S-RTS MAC Protocol To Improve AR-MAC For Solving The Hidden And Exposed Terminal Problem

A Dissertation proposal submitted by

Shalakha Sharma

Regno11007450

To

Lovely School of Computer Science Engineering

In partial fulfillment of requirement for the

Award of the Degree of

Master of Technology in Computer Science

Under the Guidance of

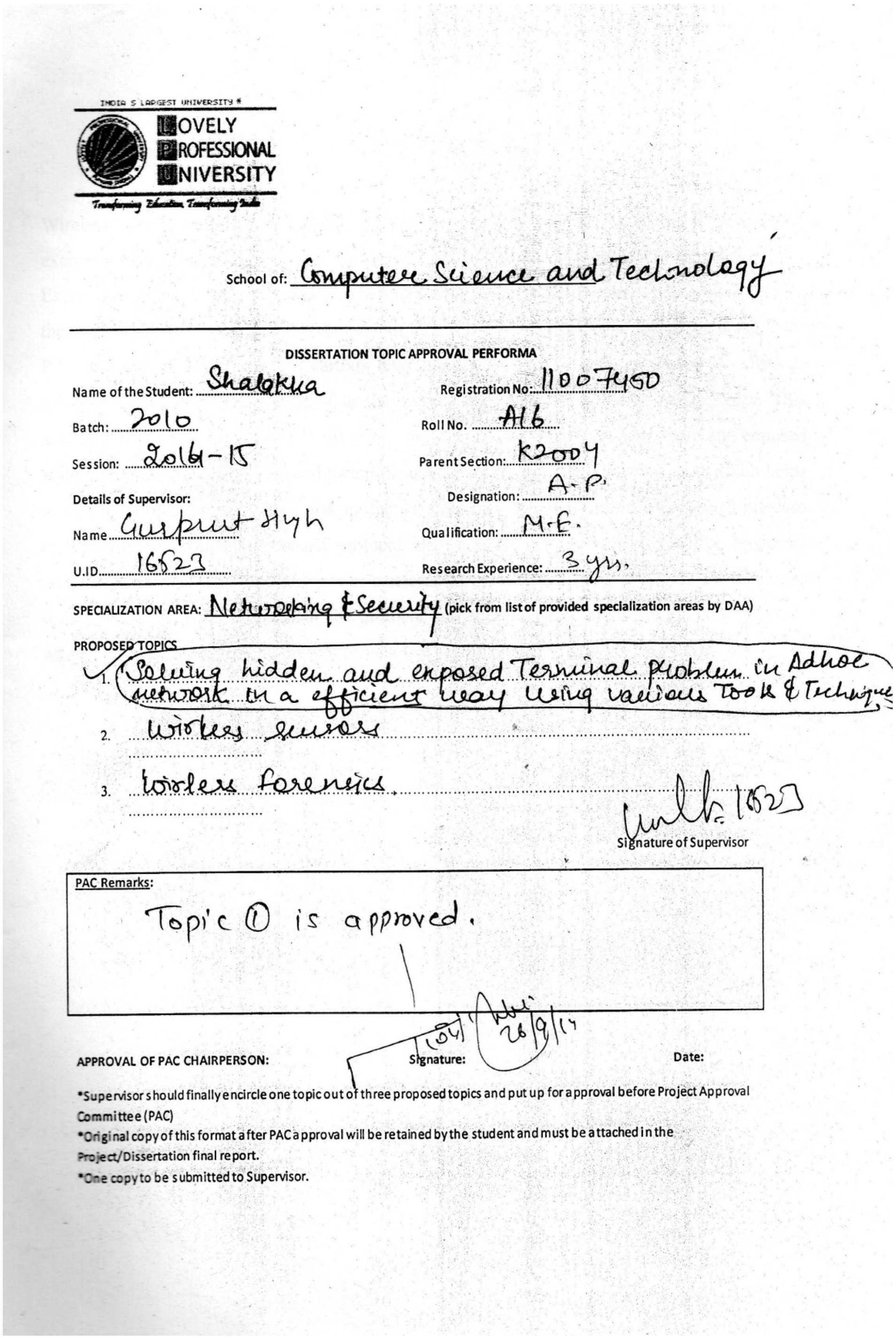
Mr.Gurpreet Singh

Assistant Professor

UID: 16523

April 2015

PAC FORM



INDIA'S LARGEST UNIVERSITY*

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

School of: Computer Science and Technology

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Shalokha

Registration No: 11007450

Batch: 2010

Roll No. A16

Session: 2014-15

Parent Section: K2004

Details of Supervisor:

Designation: A.P.

Name Gurpreet Singh

Qualification: M.E.

U.ID 16523

Research Experience: 3 yrs.

SPECIALIZATION AREA: Networking & Security (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

✓ 1. Solving hidden and exposed Terminal problem in Adhoc network in a efficient way using various Tools & Techniques

2. wireless sensors

3. wireless forensics

16523

Signature of Supervisor

PAC Remarks:

Topic ① is approved.

26/9/14

APPROVAL OF PAC CHAIRPERSON: Signature: Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

Wireless communication had proved its worth in mobile networks to facilitate information exchange with minimal data loss. Communications are made so easily feasible with the help of technology in all possible networks ,extensive amount of research work is done in the field of communication that is accessed using ad-hoc networks .However, still an effective solution for the Hidden and Exposed terminal Problem is required.

In the present scenario there are several methods to resolve the hidden /exposed node problem and one of the latest and very effective techniques is ARMAC protocol that was used to solve the hidden and exposed terminal problem using the attachment of hash codes but they had some limitations which required solution , To work on the limitations using the basic RTS/CTS mechanism , SRTS protocol is designed that works on the loop holes of the ARMAC moreover provides security and high performance to the network.

This dissertation is focused on some of the major problem of ARMAC to solve hidden and exposed node problem efficiently. Proposed technique changes pattern of the control packet which helps in solving various limitations and making the protocol immune to various attacks which increase the security of protocol. SRTS protocol also changes certain fundaments like broadcast packets which make the time and power concerns of the protocol to be satisfied It also reducing the number of collisions and packet overhead so that the communication between two parties are not disrupted and provide a transmission of data that is in a smooth and secure network. SRTS protocol will help in solving the hidden and exposed terminal problem together with the concerns of security using the basic RTS/CTS exchange to provide the world with more competent solution.

ACKNOWLEDGEMENT

I would like to express my profound sense of gratitude and respect to all those who helped me throughout the duration of this project. I am highly thankful to **Mr. GURPREET SINGH** for his support, valuable time and advice, guidance, sincere cooperation during the study and in completing the assignment of preparing the said project within the time stipulated.

This period proved for me one of the most productive and knowledgeable experiences of my career. It provided me an opportunity to upgrade my skills as well as sharpen my professional knowledge.

I would like to thank my Parents, God and friends. With their support and well wishes I am able to complete this project in time.

DECLARATION

I hereby declare that the dissertation proposal entitled,” S-RTS MAC Protocol to Improve AR-MAC for Solving the Hidden and Exposed Terminal Problem” submitted for the M. Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: SHALAKHA SHARMA

11007450

CERTIFICATE

This is to certify that Shalakha Sharma has completed M.Tech dissertation proposal titled "**S-RTS MAC Protocol To Improve AR-MAC For Solving The Hidden And Exposed Terminal Problem**" under my guidance and supervisions .To the best of my knowledge ,the present work is the result of her original investigation and study. No part of the dissertation proposal has even been submitted for any other degree or diploma. The dissertation proposal is fit for submission and the partial fulfillment of the candidate for the award of M.Tech Computer Science & Engineering.

Date-- GURPREETSINGH(Asst.Professer)

UID 16523

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

Technology and communication has come a long way since past few decades and have seen drastic changes in their entire field. Networking has a very significant role in this scenario wherein the whole base of telecommunication rests on it. Networking provides a route or a channel for the technology to connect various branches of technology that ultimately frames the structure of modern communication. A simple network could be the one we user at our homes. The laptop connected to internet is a network, any digital device connected to pc through a USB cable is a network, home Wi-Fi network or Bluetooth connection is a network.

Networking in the simplest words is nothing but a connection of series of points or nodes which are interconnected to each other via simple or complex paths, simple devices like routers, repeaters and hubs are used to transmit the data packets to all the nodes in the network. Node may be mobile. Managing such a network in which nodes are continuously moving and the infrastructure topology varies. Intelligent wireless network is able to adapt itself to such mobility issues. These networks may be of many types. There could be an internetwork of nodes in a scenario and similarly a networking between different other networks. Networking between these nodes can be studied by going through the topologies that they exhibit .Networks can be of two types that is wired network and wireless networks.

Wired networks: The network is established with the help of wires and connections that is maintained by the various topologies and it also depends upon the need of the connection required.

Wireless networks: Connections between nodes are established without the use of wires and provide the access of mobility of nodes .there are several sub-categories of the wireless networks

.

Figure 1.1 figure shows the example of networking

Benefits of networking: In modern communication technology vary in different fields

depending on the type of networking technology being used.

- *Speedy and easy communication*: Using the networking technologies available in market it gets very easy to communicate with people over large distances with an instant using video conferencing, telephones, chats etc. Therefore the data transmission rate is also very high.
- *Software and hardware sharing*: Sharing of resources get easier when there is a network among the nodes. A printer could be shared by two or machines over a network and software installed on one machine could be used by other on the same network.
- *Security*: Data integrity as well as its security is never compromised in a network. Unauthorized access of resources in a network is restricted by passwords and firewalls.

Need of networking:

Broadband connection: the networks provide the ability to have a broadband connection to connect with the internet and sharing the information. So sharing and exchanging of information is provided by the network through the various broadband connections.

Files: Transfer the files through distributed network provide middleware solutions for the software companies is not possible without the use of networks.

Peripherals and printer: Connecting with the peripherals will not be possible without a proper network in distributed networks .Moreover the easy acknowledgement of information and security can only be provided when there is a point of connection between the two parties and that is provided by the network

Drilling down to the roots of networking, the characteristics and properties of a network are determined by three basic key features.

- **Topology that network displays**: Gives the physical or geological arrangement of positioning of the nodes in a network.
- **Protocol governing the network**: It is a set of rules which determine the way communication will occur in a network.
- **Architecture of network**: Gives the basic architecture or the skeleton of the network. It could be a peer-to-peer architecture where communication occurs directly between nodes or it could be

client/server architecture wherein a node asks for a request which is served by some distant node having the required information and responds back to the request made.

<u>Topology</u>- These networks may be one of the following topologies. Refer Fig 1.2

- **Bus**- The Bus topology contains a backbone line which serves as the main communication line for all the nodes in the network which are directly connected to this main line.
- **Token ring-** The Token Ring topology uses a token which acts like a pass for the node which wants to transfer any data. The node with the token transfers the data. The nodes are connected to every adjacent node.
- **Star**- The Star topology has a central unit to which all the nodes are connected and use it to transfer data among each other.
- **Mesh**- The Mesh topology is a sort of hybrid of all the topologies which is formed by a mixture of all the topologies known. It has a very complex structure but gives much more reliability because there are more than one ways to communicate to a node.

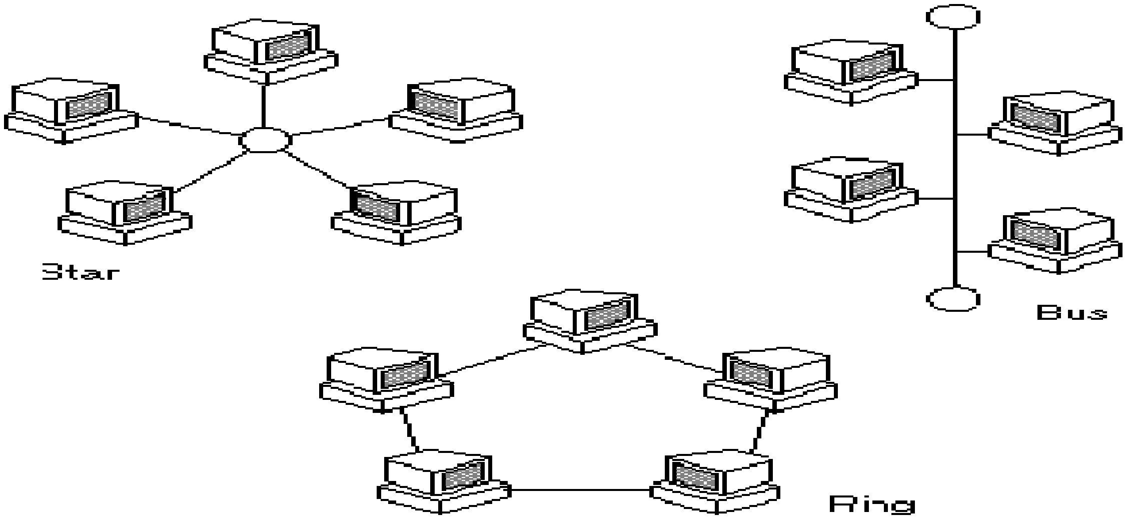


Fig 1.2- Network topologies

These network connections would require different links that would give a physical means of connection between the nodes. These physical links could be optical fiber cables, twisted cables, shielded or unshielded twisted pair cables, coaxial cables.

1.1Wireless networking:

It is serving at its best to meet the needs of internet service use of a very large scale. A wireless network can be easily accesses anywhere within its range easily without any use of extra hardware device. It is just a network which can provide you data connection without use of any wiring and can form a network in the same manner.

A wireless network is a class of computer network in which wireless data links are used for the connection of network nodes Wireless networking is a means through which telecommunications networks, homes and endeavor (business) installations get rid of the costly process of introducing cables into between various tools locations. They are generally administered and implemented using radio communication. This implementation will take place at the OSI model's physical layer. Examples of wireless networks are Wi-Fi local networks, cell phone networks and terrestrial microwave networks

Depending upon the requirement of the connections the wireless networks can be of different types and also provide the mobility to nodes. Wireless networks had proved it worth in the every field of technology and communication to provide a flawless service to its users without having the problem of connections like in wired networks.

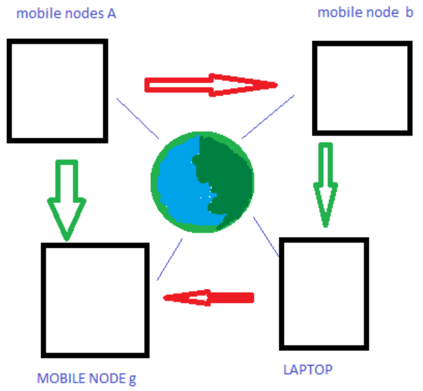


FIGURE1.3connection in wireless networks

1.1.1Types of wireless networks

1.1.1.1Wireless PAN: Wireless Personal Area Network or PAN is nothing but the networking of devices using wireless technology within a small area or region, generally created for the use of a person or two

1.1.1.2Wireless LAN: Wireless Local Area Network or LAN is used for local geographical region 100 m ranges. A wireless local area network (WLAN) links devices over a short range, by using connection of internet access.

1.1.1.3Wireless mesh network: A wireless mesh network is a network using radio nodes formed in a mesh topology. Every terminal forwards messages to the other nodes. Mesh networks can "self heal", by using re-routing techniques around a node that has less power.

1.1.1.4Wireless MAN: Wireless metropolitan area networks or WMANs are collection of several wireless LANs. Wi-MAX is a common example of Wireless MAN and is described by the IEEE 802.16 standard.

1.1.1.5Wireless WANS: Wireless wide area networks or WWANs covers huge areas, for example between towns and cities, or city and suburb. The typical system of WAN contains base station gateways, access points and wireless bridging relays. This method can be easily used to connect offices or business bodies located at two cities.

Wireless networking branches:

1. Wireless Ad-Hoc networks: It provides a flexible infrastructure and provides the mobility of nodes that can be accessed by the transmission range set for the nodes the routers and protocols are described for the connection of the nodes.

2. Intrusion detection systems: The systems are designed to detect any kind of intrusion present in the network so that they can be blocked timely to provide secure communication.
3. Wireless network security: this branch provides the various mechanism and protocols that works to provide security to the network by the trap mechanism like honey pots and detect and prevent mechanism so that a secure network is available to communicate.

