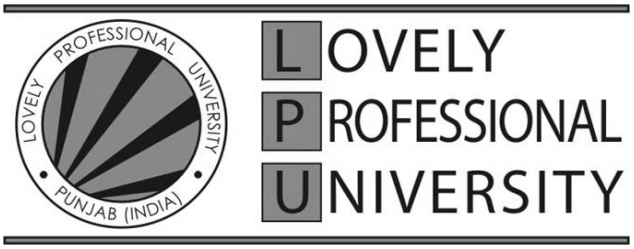

ENHANCED SECURITY PROTOCOL FOR RELIABLE DATA DELIVERY

A Dissertation submitted

By

TEDLAPU SRINIVASA RAO

To

Department of Computer Science

In partial fulfillment of the Requirement for the Award of the Degree of

Master of Technology in Computer Science & Engineering

Under the guidance of

Mr. Gagandeep Singh

(APRIL 2015)

PAC APPROVAL PAGE

LOVELY PROFESSIONAL UNIVERSITY

School of: Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the student	: TEDLAPU SRINIVASA RAO	Registration No	: 11304834
Batch	: 2013-2015	Roll No	: RK2306B41
Session	: 2014-2015	Parent Section	: K2306

Details of Supervisor:

Name	: Gagandeep Singh	Designation	: Assistant Professor
UID	: 17672	Qualification	: M.Tech
		Research Exp.	: 1 year

Specialization Area: Mobile ad hoc networks (pick from list of provided specialization areas by DAA)

Proposed Topics:-

1. Security Enhancement of Secure Protocol For Reliable Data Delivery (SPREAD)
2. Secure Reliable Multigrid Routing Protocol
3. Performance of reliability in tactical MANET

Signature of Supervisor

PAC Remarks: Topic 1 is approved. paper expected

25/9/14

10/10/14

APPROVAL OF PAC CHAIRMAN Signature: Date:

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

ABSTRACT

Here we are providing high secured concept to secure the data in the MANET environment to get the high confidentiality rate while transferring the data in the network. The Enhanced SPREAD is a concept of transforming the data into the network by dividing the secret message into multiple data parts by taking the help of secret sharing algorithms that are presented to provide High security to data by optimal encryption technique by using the advanced block cipher algorithm named as Blowfish algorithm. Here we are providing entire architecture and the three major issues that are presented in the MANET. Firstly how to get the data parts by using the secret sharing method. Then allocating the data shares onto each path should be in the optimal way so that security can be increased. Coming to the third issue, this depends on the routing protocol and multipath routing techniques in MANET.

CERTIFICATE

This is to certify that Tedlapu Srinivasa Rao has Completed M.Tech dissertation proposal titled **"ENHANCED SECURITY PROTOCOL FOR RELIABLE DATA DELIVERY"** under my guidance and supervision. To the best of my knowledge the present work is the result of his original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfilment of the conditions award of M.Tech Computer Science and Engineering.

Date: _____

Signature of Advisor

Name: _____

UID: _____

ACKNOWLEDGEMENT

I am very grateful to my project guide **Mr. Gagandeep Singh,** Asst. Prof. in Department of Computer Science & Technology, Lovely Professional University, for her extensive patience and guidance throughout my project work. Without his help i could not have completed my work successfully. I would like to thank **Mr. Dalwinder Singh**, Professor and Head, Department of Computer Science and Engineering, Lovely Professional University, for having provided the freedom to use all the facilities available in the department, especially the library. I would also like to thank my classmates for always being there whenever I needed help or moral support. Finally, I express my immense gratitude with pleasure to the other individuals who have either directly or indirectly contributed to my need at right time for the development and success of this work.

DECLARATION

I hereby declare that the dissertation proposal entitled, **E- SPREAD** 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: _____

Investigator
Regn. No._____

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

A Networking is a set of interconnected systems which are computers or mobile devices that are used to communicate one with each other. From the past few years networking is playing a very important role for the communication purpose. The person from one place can easily communicate with the other person or the group of persons within the single point of time from the local location to global location. The range, speed and efficiency of the networking are increasing day-by-day. There are many type of networks are presented like peer-to-peer network, client – server network. There are many hardware devices are present in the networking to transfer our communication from one place to other place those devices are like switches, hubs, buses router, wireless base stations and many.

There are many kinds of networks are presented in the networking those are mentioned below.

- Local area network, Control area network, Wireless local area network, Wide area network, Metropolitan area network.

The networks, which are mentioned above are deals with many forms like local, globally, with in the particular range and also in the storage devises. But in the present days the networkers are totally concentrating on wireless.

