Battery Power and Trust based Routing Strategy for MANET

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted By
Heena
(801233006)

Under the supervision of:
Dr. Neeraj Kumar
Associate Professor, CSED

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

June 2014

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*Battery power and trust based routing strategy for MANET*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Neeraj Kumar* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Signature:
Heena 1/7/14

Heena

801233006

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

1/7/14

Dr. Neeraj Kumar

Associate Professor, CSED

Countersigned by

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. K. Mohapatra)
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEGEMENT

"*No one walks alone on the journey of life just where do you start to thank those that joined you, walked beside you, and helped you along the way....."*

Thank you God for showing me the path. . .

I owe deep gratitude to the ones who have contributed greatly in completion of this thesis.

Foremost, I would like to express my sincere gratitude to my advisor, **Dr. Neeraj Kumar** for providing me with a platform to work on challenging areas of Program Slicing. His profound insights and attention to details have been true inspirations to my research.

I am also thankful to **Dr. Deepak Garg**, Head of Department, CSED and **Ms. Jhilik** , P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.

Most importantly, none of this would have been possible without the love of Papa and Maa. My family, to whom this dissertation is dedicated to, has been a constant source of love, concern, support and strength all these years. I would like to express my heartfelt gratitude to them.

I would like to thank all my friends and lab-mates for their encouragement and under-standing. Their help can never be penned with words.

Heena

801233006

ME (IS)

ABSTRACT

The communication in mobile ad-hoc networks (MANETs) is a multi-hop communication in which a source node communicates with a distant node using intermediate nodes in order to save the power. Thus the major activity in MANETs is to find a suitable route such that the delivery of the message can be done in an efficient manner. So, the route should be selected such that all the nodes in the path are trustworthy, non malicious and unselfish. However, misbehaving nodes may affect the performance of MANETs.

Source sends a Route Request packet (RREQ) in order to find a path for data communication. In order to reply RREQ Route Reply Packet (RREP) are also transmitted by destination to source. In this dissertation, we begins with the format of RREPs which consists of six constraints such as source address, destination address, battery power of node, trust value of node, packet type and node-count.

The aim of the proposal is to find out the path without any selfish node, i.e., the nodes whose energy and trust is low will not be the part of the route from source to destination. Protocol takes inputs from user and output parameters (such as suitability factor, average throughput and selfish node drop fraction) are recorded in output file known as trace file. After simulation, it can be concluded that path discovered after the use of this proposed protocol improves the performance of the network with respect to parameters throughput, suitability factor and selfish node drop fraction.

Table of Contents

List of Figures

List of Tables

Abbreviation

ABR	Associative Based Routing
AODV	Ad-hoc On-Demand Distance Vector Routing
ARAN	Authenticated Routing for Ad-hoc Network
CGSR	Cluster-head Gateway Switch Routing
CLR	Clear Packet
DAG	Directed Acyclic Graph
DSDV	Destination Sequenced Distance Vector Routing
DSR	Dynamic Source Routing
DOS	Denial of Service
ERR	Error
GSR	Global State Routing
IMANET	Internet Based Mobile Ad-hoc Network
INVANET	Intelligent Vehicular Ad-hoc Network
LAN	Local Area Network
LCC	Least Cluster Change
MAC	Message Authentication Code
MANET	Mobile Ad-hoc Network

MRL	Message Retransmission List
NLP	Neighbor Lookup protocol
QoS	Quality of Service
RRC	Route Reconstruction
RREP	Route Reply
RREQ	Route Request
RREQ-DSE	Route Request Double Signature Extension
RREQ-SSE	Route Request Single Signature Extension
SA	Security Association
SAODV	Secure Ad-hoc On-Demand Routing
SEAD	Secure Efficient Ad-hoc Distance Vector Routing
SLSR	Secure Link State Routing Protocol
SRP	Security-Aware Ad-hoc Routing
TESLA	Timed Efficient Stream Loss-tolerant Authentication
TORA	Temporally ordered Routing Algorithm
TTL	Time to Live
VANET	Vehicular Ad-hoc Network
WRP	Wireless Routing Protocol

Chapter 1

Introduction

This chapter provides the details about the introduction of mobile ad-hoc networks (MANETs) which are describes as follows:

1.1 Introduction to Wireless Networks

Wireless network [1] implies a cable free network, through which cost effective telecommunication network can be established into a building or among different equipments. This are administrated using radio waves as transmission system. Wireless networks are categorised [1] as follows:

- Infrastructured
- Infrastructure-less

1.1.1 Infrastructured Networks

An infrastructured network consists of wireless mobile nodes and base station acting as bridges which connect wireless network to cable network. In a distant data transmission mobile node determines the closest base stations and connects through it describes in fig 1.1. It states that all the data transmission occur through wireless node and base station not in different wireless nodes. Also, if the node is travelling in a certain network and then suddenly shifts to another region, it will get disconnected from old base station and communicate smoothly with new defined base station.

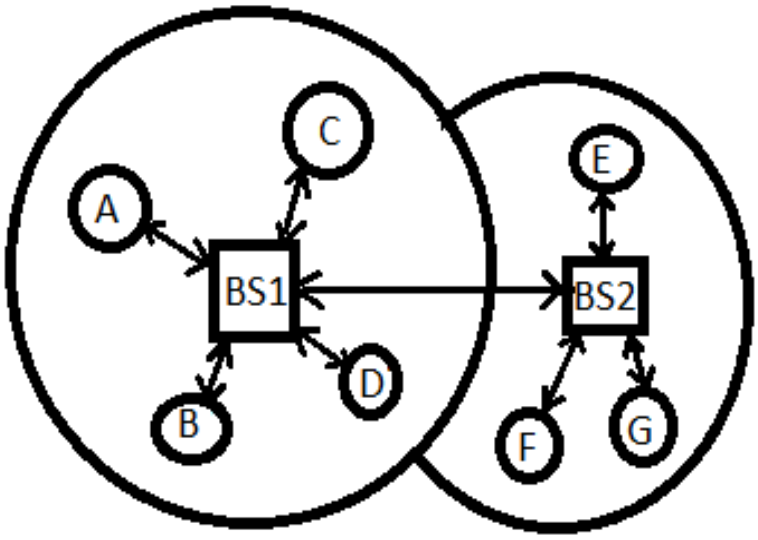

Fig.1.1: Infrastructure Based Networks [1]

1.1.2 Infrastructure-less Networks

As compared to infrastructred network, no base station exists in this network. Every node behaves as both a router and host as well. The network is roll of dynamic in nature as communication between nodes change due to movement of individual nodes, which communicate among other each other through multi-hop route as described in fig. 1.2. Therefore, this makes the system as a whole more complex. MANET is a variant of infrastructure-less network having nodes are portable equipments such as mobile phones and laptops etc.

1.2 Mobile Ad-Hoc Networks (MANET)

It is a variant of infrastructure-less network having nodes are portable equipments which communicate through radio waves as transmission system. Therefore, there is no actual infrastructure using in this, making it more flexible and relevant for temporarily connected channels, as routing different nodes in network is only challenge faced.

Now, MANET being a self-configuring infrastructure-less network gives freedom of motion to every device anywhere in network and therefore, can shifts to

different channels , ranges or devices and act as a router, as its a challenge in creating a MANET. One type of wireless ad-hoc network is MANET which has routable networking environment.

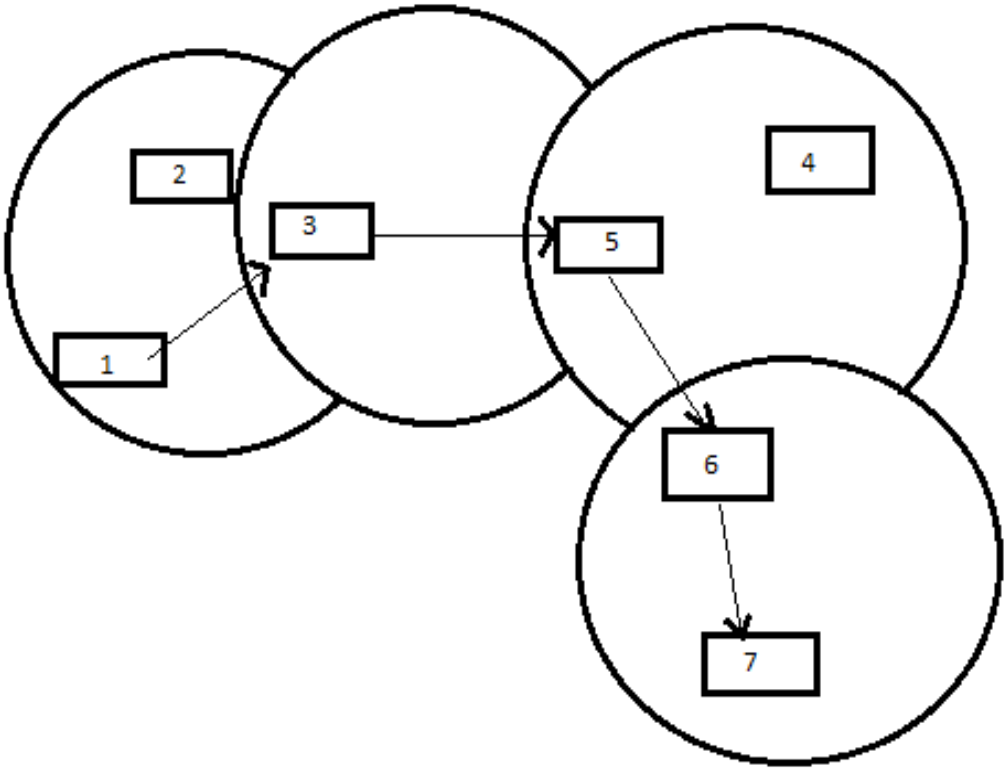

Fig.1.2: Communication between nodes in Infrastructure-less Network [1]

1.2.1 Types of MANET

MANET types [2] are categorised as follows:

- **Vehicular ad-hoc networks (VANETs):** To make association between vehicles and equipments of roadside, VANETs are needed.
- **Intelligent vehicular ad-hoc networks (InVANETs):** It helps in guiding vehicles to perform in intelligent way during accidents, drunken driving or collisions etc.
- **Internet Based Mobile ad-hoc networks (iMANET):** Which connect mobile nodes and fixed internet gateway nodes. Traditional routing algorithms cannot be applied.