4. VANET::Vehicular ad hoc networks (In VANETs) uses artificial intelligence that make vehicles to behave in intelligent agent while vehicle-to-vehicle collisions, accidents, drunken driving etc.
5. MANETS: Mobile ad-hoc network provides the mobility of nodes etc

There are many branches that are present and new developed to provide security and to ease the task using the technology.

1.2Ad Hoc Network:

Ad-Hoc networks come with a very flexible infrastructure. Mobile stations and mobile nodes and base stations are common in Ad-Hoc networks which have no specific design or structure. The whole concept works on the phenomenon of wireless networking wherein communication between nodes depends upon the reach range of nodes. A wireless network is simply a network that uses wireless data connection for connection of network devices. A mobile node once goes out of the communication range of a node; it is no more able to communicate with each other.

Figure 1.1 shows the same concept. As soon as the node D goes out of the range of node A it loses its connection with it, but still it can connect.

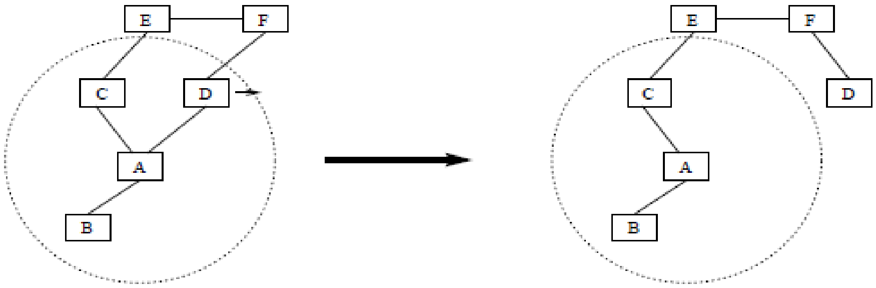


Figure1.4AdHoc networking

Ad hoc networks come under the branch f networks that provide the communication and security to the communication can only be established when they are transmission range of each other as shown in figure the that when a and D are communicating the communication is smooth but when D is out of range of A the connection is broken between the nodes

Securing such a network in which the communicating nodes are continuously in mobile mode is a necessary evil. Secure routing is needed the most in Ad-Hoc networks. There are many attacks that make routing suffer from much vulnerability. Routing tables should be robust enough to tolerate any attack. Talking about attacks in routing, it is basically because of errors that come in the routing table. In order to communicate with another node, a node may share its routing table information with it. Security attacks can arise during this point of information sharing

Routing security can suffer from external attacks or internal attacks. External attacks arise when an outside attacker injects malicious of wrong routing table information in a communication and thus changing the originality of information .This method can be successfully exploited by the attacker to result in network traffic overload or ever communication failure.

Internal attacks arise due wrong routing table information advertised by compromised nodes within a network. Finding such an error is not easy because all the compromised nodes can easily sign the routing table with their valid signatures.

Use of intelligent cryptography methods, digital signature, certificates can prove somewhat useful in protecting the security of Ad-Hoc networks but even then risks are always there.

1.2.1Advantage of Ad-HOC networks:

1. No infrastructure and lower cost: The ad hoc networks as its is based on no infrastructure property provides the benefit of connection that do not require wires etc this leads to low cost that is spent on the development of network between the two nodes, with this property it provides advantages of portability and access to the technology and to hose nodes that are far way that was not possible by wired systems.

2. Mobility: The wireless ad-hoc networks provides the advantage of the mobility to the nodes ,with no proper infrastructure to be followed the nodes can freely move and provides the portability for the new range it(cell) it move to. The mobility of node that want to communicate can only do so if it is in the transmission range of the other node.
3. Decentralized and robust :Ad hoc networks does not have a central control over the nodes provides the decentralized access and communication are held by routers that trace the path of the node in the robust way to have communication better than that in wired systems.
4. Maintenance Cost: In the wired communication a lot of money is spent on the maintenance of the wires and for the damage of the connection but in the wireless systems no infrastructure helps to reduce this cost.

5. Easy to build and spontaneous infrastructure: The establishment of the wireless networks are easy as compare to the other systems and require a rapid node to node connection with help of routing protocols that help to provide connection without centralized control.

6. The nodes of the ad hoc network can rely on any hardware or software provides the ability to get connected and communicated faster than other connections.

7. It can be set temporarily at any time.

1.2.2 Limitations of ad-hoc networks:

1. Quality of service: as the ad-hoc networks can create the dynamic organization for the communication and due to the dynamic changing topology the quality may be affected in the peer to peer link in the multi-hop environment.

2. The transmission quality is affected: the quality of service between two nodes is affected by the interference that arises in the ad-hoc networks. The nodes that are in the transmission range can only communicate each other but non neighboring nodes provide interference for the dropping of packet.

3. Limited resource: The ad-hoc networks have the property of dynamic changing the link flow that results in varying resources.

4. Highly dynamic: Ad-hoc network have the characteristics of dynamic changing topology and this change occurs due to radio transmission and due to the components of Qos.

5. Sufficient admission control: This decides that the amount of available bandwidth is enough for the transmission of packet in the presence of resources. The ad-hoc network provides a limited bandwidth may affect the end quality of service.

6. Scalability: the problems are faced in the large scaled networks due to equal node priority etc

7. Security: the infrastructure less network is very prone to the various attacks and it is hard to maintain the security of the network there are passive attacks and active attacks etc that can adhere the communication.

8. Power control: The control over the consumption of power is to be monitored in the ad-hoc networks as some communication requires high power consumption.

9. Higher error rate :Due to the problem electronic wave several problems like diffraction fading may result in the transmitted packet being garbage

10. Lower data rate: The ad-hoc networks faces a problem of reduced data rates, the characterises of waves required for communication prevents them to transfer data better than wired systems, this problem can be handled with a higher frequency can transmit more data, but then it is more prone to interference.

1.3MANETS:

Networking has now taken one leap ahead of the traditional networks. We have the intelligent networks now which exhibit self-configuring properties and are almost without any definite infrastructure. These are the Mobile Ad Hoc Networks or MANETs wherein the nodes have the ability to change their positions, and can move in any direction freely. This would ultimately change the physical links and the topology of the network. These networks need certain devices called routers which store the information related to the movement of all the nodes so as to maintain the network traffic. These were used firstly by the military and defense forces to communicate with the troops on the battlefield

MANET Stands for "Mobile Ad Hoc Network." A MANET is also characterized as a ad-hoc networks that can be accessed anywhere even at time of fly. Mobile Ad-Hoc networks or MANET is a complex system characterized by nodes that are capable of moving and changing the network topology. It has a flexible structure with no pre-defined communication infrastructure. MANET has proved to be a boon for defense and military services and is continuously growing with time.

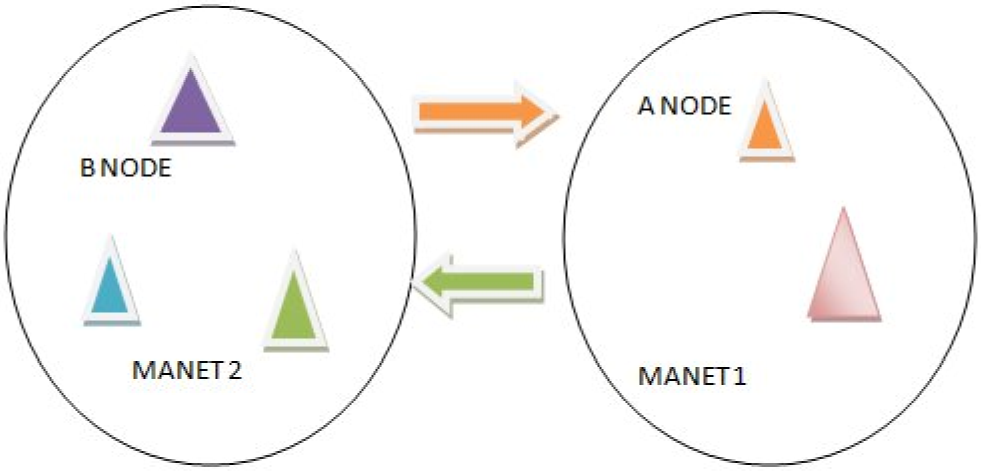


Figure 1.5 Example of MANET network

1.3.1Types of MANET:

1.3.1.1Vehicular Ad hoc Networks (VANETs): Vehicular ad hoc networks (In VANETs) uses artificial intelligence that make vehicles to behave in intelligent agent while vehicle-to-vehicle collisions, accidents, drunken driving etc.

1.3.1.2Smart Phone Ad hoc Networks (SPANs): SPANs are different from traditional hub and spoken networks, as Wi-Fi Direct, which support multi-hop relays and also there is no notion of a group leader so peers can join and leave without eliminating the network.

1.3.1.3Internet based mobile ad hoc networks (i-MANETS) : Are ad hoc networks that are created using links between the nodes and internet. They require a proper connection between nodes and any interference can adheres the communication.

1.3.1.4Military / Tactical MANETS: are used by military units with focus on enhancing and focusing on security, range, and integration with existing systems. Military based systems provide security and their update are not made public due to security reasons

1.3.1.54-G and Ad-Hoc Networking: The evolution of 4-G mobile networking has been successful because of the MANET technology and thus enabling the users to access their data anytime and anywhere with a super speed.

4-G networks basically are a kind of hybrid topology networks with the ability to integrate and combine many more network topologies and technologies with themselves [Refer fig 1.8]. A4-G network can integrate itself with many heterogeneous wireless networks like wireless LAN, WAN, PAN including other Ad-Hoc networks. Apart from this they can combine or integrate their functionality with a fixed network backbone infrastructure like the internet or PSTN. What 4-G network believes is that the future base of networks will be packet switched networking and other technologies related to it

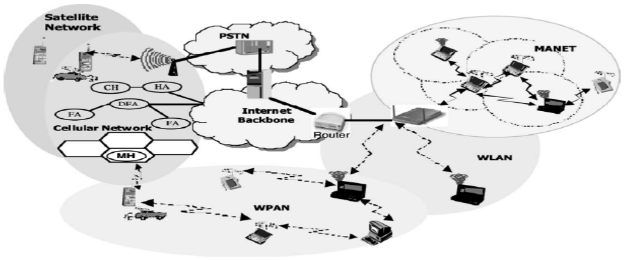


figure 1.6 4G networking

1.4Hidden Terminal Problem:

The wireless communication is very efficient on the one side but as we know there are not only boons but problems with it. The communication to be smooth and without jam requires a problem connection between the two nodes that are communicating so that any kind of disturbance on the data sent or on security of the connection is not there but the ideal situation is not always followed.

The nodes in the particular cell can sense the other nodes by the carrier sense and the transmission range When any node that is not in the range of the carrier sense of the other node, It means that node is hidden for the other node and it for that node that node does not exist as it is not in the range of the node. This leads to the hidden terminal problem.

The hidden terminal problem occurs when the nodes are trying to communicate to the same node at the same time they send the request to pair with the node. The node whose request is first received is paired for connection but the another nodes continue to send request to the node because it is not acknowledged about the connection of the two nodes because one of the nodes is hidden for it, this results in collisions of packets and jamming on the network.

Hidden nodes use carrier and packet sensing different MAC protocols. These protocols regulate access by using the means where nodes adjourn from attempting to gain access when they sense another node using the channel so they also try to establish the connection. There is also a scenario when the other nodes interfere with the connection so that they cannot establish a connection. When node gains access destination reception node interfere by sending packets for request result in collision of packets.

Suppose there is cell where there are different nodes present such that A and B are in the transmission range for each- other but the other node C that does not know A is any node(because it is hidden node for C) tries also to communicate with B , both the nodes send request for connection to the node B without having knowledge about each other as they are hidden to each other, so when the request of packet A is received first they start to establish a connection but C node could not detect the ongoing transmission between A and B and will interfere at packet reception, this results in collision of packets, jamming and communication loss

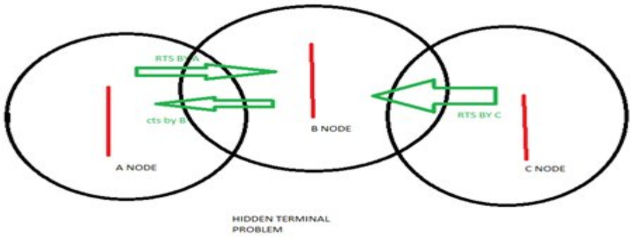


Fig: 1.7 hidden terminal problem

As in the figure it is shown as per the scenario that nodes A, B, C are of different cell and A and C are hidden so when they try to communicate it create problem and collision of packets because a AND C are hidden

1.5 Exposed Terminal Problem:

The exposed node problem is very different from the hidden problem still they affect each other. Exposed node problem and hidden terminal problem goes hand in hand and also affect the performance of each other.

According to the research, it is shown that the exposed node problem in fact dominates the hidden terminal problem by the rate of 1.3 density variations. The problem mainly occurs because of not allowance of concurrent transmission to the other nodes of the same cell where the nodes are communicating.

In this problem the node tries to communicate to the nodes that is sensing to establish connection with a node that is either busy with communication or virtually jammed and they are not allowed to communicate as they can interfere the other transmission, this leads to the whole network get jammed and no node could establish a secure connection.

Suppose there are four nodes that are in the case that A,B,C,D such that B is in the range of A and C , D is in the range of C not A and B in this case the nodes D tries to communicate to C when the transmission of A and B are going ,in this situation they are not accessed to communicate with two reasons that that c is constantly trying to communicate with .B this will show C busy when D will sense and they will create interference in on going transmission so they are blocked for the time the other transmission is going on this leads to whole create the traffic and high load on network.

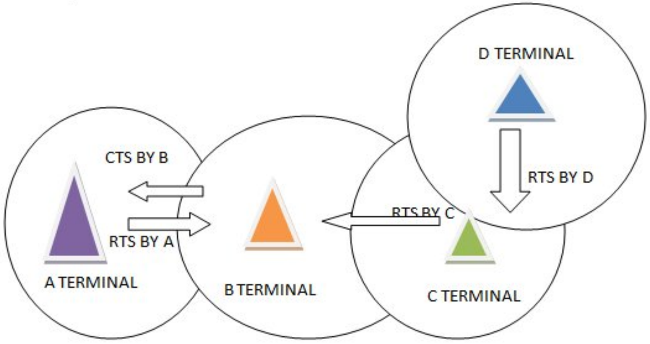


Fig: 1.8 Exposed terminal problem

Extensive amount of research is done in this field to resolve the problem, there are many ways proposed in the networks to encounter this problem various protocols are generated to like:

- Pure contention based protocol: It includes some of those mechanisms that was initiated in the primary effort to solve the problem and is based on the principle of CSMA/CA. they are divided into three groups of sender-initiated, receiver initiated, hybrid. Some of the protocols that re in this category are MACA,MACAW ,MACA-BI ,FAMA ,AA etc

- Busy tone signal based protocol: This protocol takes the benefit of one or more busy tone signals. the protocol can be divided single and multiple channel based, the main advantage of using this protocol is that busy tone is easy to detect than the MAC frames. Some of the are PUMA, busy-Simon, ri-BTMAetc.

- Power aware protocols: The main goal of the power protocol is to decrease the power consumption and can also be designed to minimize the probability of collisions to deal with the hidden node problem.

- Multiple channel based protocols: They use several channels to increase the overall performance, reduce the number collisions. There are three categories of such protocols :with common control channel, without and hybrid.

- Directional antennas based protocols: It allows the concurrent transmission of data and reception in order to boost spatial reuse. This protocol had defined a particular frequency range to catch the packets in their range so that they cannot interfere in each other transmission ,this will help in reducing the number of collisions caused in the hidden problem.

Despite of the various efforts done in this field Still the problem is present that totally disturb the network throughput and the performance of the network .Some criteria till date prevail that are untouched and that could also add-up to provide the efficient solution of the problem.