MANET (MOBILE Ad-hoc NETWORK)

MANET the name which implies that Mobile ad hoc network, which is received tremendous growth or importance from the past few years. The very fast and optimal rapid changing topology keeps the MANET in very attractive, tactical. This is also used in the military applications. Here in the MANET there is no fixed infrastructure is available, the reliability is also a one issue in MANET. There are some specific functions should be available in the MANET like the establishment of the network should be fast, must provide good security to the communication and self reconfiguration. On the other side, there are some hidden characteristics of a MANET are present, those are the broadcast nature that means only one sender and many receivers of the wireless channel which means that only one sender sends the message and all the remaining people which are accessing the network at that time can receive that message, the infrastructure less

architecture this is like no particular architecture is going to present this architecture changes by the region, the very high forms of network topology which may sense that the network topology must be in dynamic nature, and the resources of mobile device must be limited and also many new goals are presented in the MANET.

Keeping the fixed access point or fixed sources and backbone infrastructure is not always possible. This says that there is no fixed point communication is done at all the time this may varies from the topology from one region to the other region.

- The communication between the people in war zone possibly will not there.
- The communication between the two mobile devices such as like a Bluetooth will not be there because this device only ranges for 10 meters.

Applications:

Mobile ad hoc network has some different applications in the different fields such as like.

- Personal Area Networking (PAN).

  Example: cell phones, laptops.
- Military Environments (ME).

  Example: soldiers, planes, tanks.
- Civilian Environments (CE).

  Example: sports stadiums, meeting rooms, boats.
- Emergency operations (EO).

  Example: fire fighting, search-and-rescue policing.

Issues in MANET:

Secure data transformation of the data from one point to another point which means nodes, is a basic service in a mobile ad-hoc network. It is also a basic requirement in any network. Sensitive information which is important information like military information, transmitted across a mobile ad hoc network must be protected from attacks like denial of service; replication and eaves dropping these attacks are known as passive. Due to high broadcast nature the protection for eaves droppers is very difficult task. Data confidentiality is achieved by cryptography. From the cryptographic methods which are

providing security to the information are mostly relay upon the safe, secure, consistent key management system which means reliable.

Within the highly dynamic MANET that covers large region and which consists many nodes. If the node number is increased in the network which are currently participating in the network or large, then end-to-end or peer-to peer encryption is very difficult as for peer-to-peer authentication and the reliability becomes very less by changing the of dynamic session key. Up to now there is no particular key management system (KMS) is available which is must secure and trusted in MANET.

There is huge problem or we can also say it as risk that is comes from the compromised or handled nodes in a Mobile ad-hoc network. The information is going to be collected from the compromised nodes inactively that means not directly. They may also compromised by active attacks those are direct attacks, modification of message, reply attack, message duplication, changing the content of forwarded packets, halting the service, jamming the traffic or simply selectively throwing away important packets from the network.

CHAPTER 2
REVIEW OF LITERATURE

Jain Liu, 2001 In this paper the author described about the ATCP that is TCP (Transmission Control Protocol) for MANET. The Connections in Wireless Ad hoc network causes High bit rate errors, route changes frequently and portioning of data. If we use TCP (Transmission Control Protocol) on this type of Networks the Through of these connections is going to be very poor because Transmission Control Protocol gives lost Acknowledgements or Delayed Acknowledgements due to Congestion to recover this we use thin layer between Standard TCP and Internet Protocol that recovers the above problem and maintains high peer-to-peer TCP throughput. Primary goal to design an ATCP is to correct the problem running in TCP above multihop wireless networks. To solve this problem we have to design a protocol.

The protocol should follow the below characteristics.

- To setup the connections in the ad-hoc network we have to improve the performance of the TCP
  - With a high bit error rate.
  - Delays due to Route Re-computation
  - Transient Partition
- Keeps TCP's congestion control performance.
- Appropriate CWND Behavior.
- Keeps peer-to-peer TCP Semantics.
- Compatible with Standard TCP.

Mihir Bellare, 2002: In this paper the author described about the CBC algorithm and the use of the initialization vector and encryption and the decryption techniques of cipher block chaining algorithm. The organization named as IBM is introduced the block cipher encryption algorithm named as Cipher Block chaining. Initialization vector (IV) this is generally used in cryptography. We can also call the initialization vector as Stealing variable (SV), which is a fixed sized input data that is used in cryptography. This is generally generated from the random numbers or pseudo random number generator which is generally related between the segments and the data which is encrypted. Generally the

CBC is deals with the blocks of the message, which is in the sense the message is divided into number of blocks and each clock is separated by the numbering. Later performing the XOR operation between first block of the data message and initialization vector (IV). After completion of the XOR operation between the first block of the data message and initialization vector then it will generate some encrypted data. The generated encrypted data is appended by the key and performs the block cipher encryption. Once the encryption of the first block is completed then it will generates cipher text. The generated cipher text act as initialization vector to the second block plain text, that is the plain text of the second block and generated cipher text are going to perform XOR operation. The Decryption of the CBC takes exactly reverse procedure to decrypt the cipher text and to get the original plain text.

