment is greater than the proactive routing protocols.
- The routing overload is compared to the route length.

2.5.4.2.2. Temporally Ordered Routing Algorithm (TORA)

This reactive routing protocol works in combination with the LMR protocol. It uses the methods defined by LMR such as route repair and link reversal, and also the design of a DAGs. A query/reply procedures existing in LMR are also used in TORA. Most of the features and advantages of TORA are similar to LMR. In addition, one of the two main advantages of this protocol is that it reduces the broadcast of control messages to a group of adjacent nodes, even in the presence of topology changes and the second benefit of TORA is supporting multicasting,

nevertheless it doesn't add the basic performance. TORA can adjust in working with a LAM algorithm to permit multicasting. But the problem with TORA is the generation of invalid temporary routes as seen in LMR.

The advantages of TORA:

- Attempts to build directed acyclic graph before destination**.**
- Defining multiple paths.
- Best choice to use in dense networks.

The disadvantages of TORA:

- Rare to use because domination of DSR and AODV in performance with TORA.
- Results poor performance while increasing the mobility.

2.6. PROVIDING SECURITY IN MANETS

Providing Security in a MANET is the significant factor for basic networking functions such as routing and packet forwarding. The network process can be easily exposed if counter measures are not implanted into basic networking functions at their initial design phase. In contrast to the conventional wired networks, the MANET performs the basic network support functions such as routing, packet forwarding and network management without the aid of dedicated infrastructure nodes and also the open media is used for data transmission.

In contrast to the permanent nodes of a wired network, the mobile nodes of an Ad hoc network cannot be trusted to that extent in

the implementation of important networking functions. In addition, when the strong authentication infrastructure and tamper proof hardware do not exist, for instance, in an open setting where a wide-ranging authority that controls the network is not available, any node of the network can be threatened by the consistency of network basic functions like routing. The right actions of the network necessitate not just the correct implementation of significant network function by every node that participates, but also it needs every node to execute a clean share of the process. The later necessity looks to be a big shortcoming of this protocol. The mobile wireless nodes that have to put aside the limited battery power for their own operation, so that they can be active on the network for a longer period of time.

Because of the lack of a trust among the nodes, the conventional security mechanisms of wired networks based on cryptographic authorization and access control process cannot be adapted directly to the MANET. The security schemes based on cooperativeness among the participating nodes looks to be the only feasible solution for MANETs. In a cooperation based security scheme approach, the misconduct of the node can be easily identified through the association among the number of nodes, considering that a greater part of them are legitimate nodes.

2.6.1. Security Goals

The basic functionality of the security services is to offer a proper secure networking atmosphere.

The summary of important security services is illustrated as below.

1. **Authentication**: The security service must check the uniqueness of the user and ensures the recipient that the packet is from the source that it claims to be from. At the outset, the service assures that the two parties are authentic, that each entity, it claims to be legitimate at the time of commencement of communication. After then, the security service must also ensure that a third party may not obstruct by impersonating one of the two genuine parties for the purpose of authenticated transmission and reception. It can be granted by using the encryption process, digital signatures and certificates along with cryptographic hash functions.
2. **Confidentiality**: This security service assures that the data transmission over the network is not open to the illegal users. It can be done by using diverse encryption techniques in order to understand only to the legal users.
3. **Integrity**: This security function ensures that the receipt of data is precise as sent by the authorized party. That is received data should not contain any insertion, modification, or deletion.
4. **Access Control**: It restricts and controls the access to resources such as an application or a host system.
5. **Availability**: This security service allows legitimate users to get access to the resources all the times. This service assures to survive the network despite the malicious incidences.

2.6.2. Constraints in Designing a Secure Routing Protocol for MANET

In this traditional wireless networks, encryption and authentication techniques (cryptography based approaches) are incorporated into one of the most existing routing protocols, especially to avoid the impact of malicious entities in the network. Cryptographic methods can be used to prevent the crash of the external attacks by sharing authorization of the participating nodes through digital signature schemes. But the MANETS are being affected by the external attacks as well as the internal attacks. In a MANET, the decision-making, forwarding packets, key distribution and routing are normally not centralized and depend on the cooperativeness among the numerous participating nodes. The decentralized nature and as well distributed paradigm of MANET allows an attacker to launch new types of internal attacks. These internal attacks may be designed especially to damage the cooperative algorithms that are used in MANETs. Hence, in MANET the routing functionality can be disrupted either by external or internal attacks. An internal attack can be launched by any genuine participant of the network and an external attack is found to be defined as any other entity. These internal and external attacks may be either passive or active in nature.