Hidden and exposed nodes are also vulnerable to the various attacks that are RTS/CTS attacks, replay attack etc that leads to the total jam the network and create interference in the network with problem like data loss, packet overhead, more power consumption and collisions .The problem is severe and the need of research is still prevailing in this area. So in the research work we not only consider solving the hidden node problem but also concentrating on the attacks moreover on the power consumption, packet overhead and reduce packet collisions so the robust approach can be provided for better communication with no data loss.

CHAPTER 2
LITERATURE REVIEW

This chapter introduces the studies that have been done in the field to solve the hidden and exposed terminal problem ,various simulation and results are summed up to describe the problem and all the literatures lead to the prominent results in adding marking stone for my research work.

(Caishi Huang et.(2013)[3]: In their paper they have presented a joint approach to resolve the exposed and hidden terminal problems in wireless networks. In hidden terminal, the proposed technique uses the fact that different transmission rates have different received power and different SINR requirements, and therefore different interference ranges and transmission range .It is shown in the paper that for a given DATA packet broadcast rate the related hidden terminals may be mostly removed by selecting a right rate for sending RTS/CTS packets. After this, integration of the transmission power control into the solution under certain criteria are required for tackling the exposed terminal problem that has been exposed.

(**Viral V. Kapadia, 2010**)[2]:In this research paper the author mainly focuses on the hidden terminal problem and the few problems that are introduced by the use of RTS/CTS mechanism and that create the virtual jamming problem, which let the malicious node to efficiently jam a large fragment of wireless networks at minimum expense of power. They considered the various mechanism like CSMA ,RTS/CTS handshake and provided different solutions to solve the problem of hidden and exposed node like increasing the power ,use Omni -directional antennas Remove obstacles, move the nodes and protocols enhancement to solve the problem.

(katarzyana kosek,2012)[3]: In this survey paper the author described about comprehensive overview about the MAC protocols that discuss about the various methods to solve the hidden and exposed terminal problem. They discussed about pure contention based protocol ,busy tone signal based protocol ,power aware protocol, multiple channel based protocols etc field with the sub categories of all the protocols defined to resolve the problem to describe the each development done in the particular and where the disadvantage is still there. These protocols can be further compared for the better results and a hybrid remedy can be prepared for the proficient results.

(Weifeng Sun et. al in their paper(2012) : In this paper have analyzed existing studies on channel assignment algorithms and formulated channel distribution principles. This paper has developed a dynamic channel assignment algorithm called R-CA considering the problem of channel interference in multi-hop wireless mesh networks called. R-CA is a dynamic algorithm which is based on a cross-layer design which includes a network layer and a MAC layer. It is able to assign the routing and channel at the same time. It is a proposed form of DC where the channels are assigned dynamically to increase the network throughput . The simulation results in this paper show the R-CA algorithm's effectiveness in exploiting channel assignment diversity to reduce interference which leads to a noticeable better performance in a multi-hop mesh network that is IEEE 802.11 based.

(Ashikar rahman,2006): In this research paper the author describes about various problems of RTS/CTS mechanism and discussed about the virtual jamming that is created to exploit the network so that any other node trying to communicate cannot access the node. They provided the scheme of RTS verification that allows to check the node before sending so that any virtual jamming created could be stopped at the particular instant and provided a methodology to identity that whether the node is false blocked or in true communication mode by RTS validations schemes by dividing them into two phases.

(Ms. Ritu Patidar et. al ,(2012)[5] : In this research paper have explained in detail the hidden terminal problem in the case of wireless networks. These problems have an impact on the throughput performance. A brief explanation of the solution methods has also been given. After analysis of the problems, the directional antenna that is based on MAC protocol and is used with Sensor-MAC Protocol to improve the output performance of wireless sensor network has been proposed.

(M. J. Saeed et. al in their paper,(2012)[15] :They have elaborately discussed the wireless mobile ad-hoc networks and have high lighted the wireless network fundamentals in general and in particular, the mobile ad-hoc wireless networks. Besides that the core problems/issues related to wireless ad-hoc are also discussed in detail which provide an overview of the complexities that are related to the practical implementation and design of MAC layer protocols. The IEEE standard are also discussed for the analysis of the Hidden and Exposed nodes problem that is faced by the wireless ad-hoc networks and how they have been dealt by other available protocols .A new MAC level protocol is proposed in the end, which offers a new approach to the ‘Back-off’ criteria that is used by IEEE and the ‘Virtual Base Station’ concept. The results given in this paper are preliminary in nature

(Lu Wang et. al in their paper (2012)[14]: In this paper, we propose a novel Attachment Coding scheme to attach control information on data traffic. This coding scheme enables data transmission along with control transmission, without humiliating the throughput for novel data traffic. To illustrate the effectiveness of Attachment Coding, Attached-RTS has been proposed that includes a particular syntax in which the communication is followed, to fully utilize exposed terminals for concurrent transmissions. Attachment Coding describes the particular bandwidth for the RTS and CTS packets and the particular hash code for each bandwidth so that it can allow concurrent transmission .they faced some problems in communication over distributed network and had some limitations due to the habit of broadcasting the message as well as defining the limited bandwidth for each packet. They provide effective solution for simultaneous transmission.

(Khaled H. Almotairi et. al in their paper,(2011)[9]They have proposed the MMAC-HR for resolving the multichannel exposed terminal problem, that leads to poor channel utilization. MMAC-HR employs carrier sensing over all channels and does not use a channel list. Hence, nodes do not require to sense the control channel to find if any data channel is idle. Additionally, the proposed protocol uses a slow hopping and independent strategy for utilizing the multiple channels without exchanging information. Also, MMAC-HR is a distributed protocol and does not need synchronization simulation results by using ns-2, show that MMAC-HR achieves better throughput and lower delay than DCA.

(Deepanshu Shukla et. al in their paper, (2011)[11] :They have presented a simple enhancement to the IEEE 802.11 DCF MAC protocol that allows parallel transmission to occur whenever possible, reducing the loss in the throughput due to the exposed node problem. While it has long been recognized that exposed nodes should be free to transmit, the unambiguous algorithm has been presented within the IEEE 802.11 framework. This paper has made use of the viewer fact that traffic on the internet has a large number of small packets, and the accepted fact that is inefficient to use RTS/CTS for such small packets. This algorithm is local and opportunistic and therefore gives varying levels of improvement

(Ketema Adere, Ramamurthy(2010)[8]:In this research paper ,they explained the exposed and hidden terminal problem in wireless sensor networks . These problems have an effect on the throughput performance They described about the Omni-directional and directional antennas can be beneficial to transmit the data with no collisions and data loss The solution methods have been briefly explained. After the problem analysis, the directional antenna based MAC protocol that is used with Sensor-MAC Protocol to increase the performance of the output of wireless sensor network has been proposed.

(Ki Hong Kim et.,(2010)[7] ; In this paper they have presented the case study of security attacks that are based on control packets (RTS and CTS) vulnerabilities in Synergy MAC. In addition to this, it has analyzed security vulnerabilities at every handshaking stage while attacking control packets that are exchanged among nodes (source, destination, and relay). In this paper, a study on the comprehensive analysis of security vulnerabilities caused by attacker node in Synergy MAC is being made. The analytical results can be extended to cooperative wireless network security as well as WSN security design in general. As future work, the author plans to design and implement lightweight low-power authentication mechanism suitable for cooperative wireless networks.

(Aruna Jayasuriya et. al in their paper (2010)[13]: In this research paper they have evaluated the comparative throughput performance and node density of the hidden and exposed nodes of ad hoc networks with and without pre-data control schemes, such as RTS/CTS mechanism in 802.11 systems. The diagnostic and imitation results suggest that throughput performance degrades due to use of RTS/CTS like pre data handshake mechanisms. This paper shows that exposed problem dominates the hidden terminal problem and the rate of 1.3 times and the density and transmission rate is shown that as exposed problem is solve the hidden will transmission rate affectively.

(Alex Sherman et. al (2008),[6] :They introduced a new protocol, called Fair Torrent, which is simple to execute and has many enviable properties. It has been showed that this simple protocol not only maintains sprite, but has surprising good download performance in a variety of settings. By essentially matching download rates with upload rates , under various upload capacities distributions faster overall download times have been achieved .

Fair Torrent peers achieve a better consumption rate, thereby also civilizing the system by increasing the upload capacity. These results have been demonstrated in a variety of settings and derived bounds on the worst case performance.

CHAPTER 3
PRESENT WORK

3.1 Problem definition

An Ad hoc network has collection of mobile nodes that are communicating with each other without any centralized control function .To establish a proper communication various protocols are used to create a non –collision, secure communication in case of hidden and exposed terminal problem .RTS/CTS handshake is very common for solving hidden terminal problem but there are various complications during solving hidden terminal and exposed terminal both and also after introduction of RTS attack and CTS attack it is much difficult to achieve high performance with CTS/RTS handshake. In Attached-RTS hidden and exposed node problem are considered but they increase broadcasting overheads which consumes time and power ,packet overhead and they also not considered RTS and CTS attack which increase the vulnerabilities. And there are certain limitations to A-RTS:

- Low data carrying space.
- Useless in distributed networks.
- Packet collision may occur.

3.2 Objectives

SRTS MAC PRTOCOL:

1. To Solve hidden and exposed node problem in all possible networks.
2. To Resolve CTS and RTS attacks.
3. To conserve time during mechanism.
4. To conserve power during mechanism.
5. To reduce packet overheads.
6. To avoid packet collision.

3.3 Research Methodology

AR-MAC is very effective in solving Hidden Terminal and Exposed Terminal Problem but due to its limitations and problems which is stated in upper section certain changes is needed. Few changes what is proposed to avoid all the limitations and fulfilling the objectives are:

1. The process of broadcast is removed that is done in AR-MAC ,Second,
2. RTS/CTS should contain the id of sender and receiver with a sequence number.
3. If there is any node send RTS or Received RTS should be blocked for other transmission till ACK is received.
4. RTS should contain all intermediate node ids in message packet and CTS should be responded back to same sequence.
5. Always select the RTS with lowest Sequence.

The format of new control packets would be like:

RTS (source_Id, intermediate_Id… destination, Sequence No)
CTS (source_Id, intermediate_Id… destination_Id, Sequence No)
DATA (source_Id, intermediate_Id… destination_Id, Sequence No)
ACK (source_Id, intermediate_Id… destination_Id, Sequence No)

This procedure is explained by following diagrammatical sequence.

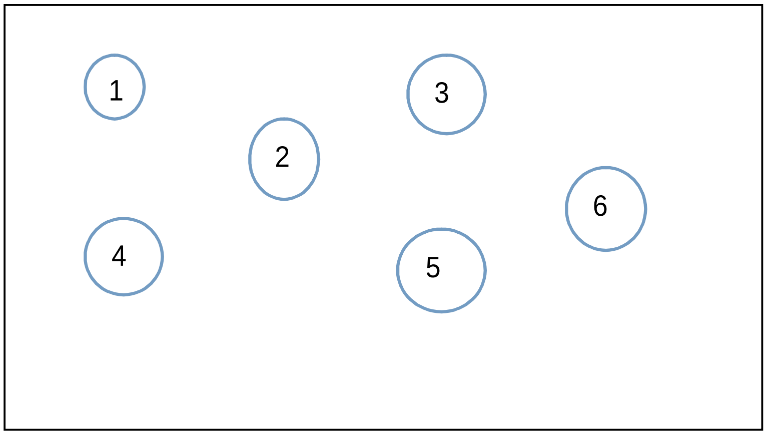


Figure (3.1) Sample network where 1 has to communicate with 4

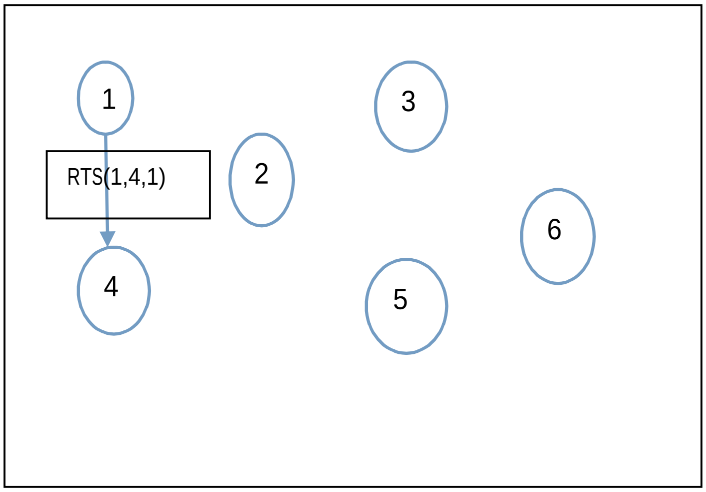


Figure (3.2) 1 is sending RTS to 4

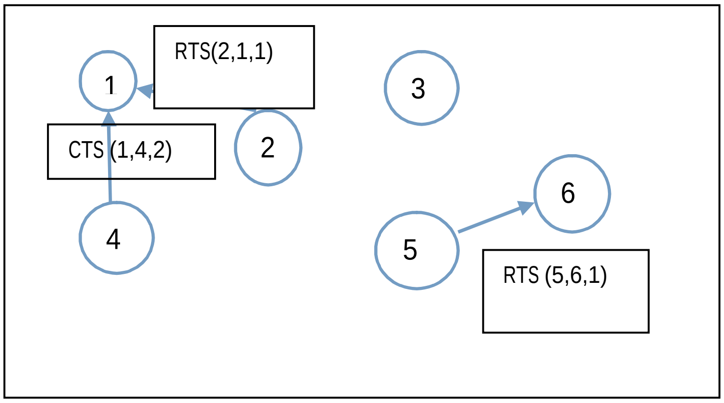
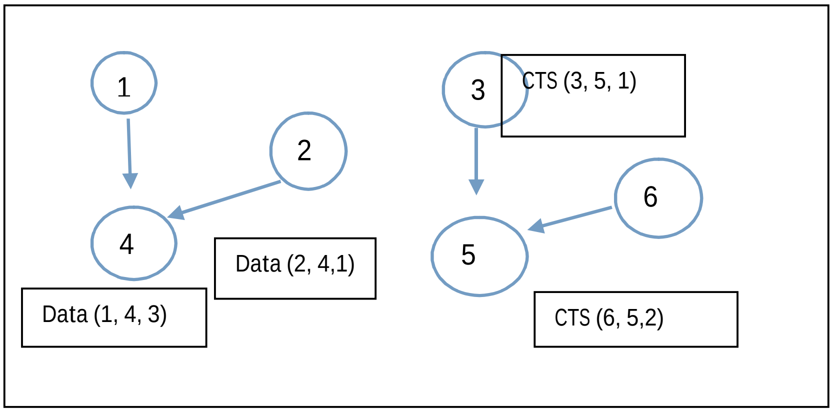


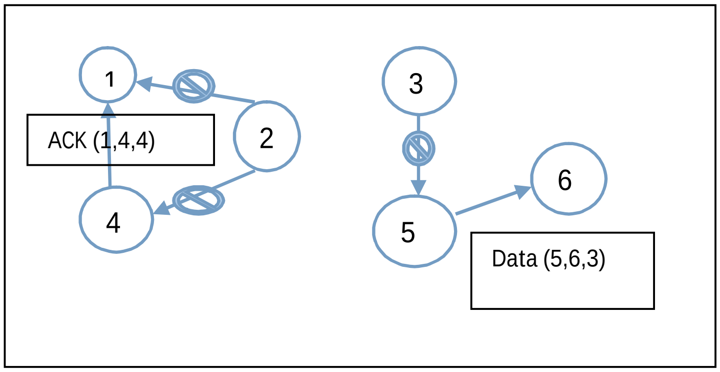
Figure (3.3) 4 is sending CTS to 1,2 is sending RTS to 1 and 5 is sending RTS to 6

As in figure 3.3, 2 is sending RTS to 1 but 1 has already sent an RTS so 1 is blocked to all message except CTS by 4 so RTS by 2 is discarded.