R. Stoleru, H. Wu, 2011 From this paper the author described that, the discovery of a neighbor in wireless ad-hoc network is a very key part of many protocols, as well as routing and localization. The networks which are affected by relay attacks those are pass on attacks, are also known as wormholes, the worm hole may selectively deny communication. In this paper the author proposed about MSND (Mobile Secure Neighbor Discovery) which measures the security against wormholes for the neighbor nodes by allowing participation of mobile nodes to securely determine. MSDN gives the concept of the graph inflexibility for detection of wormhole. In this paper, we have to care about intruders; they can attack to our communication. More attackers can form a group to record the communication at the bit level or packet level. After if they use this communication somewhere else. Wormholes may disturb communications, include localization errors. This may causes to packet dropping, selectively or DoS.

This paper also includes the concepts of

- A MSND protocol to identify the occurrence of wormholes, when the participation transforming nodes take place.
- Analysis of Security & Correctness of MSND.
- Performance can be estimate by using simulators, with low false negatives the particular wormhole can be detected.
- A true system assessment Epic mote is employed and creates hardware for robot, says the act of our future answers.

SND manages a range of technologies and techniques. This paper consists of many real world example issues finding various attacks or errors to detection of neighbor. Those are location solutions, Time based solutions, Time & location Protocols, and finally Geometry-based answers. MSDN mainly have two algorithms to protect from wormholes those are Wormhole protocol algorithm and other is verification which is preliminary check, metric multi dimensional scaling (MDS). Form this paper finally the author concludes that, the capability to decide valid neighbors securely is a significant area for different networks. The network which contains the wormholes, are failure to protect discovery of the neighbor and they may also leads to data lost, or wrong destination, problems in routing and management over the network at any cost of time. Denial of Service attacks may also possible.

Nicklas Beijar, 2011 In this paper the author described about, The ZRP (zone routing protocol) is basically a route discovery protocol, that is considering and mixes both the benefits of proactive routing protocol and reactive routing protocol approaches to maintain the topological map which is in the up to date manner that means time to time for the small network which was named as a zone, which is presented as origin on every node and within the small network called as zone. The architecture of ZRP contains three sub protocols. In the zone routing protocol we are going to concentrate on the important issues of choosing an optimal zone radius. There are two algorithms presented to find the zone radius in the ZRP. This Zone Routing Protocol (ZRP) mainly targets to find the optimal route in bulky ad hoc networks with high mobility. To go in to deep discussion about this paper we have to know about the Two Routing protocols those are, one is proactive and second is reactive routing protocol.

The proactive protocol (PRP) is used to remain an up to date topological information in the form map for the entire network, with this information we came to know about route and without delay in time should be available when packet need to be sent. The wired IP networks usually use this method for example within the Open Shortest Path First. This proactive routing uses a large bandwidth to remain routing information up to date or time to time within the table.

When compared to the PRP protocol, the reactive protocol (RRP) will not going to apply continuously to find the network connectivity. The Reactive routing protocol uses a route finding process is invoke on demand when the message packet wants to be send.

This routing protocol is used in the DSR. This Reactive routing search procedure may involve most important to maintain traffic due to total flooding. We can also call this as source on demand driven.

Coming to the zone routing protocol (ZRP) this is mainly targets to tackle the troubles by combining the best advantage of both protocol those are PRP and RRP. Basically in an Ad hoc network, the assumption is the nearby nodes will take the major part of the traffic or with minimum distanced nodes, this means avoiding the traffic for nearby nodes. To do this ZRP reducing the proactive capacity for a zone that is origin on every node. Because of this routing information maintenance or the map is easier in a small network that we can also say it as zone.

The ZRP (Zone Routing Protocol) the name says that, this is totally based upon the concept of zones which means small networks with some nodes. The routing zone is maintained for each and every node discretely and the network of adjacent nodes integrates or can be related. The zone is always maintained by its radius which is denoted by “R”. This is expressed in the terms of intermediate nodes or the hops. The zone which includes the nodes that, whose distance is from the node in issue, is at most “R” hops.