As discussed earlier, these cryptographic approaches cannot prevent insider attacks. Although these introduced cryptographic approaches can protect any relayed packet from being modified, but these have numerous limitations for securing routing protocols. For

example, they cannot stop a node from launching a packet with forged contents. Furthermore, even cryptographic schemes require high computational transparency, which may use all the computational resources and result in denial of service attacks. Some of the cryptographic approaches do not cover critical fields like hop count that changes over time. Hence, authentication and encryption approaches are no longer adequate and are not effective for defending MANETs. Hence, other solutions must be devised to balance the limitations of cryptographic methods, and this exemplifies the need for Intrusion Detection System (IDS) to secure MANET routing. The IDS can comprise a second wall of defense and their job is significant for the most of MANETs that will be deployed in unfriendly surroundings in which genuine nodes can be controlled as well as operated by adversaries. The IDS must automatically detect intrusions (sequence of malicious activities) and accordingly alarms are to be generated for finding a proper reply. Nodes that are well set with IDS enabled sensors and functioning in promiscuous mode, can easily monitor the traffic sent or received by their one hop neighbors for the sake of finding the adversary behaviors.

2.7. SECURITY VULNERABILITIES OF THE EXISTING ROUTING PROTOCOLS

The most of the existing protocols are designed with an assumption that most of the participating nodes are trustful and do not disrupt the functionality of routing protocol with malicious or selfish intent. On the other hand, in the open systems like MANET the

existence of malicious entities cannot be ignored. The unique characteristics like limited resources and even the open access nature of MANETs makes these things relatively difficult to design a secure routing protocol for MANET as compared to the traditional wired or centralized wireless networks. Numerous security approaches have been proposed to enforce the cooperation and to prevent the misbehaviors, like ARIADNE [23] and SAODV [24], ARAN [25], SEAD [26] etc. Based on the survey conducted as a part of this investigation on the existing cryptography based secure routing protocols, it is noticed that none of the accessible protocols are either perfect or able to defend all the types of attacks.

Most of the past researches in the area of MANET security are based on either cryptographic or IDS approaches. Thus the proper security solutions are not available to handle both internal and external attacks which are inevitable in MANET. The present research aims to propose effective security solutions using both the approaches to deal with both internal and external attacks. In the next section the various attacks and their security measures for MANETs are discussed in detail. The more sophisticated of these attacks and threats against existing MANET routing protocols are then discussed.

2.7.1. Types of Attacks and Exploits on the Existing Protocols

There exist so many varieties of attacks that exploit the limitations of the MANET. For instance, the route discovery or the route maintenance phase of the MANET routing protocols can be attacked by the malicious routing attacks by just preventing them

from following the normal routing specifications. So these MANET routing protocols are susceptible to different attacks ranging from simple passive eavesdropping to more complex active attacks like denial of service, jamming, impersonation, modification etc. In MANETs the mobile nodes have negligible physical protection so they are more defenseless and may be easily compromised. After compromising some of the nodes, then these can be used as initiating points to launch the malicious attacks on the routing protocols. This section discusses the functionalities of different attacks and their impact on the performance of MANET routing protocols. Currently secure routing is one of the hottest research areas in MANET.

In a broad sense the attacks on routing protocols can be categorized as follows.

- Passive attack or Resource consumption attacks.
- Active attack or Routing disruption attacks

The passive attacks try to consume the scarce network bandwidth by injecting the false packet or eavesdrop the information. Eavesdropping, traffic analysis and traffic monitoring are few examples of passive attacks. The active attacks try to disrupt the entire routing mechanism by misdirecting the routing protocols to route the packets in wrong paths. Denial of service, impersonation, modification and jamming are the few examples of active attacks. The classification of different attacks is shown in figures 2.4 and 2.5 below.