Figure(3.4): sending data to 4, 2 is sending data to 4 (Attack),6 is sending CTS to 5 and 3 is sending(CTSattack)

As in figure3.4, 2’s RTS is blocked and 2 try to send data to 4 but as sender information and sequence number is autonomous and generated by nodes so sequence number is wrong which makes 4 to discard message and same as for 3 sending CTS to 5.



Figure(3.5) 4 is sending ACKto 1, 2 is sending data to 4 (Attack), 6 is sending CTS to 5 and 3 is sending CTS to 5 (CTS attack).

As per previous figures the procedure explained which is avoiding the attacks and as the procedure does not have to broadcast messages the control packet transmission is limited and as limited packets power consumption and time also be limited, also the timer is included that will wait for the particular time in the case of no acknowledgment is given back in case of connection failure or false blocking it will set it free after the time period so that it can be available for other nodes and this also help in solving he exposed node As the protocol restricts the individual nodes it can work on any network without any restriction as the sequence number is auto-generated this solves problem regarding many attacks including RTS/CTS attacks. Moreover it will check the signal to interference and signal to noise ratio before starting the communication so that the performance of the communication is not affected and measures will be checked accordingly .this methodology could result in better result to solve the problem.

CHAPTER 4
REULTS AND DISSCUSION

The proposed methodology described in the upper sections of the report defines that SRTS protocol designed to work on the limitations of ARMAC protocol will improve the protocol by reducing the number of packets collisions, packet-overhead, reduce in time and power consumption together with the resolving the RTS/CTS attacks in all possible networks that was not provided by the ARMAC protocol.

SRTS is an effective protocol that works on the basic RTS/CTS mechanism together with the considerations of the attacks that creates a problem in the transmission of data that can work in all possible networks for solving the hidden and exposed terminal problem. ARMAC protocol that used attachment coding of hash packets for the transmission of data for solving the hidden and exposed terminal problem, but they faced some limitation in their approach is:

- Transmission of data in distributed network.
- Low data carrying space
- Packet-overhead
- High number of collision of packet
- Broadcasting the data before transmission

The process they chosen for the broadcasting of the packet before transmission to every node of the cell results in more time wastage and high packet overhead which results in collisions of packet.As per the limitations of the ARMAC protocol we designed a research methodology that will work o the limitation together with considering some unique aspects that were not included in the protocol.

When this methodology was implemented on the MATLAB the following results came forward: The simulation was created that worked on both kind of scenario that is of ARMAC protocol and SRTS protocol. The ARMAC protocol was simulated to work as defined by their methodology of attachment coding using hash codes for the nodes that want to communicate to each other in the form of:(Source node, destination node, hash code)

And similarly SRTS protocol was simulated as per the research methodology that used a particular path that is involved in the transmission together with the sequence number that is auto generated and incremented for each step ahead for the level of transmission. The format of control packets of SRTS are like:

RTS (source_Id, intermediate_Id, destinationId, Sequence No)
CTS (sourceId, intermediateId,destinationId, Sequence No)
DATA (sourceId, intermediateId, destinationId, Sequence No)
ACK (sourceId, intermediateId, destinationId, Sequence No)

When both the protocols were simulated on MATLAB with their defined methodology and under same conditions, the results was:

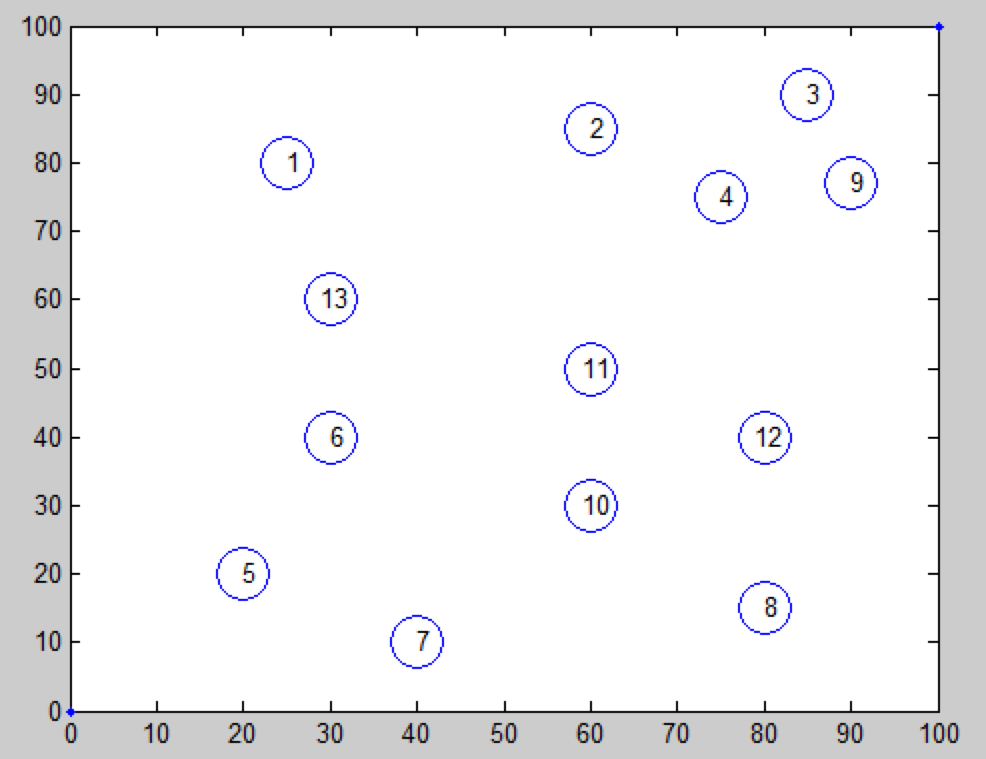


Figure 4.1 Simulated Network

This is the simulated network that is created on the tool that have some nodes designed in circles that have different transmission and carrier sense range. Communication between nodes was made using both the protocol on the same network to check the results of the performance.

SIMULATIONS for ARMAC protocol:

To make the communication between two nodes in the ARMAC protocol we entered the source node name and the destination node name to show the communication.

We entered the source node: 1

Destination node: 8

It showed a path that it will follow to reach to the from node 1 to 8 to send the RTS message .They does not included the intermediate node name in the path as the node are mobile when the intermediate nodes moved it could create problem in tracing the path.

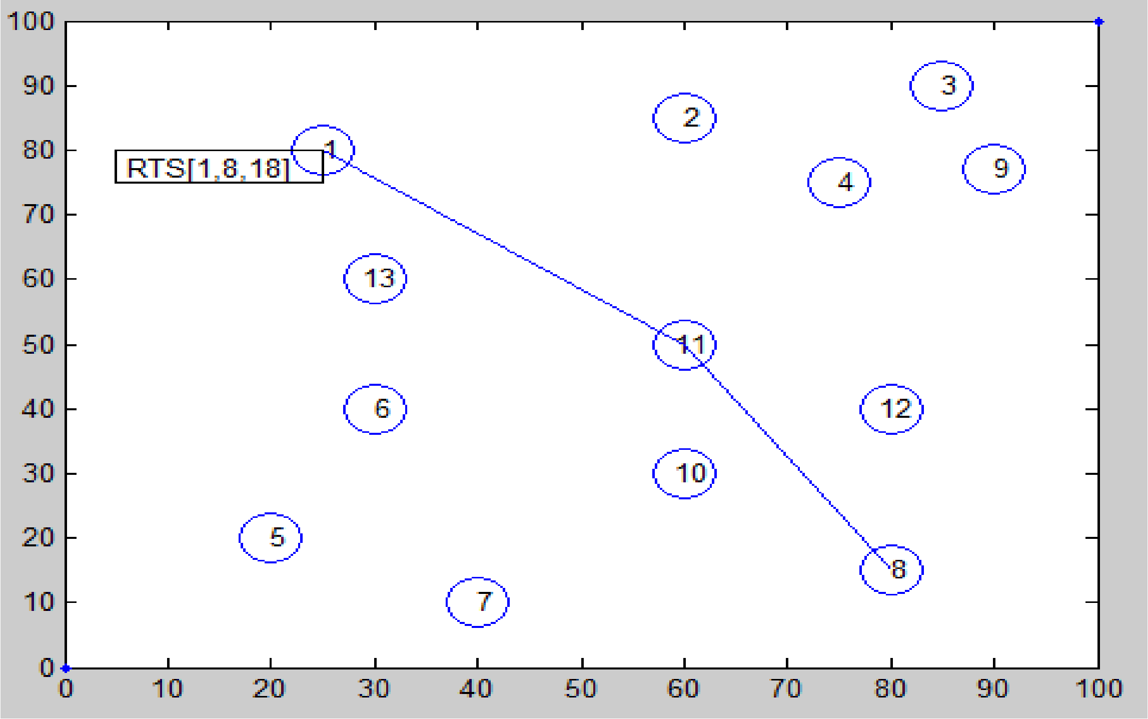


Figure: 4.2 RTS packet is sent from node 1 to 8 with the hash code 18

This is the initial step of trying to establish a connection between the nodes 1 and 8 in the sample network.

The node1 send the request to send message (RTS) to the node 8 ,but both the nodes belong to the different networks so they connected with the path using node 11. This is a drawback that their RTS packet do not contain the id of the intermediate node, as in MANETS the nodes are mobile so if the intermediate node moved the path connection from source to destination will not be fulfilled (this is one of the limitation of ARMAC protocol).

The protocol divided a particular bandwidth for the RTS and CTS, ACK packet together using the hash codes that is unique for each communication .They designed a format for sending the request and receiving it in the form of: (Source name, destination name, hash code).

In this sample network connection is to be established between the 1 and 8 the node 1 sends the RTS message in form of (1, 8, 18) where the 1 and 8 are the source and destination node respectively and 18 is the hash code that will remain same for the whole communication.

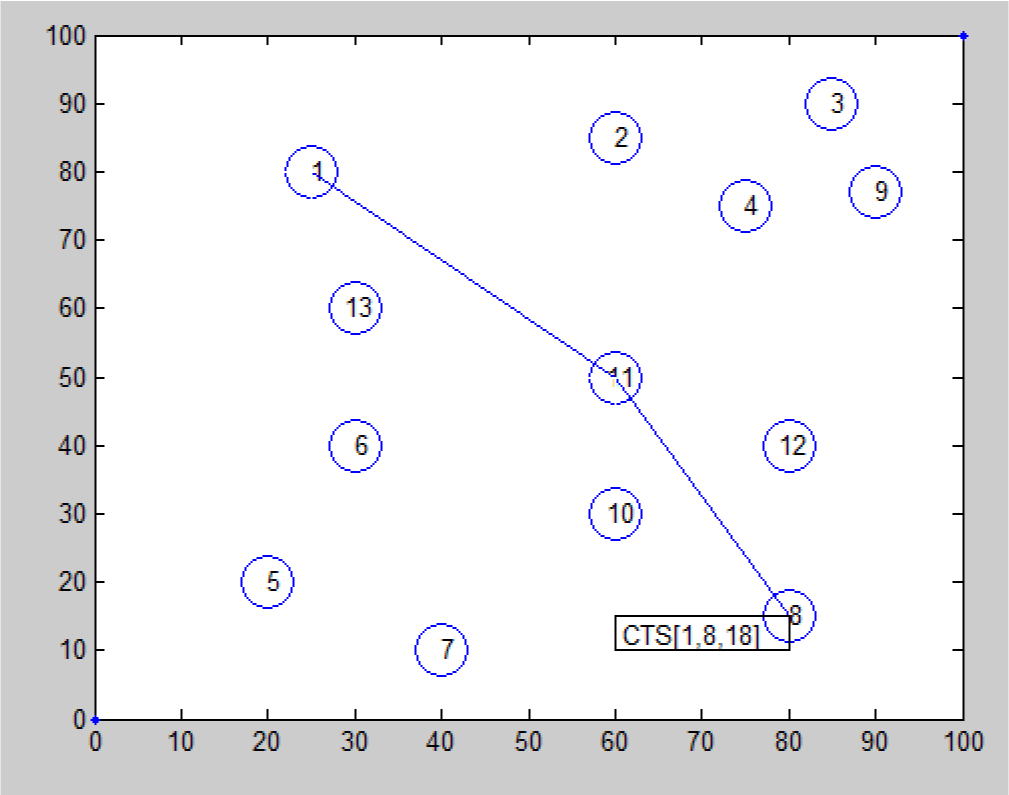


Figure 4.3 the sample network where the node 8 is sending CTS to 1

When the node 8 get an RTS request from node 1 if the node the node is free, is not involve d in any other communication then it will respond to the RTS message by the clear to send message .it will follow the same path that was chosen by the RTS message to send the request to send the CTS to the source node.

The message similarly contains the (source name, destination name, hash code) but the same problem prevails that if does not contain the id of the intermediate node though they are involve in the path of communication.

In the network of the CTS did not responded back in the time and meanwhile any other attacker send the CTS the source node will assume that it is send by the node 8 and the communication will stop so the response of CTS on time is very important for communication to be possible.

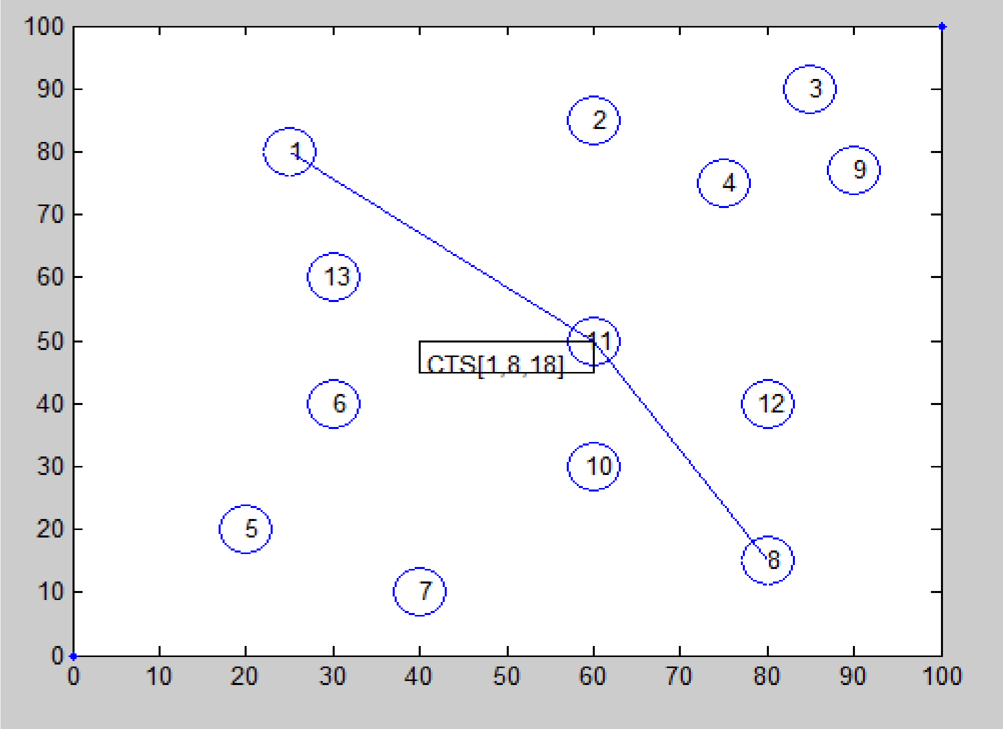


Figure 4.4 sample networks where CTS message from node is going back to source following the path.

The CTS message sent by the node 8 is going to the source node 1 following the path that was directed by the source node .They used the node 11 to reach the source node but I the node 11 is moved they do not have any path traced for node 11 that will make it difficult to communicate in distributed network. Moreover ,the time CTS is sending the attackers are in wait to send the identical CTS message so to have the data that is exchanging between the nodes or to stop the communication.