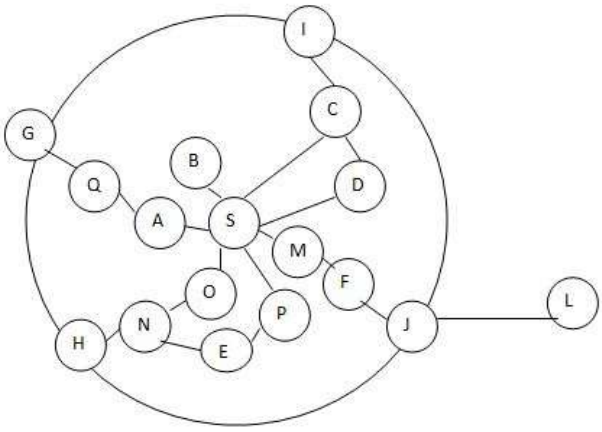

Figure 2.1: Example of Routing zone with R=3.

The nodes of the zone are mainly separated into two types those are peripheral nodes and interior nodes. Peripheral nodes are nodes which have the same distance from the central node to the zone radius “R”. If the distance from the central node is less than the radius “R” then we called those nodes as Interior nodes. In the above diagram the peripheral nodes G, I, H, J and the interior nodes are A-P also the node L presented in the diagram but it is presented away from the routing zone. In the above diagram H can be

reached in the two ways one is with the length 3 from S and other is with the length 4 from S. The node is H presented in the zone, because the shortest distance equal to the zone radius "R" i.e., 3. By adjusting the transmission power of the nodes we can synchronize the number of number of nodes in the routing zone. Decreasing the power, reduces the number of nodes within zone that can reach directly, reverse process is also possible.

Ankur Lal, 2012 In this paper the author performed an evaluation technique for the protocols AODV, DSDV, DSR and said that how the MANET is reliable. There are many routing protocols are presented to find the route in the MANET which are different in their designing because this is a random topology.

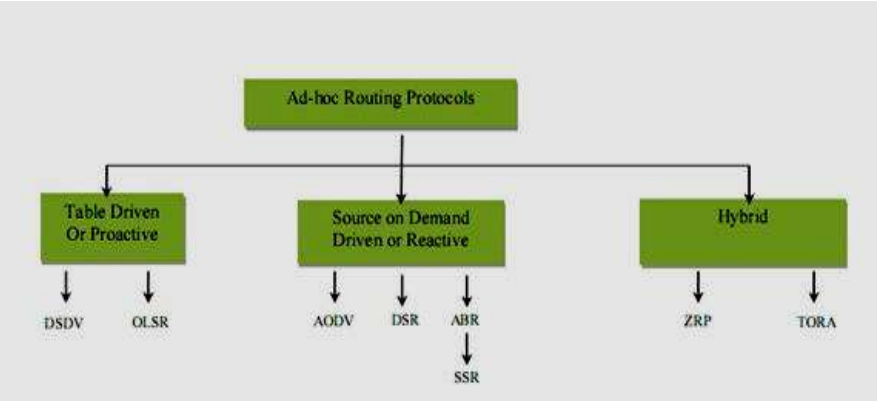

Figure 2.2. Clasiffiction of Ad-hoc routing protocols

The routing protocols mainly depend upon the two routing protocols those are PRP (proactive protocol) and RRP (reactive protocol). The PRP protocol is also known as table-driven routing protocol. In this PRP protocol every node has single table or more than single tables that contains or maintain the most recent data about the routes to several nodes that presented in network. Every row contains a next node to reach a subnet and it also gives the total cost for the route. All the routing information is stored in the table depending up on the routing data which was updated at every routing table. The routing protocol keep many of the tables which makes further overhead in the table that was routed and takes more bandwidth for example DSDV.

On the other side the routing protocols are as well as depend upon the On-demand routing protocol which is also called as reactive protocols. This protocol does not keep or continuously updates their route tables with the most recent route topology. This is lazy

protocol to approach the route. If any node desires to send a data packet to another selected node, for this the protocol initially looks for the path and then establishes a connection to send the packets and to receive the packets. Some examples for the reactive routing protocols are DSR and AODV.

In this paper firstly the author considered about the DSDV routing protocol. DSDV routing protocol is a PRP scheme that means which maintains the tables based upon the Bellman Ford algorithm (BFA) the major aim to handle the problem in the routing loop that is presented in the BFA. The DSDV using the both periodic routing updates and the updated information about routing is triggered to keep the table uniformly. Nodes may contain the busted links, when they are traveling from one place to another place. In this protocol when a node receives unlimited metric, it contains an identical or latest ordered numbers which we called as sequence with a fixed triggered metric which finds a route bring up to date broadcast, and the route which has a infinity metric is rapidly replace the new path. If any node gets a route with updated packet then it compares to the data which is already available in the form tables, now this tables are going to be updated based upon the new data with particular form.