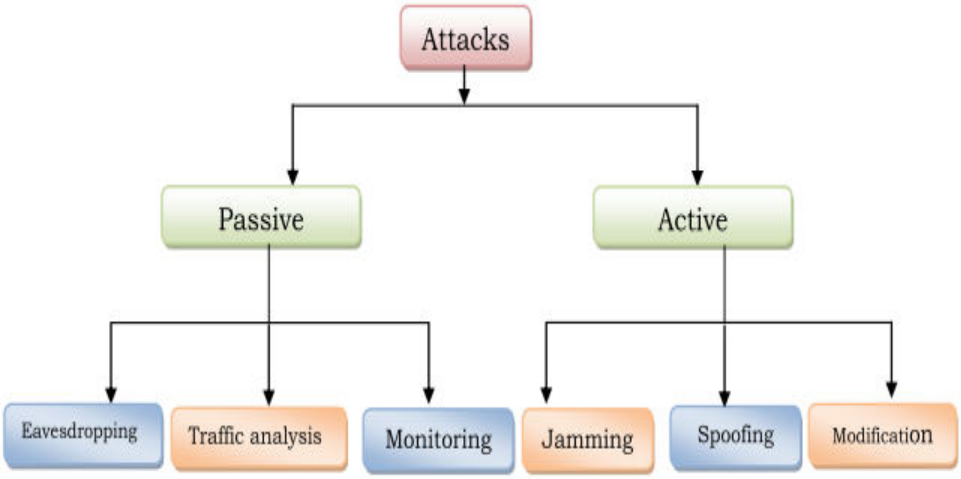

Fig 2.4: Classification of attacks

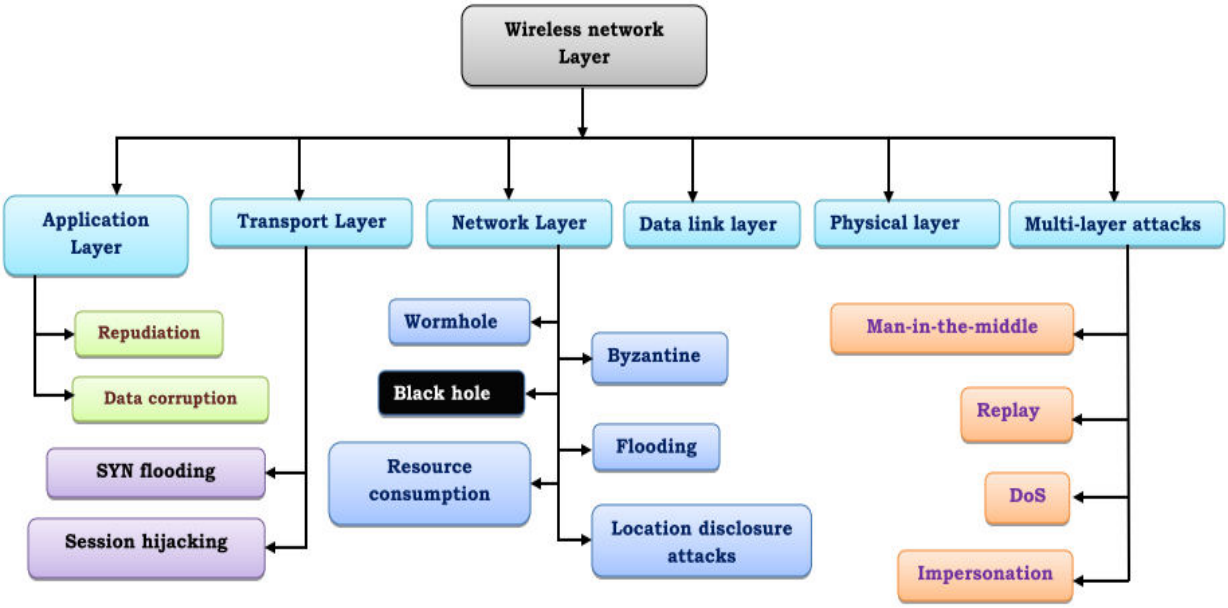

Fig 2.5: Classification of attacks in various layers

2.7.2. Routing Disruption Attacks on Existing Routing Protocols

It has been found that few attacks target only some specific routing protocols. For instance the attackers may modify the source route such as deleting node from the list, appending a new node to the list, or change the order of the list in RREP or RREQ packets in DSR protocol. The adversaries may showcase a route with a lower distance metric than the real distance or aerate a route with a huge destination

sequence number to overthrow all the routing updates from other nodes in AODV protocol.

A very wide variety of routing disruption attacks targeting these network layers have been recognized and deeply studied in many research publications. With these attacks on routing protocols, the attackers place themselves into the route between the source and destination and capture the network traffic. To introduce noteworthy delay, the packets could be relayed to a wrong path. In addition to these, the packets could also be relayed to a path that does not exist and get vanished. Attackers can introduce network congestion, harsh channel contention and also creates routing loops to disrupt the network routing functions. Several colluding adversaries may stop the source node from detecting any path to the destination, resulting in network partition, which increases network congestion, further triggers tremendous network control traffic and finally degrades the performance. Some of the routing disruption attacks have been discussed below.

2.7.2.1 Attacks on the Routing Discovery Phase [27]

These adversary routing attacks do not follow the terms of the routing protocols and aim to disrupt the route discovery phase or route maintenance phase. Some of the routing attacks that try to disrupt the route discovery phase are routing table overflow, RREQ flooding, hello flooding, routing loop, acknowledgement flooding and routing cache poisoning attacks. For better understanding of these

types of attacks the functionality of routing table overflow attack is discussed below.

