CHAPTER 2

REVIEW OF LITERATURE

2.1 Traditional Unicast Routing Protocols

A wireless mobile ad hoc network consists of a set of mobile nodes that are connected by wireless links. The network topology in such a network may keep altering arbitrarily. Routing protocols used in the customary wired networks cannot be applied directly in mobile ad hoc networks.

MANET is extremely dynamic topology, the absence of well known infrastructure for centralized administration, band width constrained wireless links, and resource constrained nodes. A variety of routing protocols for wireless mobile ad hoc networks have been proposed in the recent past. This chapter reviews the relevant literature.

The prominent unicast routing protocols for MANET can be classified into many types on the bases of different criteria. First, the routing protocols type is the distance vector Ahemed et al. (2017). These protocols were primarily designed for wired networks. The following are some of the pure distance vector algorithms Distributed Bellman Ford routing algorithm Bellman et al. (1957), Ford and Fulkerson (1962) and Routing Internet Protocol (RIP) Malkinetet et al. (1998). Pure distance vector algorithms do not perform well in wireless mobile networks due to the of twin reasons of slow convergence and count to infinity problem Andrew Tanenbaumet al. (1999). The proposed routing protocols solve the above two problems and enhance the pure distance vector protocol Asad et al. (2016) , Enhanced Routing Algorithm of this type include Least Resistance Routing Protocol (LRR) Pursley and Russell (1993), Destination Sequence Distance Vector

(DSDV) routing protocol Perkins et al. (1994), Wireless Routing Protocol (WRP) Murthy and Garcia Luna Aceves (1996), ClusterHead Gateway Switch Routing (CGSR) protocol Chiang et al. (1997) and QoS Routing Lin and Liu (1999).

The second type of routing protocols is based on link state routing algorithms Carlos et al. (2017). The protocols falling in this category are Global State Routing (GSR) Algorithm Chen and Gerla (1998), Adaptive Link State Protocol (ALP) Garcia et al. (1998), Optimized Link State Routing (OLSR) Algorithm Jacquet et al. (1998), Source Tree Adaptive Routing (STAR) Algorithm Garcia et al. (1999a), Fisheye State Routing (FSR) Algorithm Pei et al. (2000a), and Landmark Ad Hoc Routing (LANMAR) Algorithm Pei et al. (2000b).

The third type of routing protocols is the reactive routing protocol (also called on demand protocol). The on demand protocols create routes only when necessary for carrying traffic Dingde et al. (2017). Only when found necessary in these protocols, control overhead is very much minimized since periodic exchanges of route table information are not required. Several on demand algorithms have been proposed Guanglie et al. (2017). Some of them are, Lightweight Mobile Routing (LMR) Algorithm Corson and Ephremides (1995), Dynamic Source Routing (DSR) Algorithm (Johnson and Maltz (1996), Das et al. (1998), Das et al. (2000), Temporarily Ordered Routing Protocol (TORA) Park and Corson (1997), Associativity Based Routing (ABR) Algorithm Toh et al. (1997), Signal Stability Based Adaptive (SSA) routing Dube et al. (1997) algorithm Routing On demand Acyclic Multipath (ROAM) protocol Raju et al. (1999), Relative Distance Microdiscovery Ad Hoc Routing (RDMAR) algorithm Aggelou et al. (1999), Ad Hoc On Demand Distance Vector (AODV) routing algorithm Charles Perkins and Royer et al. (1999), Charles Perkins and Royer (2002), Gorka Hernando et al.

(2009), Multipath Dynamic Source Routing Protocol (MDSR) Nasipuri and Das (1999), FlowOriented Routing Protocol (FORP) Su and Gerla et al. (1999), Route Life time Assessment Based Routing (RABR) algorithm Agarwal et al. (2000), Preferred Link Based Routing Protocol (PLBR) Sisodia et al. (2002), DSR Over AODV routing (DOA) protocol Rendong Bai and MukeshSinghal (2006), Neighborhood Discovery Protocol (NHDP) Clausen et al. (2010), and Dynamic MANET On Demand Routing (DYMO) Protocol Chakeres et al. (2010), Huan et al. (2017).