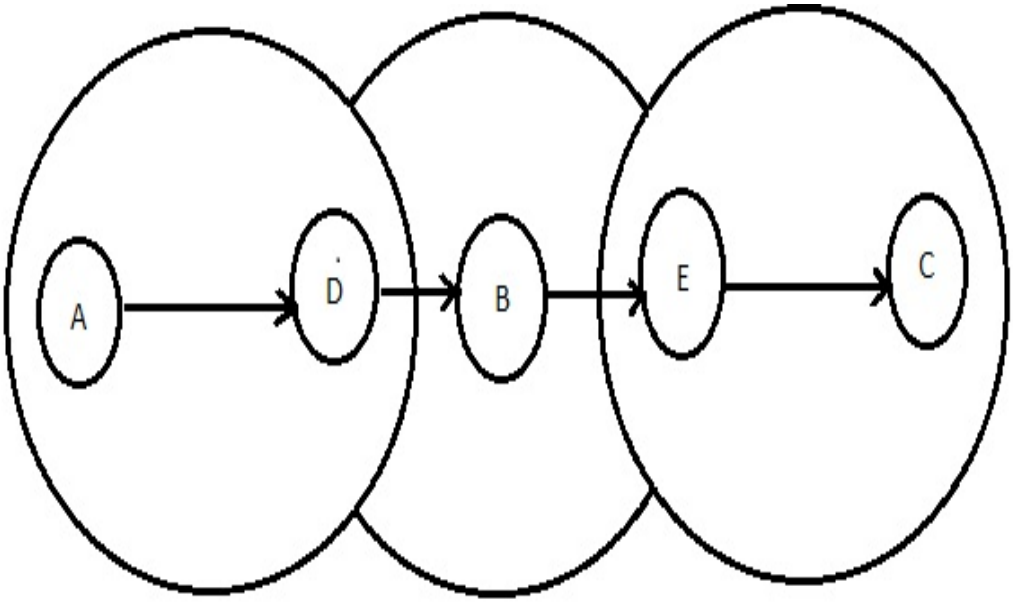

Fig. 1.3: Communication between node A and C via Intermediate node D, B,E [2]

1.2.2 Characteristics of MANET

MANET is an autonomous system which doesn't depend on any infrastructure. Depending on geological locations, power levels and co-channel interference in network, main characteristics of MANET [2] are:

- **Dynamic topology**: As there are no wires here, connection between different nodes can be created very quickly even if it is damaged at one certain location because of node's mobility.
- **Bandwidth and variable link scope**: As compared to wired networks, wireless links have less scope and quantity. It is also affected by multiple accesses. Noise interference which decreased its scope and quantity over time. It may even be less than radio's maximum transmission scope.
- **Self-configuring**: As there is no base station, all mobile nodes themselves act as routers and connect all wireless devices. Network activity, discovery of topology and traffic forwarding is done by node themselves.
- **Energy constrained nodes:** Mobile nodes depend on batteries power. As a network includes various nodes energy requirement is of most important because otherwise performance will be affected.

- **Multi-hop communications**: Ad-hoc network needs the support to transmit data over distant nodes. Mobile nodes transfer data to other across network. So that data packet can reach to target. Therefore, ad-hoc network needs support of multi-hop communication generation and transfer.
- **Limited security**: More susceptible to security attacks than wired.

1.2.3 Advantages of MANET

MANET due to its infrastructure-less structure and node mobility posses following advantages [2]:

- **Fast establishment**: MANET doesn't require previous installation. So its adaptability level for creation is high and can be easily learned and destroyed.
- **Dynamic topologies**: In MANET, nodes can shift haphazardly or can escape that is why networking topology graph vary continuously.
- **Fault tolerance**: MANET supports fault tolerance, i.e., failure of connection between nodes because of existence of routing techniques.
- **Connectivity**: In MANET, this is association between nodes to forward data packet. So centralized links and gateways are not needed for communication.
- **Mobility**: In MANET, wireless mobile nodes move in different directions due to which complexity can increase. These are handled by routing algorithms.
- **Cost**: Cost of MANET is less due to less establishment cost and it reduces power expenses at mobile nodes.
- **Spectrum reuse possibility**: Reuse of spectrum is possible due to small communication links.

1.2.4 Limitation of MANET

Although dynamic ad-hoc networking is the need of time but it also has various limitations [3]. Some of the limitations are:

- **Bandwidth**: Wireless link's capacity is more than wired ones but this rule is not followed in wireless LAN whose capacity is 2 Mbps while that of wired LAN is several Gbps.

- **Processing capability**: Processes such as routing and data transmission usually expenses a lot of power of device.

- **Energy constraints**: These devices have limited battery power backup. So, their energy can't be wasted much but some batteries saving algorithms are established.

- **High latency**: Devices in which energy conserving algorithms are there, nodes are not active when they don't send any data. But when they send data they are in latent state and so delays data.

- **Transmission errors**: Attenuation and intervention increases the transmission error and thus effect the network.

- **Security**: MANET suffers from vulnerabilities due to which attacker can find out the information which they needed. So, less security in MANET.

- **Location**: Few routing information can be achieved by location of IP address.

- **Roaming**: In MANET, fixed network roaming algorithms having connectivity graph of constant variation are not used.

- **Commercially unavailable**: Till now, MANET can't be established on large scale.

1.2.5 Applications of MANET

MANET's applications [4] are distinct which are accountable to large scale dynamic mobile networks. MANET can be implemented on large scale network having less cost effectiveness where other conventional networks are not applied. Applications of MANET are described as follows:

- **Military Tactical Networks**: In military domain, it is the first application. Using MANET, communication among units of battlefield anywhere becomes easy.

- **Personal Area Network**: Refers to inter-connection of various equipments used by one person, e.g., pen drive etc.

- **Sensor Networks**: These networks consist of sensor nodes which contain more than one sensor.

- **Collaborative Networking**: E.g., when one or more persons are sharing information on their laptops, they can't finish their work without MANET.

- **Disaster Area Networks**: Fast installation is granted by MANET where fixed infrastructure is available. Due to which communication between different persons can be increased.

1.3 Proposed Work

The proposed work includes the creation of initial trust among the nodes of the MANET by exchanging of information. This sharing of information is incorporated by the deploying agency with the creation of the initial mutual trust between the nodes and communication can takes place between the nodes without much verification. Trust factor is established through in-between nodes are used to create the route in order to secure the information of MANET. Sometimes nodes become selfish which was previously trust worthy due to lacking of power. In MANET, selfish behavior of nodes is quite frequent. Thesis involves the analysis and implementation of a navel routing strategy to deal with them. This thesis involves the analysis and implementation of a navel routing strategy handle such type of nodes. The scheme imagines that misbehaving nodes are not malicious and gives the right information about their present trust and energy value.

1.4 Organization of Thesis

Thesis is organized as below:

- Chapter 2 describes the basic features of MANETs.
- Chapter 3 describes the various prevalent security protocols in MANETS based on trust and establishes the problems based upon the literature survey.
- Chapter 4 describes about problem statement.
- Chapter 5 explains the proposed work.
- Chapter 6 describes about simulation results.
- Chapter 7 provides conclusion of proposed work and feasible future extension.

Chapter 2

Introduction to Routing

This chapter provides the details about the introduction of various routing schemes of MANETs which are describes as follows:

2.1 Routing

Routing [5] is a process of analyzing different routes in the network starting from the source to destination nodes. It is done by calculating all the routes and then restoring them or computing them. In the process of routing, firstly immediate node is selected with in network and then path of transfer of information is traced. It includes two activities- route discovery and packet forwarding. The packet forwarding is called as packet switching which can be straight forward or involves complex path. By analyzing different routes in the network and routing algorithms are generated to keep information. These routing algorithms are called as routing tables. Routing tables are of two types [6]:

- Static Routing
- Dynamic Routing

2.1.1 Static routing

In this type of process the scheme is explained manually and it doesn't depend whether the destination nodes is active or not.

2.1.2 Dynamic routing

It is active type of processing in which activeness of destination effect the routing table. The routing table is not affected by addition or deletions of router incase of static routing but it is affected in dynamic routing. Routing table is maintained by administrator in static routing and in dynamic router effect the process of routing. MANET is usually based upon dynamic type of routing protocols.

2.2 Desirable Properties for Routing Protocols

To study the MANET, additional properties are desirable in addition to traditional protocols. Following properties [7] are required:

- **Distributed Operation:** The process of routing should not be solely depend on centralized node or initialized node as in MANET nodes can enter or leave the network quickly.
- **Loop free:** It should also be loop free to increase the performance of network.
- **Unidirectional Link Support:** The concept of unidirectional link improves the process of routing.
- **Security:** MANET information should be secured. This can be done by authentication.
- **Sleep Period Operation:** In MANET, different nodes deny to transmit the information due to energy loss. The system should have capability to handle these sleep periods without negative results.
- **Multiple Routes:** These should be multiple routes. So that even if one route get effected by topographic variation, the other route become active for communication.
- **Quality of service support (QoS):** QoS is mandatory to combine with routing protocol.

2.3 Routing in MANET

In MANETs, nodes can move around, enter and exit from the network due to which network topology can vary quickly. Due to the possible variation in the network topology, mobile nodes can need a lot of communication to keep an updated static picture of the topology. Since these nodes are mobile and they operate on battery power. The links among nodes in MANETs can bi-directional or unidirectional in nature. In fig 2.1, A sends data to C via B, it is not sure that node C can use the same route to node A, The distance between nodes B and C should reduced, hence C

chooses the same route. Thus Bi-directional links can be creating by reducing the distance among nodes.

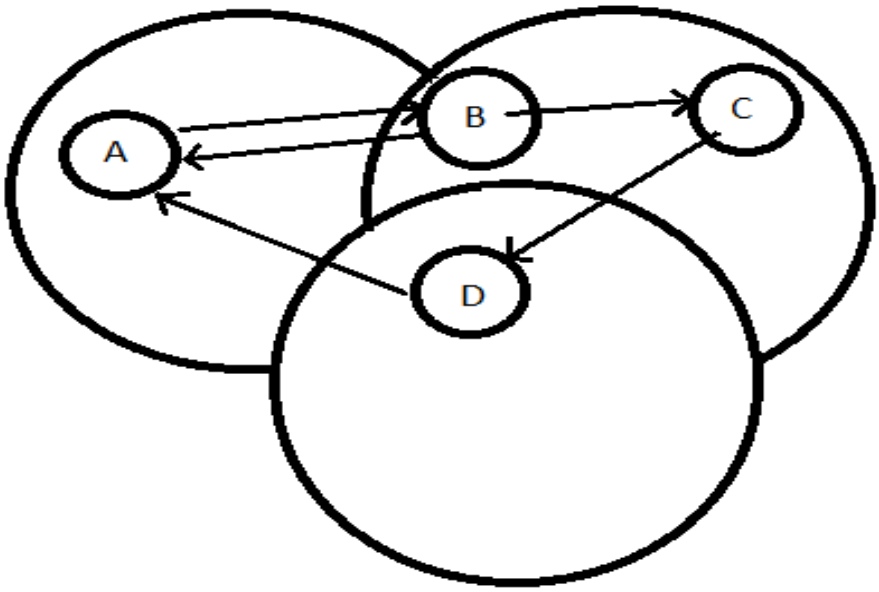

Fig. 2.1: Unidirectional Links in DSR Protocol [5]

2.4 Problems with Routing in MANETs

Due to node mobility and infrastructure-less structure of MANET, the conventional routing protocols are not suited well with it. There are features of MANETS that have to be keeping in mind while designing MANET routing protocols. These problems [8] are listed below:

- **Asymmetric links:** Due to non fixed topology of position of mobile nodes are changed frequently. Hence cause the asymmetric link problem.
- **Routing overhead:** Routing overhead is increased due to the establishment of flat route .sometime this route is created due to the changing type of nodes.
- **Interference:** In MANET, nodes generally change their positions very frequently. Due to this nature of MANET, links are created and destroyed quickly. Therefore, one communication might come in the way of another or some node can spy the information of another node. Hence all communications might be demolished. This can cause problem like interference.