- **Routing table overflow attack:** The adversary node aerates the wrong routes to the legitimate nodes with an intention to mislead them to the nonexistent nodes in the network. It normally occurs in proactive routing approaches that need to frequently update the routing information. The adversaries also try to generate adequate routes to stop fresh routes from being generated. The table driven routing approaches are more susceptible to table overflow attacks because they attempt to find the routing information in advance. Simply the attacker sends disproportionate route advertisements to the routing table of the victim.

2.7.3. Attacks on the Routing Maintenance Phase

Some attacks may target route maintenance phase by flooding wrong control messages, like link broken error messages that lead to the incantation of the expensive route maintenance or operation repairing, for instance, DSR and AODV apply path maintenance process to regain out of order paths on node movement. Similarly, there exist attacks that disrupt data forwarding phase of the routing. Also, there exist different attacks like attacks using modification, impersonation, fabrication etc for misleading the legitimate users and finally to disrupt the network routing functions.

2.7.4. Special Attacks

In addition to the above described attacks, some other special attacks those are likely in routing protocols like AODV and DSDV.

- **Wormhole Attack [28]:** It is a more severe attack in which two nodes with malicious intent relay packets from end to end of a private "*subway*" in the network as illustrated in figure 2.6.

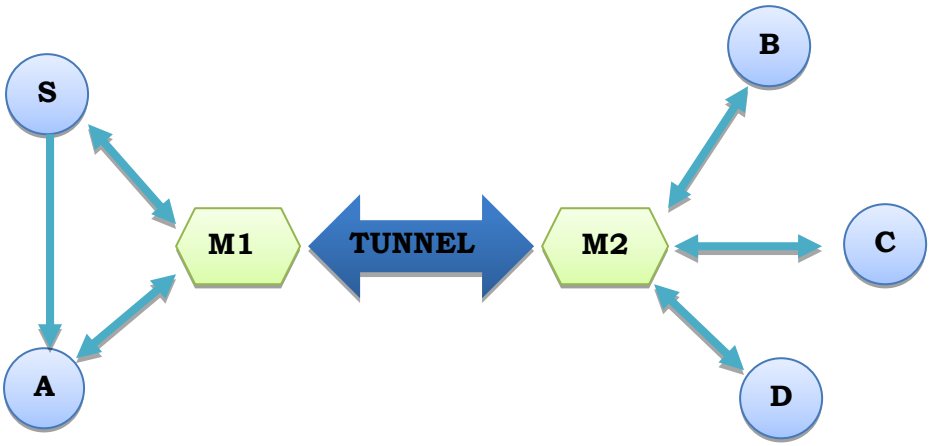

Fig 2.6: An example of a wormhole attack

In the above example, M_1 and M_2 are two nodes with a malicious intent and connect through an end to end private channel. Every packet that the node M_1 receives is relayed through the *wormhole* tunnel to malicious counterpart M_2 and vice versa. It disturbs the routing protocols normally by short circuiting the flow of the routing packets. This type of attack is very tough to detect in a network, and may severely damage the communication among the nodes in such networks. Such type of an attack can be barred from using a procedure called *packet leashes*, which validate the

information about timing in the packets to identify the fake packets in the network.

- **Blackhole attack problem:**

In this attack, an adversary node misleads the routing protocol to make a false showcase as of having the finest path to the destination or to the packet it needed to interrupt. This antagonistic node, aerates the accessibility of new routes without verifying the routing table. Like this the malicious node will always have the accessibility in replying to the RREQ and thus catch the data packet and will keep hold of it. In the protocols, based on the flooding mechanism, the RREPs of the adversary node will be received by the source prior to the reception of RREP from genuine node; consequently an adversary and bogus route will be generated. As soon as the path is established, immediately the blackhole has the choice whether to crash all or some of the packets or relay them to the address which is unknown. The way how this blackhole node fits on the data route may vary. Figure 2.7 illustrates how the problem of blackhole arises.