Protocols belonging to the fourth category improve the performance of routing protocols and reduce the control overhead of protocol through efficient utilization of the geographical information available. The geographical information about the node position can easily be obtained without incurring any significant control overhead Jian et al. (2017) The routing protocols falling in this category are, LocationAided Routing (LAR) protocol Ko and Vaidya et al. (1998) LjubicaBlazevie et al. (2005), Distance Routing Effect Algorithm for Mobility (DREAM) protocol Basagni et al. (1998), Zone based Hierarchical Link State (ZHLS) routing Joa and Lu et al. (1999), Flow Oriented Routing Protocol (FORP) Su and Gerla et al. (1999), Greedy Perimeter Stateless Routing (GPSR) protocol Karp and Kung et al. (2000), Grid Location Service (GLS) routing protocol Li et al. (2000), MRP Jangeun Jun and MihailSichitiu (2008) and Heterogeneous MANET (HMANET) Huda Al Amri et al. (2010), Jing et al. (2017a), Jing et al. (2017b).

In addition to the abovementioned routing disciplines, a few other routing algorithms have been proposed by Murthy and Garcia et al. (1996), Chiang et al. (1997), Akyildiz et al. (1997), Krisha et al. (1997), Ramanathanand Steenstrup et al. (1998), Singh et al. (1998), Chen and Nahrstedt et al. (1999), Iwata et al. (1999), Pei et al. (1999), Sivakumar et al.

(1999), ZhiRenand Jing Su et al. (2005), Chang and Tassiulas et al. (2007), and Hauspie and Isabelle (2007), Hybrid routing protocol uses table driven.

The approach to nodes within the zone and on demand approach to nodes outside the zone are described Jun et al. (2017). An essential hybrid routing protocol is Zone Routing Protocol (ZRP) Pearlman and Haas (1999), Zone based Hierarchical Link State (ZHLS) routing Joa and Lu et al. (1999), and CoreExtraction Distributed Adhoc Routing (CEDAR) protocol Sivakumar et al. (1999). The routing protocols proposed by Singh et al. (1998) and Chang and Tassiulas (2000) try to minimize the power consumption either locally or globally in the network in selecting routes. Cluster Based Routing Protocol (CBRP) Jiang et al. (1999) forms a group of nodes into clusters to improve scalability Weixia et al. (2017). There have been several surveys papers on routing protocols for wireless mobile ad hoc networks Ramanathan and Streenstrup (1996),

Broch et al. (1998), proposes the use of on-demand behavior in such protocols, focusing on its effect on the routing protocol's forwarding latency, overhead cost, and route caching correctness, drawing examples from detailed simulation of the dynamic source routing (DSR) protocol.

Royer and Toh et al. (1999), proposes an efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. Route construction should be done with a minimum of overhead and bandwidth consumption.

Gerla et al. (1999), propose a new cross-layer ad hoc multicast protocol, named MIMO-CAST, to improve efficiency of IEEE 802.11 MAC. MIMO-CAST builds a multicast tree on-demand by using control packets

exchange. It exploits Multiple-Input Multiple-Output (MIMO) by giving different weights to its multiple antennas so that a node can receive from one neighbor while blocking the interference from other nodes.

Lee et al. (1999a), propose a scheme resists DoS attack by increasing a local validation step and resists insider attack by encrypting the random number stored in the smart card, makes up the defects in selecting server by increasing the server's identity.

Jaisankar and DuraiSwamy (2009), proposed a novel agent based framework to monitor, detect, and isolate misbehaving nodes in the MANET. The proposed framework protect both routing and data forwarding operations, which aiming at improving the efficiency in detecting and isolating misbehaving nodes with a minimum overhead. In this paper local neighboring nodes collaboratively monitor each other. A novel honesty rate strategy is introduced in each node to determine the well-behaving nodes.

2.2 Multicast Routing Protocols

Multicast routing protocols for wireless mobile ad hoc networks can be classified into two types. The first type is application dependent, meant only for specific applications for which they are designed. Routing protocols falling in these categories are Role Based Multicast (RBM) routing protocol Briesemeister and Hommel (2000), Xiu et al. (2017) Content Based Multicast (CBM) routing protocol Zhou and Singh (2000), and Location Based Multicast Algorithms (LBM) Ko and Vaidya (1999). The second type of application independent generic multicast protocols is used for conventional multicasting Yang et al. (2017a), Yang et al. (2017b). It can be classified further into three different categories on the basis of the nature of multicast

topology, initialization and topology maintenance approaches. The detailed classifications of multicast routing protocols can be found Siva Ram Murthy and Manoj (2007).