2.5 Security Goals

Security consisting of a number of factors that have to be addressed which are described as follows [8]:

- **Availability:** Network resources are accessible for recognized organizations. A message should be varied or changed due to malicious attacks.
- **Integrity:** Only recognized parties can modify, preserve or transmitted information. A message could be changed.
- **Authenticity:** Existence of the origin of the message is correctly determined. Without authentication, an attacker could impersonate node.
- **Confidentiality:** Preserved or forwarded information is available only by recognized organizations. It guarantees that information is never disclosed to recognized organizations.
- **Non-repudiation:** Disclosure and confinement of associated nodes are done under this property.
- **Authorization:** It describes about duties of all nodes across network.

The mobile networks have limited transmission range. Therefore, they require intermediate nodes for communications. Routing of data is possible through three methods:

- Uni-casting (one to one)
- Multicasting (one to many)
- Broadcasting (many to many)

The unicast routing protocol of MANET can be categorised [9] into following categories described in fig. 2.2.

- Table driven
- On demand
- Hybrid

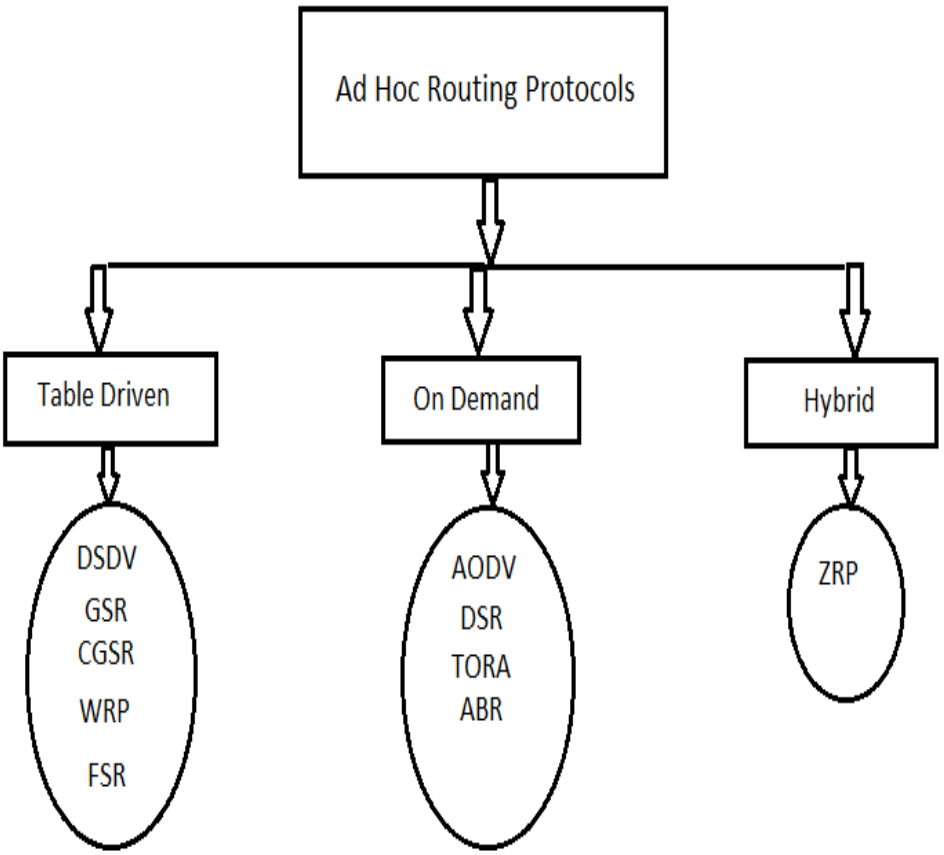

Fig. 2.2: Classification of MANET Routing Protocols [9]

2.6 Pro-Active Routing Protocols

These are also known as table-driven protocols which try to manage the persistent and updated data. Every node manages more than one table. Various updates are propagated to each node frequently. Hence, emendation can be done in the tables of corresponding nodes.

Pro-active protocols can categorised into following types:

- Destination Sequenced Distance Vector Routing (DSDV)
- Global State Routing (GSR)
- Cluster-head Gateway Switch Routing (CGSR)
- Wireless Routing Protocol (WRP)

2.6.1 Destination Sequenced Distance Vector Routing (DSDV)

DSDV [10] is pro-active algorithm. This follows the conventional techniques of routing. In DSDV, every mobile node consists of routing table having information about destination and hops to reach that particular destination. Each hope has a sequence number allotted by target node. When a node traversed then the entry of that particular node in the table is marked.

In MANET routing table is frequently send across the network to manage the table related information uniformity. Each node manages one more table in which they kept the information forwarded in the additional routing data chunks. New route broadcast enclose destination address, nodes between source and destination, sequence number corresponds to destination and a new unique sequence. Highest sequence number route is always used. The case which is having equal sequence number of two paths, then the less valued sequence number path is picked up.

2.6.1.1 Advantages and Limitations

DSDV routing protocol has following advantages and drawbacks:

- DSDV is suitable for small size network due to the high overhead of control message.
- This protocol is not suitable for high mobility rate networks.
- One path is contributed by DSDV from the source to target node.

2.6.2 Global State Routing (GSR)

GSR [11] follows the concept of link state routing. In this algorithm, each node manages a Next-hop table (consist of next hop address with the help of which information is sent to destination), Neighbor list (set of all neighbor nodes with respect to each node), Distance table (shortest distance to reach to destination) and a Topology table (information regarding link state given by destination node and timestamp). Using link state protocol, routing messages are created. After receiving routing message, topology table of each node updates, if message's sequence number is different from sequence number contained by table. Now, node updates its routing table and broadcast data.

2.6.2.1 Advantages and Limitations

GSR routing protocol has following advantages and drawbacks:

- GSR supports high mobility mobile infrastructure.
- It is suitable for high Bandwidth mobile environment.
- Routing message size is large in GSR which consumes more bandwidth. So, this is limitation of GSR.

2.6.3 Cluster-head Gateway Switch Routing (CGSR)

In CGSR [12], addressing and managing of network procedure is implemented. Due to presence of cluster head, code separation and channel utilized environment can be accomplished.

In CGSR, every time procedure to choose the cluster head is done. To avoid this complexity, a new algorithm is introduced, i.e., LCC (least cluster change). Using this algorithm, cluster head varies only when node leaves the communication range of network or more than one cluster head shares the same cluster. Example is described with the help of Fig. 2.3.

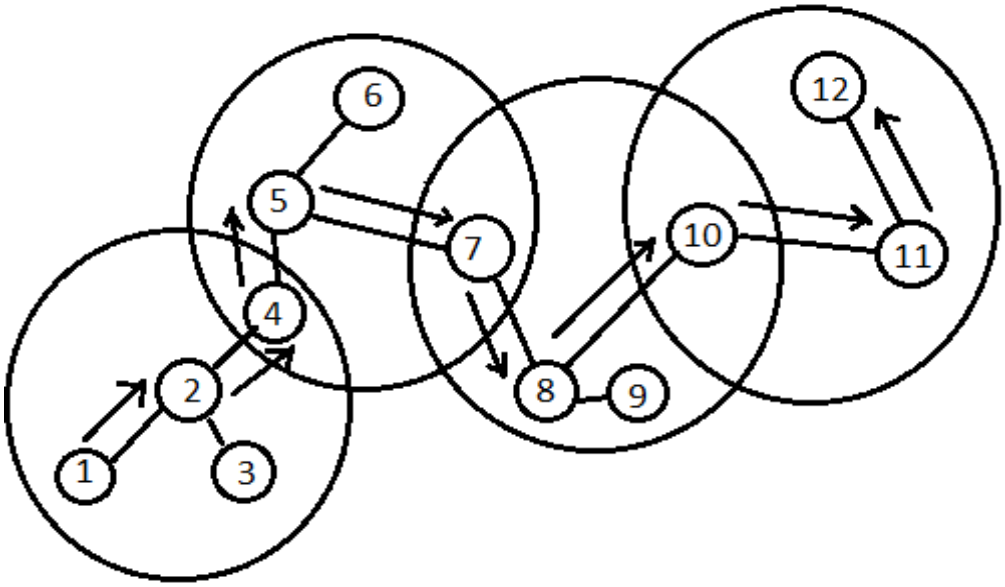

Fig 2.3: Cluster Head Gateway Switch Routing [12]

Nodes amend the changes in their corresponding cluster table after receiving data. Each node must also manage a routing table. After accepting the data, node will

check its all tables to find out the closest cluster head to reach the target node. Otherwise, node will examine only related table to find hop via which cluster head can be found. At the end, data packet is forwarded to selected node.

2.6.3.1 Advantages and Limitations

CGSR routing protocol has following advantages and drawbacks:

- Performance decreases due to the complexity and overhead in CGSR.
- Single point failure occurs at the cluster heads and gateways.

2.6.4 Wireless Routing Protocol (WRP)

WRP [12] is managing routing data packets between nodes of network. In WRP, every node consists of four tables: distance, routing, link-cost and message retransmission list (MRL) table.

MRL includes update message's sequence number, counter for retransmission, acknowledgement and update list. Some updates of update message are sent again, this is recorded by MRL. Update message are used by nodes to give the information to other node. Hence link variation process can easily occur. An update message is forwarded among neighbor nodes having update list and responses list. In the event of link failure, nodes and update message sent to their corresponding neighbor. If messages are not forwarded by node, then "HELLO" message should be sent by particular node in the given timestamp. So the connectivity can be guaranteed.

2.6.4.1 Advantages and Limitation

WRP routing protocol has following advantages and drawbacks:

- A lot of memory is required, as each node requires maintaining table of its direct neighbors, in addition to its own.
- The protocol consumes substantial amount of processing for calculating the update to the routing table since all the routing from its direct neighbors are used in the calculation.

Table 2.1 shows comparison of on-demand protocols with respect to complexity, route selection strategy, channel, structures and number to tables and freedom from loop.