Another routing protocol in this paper is. The AODV is comes below the RRP, if one existed node utilizes the path to communicate with the another selected node, then each and every node must contain the address of the selected node and distance to the selected node which the nodes entered in the routing table. To begin the process to discovery of the route a route creates an RReq (route request). This algorithm is also uses the RRep (route reply), which is used to sets up the overturn the entry of the path for the source node in its path table. This AODV totally depends upon the three factors those are RReq (route requests), RRep (route replies) and RErr (route errors).

The third routing protocol in this paper is that DSR. This is much demanded, which reduce the bandwidth this routing protocol is used especially in this situation where the transformation is low. This DSR has 2 phases those are the route request and route preservation. In this if node want to communicate with the other firstly searches for the route, if the route is already exists to the destination then it starts communication by appending the packet to the next node, otherwise the source node sends the route request message to the next with the destination IP and forms the route by looking own caches. The DSR can sustain relatively quick rate of mobility.

Finally the author performed some evaluation and concludes that the AODV routing protocol has a relatively stable throughput, for the fast change in the network topology the AODV is more preferable routing protocol. The DSDV gives the best goodput and the routing load is very less. This DSDV is more preferable if the count of nodes is very less in network and the mobility is slow or steady. The DSR routing protocol gives a good and very high throughput. This is basically deals with less number or less sized data packets. We can find many fluctuations in the throughput curve which was not preferable in wireless networks.

Wenjing Lou, 2012 In this paper the author described about the new security technology which improves the security in the MANET by multipath routing scheme. This technology is named as SPREAD, which means secure protocol for reliable data delivery. The main aim of this paper is to transform a secret message into multiple parts which may be in bits or packets, and then we have deliver these parts of message through different paths to the targeted node, if some number of data parts are hacked or observed b the intruder, the full message is not going to be revealed from the small data parts of the message which are sent by the sender.

For this paper the author discussed about the architecture of the SPREAD and appropriate design issues to handle the secure protocol, the arithmetic and mathematical model for making and rebuilding of the secret parts of the message, the best allocation to the data parts or in dealing the security issues the data parts are go through the multiple routes and the techniques to discover the multipath route in the network. There are two major techniques in the SPREAD those are multi-route routing and distribution of the secret message. Assume that nodes which want to send a secret data to the destination node that is several hops left which means that many nodes were presented between two nodes.

The author mainly targets to that how to design the idea of the SPREAD and how to develop a security enrichment protocol to send the message securely which also termed as data delivery service in MANET. We are going to concentrate on the three major design issues of this paper those are, how to partition the data into several pieces or parts, and how these parts of message are placed in each path in the network, and finally how can we choose the multiple ways in the network. The fundamental design of the SPREAD paper comes from the subsequent observations, if there is messenger which takes the

entire data from one place to the other place across a network region. If third party who is unauthorized person hacked the message, while the message improved fully by the participants or observers or intruders if many communications are deployed, each node only carries the part of the data and takes different ways across the network. In this system, we use the threshold underground algorithm for distribution to partition the data into number pieces or parts. By the (T, N) distribution scheme for secrecy, the secret data can be capable of dividing into "N" number of pieces which we called as data parts, and to conciliation the data, the intruder have to hack minimum "T" parts of the data. With less than the "T" parts, the intruder will not get anything information about the secret data and has no good way to get secret by the intruder, who will not get anything forever about the message which we are sending. The second aim is that how to allocate the parts of the data into every chosen way, so that the intruder has very less possibility to allowance the data. The third aim is the multi-path routing it says that how to discover the preferred number of ways in a MANET and how to send the parts to the targeted node by means of these ways? This a very big challenge in MANET to route and send the data from one node to the desired node because the nodes are able to move from one location to the other location and the network topology can modify continuously from time to time by the behavior of nodes, dramatically, and unpredictably. The secret sharing system of "N" of pieces and "T" parts is given in the methodology diagram.

In this paper we will transfer some data file from one node to another node. The system will generate the packets and transfer those packets to destination with the help of the internal nodes in the MANET. The system checks whether all the packets are transferred to the destination or not if the packets are successfully transferred to the network then system will shows some message and the data will store in the Destination node. If there is any path disturbance occurs then system automatically choose alternative path and transfer the data to the destination node.