The first category of routing protocols is based on the nature of the multicast topology routing algorithms. The algorithms falling in these categories are Multicast Core Extraction Distributed Ad Hoc Routing Protocol (MCEDAR) Sinha et al. (1999), Bandwidth Efficient Multicast Routing Protocol (BEMRP) Ozaki et al. (1999), Multicast Ad Hoc On Demand Distance Vector Routing Algorithm (MAODV) Elizabeth Royer and Perkins (1999) and On Demand Multicast Routing Protocol (ODMRP) Lee et al. (1999). There have been several survey papers on multicast routing protocols for wireless mobile ad hoc networks Luo Junhai et al. (2008), Hoang Lan Nguyen and UyenTrang Nguyen (2008), Macker et al. (2010).

The second category of multicast protocol is classified into two variants. When the group arrangement is initiated only by the source node, then it is called a source initiated multicast routing algorithm, as for example Neighbor Supporting Ad Hoc Multicast Routing Protocol (NSMP) Lee and Kim (2000), Dynamic Core Based Multicast Routing Protocol (DCMP) Das et al. (2002a), Content Based Multicast (CBM) algorithm Zhou and Singh et al. (2000) and Dynamic Multipath Source Routing (DMSR) algorithm Peng Yang Biao Huang et al. (2008) . When initiated by the receivers of the multicast group, it is called a receiver initiated multicast routing algorithm. Routing algorithms falling in this category are Differential Destination Multicast protocol (DDM) Ji and Corson (2000), Weight Based Multicast (WBM) Routing Protocol Das et al. (2002b), Preferred Link Based Multicast Routing (PLBM) algorithm Sisodia et al. (2003) and Mobility based Multicast Routing Algorithm (MMRA) protocol Javad Akbari Torkestani and

Mohammad Reza Meybodi (2010a), Javad Akbari Torkestani and Mohammad Reza Meybodi et al. (2010b).

The final category of multicast protocols is based on the topology maintenance mechanism. Routing protocols falling in this category are Forward Group Multicasting Protocol – Receiver Advertising (FCMPRA) Chiang et al. (1998), Core Assisted Mesh Protocol (CAMP) Garcia Luna Aceves and Madruga (1999) and Dissemination of Multicast Aggregated State (DIMAS) Rolando Menchaca Mendez and Garcia Luna Aceves (2010). There have been several survey papers on the topology maintenance multicast routing algorithm for wireless mobile ad hoc networks Javad Akbari Torkestani and Mohammed Reza Maybodi (2010a) and Katerina Papadaki and Vasilis Friderikos (2010).

2.3 Secure Routing Protocols

Unlike the traditional wired network, where dedicated routers and centralized controllers are used for controlling the network, nodes in wireless mobile Ad Hoc networks act both as nodes as well as routers for other nodes. In the absence of a centralized controller and dedicated routers, providing security becomes a challenging task in these networks. Several methods have been proposed for protecting the networks from malicious nodes. These rely on cryptographic systems, symmetric or public key management and hash chains.

The secure mobile ad hoc routing problem has been extensively investigated and a number of secure routing algorithm have been proposed in the literature, to name a few, Secure Ad Hoc On Demand Distance Vector Routing (SAODV) Manel Guerrero Zapata et al. (2001), Secure aware Ad hoc Routing (SAR) Yi et al. (2001), Authenticated Routing for Ad Hoc Networks

(ARAN) Sanzgiri et al. (2002), Secure Efficient Ad Hoc Distance Vector Routing (SEAD) Hu et al. (2002a), Ariadne (Hu et al. 2002b), SRP Papadimitratos and Haas (2003) and SAODV Songbai et al. (2009). All these secure routing protocols focus on protecting the correctness of the routing table information maintained at each node while leaving the data packet forwarding typically unprotected. These protocols take the proactive approach and prevent malicious attacks by protecting the routing messages through cryptographic primitives.