Table 2.1: Comparison of Table Driven Routing Protocols

	DSDV[10]	GSR[11]	CGSR[12]	WRP[12]
Route Selection	Link State	Shortest path	Shortest path	Shortest path
Channel	Single	Single	Multiple	Single
Topology	Full	Full	Full	Reduced
Uni/non-uni Protocol	Uniform	Uniform	Non-Uniform	Uniform
Broadcast	Full	Local	Full	Local
Route Computation	Distributed	Distributed	Distributed	Distributed
Structure	Flat	Flat	Flat	Flat
Routes	Single	Single/ multiple	Single/multiple	Single
Source Routing	No	No may be Yes	No may be Yes	No
Update	Hybrid	Periodic	Periodic	Hybrid
Update Information	Distance Vector	Distance Vector	Distance Vector	Distance Vector
Update Destination	Neighbors	Neighbors	Neighbors & Cluster-head	Neighbors
Method	Broadcast	Broadcast	Broadcast	Broadcast

2.7 Reactive Routing Protocols

These are also known as on-demand protocols. Node needs a path to reach the target node and it starts the process of route discovery. The procedure is accomplished when

a path is found or all feasible paths have been determined. After the completion of route discovery mechanism, route maintenance mechanism is followed until target node is traversed long each route from source node. These protocols yield a passive mechanism to routing. Source initiated protocols are categorised as below:

- Ad-hoc On-Demand Distance Vector Routing (AODV)
- Dynamic Source Routing (DSR)
- Temporally Ordered Routine Algorithm (TORA)
- Associative Based Routing (ABR)

2.7.1 Ad- Hoc on-Demand Distance Vector Routing (AODV)

AODV [13] is relied upon DSDV. Essential broadcasts are decreased by generating pass on the basis of on-demand protocol. Node forward the packet to target node and is does not have the valid path to reach the destination node, it follows the route discovery procedure. Node forwards a route request (RREQ) packet, its neighbors which again then forward the request to their corresponding neighbors and so on. Fig 2.4 illustrated the proliferation of the broadcast RREQ. Destination sequence number utilizes to guarantee about loop free routes. Each node handles its own broadcast ID and sequence number. For each RREQ broadcast ID is increased together with IP address of node which uniquely determines RREQ. The source node consists of RREQ and ID. If in-between nodes have new path to reach the target node then only reply is sent to the RREQ.

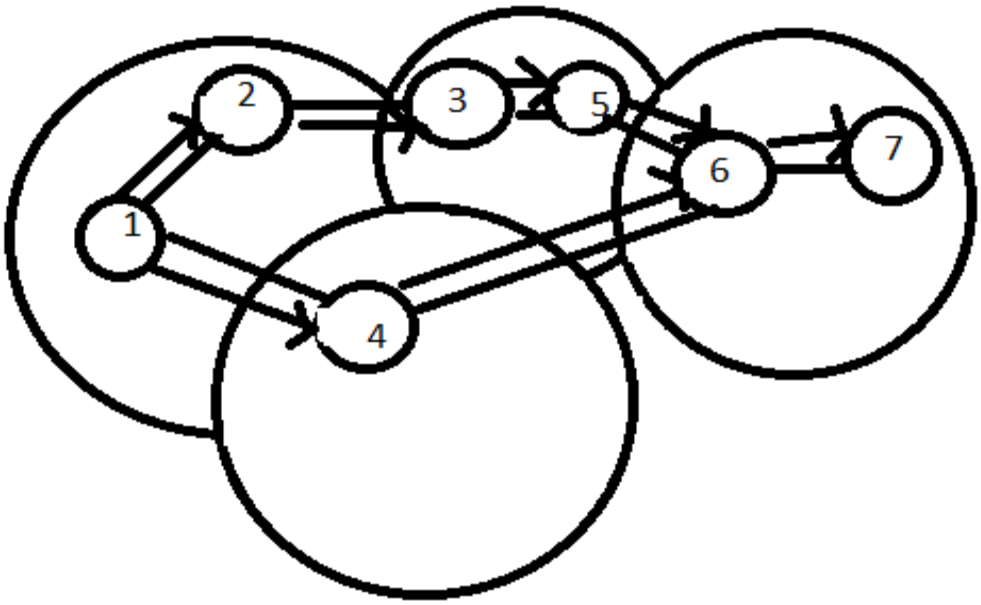

Fig 2.4: Propagation of RREQ Packet [13]

Nodes except source and target examine their tables to find out the address of neighboring node which had sent the broadcast packet. Hence the reverse part is generated. The same copy of RREQ packet accepted later is rejected. When node except source receives RREQ, that particular node forwards a route reply (RREP) to node from which RREQ is accepted. Due to this forwarded information a new valid route is introduced. A timer is attached with every route entry which origins the elimination of entry if not utilized. Routes maintenance: if source shifts, it will restart route discovery process to determine a fresh route to the target node. If a node encounter in route shift's its upstream neighbor detects the shift and proliferated a link breakage warning message to working upstream neighbors to instruct them about this change. These nodes are further proliferated link damage warning to their upstream neighbors, and so on until reaches up to source. The source may select to restart the route discovery procedure for a particular target is essential factor. For the management of local communication of all nodes in the network "Hello" messages may be utilized.

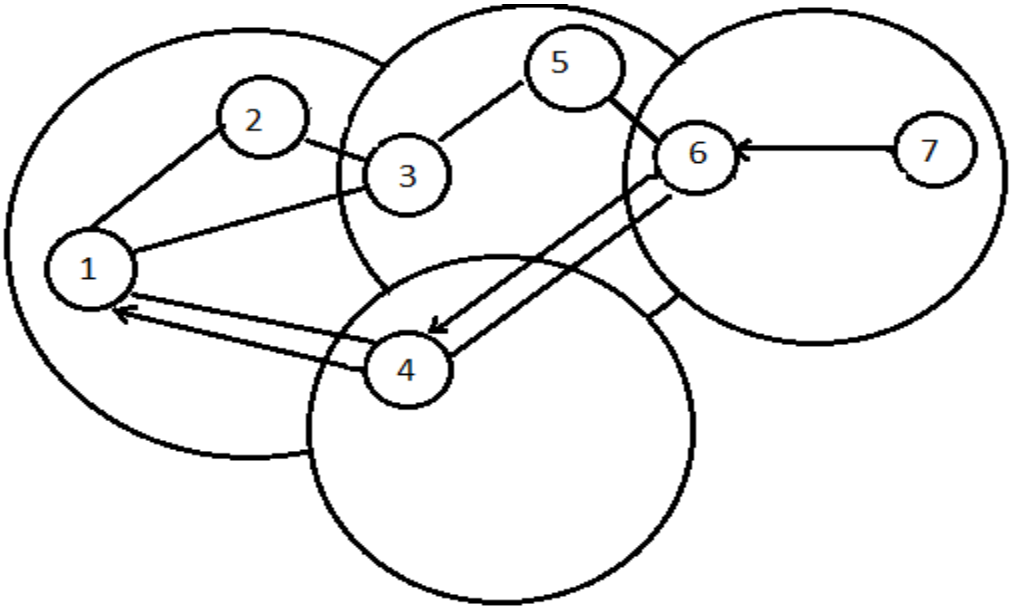

Fig 2.5: Path Taken by RREP Packet [13]

2.7.1.1 Advantages and Limitation

AODV routing protocol has following advantages and drawbacks:

- AODV used a DSDV with few enhancements to contribute routing in AODV, which has less control message overhead.
- It provides loop-free routing.
- For large MANET, AODV can be utilized efficiently.

2.7.2 Dynamic Source Routing Protocol (DSR)

DSR [14] is based on-demand protocol. It is relied upon the basic idea of source routing. Nodes are requisite to manage route caches which consisting of various known paths. Route caches are frequently updated as the fresh paths are found in the network. The protocol includes two major phases: route discovery and route maintenance. When node desires to forward some information to target node, initially it reviews its route cache to find out whether route has existing already to the destination or not. If route is unexpired to the destination then it will forwards the information via this route only otherwise will choose some other route by starting the route discovery process. This route request involves the target address.

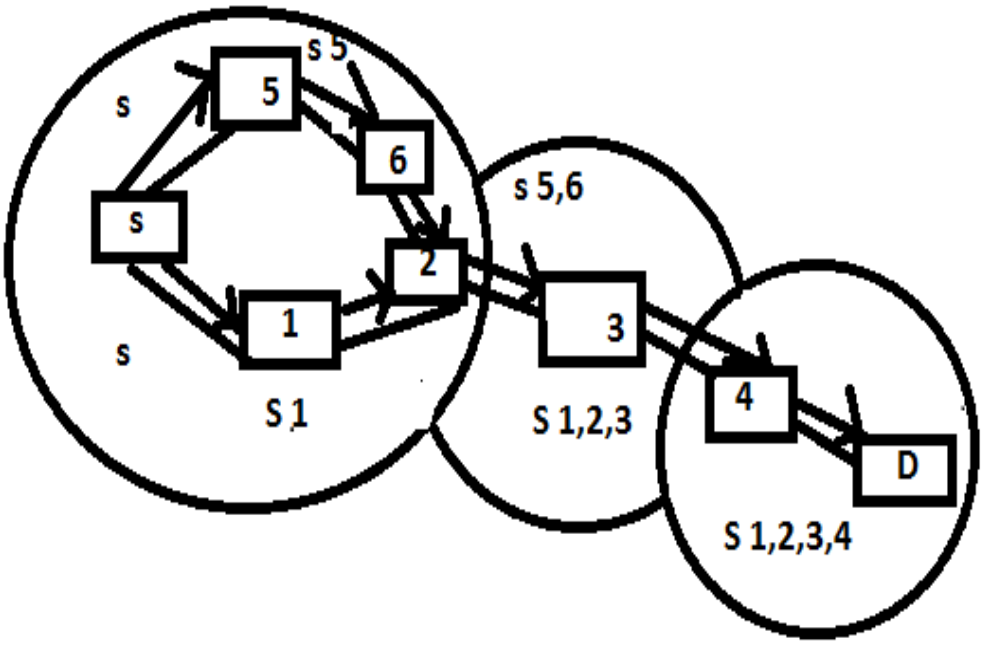

Fig. 2.6: Building of the Route record During the Route Request Discovery [14]

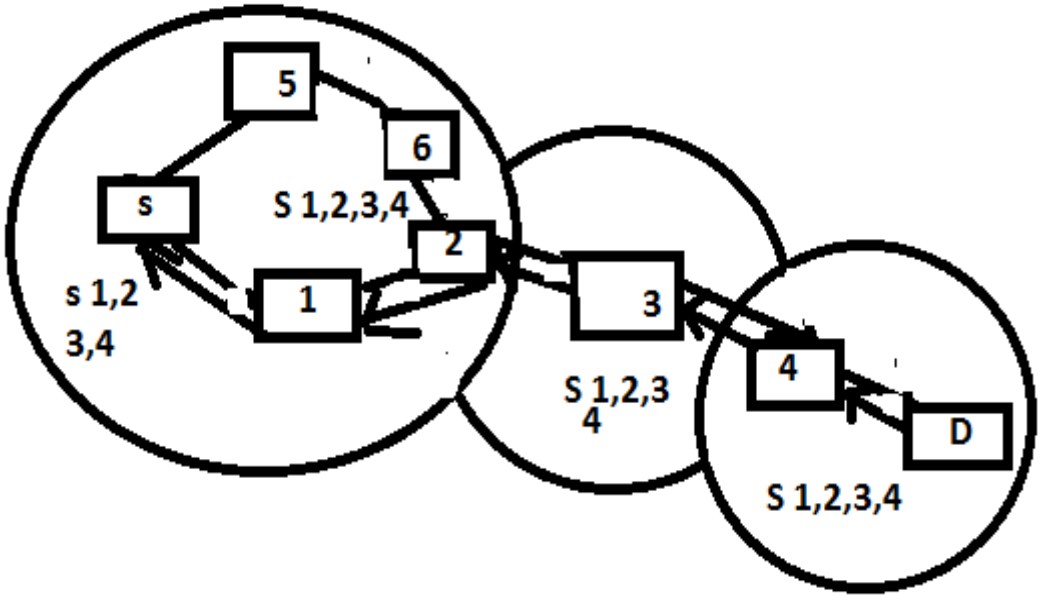

Fig. 2.7: Propagation of RREP back to Source from Destination node [14]

RREP is established when either RREQ reaches the target own its own, or it reaches an in-between node of the network which recognizes the path to the destination. Fig 2.6 illustrates that if the node creating a RREP for the destination node of the network then it puts the route report into RREP. . If in-between node has given the reply, then cache path of that node is added to the route record and RREP is created. Responding node should have the path to the beginner node in this route cache, if want to reply back to RREP. Responding node should utilize that particular path. Fig 2.7 explains the propagation of RREP back to the source from target.