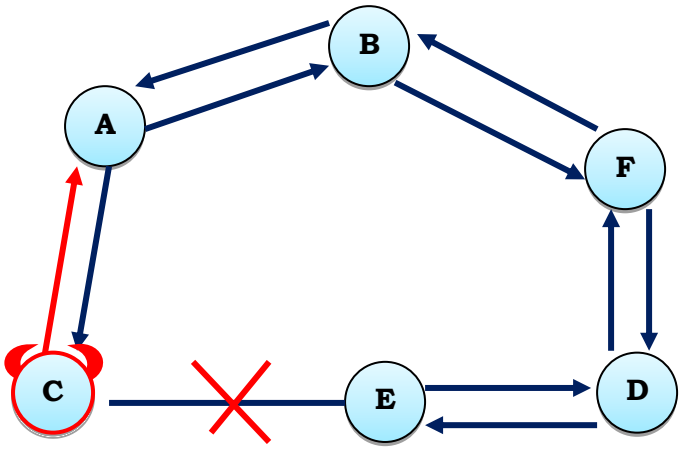

Fig 2.7: Blackhole attack

In this example, the node “A” wish to send data packets to destination node “D” and kick off the process of route discovery. If node “C” is an adversary node with blackhole features, then it claims that it has a fresh enough path to the particular destination as soon as it receipts the RREQ packets. It sends the reply to node “A” earlier than any other node. By this way the node “A” is misdirected by the blackhole node and considers this as the lively route and thus completes the present route discovery process. The node “A” disregards all the replies from other nodes and starts inputting packets to node “C”.

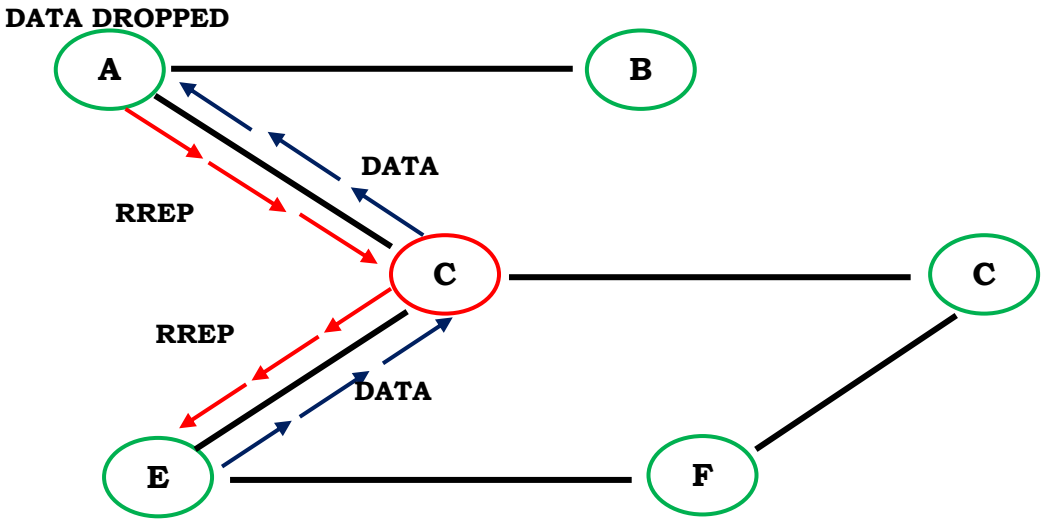

Fig 2.8: The illustration of blackhole attack problem

By this way all the data packets are relayed through the node “C”. Then the node “C” drops all the received packets. By this way, the sender and destination are in no position to communicate any more in a state of blackhole attack.

So the AODV routing protocol has no clue to compete with blackhole attack and fails to provide the secure data communication. As discussed earlier, the MANETs are most susceptible to the

malicious attacks like blackhole attacks. Therefore, secure routing is so essential in MANETs. Prior to continue the investigation that leads to the proposal of a new secure routing protocol, the existing secure routing protocols of MANETs are discussed in detail in the next section to understand the different security mechanisms and their merits and shortcomings.

2.8. SURVEY OF EXISTING SECURE ROUTING APPROACHES

As discussed in the preceding section, the security has become a primary concern in MANETs. The distinctiveness of MANETs creates both challenges and opportunities in acquiring security goals. There are present quite a few proposals that try to design a security extension of available routing protocols of MANET [29, 30], with an objective to present a defense against the different attacks as discussed in the previous section. In this section several secure extensions of different traditional routing protocols using both intrusion detection system and cryptographic approaches are discussed in detail.

2.8.1. Security Extensions of Existing Routing Protocols Using IDS Approach.

The different aspects of some of the IDS based existing secure routing protocols are discussed in this section.

REAct - Resource Efficient Accountability Routing Protocol: The REAct [31] is an on demand malicious detection scheme that is based on the random audits. The REAct tries to identify the adversary nodes based on a sequence of arbitrary audits which are usually triggered

when the performance of the routing protocol suddenly drops. The source and destination pair can be able to find autonomously disobedient nodes of any number using REAct based on behavioral proofs provided by the nodes. The REAct is exclusively designed to compete with only non cooperative blackhole attacks. It fails to succeed in the collaborative blackhole scenario for the reason that the other adversary node is capable to control a false proof and is sent to the audit appraisal node. The approach of behavioral proof only stores the information of communicating packets instead of the node's identity. So it does not succeed in validating the originator of the behavioral proof. As a final point, by means of the binary search method one can discover the invader and it is effortlessly uncovered to audit appraisal information of nodes. The invader is also can deceive source by altering its behavior vigorously.