Kong et al. (2001), explain a solution that supports ever present services to mobile hosts. In the design, the author allocate the certification authority functions through an unknown threshold unknown distribution mechanism, in which each entity holds a secret share while multiple entities in a local neighborhood jointly provide complete services. Thus no single entity in the network knows or holds the whole system secret (e.g. a certification authority's signing key). Instead, each entity holds a secret share of the certification authority's secret key. Multiple entities, say 'k' in one hop network locality, jointly provide total security services, as if a single omni present certification authority is provided to them.

Pi Jian Yong et al. (2006), propose a novel cryptography for ad hoc network security, where the author presents a new digital signature protocol for identity authentication and key agreement scheme. Their scheme has no central administrator. They have shown the ability of their scheme to withstand man in middle and Byzantine mode conspiracy attacks.

Hubaux et al. (2001), have made a survey of the threats and the possible solutions for the security of an ad hoc network. They have extended the idea of the public key infrastructure. Their system is similar to Pretty Good Policy (PGP) in the sense public key certificates are issued by the users.

However, they do not rely on certificate directories for the distribution of licenses. They have presented two algorithms in this connection. Zhang and Lee (2000), were among the first to study the problem of intrusion detection in wireless mobile ad hoc networks.

Different types of attacks on MANET were discussed by Suresh et al. (2015). They have designed a security mechanism by which many of those attacks can be minimized or even completely eliminated. Sudha Rani et al. (2012), have proposed a detection and prevention of wormhole attack in stateless multicasting. Their scheme has no central manager. They have shown the ability of their schemes to handle wormhole attacks.

Leonidas Georgiadia et al. (2006), have made a survey of the threats and the possible solutions for resource allocation and cross layer control in wireless networks. Raj et al. (2009), have proposed a solution for black hole attacks. It was implemented in prominent AODV protocol based MANET. Tsou et al. (2011), have developed a novel scheme BDSR to avoid black hole attack on the basis of proactive and reactive architecture. Yu et al. (2007), proposed a solution of a distributed and cooperative black hole node detection and elimination mechanism. Solda et al. (2011), have provided a solution for blacklisting attacks, the author studied the problem of forecasting attack sources based on past attack logs from several contributors. They have formulated this as an implicit recommendation system by Ayyaswamy et al. (2011).

Hernandez et al. (2014), have introduced a fast model to evaluate the selfish node detection in MANET using a watchdog approach. They have estimated the time of detection and the overhead of collaborative watchdog approach for detecting one selfish node. Singh et al. (2014), implemented a security based algorithmic approach in MANETs. In this analysis, an empirical and effective

approach was proposed to optimize packet loss frequency. Jyoshna et al. (2012), have proposed a solution for Byzantine attacks in ad hoc networks using SMT protocol that provides a way to secure message transmission by dispersing the message among several paths with minimal redundancy. Megha Arya and Yogendra Kumar Jain (2011), have provided a solution for gray hole attack. They use an intrusion detection system (IDS) to monitor the network or system, for selfish activities or policy violation, and produce reports to a management station. It takes over the sending of packets. Following this, the node just drops the packets to launch a (DoS) denial of service attack. If neighbor nodes that try to send packets over attacking nodes lose the connection to the destination, they may want to discover a route again by broadcasting RREQ messages by Ayyaswamy et al. (2009 & 2010).

B.B. Jayasingh and B. Swathi (2010), have proposed a mechanism that detects the jellyfish attacks at a single node that can be effectively deployed for all other nodes in the ad hoc network. They have provided have provided a solution that detects the jellyfish reorder attack on the basis of the reorder density which is a basis for developing a metric.

The research paper of Timothy et al. (2010), focuses on jamming at the transport/network layer. The jamming at this layer exploits AODV and TCP protocols, It is shown to be very effective in simulated and real networks when it can sense victim packet types. However, the encryption is assumed to mask the entire header and contents of the packet so that only packet size, timing and sequence is available to the attacker for sensing Suresh et al. (2015).

Kurkure and Chaudhari (2013), have done a comparative analysis of the selfish node detection methods based on detection time and message overhead. A collaborative watchdog method has been used to identify the

selfish nodes and diminish the detection time and message overhead. Sahu and Sinha (2013), suggested a cooperative approach for understanding the behavior of IDS in MANETs. The authors describe various attacks and techniques used for intrusion detection which was proposed to provide a high performance. (Patel et al. 2014), have used an AODV protocol for trust based routing in ad hoc networks, which have limited physical security, reduced infrastructure, restricted power supply, mobility network and changing network topology Ayyaswamy et al. (2009), Jawhar et al. (2015), suggest a reliable routing protocol for enhanced reliability and security of communication in the MANET and sensor networks.