2.7.2.1 Advantages and Limitations

DSR routing protocol has following advantages and drawbacks:

- If a host shifts, DSR frequently grasps the topology variation that happens.
- Less or no overhead is required.
- Multiple which reduce the mechanism of route discovery is stored.
- Collision can occur for the control message.

2.7.3 Temporally Ordered Routing Algorithm (TORA)

TORA [15] is a loop free, and distributed algorithm, which is relied upon the basic idea of link reversal. It acts as highly dynamic infrastructure. TORA gives many routes to reach source and destination. Source node starts the TORA protocol. TORA executes three functions: route creation, maintenance and erasure. During creation of route and maintenance phases, in-between nodes utilizes “height” factor to reach the target node via creating directed acyclic graph (DAG). At time of movement of node, DAG route is damaged and then route maintenance becomes necessary. If last downstream link fails or damaged then new reference level is generated which results the generation of that reference level by adjacent nodes, efficiently coordination to the link breakage. Links are reversed to follow variation of nodes. Hence they can work smoothly with new reference level.

Time of link breakage is an important factor of TORA. Route erasure function of TORA consist of clear packet (CLR) which is broadcasted in such a way so that flooding can occur in the network, to delete the expired or false routes.

2.7.3.1 Advantages and Disadvantages

TORA routing protocol has following advantages and drawbacks:

- In less node mobility networks, TORA is best for used.
- In large or congested networks, TORA gives best results for routing.
- TORA stores the bandwidth usage. Due to less communication overhead, the adaptability increases in TORA.
- With certain variation in topology occurrence of routing loops increases.
- High power consumptions and large amount of processing is there.

2.7.4 Associative Based Routing (ABR)

ABR [16] is a bandwidth effective distributed routing protocol. Source node is used to start the ABR protocol process. Point to point and broadcast routing mechanisms are used in this protocol. Two kinds of routing mechanism are used in packet radio network. One is 'point-to-point' routing having source or in-between nodes of the network will take the decision for picking the route. Hence 'point-to-point' routing procedure is a connection based routing. Second one is 'Broadcast routing' defined as the source forwards the packet to all like a wave front and hence, nodes are not required to calculate the path. This procedure is based on connection less routing technique. Associativity property is used to finding route to target. Associativity refers to connection establishment of any node with other in the network over time and space.

There are two phases: Discovery of route and Route Reconstruction (RRC) phase. Every node has a unique ID and unique sequence number which help to identify the node. To show the existence, node produces an alert message after a particular time period. Neighboring nodes refreshes their corresponding tables after

receiving alert message. Now, node updates its table according to the alert message from the particular node. There is no deadlock in the ABR protocol. ABR protocol is free from loops.

2.7.4.1 Advantages and Limitation

ABR routing protocol has following advantages and drawbacks:

- Source node is used to initiate ABR protocol.
- Best for small size MANET.
- Due to associativity, ABR gives shortest path and quick root discovery mechanism.
- The route caches are not utilized for discovery of routes leading to consumption of bandwidth.

Tables 2.2 describes the comparison of various protocols such as ADOV, DSR, TORA, and ABR, in terms of complexity, structure, update information, route selection and channel.

Table 2.2: Comparison of On-Demand Routing Protocols

	AODV[13]	DSR[14]	TORA[15]	ABR[16]
Route Selection	Shortest path	Shortest path	Shortest path	Single strength
Channel	Single	Single	Multiple	Single
Topology	Full	Full	Reduced	Full
Uniform/non-uniform	Uniform	Uniform	Uniform	Uniform
Broadcast	Full	Full	Local	Full

Route Computation	Broadcast	Broadcast	Broadcast	Broadcast
Structure	Flat	Flat	Flat	Flat
Routes	Multiple	Multiple	Multiple	Single
SourceRouting	No	Yes	No	Yes
Update	Event driven	Event driven	Event driven	Event driven
Update Information	Route error	Route error	Node's height	Route error
Update Destination	Source	Source	Neighbors	Neighbors/ source
Method	Unicast	Unicast	Broadcast	Unicast/Broadcast

Chapter 3

Literature Survey

This chapter provides details about the most relevant existing work in literature which are described as follows:

3.1 Secure MANET Routing Protocol

A secure routing protocol [17] is a conventional protocol which manages the routing mechanism among various nodes. This simply based on idea that new node for broadcast purposes and every node should know about nodes which are present in the surrounding and the way to reach to them.

If we talk about internet routing support for host is called as ‘mobile IP’ technique. The host can be connected directly on fixed network or via a wireless communication. The basic goal of mobile networking is to enlarge ability in the wireless domains where routers and hosts can be connected to form an infrastructure in an improvised manner.

In this chapter following secure protocols for MANET are described:

- Authenticated Routing for Ad-hoc Networks (ARAN)
- ARIADNE
- Secure Ad-hoc on-Demand Protocol (SAODV)
- Secure Efficient Ad-hoc Distance Vector Routing (SEAD)
- Secure Routing Protocol (SRP)
- Security-Aware Ad-hoc Routing (SAR)
- Secure Link State Routing Protocol (SLSR)

3.1.1 Authenticated Routing for Ad-hoc Networks (ARAN)

Securing protocols [18] face problems due to in adequacy of pre disposed environment, control and rationalized policy. First, we describe exploits that are possible against MANETs. Second, we define the difference among heterogeneous environments. This approach is important due to security satisfaction than an application requires. ARAN [19] includes authentication and message integrity. ARAN has more performance cost with respect to DSR or AODV. If compared with previously done work (e.g. [20]), ARAN costs more at every node.

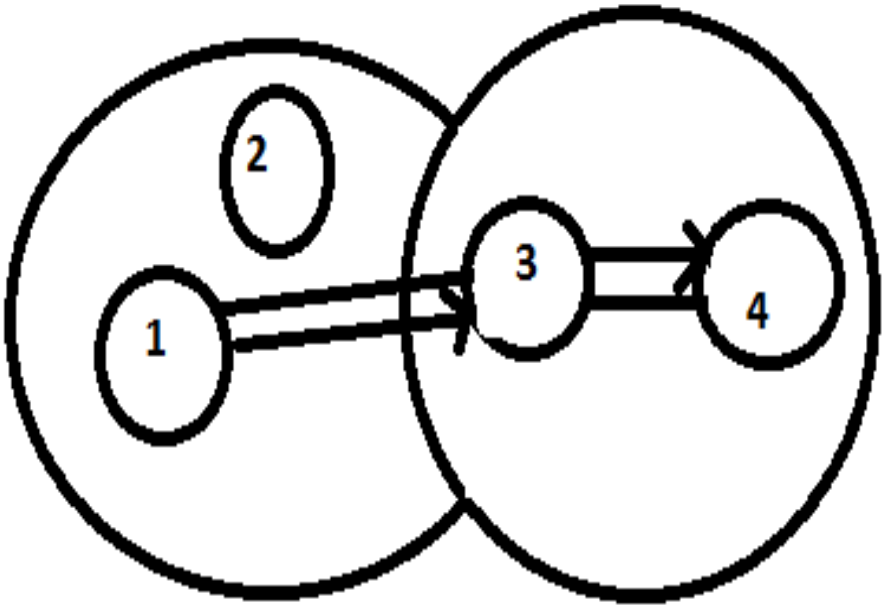

Fig 3.1: Route discovery in ARAN protocol [19]

Route maintenance in ARAN protocol is attained by broadcasted error (ERR) messages by nodes to record damaged pathways. The ERR message hinder any mischievous nodes. To protect from any reply intrusion is also has a time interval. Those nodes rebroadcast the ERR packets when they receive it which have pathways with nodes which have damaged links.

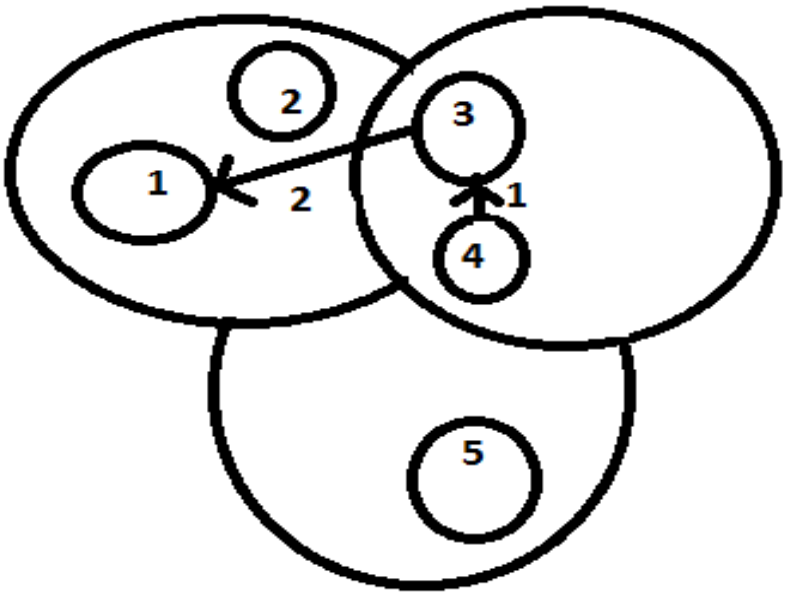

Fig. 3.2: Route maintenance in ARAN protocol [19]

Certificates used in ARAN are usually for limited time and certification server broadcast a cancellation data packet in case of cancelled certificate. The cancellation procedure is not protected. Any mischievous nodes which is creating problem in the network might not forward a revocation message. The ARAN protocol requires a trusted certification from existing authority. Public key cryptography provides certification in ARAN.