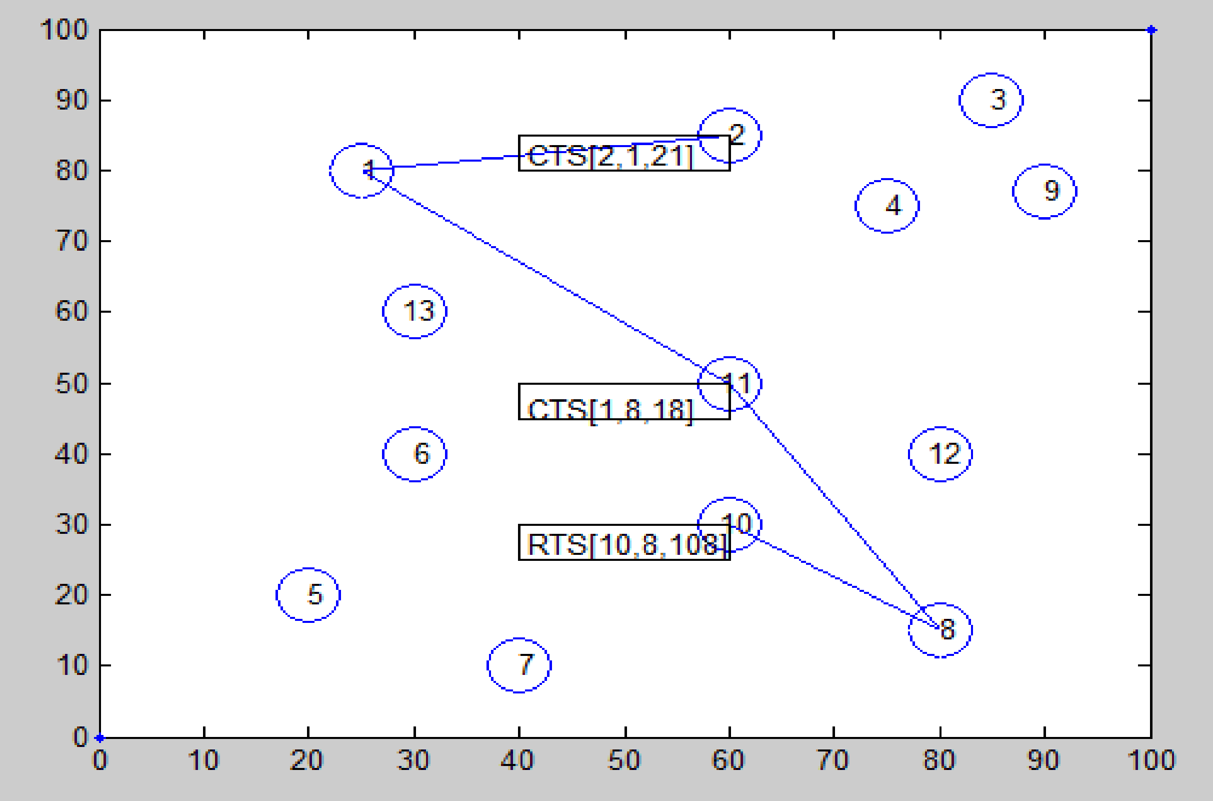


Figure 4.5 the sample network where the RTS and CTS attack occurred on node 1 an 8.

When the node sends the CTS packet to the source node the attackers try to attack to the source node as they want to manipulate or hack the data.

In this sample network node 2 (attacker) is sending a CTS attack on the node 1 similarly node 10 is sending the RTS attack .when this CTS attack is reached first the source node assumed that it is a response to the RTS packet sent to node 8 and it accept the CTS message as there is no path defined for the CTS packet.

This results in the attack to stop the communication as there is no vulnerabilities to attack taken by the ARMAC protocol as similar hash codes can be used be the attacker to intrude into the communication.

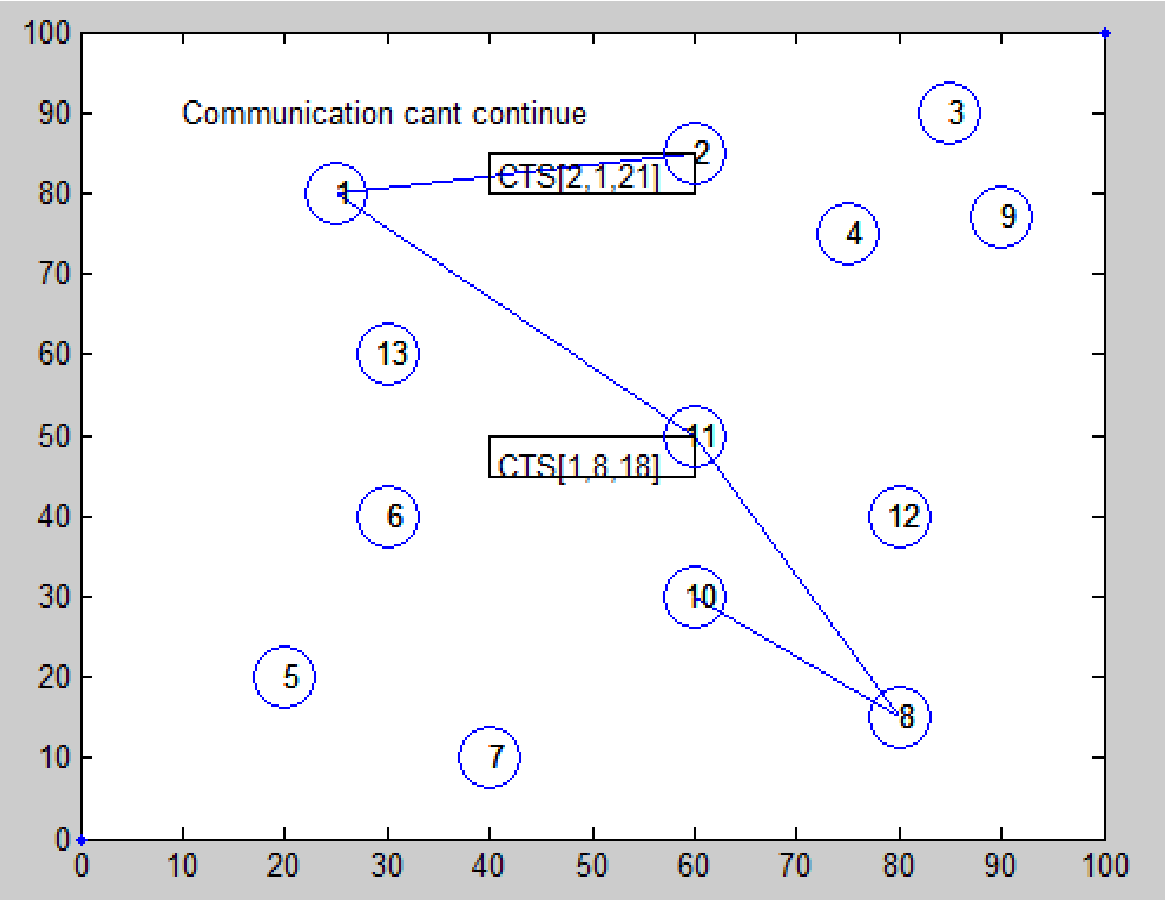


Figure 4.6 sample network where the communication cannot be continued due to attacks (CTS)

When the CTS message was responding back from the destination node any other node (2) attacked the node 1 with the same CTS message source node that do not have particular path to trace the authentication of the node accepts the node 2 request assuming the it is the node with whom the pair connection was requested.

So in this protocol the response for the CTS should be in a time frame to stop the attackers and continue the communication.

These simulations show that the communication between the nodes stops due to attackers and moreover it could also be stopped when the nodes moved from one place to another.

Moreover, the protocol have the habit of broadcasting the message to every other node that it is busy it consumes a lot of time ,power and results in collision of packet and packet overhead.

SRTS PRTOCOL SIMULATIONS: To observe the proposed methodology used for SRTS protocol we similarly created a sample networks as done in the case of ARMAC to check the working of protocol under same environment.

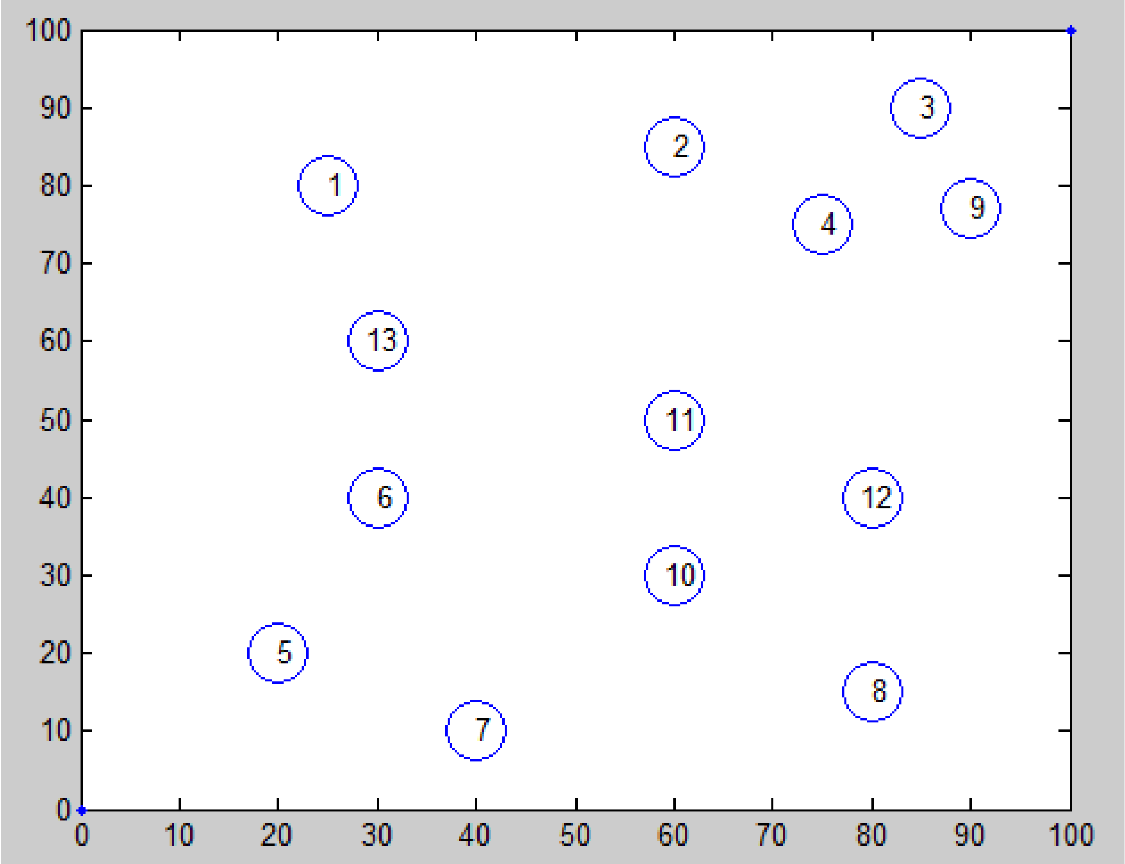


Figure 4.7 sample network.

This is the simulated network that is created on the tool that have some nodes designed in circles that have different transmission and carrier sense range. Communication between nodes was made using both the protocol on the same network to check the results of the performance.

When the SRTS protocol was simulated on the network that has different transmission range.

To establish a connection between the nodes with SRTS protocol under same environment in which the ARMAC worked we described the

Enter the source node1

Enter destination node 8

The packet of request from the source to the destination contains the id of the sender, receiver and intermediate together with the sequence number that is auto generated, so even if the intermediate node moved we will have the proper id of the node that can be traced .Moreover, the sequence number is auto generated then it will not help attackers as the sender and receiver know the whole path from where data is communicated together with sequence number

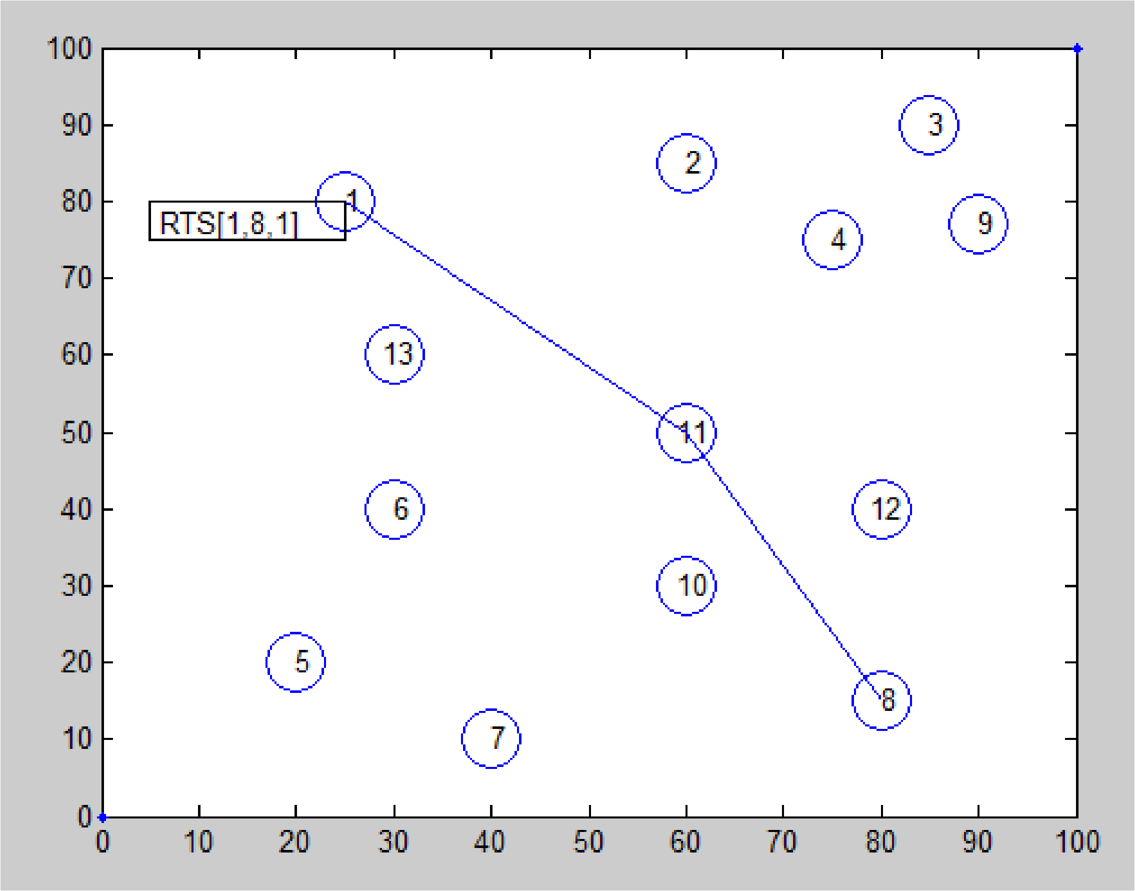


Figure 4.8 node 1 is sending the RTS to node 8

In the simulated network the nodes are trying to establishing connection with the node that is in the transmission range with each other or by communicating through the intermediate nodes in distributed networks.

Node 1 sends the request to pair message to the node 8 via the intermediate node 11.the format of the packet include the (source-id, intermediate –id, destination-id, sequence number) which contains the id of the whole path that is needed to be followed and as the sequence umber is auto generated each nodes knows what sequence number is on and respond accordingly.

When the node sends the request to pair it is the message that is send when to check that the particular node is free and wants to communicate to the other node .the RTS message in the SRTS protocol covers through the node 11 that is intermediate node to cover the communication in distributed network, even if the node11 is moved they message contains the id of the node so they can be traced to finally reach node 8 via node 11.