Various P2P media streaming systems have been deployed successfully and corresponding theoretical investigations have been performed on such systems Shen et al. (2011). The author Wang et al. (2011), have made a thorough investigation of the evolutionary dynamics of flexible security mechanism namely, reciprocity based incentive mechanism, in P2P systems based on evolutionary game theory (EGT). By soft security mechanisms relate to social control mechanisms to overcome peers selfish (rational) behavior and encourage cooperation in P2P systems.

Trust management plays a major role in IoT for reliable data fusion and mining, qualified services with context awareness, and enhanced user privacy and information security Yan et al. (2014). It helps to overcome perceptions of uncertainty, risk and engages in user acceptance and consumption on IoT services and applications, Yan et al. (2014), Sheng et al. (2013) and Cheng et al. (2012). However, current literature still lacks a comprehensive study on trust management in IoT Yan et al. (2014). Authenticated key agreement protocol is a useful cryptographic primitive, which can be used to protect the non-confidentiality, integrity and authenticity of transmitted data over insecure networks Yang et al. (2014).

Built upon opportunistic routing and random linear network coding, Code Pipe not only simplifies the coordination of transmission between nodes but also improves the multicast throughput significantly by exploiting both intra batch and inter batch coding opportunities Peng et al. (2012). In particular, four key techniques namely, LP based opportunistic routing structure, opportunistic feeding, fast batch moving and inter batch coding, are proposed to offer the substantial improvement in throughput, energy efficiency and fairness Peng et al. (2012).

The author Yen et al. (2011), have proposed a multi constrained QoS multicast routing Athanasios and Vasilakos (2011), the method using the genetic algorithm. The proposal will be flooding limited WaiQuan et al. (2014), using the available resources and minimum computation time in a dynamic environment. The genetic algorithm improves through selection of the appropriate values of parameters such as crossover, mutation and population size tries to optimize the routes.

The author Cheng et al. (2012), have proposed an assignment strategy with topology preservation by organizing the mesh nodes with the available channels and aim at minimizing the co channel interference in the network. The channel assignment with the topology preservation is proved to be NP hard with the impossibility in finding the optimized solution in polynomial time. They have formulated a channel assignment algorithm named as DPSOCA which is based on the discrete particle swarm optimization and can be used to find the approximate optimized solution Cheng and Attar (2012).

All the above schemes can be implemented only to protect the system from an attacker, but does not deal with the quarantining attackers Naisue et al. (2009), Zeng et al. (2013). The TBUT systems not only detect

the mischievous nodes but also prevent their further participation in the network.

All the above schemes can only protect the system from the attacker, but do not deal with quarantining attackers. The twin systems of watchdog and path rater Sergio Marti et al. (2000), not only detect the mischievous nodes but also prevent their further participation in the network. SCAN Hao Yang et al. (2006), also has a similar action, but it is more comprehensive, in the sense that not only packet dropping but also other misbehavior like giving wrong hop count is covered.

Router guard Nidal Nasser and Yunfeng Chen (2007) is similar to the path rater and is run by each node. Router guard introduces a more detailed and natural classification system that rates each node into one of the five classes like fresh, member, unstable, suspect and malicious. Accordingly, each node is treated differently.

There have been several survey papers on secure routing protocols for wireless networks Capkun et al. (2003a), Capkun et al. (2003b), proposed a global description of the building blocks used by the basic operation of the network and rely on various concepts of self-organization. Routing uses a combination of geography-based information and local MANET-like protocols. Term node positioning is obtained by either GPS or a relative positioning method. Mobility management uses self-organized virtual regions.

Hao Yang et al. (2004), propose a two important facts for energy consumption: 1) Different from previous literature, the cost of measure processing is not trivial. As the number of measurements increasing, it is a considerable percentage contrasted to transmission cost. 2) The value of

measurement constantly changes along the routing, which may cause a cost jump in a specific location.

Azer at el. (2007), propose a role of Certification Authorities (CAs) in securing ad hoc networks communication and introduce the concept of certification authorities and their selection and we survey and classify the certification schemes and give a brief overview on the revocation schemes.