3.1.2 Ariadne

Routing messages can be certified by Ariadne [21] by any of the three schemes: shared secrets between each pair of nodes or communicating nodes or digital signatures. But we are basically interested with the use of Ariadne with TESLA (Timed Efficient Stream Loss-tolerant Authentication) [22, 23] which need time synchronization but this synchronization can be escaped by using pair wise shared keys.

Ariadne adopts an end to end scheme for its security. It imagines presence of common secret key among the nodes and with help of message authentication code (MAC) certifies point to point message among nodes. It also take help of TESLA broadcast authentication protocol for authentication of broadcast messages in which

the sender produces one way key chain to describe the program or agenda to reveals key of chain in an order which is opposite from the path where it is produced.

When node broadcast a desired pathway, it consist of its own address, target node address, identification number of packet, TESLA [24], i.e., time gap which signifies the conventional time of appearance of the desired node at its station, a hash chain which compromises of its own address, address of target, ID and time gap and to empty lists i.e., node and MAC list. Validity of time interval of TESLA is examined by the neighbor node that accepts the RREQ. If time interval is not genuine then the packet is cancelled. The MAC is calculated by using TESLA key. When destination or target node receive key it examines the validity of the route. If keys from described time gap are not revealed and hash chain is documented then only the request for any part is treated seriously.

RREP includes fields same as RREQ and it includes destination MAC fields which is fixed to the computed MAC of the undertaking fields of the RREP and common key among source and destination. The RREP is sent back to the source involved in the node list. After accepting RREP, source examines the authenticity of each entry in key list and MAC list.

ERR (having TESLA details) message is generated by the node. Each node sends ERR to the destination. In-between nodes check ERR message. Ariadne uses MAC to provide the authentication to required table is the necessity of Ariadne.

3.1.3 Secure Ad-hoc On-Demand Distance Vector (SAODV) Routing Protocol

SAODV [25] is an enhancement of AODV. Secure AODV mechanism is based on the assumption that each node is having authenticated public keys of all nodes. Initiator of routing control packet affix its RSA signature and hash value is verified by in-between nodes. Hash chain's k^{th} element is created by in-between nodes, where k is the transverse hops. SAODV gives to substitutes for RREQ and RREP. When a RREQ forwarded then signature is attached to the packet which is generated by the sender. In order to establish the reverse path of the source, node mark RREP using private key and sent back. In-between nodes are also validating the signature. Routing table is updated with the signature of sender.

Purpose of SAODV is to utilize the sign to verify RREQ, RREP and hash chain. Network nodes give certification to AODV as SAODV. In SAODV [20], a RREQ consists of a route request single signature extension [RREQ-SSE]. When sending a RREQ, node examines validation of RREQ. It then sends one RREQ for every root discovery. Those nodes then increment RREQ header field.

When RREQ reaches destination, last node then examines the validation in RREQ-SSE. If RREQ is ok, target send back RREP. RREP-SSE gives validation for RREP. Node sent RREP examines signature enhancement. If signature is ok then the sending node fixed its table for the RREP's source. In-between nodes answering to RREQ consist of RREP-DSE (route request double signature extension). If in-between nodes had preserved RREP and sign in its RREP–DSE, then sends back same RREP.

SAODV utilizes the assumption that RREQ and RREP field are considerably overlap, due to this overhead decreases. If node sends RREQ-DSE, it receives the path and signature as it had previously sent RREP. Every node sends signed RREP. Destination sequence number information is not altered by nodes which are installed on SAODV, because destination sequence number is not validated by target.

During any attack in ARAN, it requires to validate only one signature- in RREQ, beginner's signature is considered for validation or in RREP, target's signature is considered. Attacker may attach the corresponding verified outer signature with non valid inner signature. Hence, any fake file only consists of fake outer signature. But validation cost is same as SAODV.

3.1.4 Secure Efficient Ad-hoc Distance Vector Routing (SEAD)

In SEAD, nodes frequently switch information with other in the network and every node has the information regarding path from present node to all destinations.

3.1.4.1 Basic Idea

SEAD [26] authenticates sequence number and update message of related table. Receiver of SEAD also validates the source node. In SEAD, every update message's source should also validate.

3.1.4.2 Features

SEAD features are described as below:

- SEAD utilizes an efficient hash chains.

3.1.4.3 Weakness

SEAD weaknesses are described as below:

- SEAD does not handle wormhole attacks.

3.1.5 Secure Routing Protocol (SRP)

SRP [27] was an enhancement of presence of reactive protocols. SRP guarantees about the information given and avoid unwanted replies. SRP depends on security association (SA) among the source (S) and the destination (T). The SA could be created by utilizing hybrid key circulation. S and T can switch a private symmetric key (KS, T) with help of exchange of public keys.

3.1.5.1 Strengths

SRP strengths are described as below:

- Neighbor discovery procedure manages information of MAC and IP address.
- In DSR protocol, 6-word header is used.

3.1.5.2 Weaknesses

SRP weaknesses are described as below:

- Route cache poisoning attack exists.

3.1.6 Security Aware Ad-Hoc Routing (SAR)

SAR [28] is common infrastructure for reactive protocol. Private key is shared among nodes. SAR expands routing procedure with hash and symmetric encryption.

SAR when installed on AODV amends two fields to RREQ and one field to RREP. First field added to RREQ packet is security needed field and is fixed by the sender. Second field added to RREP is security guaranteed field which indicates maximum level of security given. If the security requirement field is represented in vectors then the security guarantee field value is computed by adding the security related values in the route. Calculated values are added to the security range of RREP and return to sender. The calculated values also added to related table to share the security related data.

3.1.6.1 Features

SAR features are described as below:

- SAR enables security services relied on the cost-benefit analysis.
- In SAR, established routes may not be shortest among two transmissions with respect to hp count. Hence the validation of security is guaranteed.

3.1.7 Secure Link State Routing Protocol (SLSP)

3.1.7.1 Introduction

SLSP [29] gives table driven topology discovery. SAR sometimes is used as stand-alone protocol.

3.1.7.2 Operation

To function effectively without central key, it activates all its nodes in the network to broadcast their public key to other. Circulation of MAC increases mechanism by hidden nodes from eavesdropping at data link layer. To achieve this thesis aim, neighbor lookup protocol (NLP) is formed as an basic part of SLSP.

Based on MAC, data packets are accepted from other nodes at various rates. The rate which control packets are coming increases the rate of elimination of malicious nodes.

3.1.7.3 Features

SLSP features are described as follows:

- SLSP can work in changing topology and membership's network.
- SLSP has ability of variation in its scope among local and network.
- SLSP provides the assurance of round robin scheme

3.2 Comparison of Secure MANET Routing Protocols

A secure routing protocol helps against all kinds of attacks due to vital type of MANET and various situations. E.g., designing a common solution is difficult that can give sufficient protection in all possible situation using wireless networks.

Table 3.1 describes a comparison of the discussed secure routing protocols to various attacks.

Table 3.1: Comparison of security aware MANET routing protocols

Protocol / Performance parameter	ARAN [19]	ARIDANE[22]	SAODV [25]	SEAD [26]	SRP [27]
Routing approach	Reactive	Reactive	Reactive	Proactive	Reactive
Routing metric	None	Distance	Distance	Distance	Distance
Encryption Algorithm	Asymmetric	Symmetric	Asymmetric	symmetric	symmetric
MANET Protocol	AODV/DSR	DSR	AODV	DSDV	DSR/ZRP

Synchronization	No	Yes	No	Yes	No
Central trust authority	Certificate authority (CA) required	Key Distribution Center (KDC) required	CA Required	CA Required	CA Required
Authentication	Yes	Yes	Yes	Yes	Yes
Confidentiality	Yes	No	No	No	No
Integrity	Yes	Yes	Yes	No	Yes
Non-Reputation	Yes	No	Yes	No	No
Anti-spoofing	Yes	Yes	Yes	No	Yes
DoS Attacks	No	Yes	No	Yes	Yes
Location Discloser	No	No	No	No	No
Black-hole attack	No	No	No	No	No
Reply	Yes	Yes	Yes	Yes	Yes
Wormhole	No	No	No	No	No
Routing table Positioning	Yes	Yes	Yes	Yes	Yes

Chapter 4

Problem Formulation

This chapter describes the problem statement which is explained as follows:

4.1 Problem Statement

In MANET, multi hope communication is used. Source sends data to farthest nodes in order to make association among them via in-between nodes, so as to store the battery. Main function of MANET infrastructure is to discover an appropriate path so that message delivery can be assured. So path must be picked in such a way that all nodes are trust worthy and non selfish. However, misbehaving nodes [30] may affect on network performance.

The aim of the routing protocol is to find out the path without any selfish node, i.e., the nodes whose energy and trust is low will not be the part of the route from source to destination. Protocol takes inputs from user and output parameters (such as suitability factor, average throughput and selfish node drop fraction) are recorded in output file known as trace file.

Chapter 5

Proposed Work

This chapter provides the details about the most relevant proposed work which is described as follows:

5.1 The Proposal

Source sends a RREQ in order to find a path for data communication. In order to reply RREQ, RREP will be transmitted by destination to source. Proposal begins with the format of RREPs explained in Fig. 4.1.

Packet Type	Source Address	Destination Address	Battery power of node	Token of node	Node_Count

Fig. 4.1: Modified Format of Route Reply Packet

- **Battery power of node**: This field contains the energy of a node which is having least energy in the route from destination node to source node.
- **Token of node:** This field contains the trust value of a node which is having least trust value in the route from destination to source node.
- **Node_count:** This field includes the total number of nodes from source to destination node.

Target node will enter its battery power and token value in the RREP. The nodes in the path among destination to source will receive the RREP from previous node and perform the following actions on the RREP:

- If battery power of current node is less than the battery power field of RREP, then battery power field will be replaced by the battery power of the present node.
- If token value of present node is less than token value of RREP, then token value field will be replaced by the token value of the current node.

Source receives multiple RREPs from various routes. This proposal helps the source node for choosing a path to destination node on the basis of various factors, i.e., battery power, trust and number of nodes. The proposed Routing Mechanism will pick a path which contains non-selfish and trustworthy nodes. Through RREPs, source node will receive the battery power and token value of various routes. In this proposal, 0.5, 0.3, 0.2 probabilities are assigned to battery power, token value and Node count respectively. Source node will apply these probabilities on the received battery power and token values of various paths and calculate Suitability Factor of various paths according to the following formula (1):

Suitability Factor = 0.5 * battery power of Route Reply Packet + 0.3 * token value of Route Reply packet – 0.2 * Node_count (1)

5.2 Designing the Routing Protocol

Aim of protocol is to find out the path without any selfish node, i.e., the nodes whose energy and trust is low will not be the part of the path from source to target. The strategy used is described as below:

Inputs are as follows:

- Network area
- Number of nodes.