Hani Q.R. Al-Zoubi, 2012 From this paper the author concludes that how analysis performance for the effect of MHL in dynamic source routing (DSR). DSR in the MANET is going to be analyzed for the performance. The effect of MHL (maximum header length) on a selected performance matrix was studied for different DSR network. The matrix may include or involved that the average peer-to-peer delay, the number of dropped packets and also the average packet size. While keeping the optimum network

performance result is showed for the possibility of selecting dynamic value of MHL. This is depends upon many factors or parameters like number of nodes, network diameter and transmission range for the nodes. In this paper they applied many formulas and simulators for the above parameters to analyze performance of DSR by the effect of maximum heard length. Finally the author concludes that it was possible to select dynamic values of MHL without harming the overall network throughput. As usual the overall network throughput depends upon the number of nodes, network diameter and transmission range for the nodes however all these parameters should decided by the network administrator.

Marjan Kuchaki Rafsanjani, 2012 From this Paper the author described that how to improve public key management which was self organized in the MANET. Managing of the key in the MANET is the fundamental problem in now days, because lots of intruders are present to hack the communication between the two parties. This paper mainly deals with the comparison between certification based authentications between the two nodes. There are some requirements for this approach that is for efficient authentication which is certificate based for mobile ad hoc networks. Those necessities are given below.

- Distributed authentication
- Resource awareness
- Efficient Certificate management mechanism
- Heterogeneous certification
- Robust pre-authentication mechanism

Finally this paper concludes that self organized public key management scheme is merge them to describe necessities of efficient certificate based authentication for ad hoc network and also to improve efficiency. In this process the user in the MANET can only perform the authentication based upon information which is local based, even if security is done in own planned way.

Schneier, Bruce, 2012: In this paper the author has explained about the blowfish bloch cipher algorithm and its working procedure. The Blowfish contains the variable length of key sizes from 32 bits to 448 bits. This also contains the size of the block cipher with 64 bit. The blowfish algorithm generally contains two parts those are expanding the key and

the encryption of the data part. The expansion of the key part generally translates the key into at most 448 bits also into different number 4168 bytes of sub-key arrays. The encryption of the data is performed by the fiestel structure network that contains 16 rounds. And each and every round depends on the key. That also depended by the permutation and the substitution of key dependent. All the rounds in a feistel structure perform XOR and the 32 bit word addition. The addition operation contains index with four array data loops for each round.

CHAPTER 3
PRESENT WORK

3.1 PROBLEM FORMULATION:

While transferring the data from the source node to the destination node it should be delivered very securely to the destination node. While transferring the data in the network it will not be compromised by any unauthorized person. The data in the SPREAD is divided into number of blocks according to the multiple paths that are present in the network. The blocks are assigned in to the paths by using (T, N) secret sharing scheme which uses CBC (Cipher block chaining) block cipher algorithm to encrypt the data. Here in our Enhanced SPREAD (Enhanced Security Protocol for Reliable Data Delivery) we are affecting the (T, N) secret sharing scheme by replacing the cipher block chaining algorithm with Blowfish algorithm to make the data very secure while it transferring through the network.

Cipher Block Chaining: The organization named as IBM is introduced the block cipher encryption algorithm named as Cipher Block chaining. This is introduced in the year of 1976. The text which the sender wants to send to the receiver is known as plaintext. While sending the plain text every block of the plain text is performed with the XOR operation with the previous generated cipher text block before it is being encrypted. Similarly the plaintext blocks are used to generate cipher text block up to the end of text. The vector named as initialization vector which is used for the first block of the encryption to make the message unique.

Initialization vector (IV) this is generally used in cryptography. We can also call the initialization vector as Stealing variable (SV), which is a fixed sized input data that is

used in cryptography. This is generally generated from the random numbers or pseudo random number generator which is generally related between the segments and the data which is encrypted. This initialization vector is used for first block of the encryption, once the initialization vector is compromised then the block chaining algorithms can be compromised easily. This is generally known as nonce (number used once) it means there is no repeatable number.

Encryption procedure for Cipher Block Chaining (CBC):

Generally the CBC is deals with the blocks of the message, which is in the sense the message is divided into number of blocks and each clock is separated by the numbering. Later performing the XOR operation between first block of the data message and initialization vector (IV). After completion of the XOR operation between the first block of the data message and initialization vector then it will generate some encrypted data. The generated encrypted data is appended by the key and performs the block cipher encryption. Once the encryption of the first block is completed then it will generates cipher text. The generated cipher text act as initialization vector to the second block plain text, that is the plain text of the second block and generated cipher text are going to perform XOR operation. This process will continue up to all blocks are going to complete. The below figure explain about encryption about CBC.