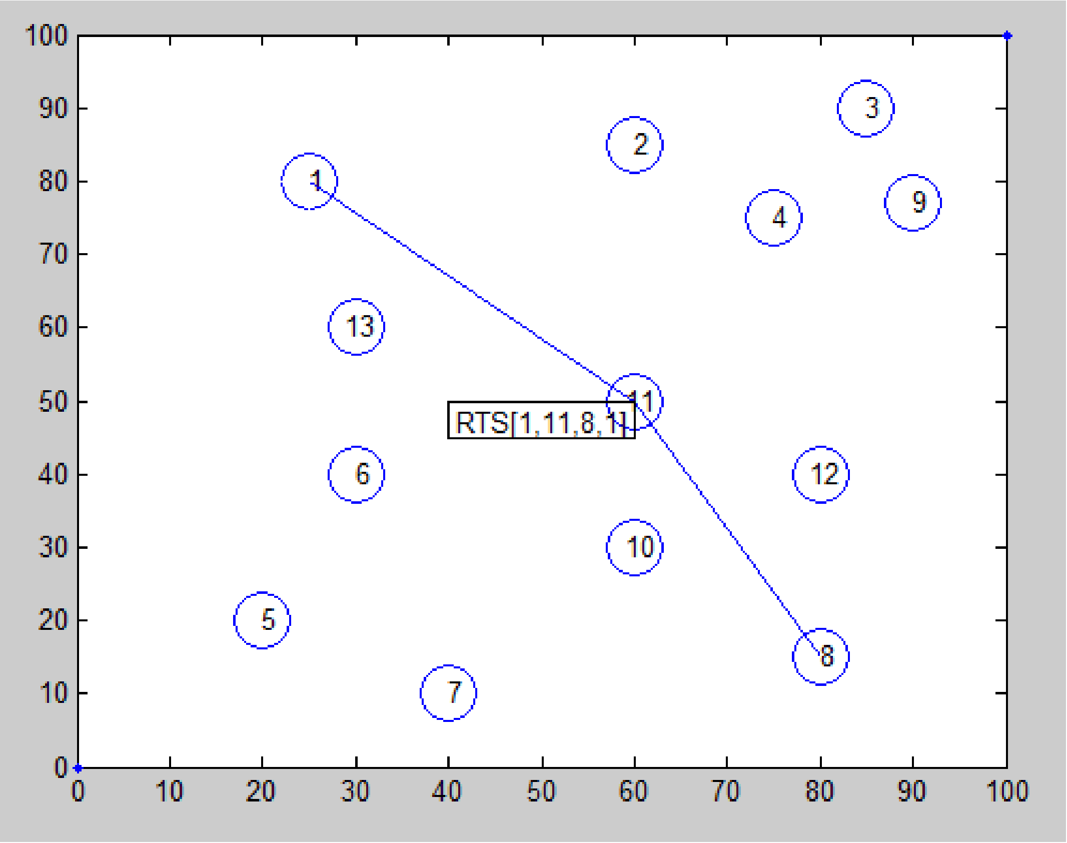


Figure 4.9 sample network where RTS is traversing through the intermediate node 11.

In the simulated network node 1 is trying to establishing the connection with the node 8 ,the message is traversing through the intermediate node to reach the node 8.

It contains the id of all the involved nodes with the sequence number to prevent the attacks that could occur to stop the communication as when the attacker will send the request the node will know the exact path with the sequence number that will not match so it will not respond to the packet (attacker).

Unlike the ARMAC protocol they do not divide the particular bandwidth to sending and receiving the packets as it limit the data carrying space .moreover, they do not broadcast the message of busy in communication to every other node of the range as it waste lot of time and power and results in high number of collisions.

Before starting the communication the SRTS protocol check the noise ratio of the network if some concurrent transmission is going on and if the SNR>60 then the adjacent nodes cannot communicate.

The node that is under communication blocks itself for the particular period of time when the communication is on and if the destination node does not respond back the timer is turned off and the node can communicate with other nodes.

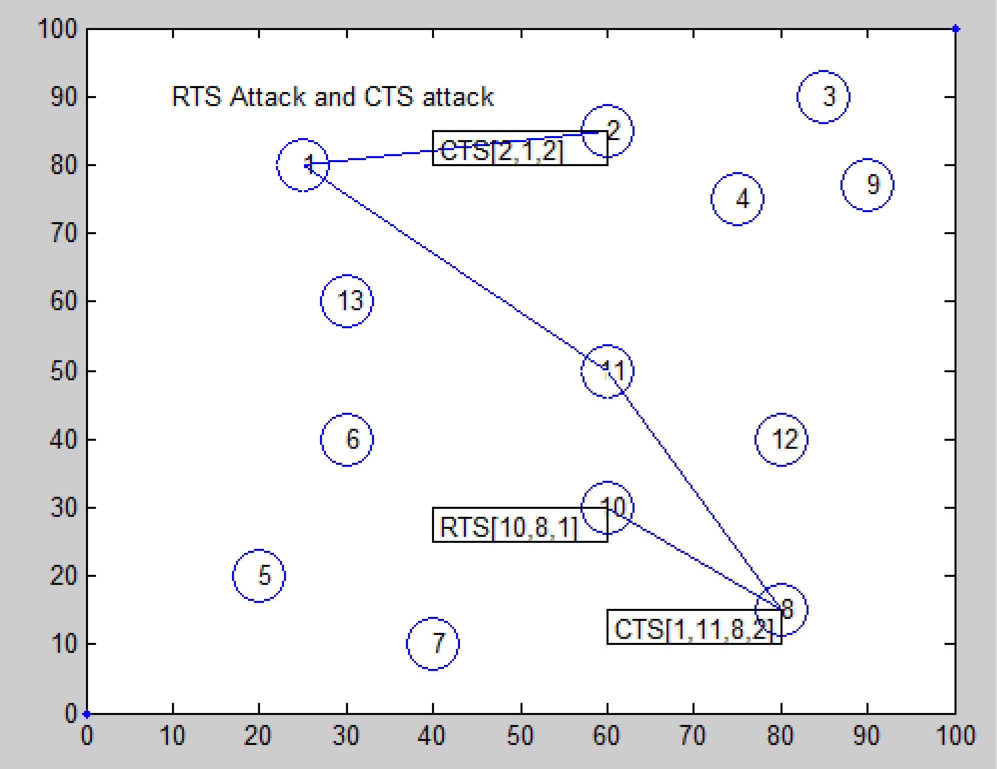


Figure4.10 node 8 is sending the CTS and node 2 and 10 are sending the CTS and RTS attacks

After receiving the request to send message from the source node 1 ,if the destination node is free and want to get involved in the communication respond to the message using the same clear to send message using the same path directed by the source node in the same format.

As it is clear the destination node 8 is responding to the message by the source node by sending the CTS using the same format of source-id, intermediate-id, destination-id, sequence number, but here the sequence number is turned into 2 as it is auto generated for the next level of communication.

When the node 8 is sending the CTS some other nodes (attackers) who want to stop the communication or manipulate the data also send the RTS Attack and CTS attack so that the source node assumes that this is the real message node and pair with that node, but as the path decided is known by both the nodes they cannot with their ids, so id any attacker will attack the node knows that this message do not contain the path ids together with the sequence number that it should contain so it will not respond to the attacker and remain blocked for them to continue the communication between the nodes.

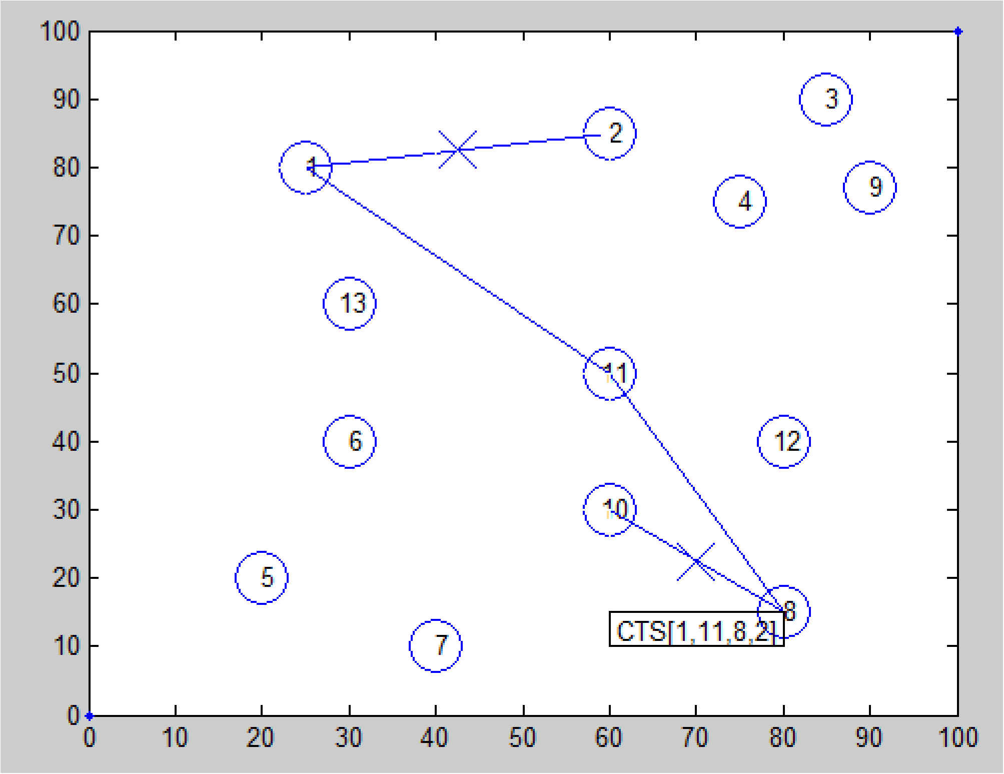


Figure 4.11 sample network where the attackers are blocked to continue the comunication.

When the node 8 is sending the CTS some other nodes (attackers) who want to stop the communication or manipulate the data also send the RTS Attack and CTS attack so that the source node assumes that this is the real message node and pair with that node, but as the path decided is known by both the nodes they cannot with their ids, so id any attacker will attack the node knows that this message do not contain the path ids together with the sequence number that it should contain so it will not respond to the attacker and remain blocked for them to continue the communication between the nodes.

It is clear feom the sample network that the nodes of the attackers node 2 and 10 is blocked by the nodes tat are in communication as they could not succeed in attacking the nodes as their path id and the sequence number did not match and was easy to identify that they are not the autthorised nodes .

In this way if any attack comes in front of communication they can be dealed and the ongoing transmission is not affected.

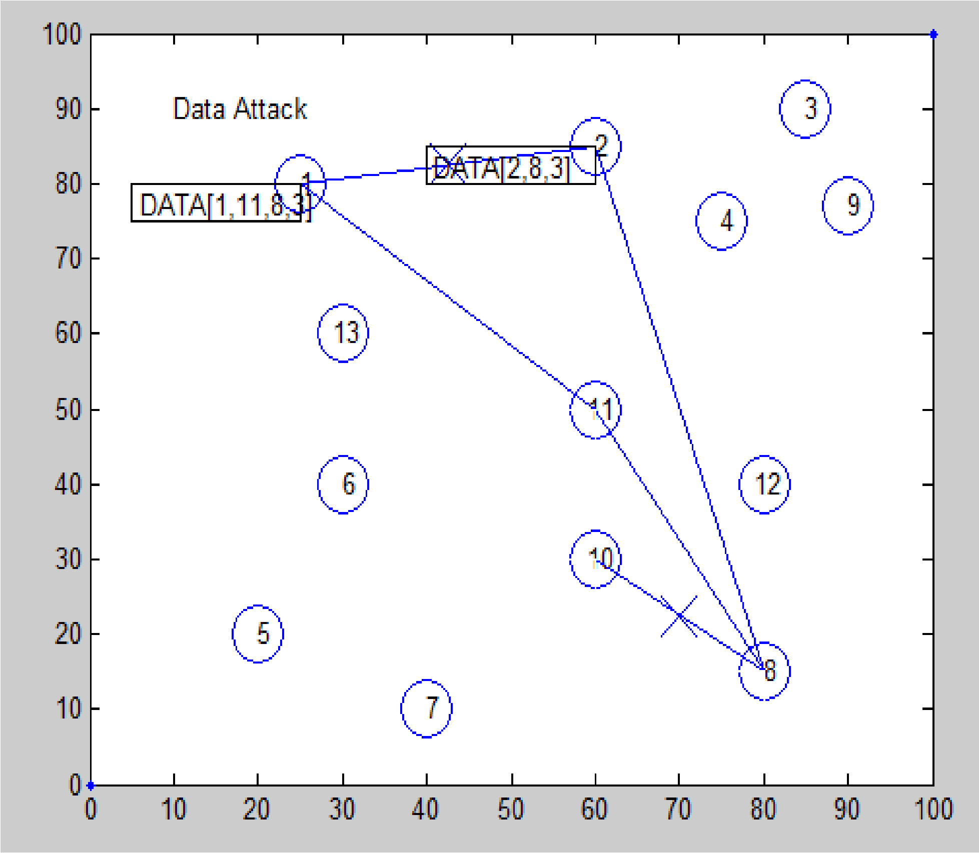


Figure 4.12 sample network where data attack is done on the nodes.

When the source node gets the CTS message from the destination node they start transmission of data between the nodes so again the data attack is done by some node so that they can access the transmission going but as similarly the path ids and the sequence number is not matching the nodes get it identified that they are not the authorized node and block them. In this way the data is sent to the transmitting nodes successfully without the data being manipulated

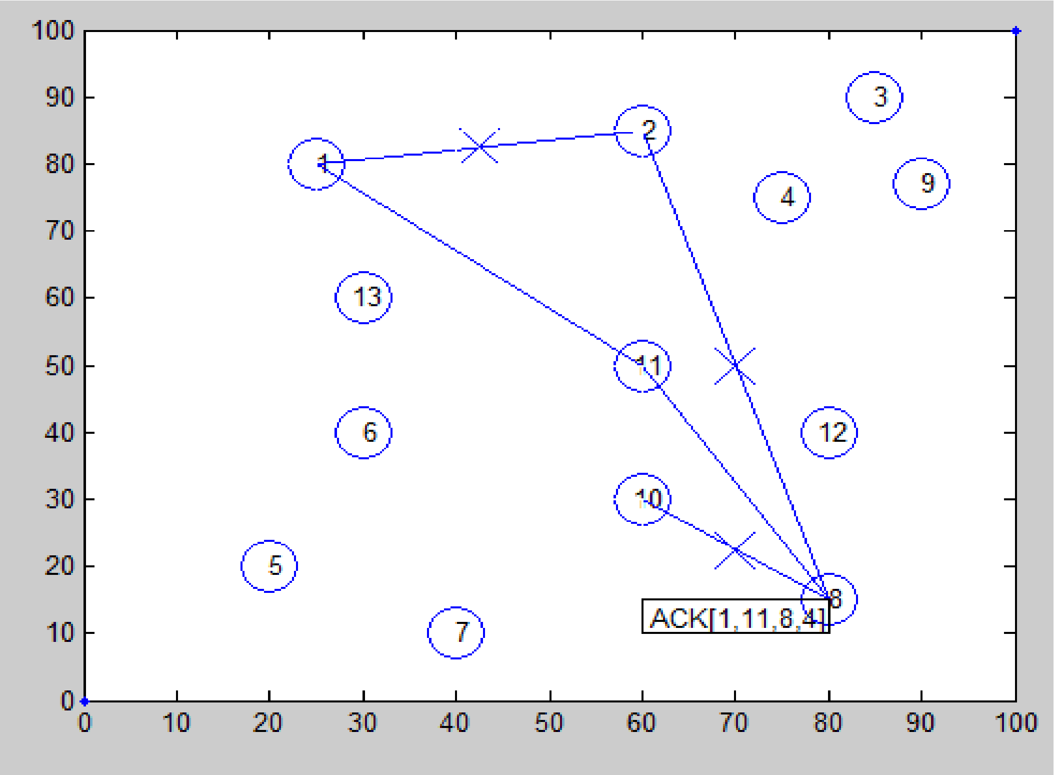


Figure 4.13 sample network where ACK message is sent by the destination node 8

When the data attack is blocked by the nodes the data is transmitted without any problem .The communication between the nodes being smooth and when the data is all transmitted to the destination node ,it reply to the source node with the ACK message to acknowledge him with the data being received.

In this way the whole process of communication is made possible in the SRTS protocol. They not only work on the transmission of nodes but also on the securing the connections from the RTS and CTS attacks.