Lei Feng Yu et al. (2007), propose a CPK as the security mechanisms of ad hoc networks with the purpose of high-level security as well as excellent performance and investigates several security schemes, and evaluates the scalability, the availability and the robustness of the schemes by extensive simulations.

Ding Xuyang et al. (2007), propose a simple and comprehensive analysis of energy consumption and three necessary principles for energy-efficient topology control for wireless sensor networks. Topology control should (1) consider power control and sleep scheduling jointly, (2) be aware of traffic load, and (3) be done in conjunction with routing.

Xiaobo Zhou and Liqiang Zhang (2008), propose a minimum power and maximum rate problems for the MARC system with lossy relaying are formulated and the resulting nonconvex problems are solved via successive convex approximation (SCA).

Zhenxia Zhang et al. (2010), propose a location verification approach to prevent position-spoofing attacks on VANETs. Cooperative Location Verification (CLV), which is our approach, basically used two vehicles, a

Verifier and a Cooperator, to complete the verification of a vehicle (Prover). The Verifier and Cooperator sent a challenge to the respective Prover and the Prover was required to reply with its location information immediately which was based on radio frequency. The Verifier then verified the claimed location according to the Time-of-Flight of the signals in those two challenge-response procedures.

Raju and Rehan Akbani (2006), propose a new Hybrid Trust Management System (HTMS) that combines Role Based Trust Management (RBTM) with Reputation Systems (RS). At any point in time, the privilege level of an entity is determined not only by its role in the system, but also by its reputation score, which in turn is based on its behavior. If a privileged node becomes compromised and conducts several malicious or risky transactions, its privilege level is quickly reduced to limit its access to resources and minimize the damage it can inflict further. The system uses a global, network-wide perspective in order to thwart global attacks.

2.4 The Network Layer Routing Protocols

The network layer unicast routing protocols for mobile ad hoc networks can be classified into several types on the basis of different criteria as discussed in section 2.1. In this section, some of the prominent unicast routing protocols for network layer are detailed. The routing protocols are, Wireless Routing Protocol (WRP) Murthy and Garcia Luna Aceves et al. (1996), Fisheye State Routing (FSR) protocol Pei et al. (2000a), Dynamic Source Routing (DSR) protocol Johnson and Maltz et al. (1996), Ad Hoc On Demand Distance Vector (AODV) routing protocol Charles Perkins and Royer et al. (1999) and Zone Routing Protocol (ZRP) Pearlman and Haas et al. (1999).

2.4.1 Wireless Routing Protocol

Wireless Routing Protocol (WRP) is a distance vector routing algorithm for packet radio networks. It has the goal of maintaining routing information among all nodes in the network. As the network topology changes, it relies on communicating the changes to its neighbors, which propagates throughout the entire network. WRP belongs to the class of path finding algorithm avoiding of the 'count to infinity' problem, which eliminates looping situations and provides faster route convergence when a link breakdown event occurs.

2.4.2 Fisheye State Routing

Fisheye State Routing (FSR) uses the fisheye method for reducing the information required to represent graphical data, to reduce routing overhead. The basic principle behind this approach is the property of a fish eye that can capture pixel information with greater accuracy near the focal point of the eye. FSR maintains the topology of the network at every node but does not flood the entire network with information, as is done in link state routing protocols. Instead of flooding, a node exchanges topology information only with its neighbors. A sequence numbering is used to identify the recent topology changes. Complete topology information of the network is maintained at every node and the desired shortest paths are computed as required. The topology information exchange takes place periodically rater than being driven by an event. This is because the instability of the wireless links may cause excessive control overhead when event driven updates are employed. The routing overhead is significantly reduced by adopting different frequencies of updates for nodes belonging to different scopes.

2.4.3 Ad hoc On Demand Distance Vector (AODV)

Ad hoc on demand distance vector (AODV) routing algorithm uses an on demand approach for finding routes. That is to say, a route is recognized only when required by a source node for broadcast data packets. In an on demand routing algorithm, the source node floods the route request (RREQ) packets in the network when a route is not available for the desired destination. It may obtain multiple routes from a single route request. AODV uses destination sequence number DestSeqNum to determine a current path to the destination. A node updates its path information when the DestSeqNum of the current packet received is greater than the last DestSeqNum stored in the node.