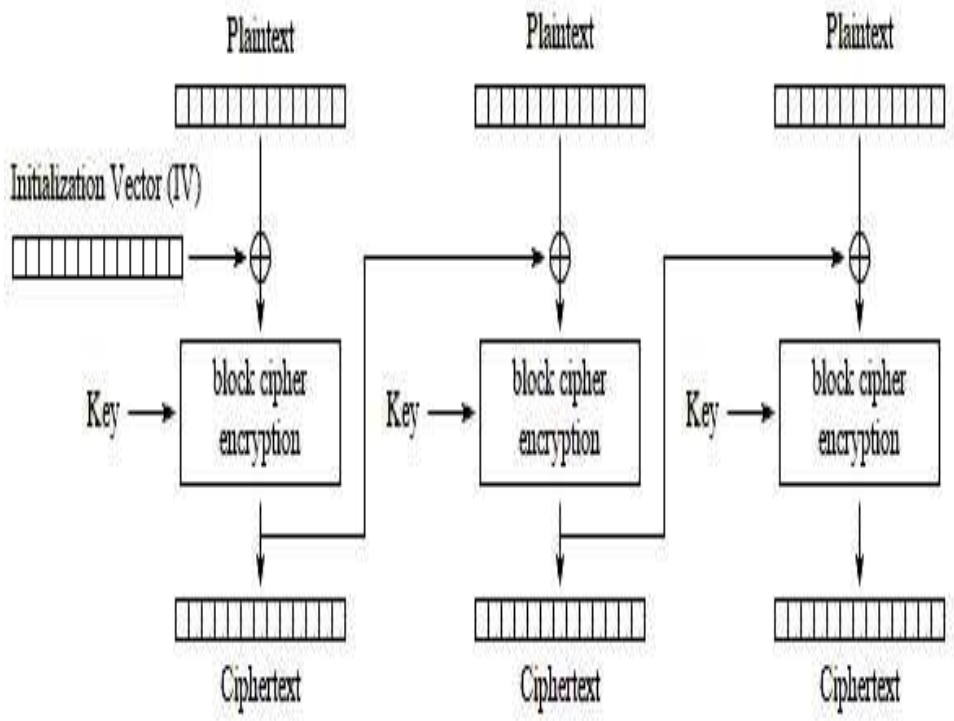

Figure 3.1: Encryption of CBC.

The mathematical representation formula for CBC encryption is

$$C_i = E_k (P_i \text{ XOR } C_{i-1}),\ C_0 = IV$$

Decryption procedure for Cipher Block Chaining (CBC):

The decryption procedure is performed at the receivers end. Once the cipher text is reached to the receiver side then receiver has to perform the decryption to get the original message. The first cipher block is going to be performed in to block cipher decryption with the same key used at the sender side. After decryption done the generated decrypted text and the initialization vector are performed with XOR operation to get first plain text message block similarly for the second block cipher text is also done by the plain text which generated previously as initialization vector to the second block.

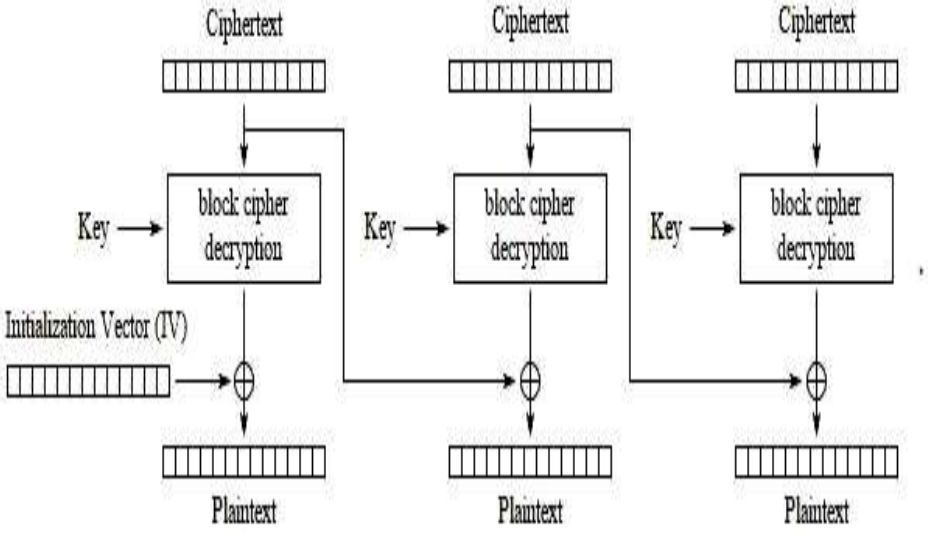

Figure 3.2: Decryption of CBC.