Unlike the ARMAC protocol they do not have a habit of broadcasting the packet that helps to reduce the packet overhead and power consumption with no time wastage .The pattern of sequence number with the ids used by the nodes help them to secure the network from the attackers .

So when the attackers are dealt with the time the mechanism is completed on time and the attacks are resolved with low number of collision.

When the simulation worked on both the protocols there was different results for both the scenario they were:

1. **Time required during the mechanism:**

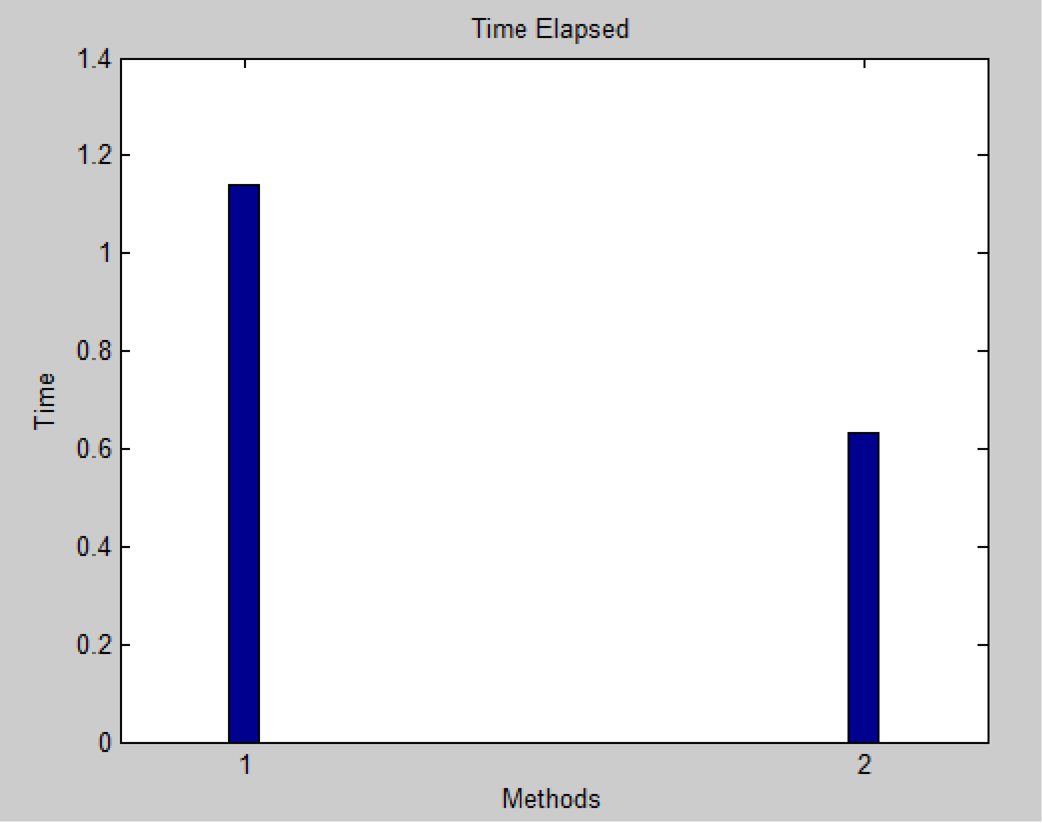


Figure 4.14 the time required for the communication between nodes.

The objectives of the SRTS protocol described that it will require less time as compare to the ARMAC protocol .Now it is shown in the figure that the time spent on transmitting the data between two nodes is less in the SRTS protocol(2) than in ARMAC protocol(1).

The reason of more time required in the ARNAC was that they used to broadcast the message before transmission to every other node before transmission to acknowledge them that they are involved in the transmission this lads to wastage of time moreover they did not considered the intermediate nodes due to their limitation to work on distributed network .but in the reverse SRTS protocol have no habit of transmitting the broadcast message as it blocks the node for the time of transmission so that no other node can communicate to that node. Moreover, they have defined a particular path that is needed to be followed for the transmission of data with includes the id of the sender, receiver, intermediate nodes together with the sequence number that is auto generated this leads to less time wastage in the transmission then in the ARMAC protocol.

2. **Packet Overhead:**

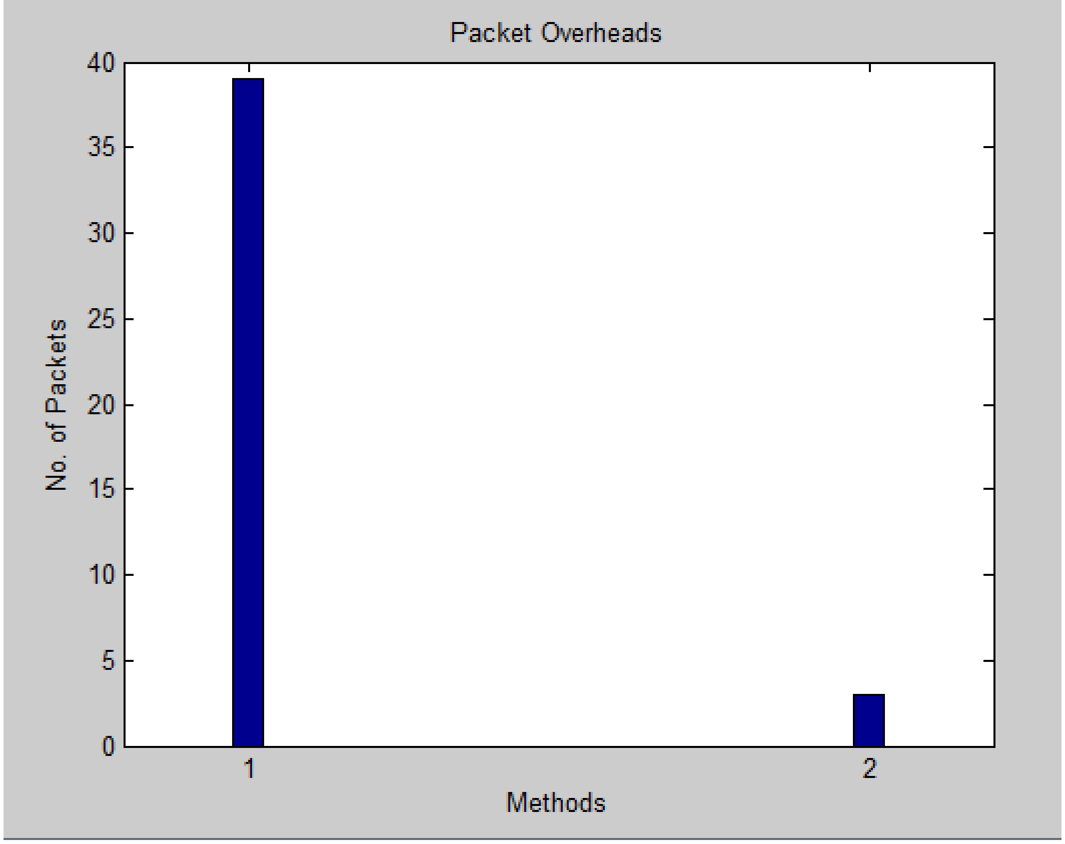


Figure 4.15 packet overheads

SRTS protocol promised to provide reduce number of packet overheads in the objectives and as shown in the above figure for the particular simulation created on the network the no of packet overheads is different for both the protocols. The ARMAC protocol has high number of packet overhead (1) than (2) in SRT protocol.

The number of packets generated in the particular time frame defines the packet overhead ,As we know that the ARMAC protocol have the habit of broadcasting of the message before transmission so he number of packets are generated to acknowledge every node together the transmission packets are also generated this results in huge number of packet generation that also results in more number collisions .But in the SRTS protocol they do not broadcast the message so the number of packet generation is low as only those packets are generated that are for the communication process and the packets generated are the resultant of the packets that are generated in the initial of transmission so the chance of packet overhead and the packet collision is very low.

3. Power consumption

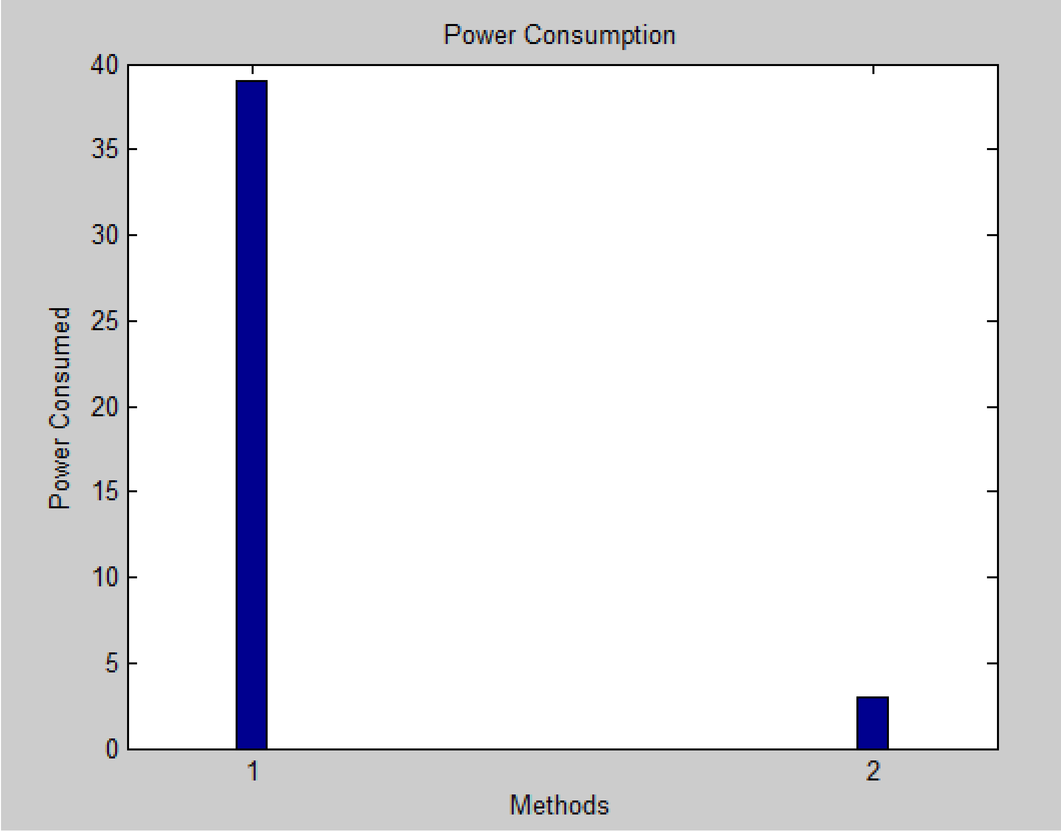


Figure 4.16 power consumption of the ARMAC (1) is more than SRTS (2)

When both the protocols were simulated using the same simulated environment than as the methodology described by both the protocols, The ARMAC protocol have the habit of broadcasting the packet of transmission to every other node that the node is busy ,a lot amount of power is wasted in sending the packets and in waiting for the response from the nodes .moreover they have described the bandwidth of each packet to send or receive so adjusting the message according to the given format also involves a lot of power. But in the SRTS protocol the methodology do not have the habit of broadcasting the packet as it blocks the node that is in communication so that if any other node tries to pair find the node block understand that it is busy in the communication ,this reduces the amount of power required that could e used in the transmission mechanism.

So it is shown in the figure that the power consumption is less in SRTS than ARMAC because of the specified reasons

4.COLLISIONS:

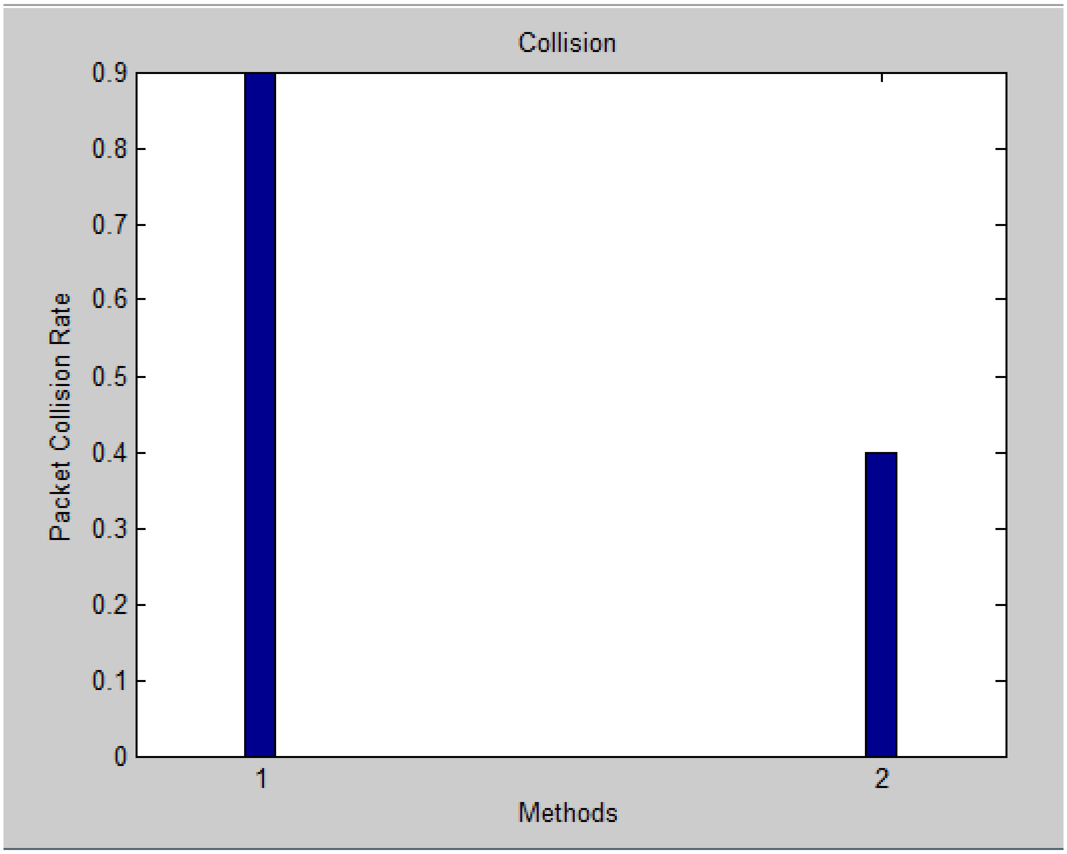


Figure 4.17 shows the packet collision rate is high in ARMAC (1) than in SRTS (2)

When in the simulated network the nodes try to establish the connection they send the packets for request and data packets that sometimes collide with each other or with the other packets of the nodes that are attacking or communicating with other nodes.

The reason of collision of packet may be high packet overhead ,reason of high rate of collisions in ARMAC is due to the reason of broadcasting of packet if the broadcast is done there are large number of packet generated and high number of packet is for the communicating parties that result in the collision of packet and data loss. But in the SRTS protocol the broadcast s not done and only the packets that are involved in the transmission are generated and even that are single sided and any attacker's nodes message is blocked so the collision rate is low as compared to the base protocol.

Thus, this is the result of high collisions in the network so the 1 have high collision rate than 2.