If the node possesses a route towards the destination with a sequence number greater than the RREQ packet, it unicasts a route reply (RREP) back to the neighbor from which it received the RREQ packet, indicating the possession of a valid route to the destination. Duplicate copies are deleted when RREQ is received multiple times as indicated by BcastID, SrcID pair. All intermediate nodes have the correct route to the destination, or the destination itself is allowed to send a route reply (RREP) to the source. Every intermediate node, while forwarding an RREQ, enters the previous nodes address and it's BcastID. A timer is used for deleting this entry in case an RREP is not received before the stipulated time.

When a node receives RREP packet information relating to the previous node from which packets were received, it is also stored for forwarding the data packet to the next node as the next hop towards the destination. The source and destination nodes are notified with the breaks, of the links break which is determined by observing the periodic beacons or through link level acknowledgments.

When a source node learns about the path break, it reestablishes a path to the destination, if required by the higher layers. If an intermediate node detects the path break, the node informs the end nodes by sending an unsolicited RREP with hop count set as infinite value.

2.4.4 Dynamic Source Routing (DSR)

DSR is a source routing protocol. The sender knows the entire hop by hop route to the destination node D and route cache uses to store the information. The data packets take the source route in the packet header. When a source node S wants to send a data packet to a destination node D for which it does not already know the route, it uses a route detection process to decide such a route dynamically. For route discovery, each node receiving an RREQ rebroadcasts it, unless it is the destination node D or has a route to the destination node D in its route cache. Such a node replies to the RREQ with a route reply (RREP) packet that is routed back to the original source. The route approval backed by the RREP packet is cached at the source for future use. DSR includes a path maintenance mechanism for handling the dynamics in the network topology. If any link on a source route is broken down, the source node is notified using a route error (RERR) packet. The source eliminates any route using this link from its cache. A new route detection process must be initiated by the source if this route is still wanted.

2.4.5 Zone Routing Protocol (ZRP)

ZRP is a hybrid routing algorithm, which efficiently joins the best features of both proactive and reactive routing algorithm. An intra-zone routing protocol (IARP) is used in the zone where a particular node uses proactive routing. The reactive routing used beyond this zone is referred to as intera-zone routing protocol (IERP). Each node maintains the information

relating to the routes to all nodes within its routing zone by exchanging periodic route update packets. Hence, larger the routing zone, higher is the update control traffic. The IERP is accountable for finding paths to the nodes, which are not within the routing region. When the node has data packets to a particular destination, it checks its routing table for a route. If the destination lies within the region, a route exists in the route table. A search to find a route to that destination is required when the destination is not within the region.

2.4.6 Comparison of two On Demand Routing Protocols

Several comparative studies have been made between DSR and AODV Broch et al. (1998), Das et al. (1998), Das et al. (2000), Asad Amir Pirzada et al. (2006) and Nor Surayati Mohamad Usop et al. (2009). Though they share the on demand performance in that they begin routing activities only in the presence of data packets in need of a route, several of their routing mechanics are very different. In particular, DSR uses source routing, whereas AODV uses a table driven routing framework and destination sequence numbers. DSR does not have any timer based activity, while AODV has the same to a certain extent. In DSR, several additional optimizations such as Salvaging, Gratuitous route repair and dishonest listening have been proposed which have been found to be very effective. The advantage of the on demand schemes is that they do not use the significant amount of network bandwidth. We have chosen AODV because

- AODV consumes less memory compared to DSR, which consumes more memory for a route cache, each data packet carries complete route information in the header.
- AODV is efficient in high mobility networks, but DSR protocol is efficient only in networks with small mobility.

The research work has also incorporated the promiscuous hearing feature in the proposed AODV based models.

2.5 Protecting the Network Layer from Malicious Attacks

The network layer is responsible for the host to host delivery and for routing the packets through the routers. There are two important activities of network layer operations, routing control messages and data packet forwarding.

Important Challenging issue protects the network layer from malicious attacks in both wired and wireless networks with the issues being very high in a mobile ad hoc network. Malicious nodes can readily function as routers even in the absence of suitable protection and prevent the network from properly delivering the packets. For example, they can declare incorrect routing updates which are then spread in the network or drop all the packets passing through them. Our work rests on the foundations of two excellent systems already proposed, the twin systems of watchdog and path rater and SCAN are also discussed in detail.