IAODV - Improved AODV Routing Protocol: The IAODV [32] is the enhanced version of the AODV protocol. The IAODV mainly integrates two features into the AODV routing protocol. They are path accumulation and multipath. The distinct path AODV starts a fresh route discovery process when it discovers a path breakdown to the destination, while at the multi-path it generates a fresh enough route by the time all the available routes expire or fail. In this secure extension of AODV the source node selects the shortest one hop neighbor and subsequently shortest paths based on the route requests. If the neighbor node exists in its routing table, then the information packet is routed else it is marked as malicious and sends

fake packets to that node. The source node once again invokes the route request and informs all the one hop neighbor nodes about the malicious nodes and add the status of the invader to the routing table of the source. The control overhead of the AODV routing protocol is effected by twofold as compared to IAODV. The IAODV has a more PDR, a smaller amount of end-to-end delay as well as lesser routing control overhead as compared to other security extensions. There is no path of accumulation in AODV and it is a distinct path on demand routing protocol with a smaller amount of security while hybrid IAODV is incorporated with path accumulation being more secure than AODV. The end-to-end delay is nearly similar in all scenarios for both AODV and IAODV but there is a raise in the routing control overhead.

Watchdog and Pathrater: It [33] was basically designed to better the throughput of the MANET in the company of selfish nodes. The Watchdog unit overhears the transmission media to ensure whether the neighbor node truly relays the packet or not. The second one is the Pathrater unit that could help in determining the likely paths exclusive of the compromised nodes. The Pathrater method computes the path metric of every route and chooses the route with the best metric value. The benefit of the Watchdog method is that it can discover the misconduct of the nodes at the relaying level and not just at the connection level. On the other side, the shortcoming of the Watchdog method is that it may not notice a malicious node in the existence of the receiver collisions, the ambiguous collisions, restricted

overhearing rage collusion, the inadequate transmission power and limited dipping of packets. The major drawback of the Pathrater method is its behavioral deceit, inflexible binary state and new node anonymity, encouraging selfishness and greed and re-entrance of the previously malicious node.

CORE - A Collaborative Reputation Routing Protocol: The CORE [34] was designed based on the reputation and monitoring scheme. With this technique every node receipts information from every other node. This routing protocol permits only the information of a positive nature to pass through in contrast to the CONFIDANT protocol which allows the negative reports also. The CORE can prevent the DoS attacks as it does not allow the reports of a negative nature. The system gives a negative rating by the time the node doesn't work together and its standing is decreased. But at the same time from the receipt of positive reports from a node its reputation is increased.

OCEAN - Observation-based Cooperation Enforcement in Ad hoc Networks Routing Protocol:

It [35] is the improved version of the dynamic source routing scheme. In this protocol each node maintains rating for every neighbor and observes their behavior using promiscuous mode of functioning. The negative and positive actions are stored through the response of the one hop neighbor, which is likely to relay the packets. All the ratings are initially set to the unbiased value. The decrement value is always preferred to be larger than the increment value. If the rating of the node dips below some threshold value, then the node is added to

the malicious record. But the OCEAN routing protocol is not efficient in minimizing the throughput of the malicious node and doesn't take any countermeasure to put off collusion.

This section discussed some of the intrusion detection enabled secure routing protocols in detail and compared these by highlighting their characteristics, features and differences. Based on this survey it can be summed up that every secure routing protocol has particular benefits and limitations, and can be suitable for a specific application setting.

2.8.2. Security Extensions of Existing Routing Protocols Using Cryptographic Approach

The different aspects of some of the cryptography based existing secure routing protocols are discussed in this section.

ARAN -Authenticated Routing for Ad hoc Networks: This [36] is a reactive secure routing protocol that discovers and defends against malicious activities approved by third parties and peer nodes in the mobile ad hoc network surroundings. As a branch of the minimal security policy for MANET, ARAN initiates a message integrity, non-repudiation and authentication. It consists of a primary and obligatory stage certification process, end-to-end authentication and a voluntary subsequent stage that provides safe direct paths.

The advantages of the ARAN secure routing protocol are

- Secure as long as there is no cooperation from the certificate authority
- Confidential as it includes the public key encryption

- Covered network structure
- Successfully opposes most of the attacks.