- Transmission range which is used to find out the neighbor list of each node.
- Source and Destination node.

After having the following information a neighbor list is generated. First source node sends the RREQ to all its neighbors then all the nodes who received RREQs sends these packets to their neighbors and so on. When destination node receives RREQ, it generates RREP and transmits it back to source node through all those paths through which it has received RREQ.

5.3 Assumptions

The following assumptions were made in protocol:

- Source and Destination nodes loose 5 units' battery in transmitting and receiving RREQ, intermediate node looses 1 unit of battery.
- Source and Destination nodes loose 2 units' battery in transmitting and receiving RREP, intermediate node looses 1 unit of battery.
- Each node is assigned 400 unit of power and 50 unit of trust initially
- When a node is found to be a trust breaker its trust value is reduced by 3 units.

5.4 Proposed Algorithm

The protocol takes various inputs from user like area of the network (A), number of nodes (n) that a network contains and transmission range (R) that is used to determine the neighbor list of every node. Initially each node has assigned 400 joule battery power and token value 50. T is the set of true paths and -1000 value assigned. P is the set of total paths among source and destination. E is the set of total energy of paths and D is set of total number of paths dropped due to less energy of path or less trust value. E^{avg} and T^{avg} are the average energy and average throughput respectively. T^{avg}, suitability and selfish node drop fraction (Sdf) are calculated as output parameters.

5.4.1 MRREP (modified route reply packet) Algorithm

Input: A, n and R

Output: T^{avg}, suitability and Sdf

1) **For** (i=1; i<=n; i++)
2) Create a neighbor list of each node having neighbor node and synchronized channel value.
3) **End for**
4) **For** (q=1; q<150; q++)
5) Path matrix is created based on neighbor list which represents multipath among source to destination node.
6) Path_count is calculated which represents the total number of paths among source and destination.
7) **For** (i=1; i<=path_count; i++)
8) Particular value of battery power of each node is reduced based on node's presence in route.
9) **End for**
10) **For** (i=1; i<=path_count; i++)
11) Channel matrix is created which represents channel from one node to other and value of token is reduced accordingly.
12) **End for**
13) **For** (i=1; T[i]!= -1000; i++)
14) Energy [T[i]], number of nodes [T[i]] and trust [T[i]] is calculated by multiplying with factor 0.5, 0.3, and 0.2 respectively.
15) Suitability factor is calculated according to above given formula.
16) **End for**
17) **For** (i=1; i<=n; i++)
18) **If** (E[i] >0)
19) E^{avg} is calculated.
20) **End If**
21) **If** (E[i]<=20)

22) Selfish factor is incremented.

23) **End If**

24) **End for**

25) **If** (P!=0)

26) T^{avg} is calculated as the number of paths containing non-selfish and trustworthy nodes to the total number of paths generated.

27) **End if**

28) **If** (D!=0)

29) Sdf is calculated as the number of paths dropped due to selfish behavior of node to the total number of paths dropped.

30) **End if**

31) **End for**

5.4.2 Description of MRRP Algorithm

- **Line (1-3):** Describes that neighbor list of each node is created which consist of information regarding neighbor node and synchronized channel value.

- **Line (4):** Algorithm runs 150 times. So as to calculate the average value of output parameters.

- **Line (5-6):** Path matrix is created based on neighbor list which represents multipath among source to destination node. Path_count is calculated which represents the total number of paths among source and destination.

- **Line (7-9):** Fixed value of battery power of each node is decreased based on node's presence in route.

- **Line (10-12):** Channel matrix is created which represents channel from one node to other and value of token is reduced accordingly.

- **Line (13-16):** Suitability factor of each route is calculated based on formula defined above.

- **Line (17-22):** E^{avg} is calculated based on energies of nodes of route and selfish factor is calculated based on nodes having less energy than minimum energy of node defined.

- **Line (23-25):** T^{avg} is calculated as the number of paths containing non-selfish and trustworthy nodes to the total number of paths generated.

- **Line (26-28):** Sdf is calculated as the number of paths dropped due to selfish behaviour of node to the total number of paths dropped.

5.4.3 Complexity

Complexity of MRRP algorithm is O (n^2), where n is the number of nodes that a network contains.

Chapter 6

Protocol Simulation and Results

This chapter describes the most relevant details about protocol simulation and results which are as follows:

6.1 Simulation

This Protocol was designed in C++ in which an area of 40*40 sq. unit's size was chosen. The nodes were distributed randomly in the given area and above listed performance metrics results were recorded in the Trace file.

Table 6.1: Simulation Parameters

Number of nodes	15,20,25,30
Routing Protocol	DSR
Traffic Model of Sources	Constant bit rate
Mobility Model	Random way point
Initial battery power of node	400
Initial token of node	50

6.2 Results and discussion

This protocol was designed in C++. Input parameters are as follows:

- Number of Nodes
- Transmission radius of each node

The following parameters were recorded as output:

- Average Throughput
- Selfish Node Drop Fraction
- Suitability

6.2.1 Output File

A trace file (output file) is generated as a result of simulation [30] which contains the recorded values of all the parameters which are studied in this dissertation. Various transmission ranges and number of nodes are taken to measure the working and results of simulator.

- **Average Throughput:** It is referred as the number of paths containing non-selfish and trustworthy nodes to the total number of paths generated.

Table 6.2: Average Throughput in proposed Routing Protocol

Transmission Range (m)	No. of Nodes=15	No. of Nodes=20	No. of Nodes=25	No. of Nodes=30
5	0	0	0	0.310345
6	0.310345	0.310345	0	0
7	0	0	0	0.079787
8	0	0	0	0
9	0	0.175182	0	0.053232
10	0	0	0	0.018325
11	0	0	0	0
12	0.018325	0	0.102612	0
13	0	0	0.023018	0
14	0	0.135377	0	0.006692

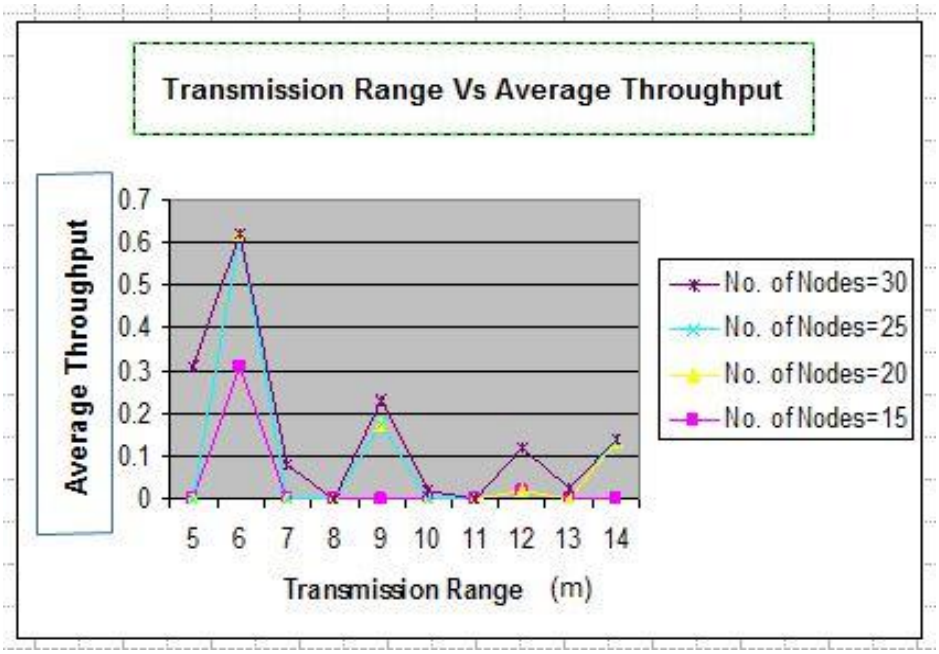

Fig. 6.1: Average Throughput in proposed Routing Protocol

- **Selfish Node Drop fraction:** It is defined as the number of paths dropped due to selfish behavior of node to the total number of paths dropped (due to no route between source and destination or selfishness).

Table 6.3: Selfish Node Drop fraction in proposed Routing Protocol

Transmission Range (m)	No. of Nodes=15	No. of Nodes=20	No. of Nodes=25	No. of Nodes=30
5	0	0	0	0
6	0	0	0	0.188841
7	0	0	0	0
8	0.020408	0	0.190184	0.134796
9	0	0	0	0.045045
10	0	0.200873	0.148883	0.274363
11	0	0.136628	0.197647	0.408012
12	0.515759	0.151515	0.313158	0.32
13	0.427553	0.505007	0.463047	0.46002
14	0.283951	0.513889	0.385276	0.472281

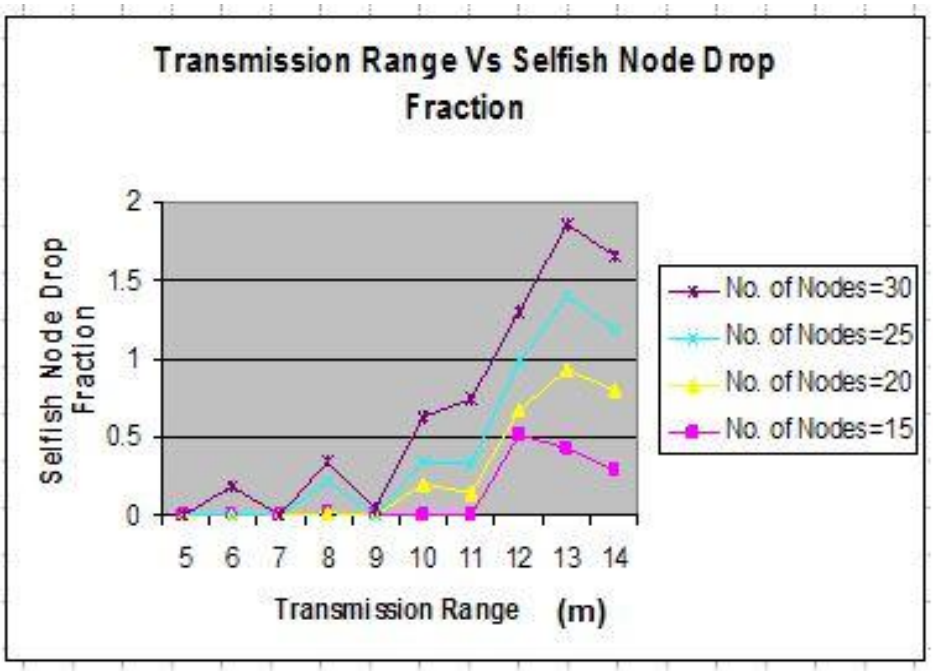

Fig. 6.2: Selfish Node Drop fraction in proposed Routing Protocol

- **Suitability:** It is defined as the suitability factor of the best path to the summation of the suitability factor of all non-malicious and trustworthy paths.