2.5.1 Watch Dog and Path rater

The author Sergio Marti et al. (2000), have introduced two extensions to the Dynamic Source Routing Protocol DSR Johnson and Maltzet (1996), to reduce the effect of routing misbehavior namely watchdog and path rater. The watchdog recognizes misbehaving nodes, while the path rater avoids routing packets through these nodes. When a node forwards packets, its watchdog confirms that the next node in the path also forwards the packet. The watchdog does this through promiscuous attention to the next hop broadcast. If the next node does not forward the packet, then it is

misbehaving. The watchdog detects the misbehavior and sends a message to the source, notifying it of the misbehaving node.

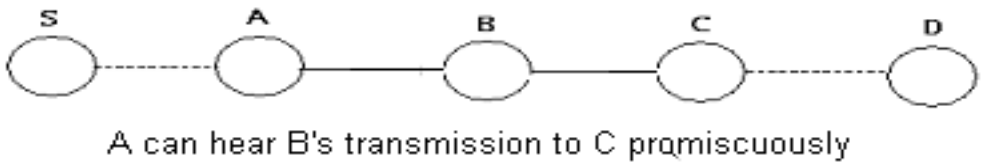

Figure 2.1 Watchdog Mechanism

The watchdog method which detects disobedient nodes is illustrated in Figure 2.1. Assume that there exists an active path from source S to destination D through midway nodes A, B and C. Node A cannot broadcast all the way to node C, but it can overhear what node B is transmitting. Therefore, node A is in a position to tell whether node B has correctly forwarded the packet sent from node A to node C. If encryption is not performed separately for each link a costly proposition node A can tell whether node B has tampered with the payload or the headers.

The path rater run by each node in the network, join and the knowledge of disobedient nodes with link consistency data to pick the route most likely to be reliable. For this purpose each node maintains a rating for every other node it has knowledge of a node always rates itself with a rating of 1.0, neutral rating is 0.5, the path rater increase the rating of nodes on all actively used paths by 0.01 at every periodic intervals 200 m/s interval decreases a nodes rating by 0.05. When a link failure is noticed during packet forwarding and the node becomes undetectable and all disobedient nodes are allocated by a special negative value of –100. The path rater does not make any change in the ratings of nodes for the current active user. If there are

alternative paths available, the path rater selects the path which has the highest metric.

In this method, 17 % throughput was achieved in the presence of 40% of the malicious nodes, while overhead transmission to data transmission ratio increased from the standard routing protocol's 9 % to 17 %

2.5.2 SCAN

In SCAN Hao Yang et al. (2006) two ideas are exploited to protect the mobile ad hoc network (i) information cross validation by which each node watches neighbors by crosschecking the overheard transmissions and (ii) local collaboration where the neighboring nodes collectively watch each other. In SCAN, each node watches the routing and packet forwarding behavior of its neighbors and separately detects the existence of malicious nodes in its neighborhood. This is made probable due to the wireless nature of the medium and all the involved nodes are within each other's broadcast. They have modified AODV protocol and added a new field next hop in the routing messages to permit cross checking and enable association for each node to the overhead packets as a consequence.

While each node watches its neighbors separately, all the nodes in the neighborhood work together to find a guilty malicious node. An agreement between a minimum of 'k' neighboring nodes is required for finding a guilty malicious node. Once its neighbors find guilty a malicious node, the network responds by depriving it of its right to access the network. In SCAN, each node must have a valid token to work in association with other nodes. They use asymmetric key cryptography to stop forgeries of tokens. A collection of nodes (minimum k) can collaboratively sign a token, whereas no single node can do this. Additionally, each node has to get its

token renewed once in a while by its neighbors. A node which constantly behaves properly can get its token renewed at less frequent intervals as compared to a fresh entrant node.

2.6 Summary

This Chapter has reviewed the research work done both in unicast and multicast routing protocols. Attention has also been paid to careful listening on secure routing protocols that have been proposed. Special mention has been made of SCAN and Watchdog which have attempted to protect the network layer from attacks. The next chapter describes the implementation of Generic ETUS protocol. This TBUT and CLUS module is very important and is used as an add on component for the umpiring modules described in Chapters 4 and 5.