The disadvantages of the ARAN secure routing protocol are

- High memory requirement
- High processing overhead

ES-AODV - Effective Security AODV Routing Protocol: This [37] is an extended version of the popular reactive AODV routing protocol. The main focus of this protocol is on the IP layer of the network. This was designed to offer a secure solution which is strong enough to resist active internal attacks inside the network for effective communication in MANET applications. This model of implementation is based on the analysis of different malicious behaviors and mutual effort of all the participating nodes. The design of ES-AODV comes from the fact of determining a trusted end-to-end path which is free of adversary nodes.

The advantages and shortcomings of ES-AODV:

Based on the extensive analysis of the simulation results, we concluded that this secure routing protocol adapt well to the scale of the network. But on the other side with increased mobility in MANET, it fails to execute better than the traditional existing AODV protocol.

ARIADNE - A Secure On-Demand Routing Protocol for Ad Hoc Networks: This [23] is also a reactive secure ad hoc routing protocol based on a DSR protocol that depends on highly effective secret key cryptography to withstand the compromise of malicious nodes. By using the MAC and a common secret between the two communicating

entities this protocol tries to provide a point-to-point authorization of the routing message. This security extension routing approach uses the TESLA broadcast authorization protocol for validation of a broadcast packet such as route request.

The advantages and disadvantages of ARIADNE: It can cope up with the attacks such as the impersonation, modification, and fabrication of routing messages and, in a newer version, even the wormhole attacks which are performed by the malicious nodes. This protocol is also shielded from a flood of route request control packets that would lead to the special type of attack called cache poisoning attack. But on the other hand, this protocol doesn't take the selfish nodes into consideration.

SEAD - Secure Efficient Ad-hoc Distance Vector Routing Protocol:

This secure routing protocol [26] is an enhanced version of the proactive DSDV routing protocol. It uses a hash chain mechanism to validate the sequence number and metric of an updated message in the routing table. Further, the recipient of SEAD also validates the originator and assures that the routing data is originated from the genuine entity. The source of each routing update message should also be validated in SEAD or else an adversary may generate routing loops using the attacks such as impersonation attack.

The advantages and disadvantages of SEAD:

It makes use of an economical and effective one way hash chain mechanism instead of depending on costly asymmetric cryptography functions. The SEAD fails to counter with wormhole attacks.

SRP - Secure Routing Protocol: In contrast to the above security extension routing approaches the SRP [38] was designed as an extension based on several existing reactive routing protocols. So it is compatible with a wide variety of protocols. The SRP can compete with adversaries that upset the path discovery process and assure the acquirement of accurate topological information. This secure routing protocol permits the designers of a route discovery procedure to notice, and remove the fake responses. The SRP completely depends upon on the security relationship available between the source (S) and destination (D) nodes. The security association would build using the public keys of the two communicating entities based on hybrid key distribution. The S and D can swap a common secret key (KS, D) using the public keys of each other to set up a secure link. Then the S and D can promote the authentication of routing messages and continue to the mutual authorization of each other.

The advantages and disadvantages of SRP:

The SRP can cope up with non-colluding adversary entities that corrupt or modify, fabricate, replay the routing packets. The initial edition of SRP suffers from the attack of route cache poisoning, but later on it overcomes with the new versions. On the other side, the SRP also suffers from the short of an authentication mechanism for

route maintenance control messages. This protocol also fails to combat with wormhole attacks.

SAODV - Secure Ad hoc On Demand distance Vector routing protocol: The security extension [24] is an enhancement over the traditional AODV protocol and, is designed based on the consideration that each node in a network possesses certified public keys. With this protocol the source augments its RSA digital signature and the final component of a hash chain mechanism to the routing control packets. As packets travel through the network, the intermediary node authorizes the digital signature and the value of the hash using cryptographic scheme. The intermediary nodes seeds the k^{th} component of the hash chain procedure, where k represents the number of transverse hops, and put it in the packet. On receipt of a packet the destination node signs the RREP message with its own privacy key and replays it back to the source. The possession of certified public keys facilitates the intermediary parties to validate all in transit control routing packets. This protocol mainly works by utilizing the fresh extension message of the existing AODV protocol.

The advantages and disadvantages of SAODV:

It can defend the route discovery procedure of the AODV routing protocol by providing security features such as authentication, non repudiation and integrity. But it imposes a lot of processing control overhead due to the reason that it uses the asymmetric key cryptographic principle.

SAR - Security-Aware Ad-Hoc Routing Protocol: This [39] is not the

secured version of any particular protocol, but it is the comprehensive structure of any reactive MANET routing protocol. The SAR mandates that nodes with a similar trust level be obliged to share a private key. The SAR uses hash functions and secret key encryption mechanisms to enhance the routing process. It assures the message integrity using the signed hash digests and ensures the confidentiality by way of encrypting of packets. It dynamically controls the selection of routes stored in the routing table using the security information. This security protocol doesn't always guarantee the shortest path between any two communicating parties, but it ensures to provide the routes with the quantifiable guarantee of security. In route establishment process, if each node on the direct path suits the security requirement, then this protocol may choose it as an optimal path.