5.Successful completion:

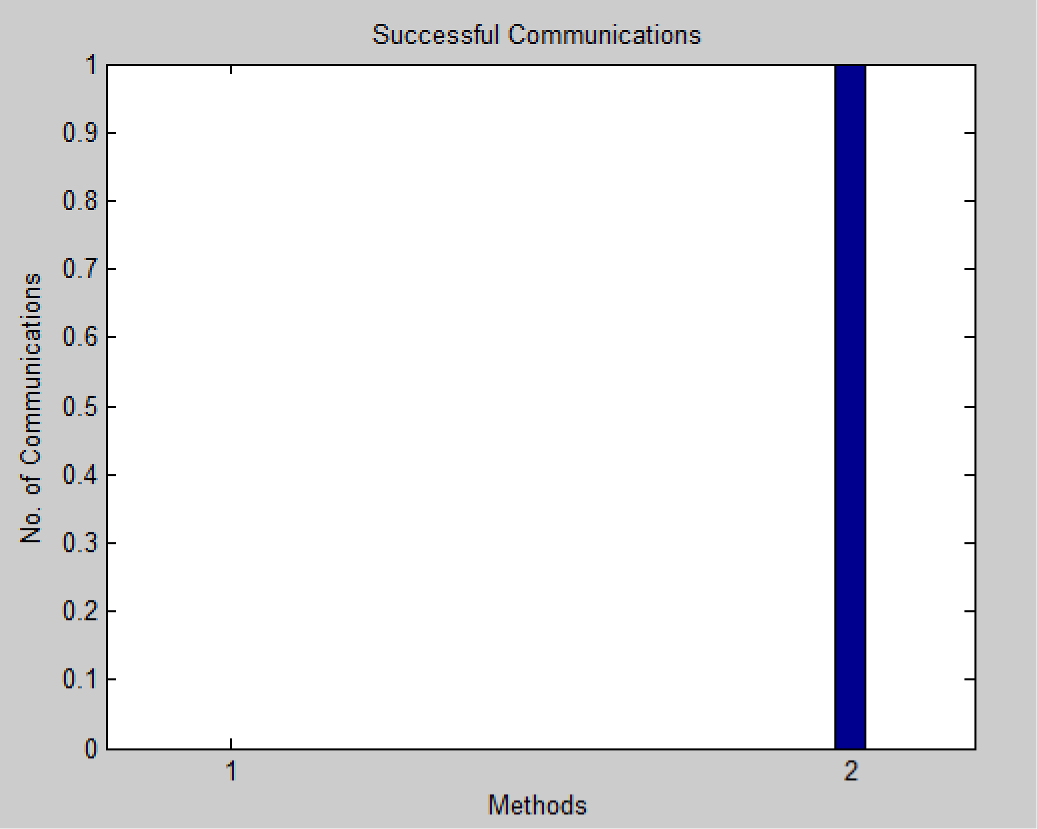


Figure 7.18 shows the number of successful communication between the two methods.

When the protocols were run on the simulated network with the described methodology the simulated environment contained many attacker node and complication to test both the protocols using the same scenario both the protocols worked according to their methodology that result in no successful completion in the ARMAC protocol as they could not handle the attack tat was tried to stop the communication and the attacker successes in stopping and manipulating the transmission this resulted in stopping the communication and no successful completion is there because the nodes paired could not complete the transfer. But in the SRTS protocol the attackers were resolved and that could not influence the ongoing transmission and the nodes paired and completed the transfer without any problem.

So the successful completion shows that the transmission is completed with smooth and problems got resolved in time so the ARMAC was not successful for the particular simulation than SRTS.

6. ACCURACY:

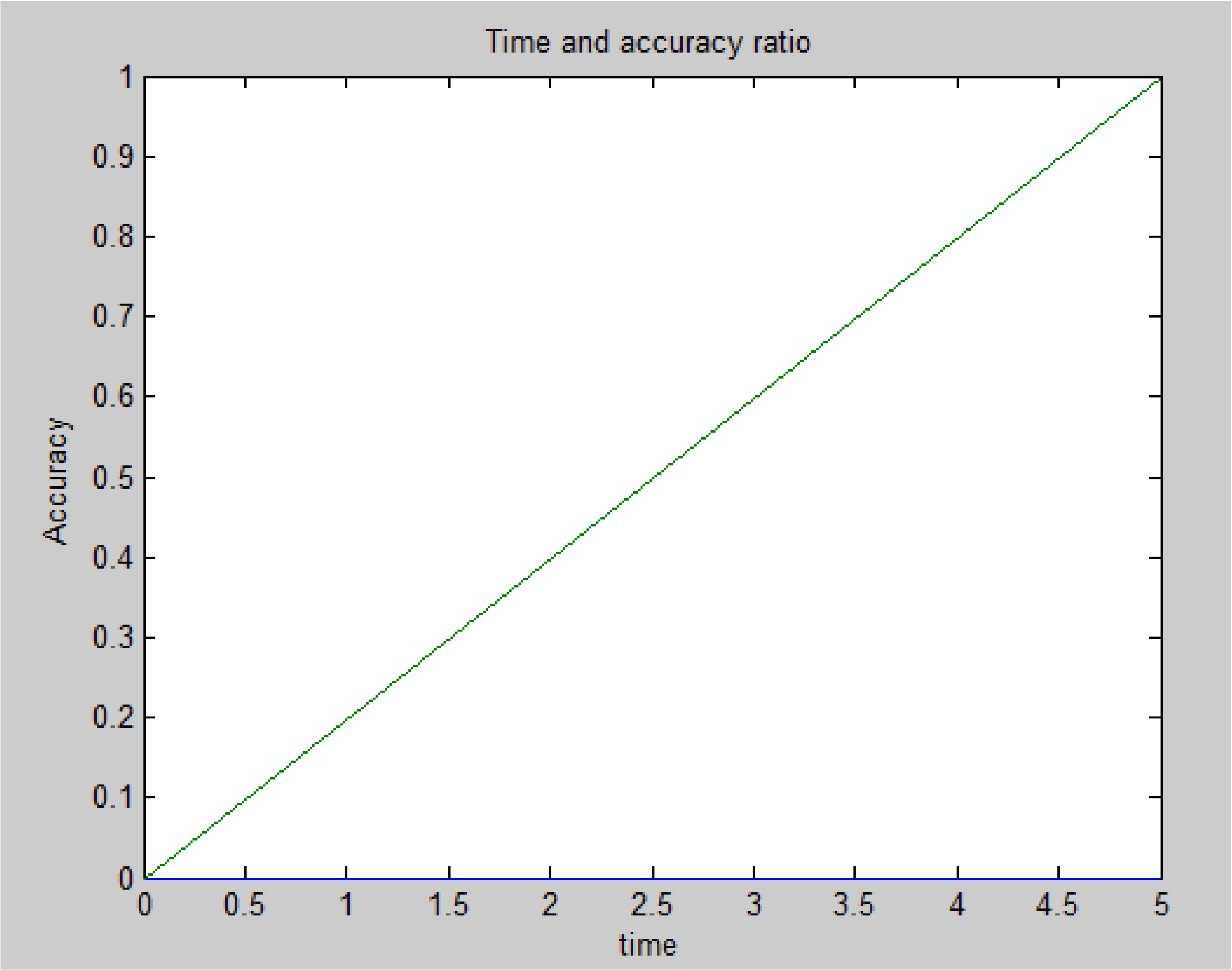


Figure 7.19 shows the time with accuracy ratio for the accuracy of methods

The accuracy of any protocol can be described when it is completed within the time frame with the defined methodology without any problem the SRTS protocol works with the full accuracy and it provide the successful communication within the time frame so that any problem is not do not stop the connection by resolving the attacks

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

The research proposed in this paper mainly focus on solving the hidden and exposed terminal problems by working on the limitation of ARMAC protocol that used attachment coding for resolving the problem to provide concurrent transmission.

The methodology defined in the paper will be efficient not only to resolve the problem of hidden and exposed node but will also work upon various attacks that occur during transmission The research work mainly focuses on solving the problem regarding many attacks which includes RTS/CTS attacks.

AR-MAC is very effective in solving Hidden Terminal and Exposed Terminal Problem but due to its limitations and problems which is stated in upper section changes are required. Few changes what is proposed to avoid all the limitations and fulfilling the objective are, first, RTS/CTS should contain the id of sender and receiver with a sequence number. Second, if there is any node send RTS or Received RTS should be blocked for other transmission till ACK is received. Third, RTS should all intermediate node ids in message packet and CTS should be responded back to same sequence. Fourth, always select the RTS with lowest Sequence. The procedure explained in this thesis work avoids during attacks and as the procedure does not have to broadcast messages the control packet transmission is limited and as limited packets power consumption and time also be limited. As the protocol restricts the individual nodes, it can work on any network without any restriction as the sequence number is auto-generated thereby solving the many attacks problem.

Though there are various protocols and mechanism researched so far for the solution of this problem but the RTS –CTS mechanism was the primary effort started by researchers so any progress in this area will not only make it more worthy for the solution of the problem but also defines an proficient way to resolve the problem considering the attacks that occur nowadays during transmission .So it uses the basic technique defined with more modification to provide better communication with no data loss and jamming. so the future scope lies that this protocol will help to provide the better communications in MANETS and with secure connection with no data loss. The future scope also includes that the methodology checks the SNR ratio before transmission so it does not allow if the SNR ratio of their adjacent nodes is more than 60 that provides an area for research to be done in future to provide adjacent nodes the privilege for concurrent transmission.

CHAPTER 6
REFERENCES

[1] D. Halperin, W. Hu, A. Sheth, D. Wetherall, “Predictable 802.11 Packet Delivery from Wireless Channel Measurements”, in ACMSIGCOMM, 2010.

[2] Viral V. Kapadia, Sudarshan N. Patel and Rutvij H. Jhaveri, “COMPARATIVE STUDY OF HIDDEN NODEPROBLEM AND SOLUTION USING DIFFERENT TECHNIQUES AND PROTOCOLS” JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617

[3] Caishi Huang , Chin-Tau Lea , Albert Kai-Sun Wong,” A joint solution for the hidden and exposed terminal problems in CSMA/CA wireless networks” in ELSEVIER,17 June, 2012.

[4] Lu Wang, Kaishun Wu,Mounir Hamdi, “Attached-RTS: Eliminating Exposed Terminal Problem in Wireless Networks” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,2012.

[5] Ms. Ritu Patidar, Prof. Dinesh Chandra Jain, “ Solving the Hidden Terminal problems Using Directional-Antenna Based MAC Protocol for Wireless Adhoc Networks” ijarcsse, Volume 2, Issue 5, May 2012.

[6] Alex Sherman, Jason Nieh, and Cliff Stein, “FairTorrent: Bringing Fairness to Peer-to-Peer Systems” Technical Report CUCS-029-08 May, 2008

[7] Ki Hong Kim, Daejeon, Korea, “Security Attack based on Control Packet Vulnerability in Cooperative Wireless Networks” The Ninth International Conference on Networking and Services 2013.

[8] Ketema Adere, Rammurthy, “Solving the Hidden and Exposed Terminal problems Using Directional-Antenna Based MAC Protocol for Wireless Sensor Networks” 7th International Conference on Wireless and Optical Communication Networks, Colombo(2010).

[9] Khaled H. Almotairi and Xuemin (Sherman) Shen, “Multichannel medium access control for adhoc wireless networks” WIRELESS COMMUNICATIONS AND MOBILE COMPUTING(2011).

[10] Liu Kai*, Xing Xiaoqin, “A New Exposed-terminal-free MAC Protocol for Multi-hop Wireless Networks” Chinese Journal of Aeronautics 22(2009) 285-292.

[11] Jissy Liz Jose, Jayasudha JS, Sabu M. Thampi, “Sybil Resilient Identity Distribution in P2P Networks” ICACCI, CHENNAI, India, '12, August 03 - 05 2012.

[12] IEEE 802.11 Standard. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.New York: IEEE, 1999.

[13] Liu K, Wong T, Li J, et al. Performance analysis of UPMA protocol for wireless multihop mobile ad hoc networks. Proc IEEE WCNC 2003. 2003; 971-976.

[14] CaiZ J Lu M, Wang X D. Channel access-based self-organized clustering in ad hoc networks. IEEETransactions on Mobile Computing 2003; 2(2): 102-113.

[15]] IEEE 802.11 Standard. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.New York: IEEE, 1999 [41] Tzamaloukas A, Garcia-Luna-Aceves J J. Channelhop- ping multiple access. Proc IEEE ICC 2000. 2000.415- 419.

[16] Chen J, Sheu S, Yang C. A new multichannel access protocol for IEEE 802.11 ad hoc wireless LANs.Proc IEEE PIMRC 2003. 2003; 2291-2296.

CHAPTER 7
APPENDIX (GLOSSARY OF TERMS)

This chapter of the report includes all the definitions of the terminology used in the research work so that a clear understanding of the concept is developed .Some of the important terminologies need to know before the definition of my problem are:

Request To Send: This is a request command sent by the terminal to another terminal before establishing the connection .This request clarify that the node is not busy and is interested in the pairing for communication, the respond for the pairing is giving by the CTS command to the other node to declare that the node is not busy and ready for communication.

This RTS process helps in establishing a smooth connection between the nodes and help to reduce the false blocking so that those nodes that are ideal can be paired for communication and also helps in solving the hidden node problem.

Clear To Send: This is respond command sent by the destination node to the source node in response to the RTS request sent by it. This command defines that the node is clear and is not involved in any other transmission.

After getting the response from the destination node, the source node sends a data packet for the transmission of data in this way the communication is established between two nodes by prior identification that nodes are free and interested for transmission; this is the mechanism of CSMA.

Data packet: This is the packet that contains the data for communication that is sent after the CTS command given by the destination node .Data packet is sent only after the secure connection is established between the nodes and the way of transfer between the nodes varies for different protocols. When data has to be transmitted, it is broken down into similar structures of data, which are reassembled to the original data chunk once they reach their destination.

Acknowledgment: This is a command sent by the destination node to acknowledge that it received all the data sent by the source node moreover it also describe that whole complete data is sent without any packet loss.

When this command is received by the source node it stop sending the packets and realize that data is sent to the destination.

Carrier Sense Multiple Access: This is the mechanism defined to resolve the hidden and exposed terminal problem .It includes all request to send, clear to send, data and acknowledge packet.

This mechanism used to sense the nodes before establishing the connection so the hidden problem do not occur and moreover the virtual jamming and false blocking is also not addressed while communication.

Cell: It is area in which the node can sense the other nodes for transmission. In wireless telephony, a cell is the geographical area covered by a cellular telephone transmitter. The transmitter facility itself is called the *cell site*. In Manets the cell range can vary from mile to twenty mile moreover it also depends upon the transmission range of the nodes.

ARMAC protocol: This is the protocol of the base paper that is chosen for the research work .The protocol works on the exposed nodes to provide the concurrent transmission by using the concept of attachment coding by diving the bandwidth of each RTS and CTS packet together with the hash-codes .The paper is efficient for the solving the problem using the basic RTS/CTS mechanism but they had various limitations that is addressed in this research work to make it more proficient to provide the solution of the problem.

S-RTS protocol: this is the protocol defined in the research work that works on the limitations of the ARMAC protocol moreover it also works on some criteria like security, time and performance. It is the modification of the ARMAC protocol so to provide better connection between the nodes with more security .Details of the protocol is explained in the objectives and research work covered.

Hidden node: The node is called hidden when they are not in the transmission range of each other and they cannot sense the other node .Because of this when they try to communicate to the same node they create collision of packet because they transmit at same time moreover as they are hidden to each other they do not know the reason of collision and they create the jam on the network.

Exposed node: the nodes are said to be exposed when the node is trying to communicate to the other node but they cannot because the node is in communication with other node or the nodes of the same cell are in communication that do not allow the concurrent transmission.

RTS Attacks: It is a kind of attack that is done on the node in which the attacker acts like a source node who tries to communicate by sending the false data packet or by intentionally blocking the node that is false blocking so that it cannot pair with any other node .It can also act as a node so the source node get confused from where the request are emerging and accept the request.

CTS Attack :It is a kind of attack in which the node send a CTS command to one of the source node that are trying to communicate so that the node accept the request and share the data with the unauthorized node .This is mainly done to stop the communication and even to manipulate the data sent between the two nodes.

Data attack: this attack is done when some other node that is not involved in the transmission tries to send the data to the destination data. As we know the data sent by the attacker is not valid so before the data from the true source nodes arrives the attacker send the data from false node so to corrupt the communication with invalid data transfer.

Acknowledgment attack: This is done when some other node (attacker) sends the acknowledge message to the source nodes declaring the data has been received so that source node can be acknowledge and stop sending data packets .This is done mainly o stop the transfer of data packets and to create a jam as the destination node is engaged and waiting for the data packet but the source node is acknowledged about data transfer is complete.