Table 6.4: Suitability in proposed Routing Protocol

Transmission Range (m)	No. of Nodes=15	No. of Nodes=20	No. of Nodes=25	No. of Nodes=30
5	0.499017	0.623831	0.33389	0.345647
6	0	0	0.601406	0.424657
7	0.823579	0.588344	0.428514	0.28006
8	0.496282	0.821114	0.301602	0.287624
9	0.798601	0.291297	0.614131	0.298073
10	0.488811	0.545742	0.426833	0.191932
11	0.494141	0.491568	0.24046	0.226889
12	0.269727	0.451225	0.240687	0.265004
13	0.290061	0.244319	0.216074	0.151221
14	0.316965	0.174401	0.184053	0.168509

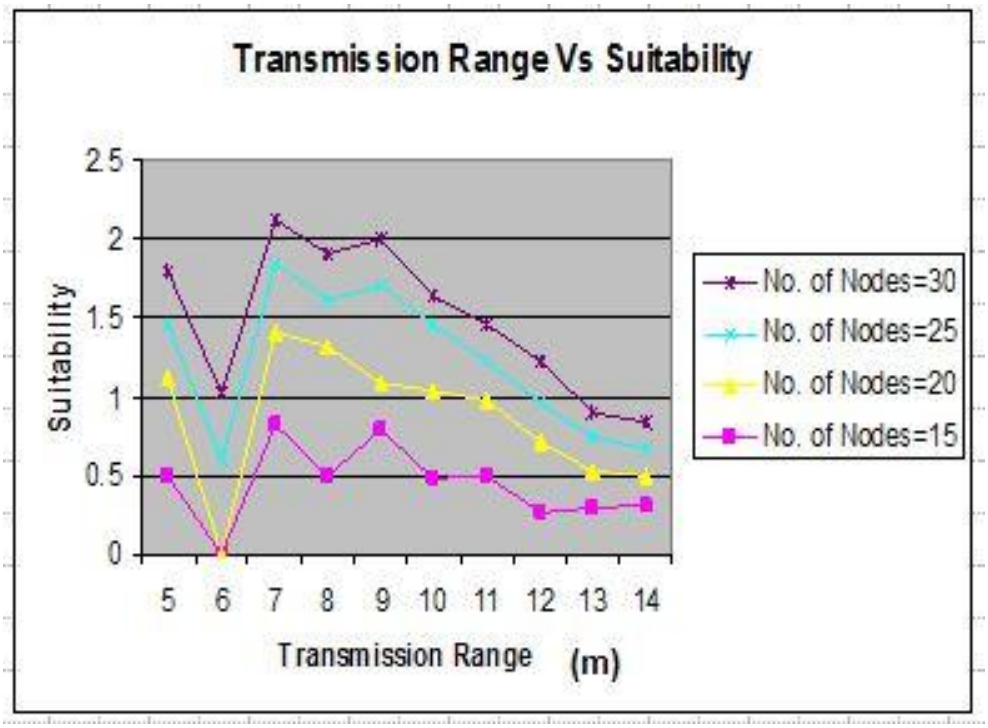

Fig. 6.3: Suitability in proposed Routing Protocol

6.3 Merits

- Path with the highest energy and trust is chosen so the probability of path being selfish is reduced.
- It generates all multi-hop paths between source and destination.

6.4 Demerits

- In real world systems nodes may give false information regarding energy and trust status in order to conserve their energy.
- In this network do not RREQ does not include TTL (Time to Live) field, so the packet will traverse through the whole network.

Chapter 7

Conclusion and Future Scope

This chapter describes conclusion and future scope which are follows:

7.1 Conclusion

In this work, a new protocol has been implemented for MANET. The proposed protocol is power and trust aware keeping in view the power and trust constraints of nodes being used in ad-hoc network.

A node can become selfish when the energy of the node reduces below threshold value. A node can also be considered as selfish if its trust value reduces below threshold value. Selfish nodes do not allow other nodes to use its scarce resources such as battery. Main function of MANET infrastructure is to discover an appropriate path so that message delivery can be assured. So path must be picked in such a way that all nodes are trust worthy and non selfish. However, misbehaving nodes may not follow the cooperation paradigm and create a serious affect on network performance.The proposed protocol reject the paths containing selfish and non trusted nodes. The proposed protocol discovers a path among source and destination on the basis of Energy, Trust and Number of Nodes. Discovered path is free from selfish and non-trusty nodes. The path discovered after the use of this proposed protocol improves the performance of the system.

Protocol's performance is tested with the help of program which is designed in C++.This implementation in C++ used to check the performance of the protocol under various conditions. This performance has been illustrated in the forms of the graphs and tables in the previous chapter of dissertation. Graphs represent how the output varies with change in the number of nodes in the system and transmission range. Results are quite satisfactory indicating that the proposed protocol has feasible implementation.

7.2 Future Scope

The testing of the protocol in the present work has been done in isolated environment where conditions are not standard. However to check the actual applicability of protocol it is mandatory to check this protocol under an industrial standard environment. So that actual rating of a proposal can be made. Such an environment can be provided by standard software's like NS2 and Qualnet. However to test a protocol in NS2 and Qualnet the C++ code of the protocol has to be physical augmented. The implementation of the protocol in C++ has accomplished this task.

Now, the future work is to customize this implementation so as to create its augmentation compatibility with NS2 and Qualnet. Then the proposed protocol can be actually tested in the standard condition and its performance can be compared with the other existing routing protocol.

The proposed protocol can also be used in Grid Computing and Cloud Computing with some changes.

Publications

1) Heena and N. Kumar, " A Systematic Review on Detection of Selfish Nodes in Mobile Ad-hoc Network" International Journal of Research in Advent Technology (IJRAT), vol. 2, no. 2, pp. 188-194, February 2014.

2) Heena and N. Kumar, "Battery Power and Trust based Routing Strategy for MANET" IEEE International Conference on Advanced Communication Control and Computing Technologies, pp. 1559-1562, May 2014.

References

[1] J. Elson and K. Römer, "Wireless sensor networks: A new regime for time synchronization" ACM SIGCOMM Computer Communication Review, vol. 33, no. 1, pp.149-154, 2003.

[2] S. Singh, M. Woo and C.S. Raghavendra, "Power-aware routing in mobile ad-hoc networks" In Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking, pp.181-190, 1998.

[3] J. P. Macker and M.S. Corson, "Mobile ad-hoc networking and the IETF" ACM SIGMOBILE Mobile Computing and Communications Review, vol. 2, no. 1, pp.11-13, 1999.

[4] H. Bhakht, "Survey of routing protocols for mobile ad-hoc network" International Journal of Information and Communication Technology Research, vol. 1, no. 6, 2011.

[5] L. Xiaoqi, M. R. Lyu and J. Liu, "A trust model based routing protocol for secure ad-hoc networks" In Aerospace IEEE Conference 2004, vol. 2, pp. 1286-1295, 2004.

[6] H. Fu, J. Forslow and J. G. Park, "Web-based configuration management architecture for router network" IEEE Conference on Network Operations and Management Symposium, pp. 173-186, 2000.

[7] E. M. Royer and C. K. Toh, "A review of current routing protocols for ad-hoc mobile wireless networks" IEEE Conference on Personal Communications, no. 2, pp. 46-55, 1994.

[8] L. M. Feeney, "An energy consumption model for performance analysis of routing protocols for mobile ad-hoc networks" Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.

[9] C.C. Chiang, W. Liu and M. Gerla, "Routing in clustered multihop mobile wireless networks with fading channel" In proceedings of IEEE SICON, vol. 97, no. 4, pp. 197-211, 1997.

[10] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers" In ACM SIGCOMM Computer Communication Review, vol. 24, no. 4, pp. 234-244, 1994.

[11] T. W. Chen and M. Gerla, "Global state routing: A new routing scheme for ad-hoc wireless networks" IEEE International Conference on Communications, vol. 1, pp. 171-175, 1998.

[12] E. M. Royer and C.K. Toh, "A review of current routing protocols for ad-hoc mobile wireless networks" IEEE Conference on Personal Communications, no. 2, pp. 46-55, 1999.

[13] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing" In IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, 1999.

[14] D. B. Maltz and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad-hoc networks" Ad-hoc networking, vol. 5, pp. 139-172, 2005.

[15] V. D. Park and M.S. Corson, "A performance comparison of the temporally-ordered routing algorithm and ideal link-state routing" In IEEE Conference on Computers and Communications, pp. 592-598, 1998.

[16] C.K. Toh, "Associativity-based routing for ad-hoc mobile networks"Wireless Personal Communications, vol. 4, no. 2, pp. 103-139, 1997.

[17] P. Papadimitratos and Z.J. Haas, "Secure routing for mobile ad-hoc networks" In Proceedings of the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), pp. 193-204, 2002.

[18] R. Canetti, D. Song and J. D. Tygar, "Efficient and secure source authentication for multicast" In Network and Distributed System Security Symposium NDSS, vol. 1, pp. 35-46, 2001.

[19] D. LaFlamme, B. Dahill and E.M. Royer, "Authenticated routing for ad-hoc networks" IEEE journal on Selected Areas in Communications, no. 3, pp. 598-610, 2005.

[20] R. Canetti, D. Song and J. D. Tygar, "Efficient and secure source authentication for multicast" In Network and Distributed System Security Symposium NDSS, vol. 1, pp. 35-46, 2001.

[21] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad-hoc networks" Wireless networks, vol. 11, no. 1-2, pp. 21-38, 2005.

[22] A.Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast" In Network and Distributed System Security Symposium NDSS, vol. 1, pp. 35-46, 2001.

[23] A. Perrig, R. Canetti, J. D. Tygar and D. Song, "Efficient authentication and signing of multicast streams over lossy channels" In IEEE Preceedings of Security and Privacy, pp. 56-73, 2000.

[24] M. Stemm, "Measuring and reducing energy consumption of network interfaces in hand-held devices" IEICE transactions on Communications, vol. 80, no. 8, pp. 1125-1131, 1997.

[25] M. G. Zapata, "Secure ad-hoc on-demand distance vector routing"ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6, no. 3, pp. 106-107, 2002.

[26] Y. C. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad-hoc networks" Ad-Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.

[27] H. Li and M. Singhal, "A secure routing protocol for wireless ad-hoc networks" In Proceedings of the 39th Annual Hawaii International Conference on System Sciences, vol. 9, pp. 225a-225a, 2006.

[28] S. Yi, P. Naldurg and R. Kravets, "Security-aware ad-hoc routing for wireless networks" In Proceedings of the 2nd ACM international symposium on Mobile ad-hoc networking & computing, pp. 299-302, 2001.

[29] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad-hoc networks" In Symposium Preccedings on Applications and the Internet Workshops, pp. 379-383, 2003.

[30] A. Babakhouya, Y. Challal and A. Bouabdallah, "A simulation analysis of routing misbehaviour in mobile ad-hoc networks" In Second International Conference on Next Generation Mobile Applications, vol. 8, pp. 592-597, 2008.