The advantages and disadvantages of SAR:

The SAR guarantees to establish routes with quantifiable security. But always it may not provide the shortest path between any two pairs of nodes. Sometimes it may not succeed to discover the path if the MANETs do not comprise a path on which every node satisfies the security necessities instead of being just connected.

SLSP - Secure Link State Routing Protocol: It [40] can be used as a separate protocol or can be combined with some reactive routing protocol to use it as a part of the hybrid routing framework. For efficient functioning with no central key administrative authority, the SLSP allows all the nodes to occasionally forward their public keys to all other nodes within their zones and also allows every node to relay

the signed HELLO messages that consist of its MAC and IP address pair in its on hop neighbors in this regard. The sharing of MAC address makes the scheme more strengthened by frightening nodes from spoofing at the level of the link layer. The SLSP can be able to function efficiently in the networks of frequently changing topologies and memberships.

The advantages and disadvantages of SLSP:

It is flexible against the standalone adversaries and is also able to change its range between the local and system wide topology discovery. It implements a round robin servicing method to offer the guarantee that the gentle control traffic will be forwarded even under the blockage of DoS attacks.

The merits and demerits of different secure routing protocols are listed in table 2.1.

Attack	PROTOCOL					
	ARAN	ARIADNE	SEAD	SAODV	SLSP	SAR
Wormhole	No	No	No	No	No	No
Denial of Services	No	Yes	Yes	No	Yes	No
Blackhole	No	No	No	No	No	Yes
Rushing Attack	Yes	Yes	Yes	No	No	No
Replay	Yes	Yes	Yes	Yes	Yes	Yes
Location Disclosure	No	No	No	No	No	No
Routing Table Poisoning	Yes	Yes	Yes	Yes	Yes	Yes

Table 2.1: The comparison of different secure routing protocols

So for a lot of investigation have been done in the area of an efficient secure routing protocol design for MANET. Our survey of different secure routing protocols reveals that the numerous challenges still remains in this area of security for wireless networks. At the outset the network setting is not properly devised and accordingly lacks an official procedure to make a complete valuation of the proposed secure routing protocols. One more problem that is identified is the design of a competent routing protocol that provides well-built network security and as well as elevated performance. Even though investigators have designed several security extensions for the available protocols, but most of these extensions ignore the importance of performance optimization.

In the present investigation the different secure routing protocols are compared by highlighting their characteristics, differences and features. Based on this survey it can be considered that each protocol has particular benefits and limitations, and can be suitable for a specific application setting.

2.9. MOTIVATION

MANETs are ideally suited for emergency response operations since they do not rely on fixed infrastructure nor they are difficult to set up in quick time. Each node in a MANET has to perform a dual role as an end system to perform user functions and a router to perform network routing functions. Because of the features like dynamically changing topology, open medium, lack of centralized administration, unclear defense mechanism and the use of

cooperative algorithms, the MANET frequently suffers from security attacks. In addition to the inbuilt vulnerabilities of the wireless channels, the routing system of MANETs is one of the main areas of security risk. All aspects of wireless data transfer need to be properly secured, as emergency services require the transaction of valuable and private data while working in the field. The motivation factor of this dissertation is to design a secure routing protocol for MANET that may be employed for field workers performing emergency rescue work during a crisis situation even if all other existing communication systems are unavailable.

2.10. PROBLEM STATEMENT

In this field of MANET routing protocols, there are group of problems to be handled like routing optimization, quality of service, power awareness and more importantly security issues. In this investigation, the attention is primarily focused on the security issues related to the routing protocols of MANETs. So, the investigation started with the reading of different research directions in this vast field and analyzed the different existing routing protocols and their security extensions. It finally ended up with interest to work on AODV protocol and studied the various routing aspects of it. It is decisively understood that AODV protocol is completely defenseless to the special attacks like blackhole, grayhole and other denial of service attacks. In furtherance of our interest an attack type called blackhole has been selected as a case study, being the reason that AODV has no clue to compete with this type of attack. Subsequently, more focus

was developed on secure routing protocols and their diverse mechanisms in protecting MANET against the compromised, selfish and malicious nodes. The available secure routing protocols such as SAODV, ARAN, SRP, ARIADNE and others were studied in detail. Then it was decided to propose a secure routing framework with an objective to overcome the limitation of the existing security solutions as an extension to the traditional AODV protocol based on an intrusion detection system and cryptographic approaches in the context of MANETs.