The mathematical formula for the CBC decryption is

$$P_i=D_k\,(C_i)\ \text{XOR}\ C_{i-1},\ C_0=IV$$

Where

P= Plain text.

C= Cipher text.

IV= Initialization Vector.

I= Index of the block.

CBC is generally fails due to the sequential encryption procedure which is not doing parallel. If there is a single bit change in the plain text or in the initialization vector then it shows affect on all the cipher text blocks. Similarly single bit change to the cipher text causes errors to all the equivalent plain text blocks. Due to the failure in the CBC block cipher algorithm we are going to use Blowfish block cipher algorithm in our ESPREAD technique.

Blowfish Block Cipher Algorithm:

Blowfish Encryption Algorithm: there are many symmetric block ciphers algorithms that are presented in the network security. There is one of the best symmetric algorithms that are presented in the networking named as Blowfish symmetric block cipher algorithm. The blowfish algorithm is generally used to protect the data from the intruders

and effectively used in encryption of the data. The blowfish is a good securing algorithm because it is following variable length of key sizes from 32 bits to 448 bits. Blowfish is a block cipher encryption algorithm which is developed in the year of 1993 by the cryptographer named as Bruce Schneier. Blowfish is very fast encryption algorithm and free algorithm than the all existing encryption algorithms. This is totally free algorithm which says that blowfish is a license-free and any user can use this algorithm freely.
The main features of blowfish algorithm explained below.

- This algorithm generally deals with data message in big blocks.
- It consist block size of 64 bits.
- It has a variable key length from32 bit to 448 bits.
- This is very efficient and also uses very normal and simple operations.
- This contains the number of iterations those are changeable, (to avoid from the attack named as brute-force).
- This uses sub-keys, for key which is of one way hash, (by using this is perhaps the security for the larger blocks).
- This blowfish generally does not have the single structure which is decreasing the complexity of thorough search.
- This blow fish contains the very simple and understandable design. This describes that algorithms is feistel and iterated block cipher.

3.2 OBJECTIVE OF STUDY:

Enhanced SPREAD (Enhanced Secure Protocol for Data Delivery) which is deals with the secure data delivery from the source node to the destination node. In this Enhanced SPREAD we are initially dividing the data in to multiple data blocks. Later these blocks are going to share to the different paths through the Threshold secret sharing scheme. Finally these shares are going to transfer through the multipath routing from the source node to the destination node. Here the Enhanced SPREAD is the paper is to get the more securable delivery with optimum result with very effective and efficient results.

3.3 METHODOLOGY:

ENHANCED SPREAD OVERVIEW

3.3.1 SYSTEM MODEL

The idea for this Enhanced SPREAD comes for the observation. While we are transferring the data through the network it may be captured by any intruder. Then this may caused the loss of information or revealing the secrecy in data. Our Enhanced SPREAD deals with same process while source node sending data to the destination node then source node initially select the multiple paths that are used to reach the destination by using multipath routing. This also considers some properties like disjoint nodes. Then source node selects the Threshold secret sharing algorithm. Based upon the security level of the data the sources node adjusts the data parts on to the multiple paths and send to the destination. Upon receiving the multiple data parts by receiver node and he can adjust the data by Threshold secret sharing algorithm.

We are dealing with the key management by the neighbor nodes. Intruder may capture the message that is traveling through the particular node. Once the node is decrypted by the intruder then entire data that is passing to that node will be captured and then intruder can rebuild the original message. Here we mainly were concentrating on the three major design issues in the MANET. This is depends upon the cryptography, optimization and the network routing. In this cryptography deals with how to divide the data into multiple data parts, optimization is to how these data parts have to put on the multiple paths and finally network routing deals with how to select these multiple paths. This Enhanced SPREAD gives optimal solutions for three issues that are presented in the MANET. Those are security, reliability and cost metric. Each of the issue that is presented in Enhanced SPREAD is explained in the following sections.

3.3.2 GENERATION OF SHARABLE MESSAGE

The brief explanation of the Threshold Secret Sharing is given in this section. This is required to make the data into multiple data parts. Let's consider secret of the system is K and we divided the entire data in to N number of parts and we also called them as shares. The shares are *S1, S2, S3 . . . , SN.* All the paths holds one share each respectively, those are like P_1, P_2, P_3 . . . , P_N. This algorithm divides the shares according to its theory that fewer than T shares will not give any information to the intruder. The data parts which are T out of N can use to reconstruct the secret data K. This process is known as (T, N) Threshold Secret sharing scheme. This scheme contains two algorithms known as dealer

and combiner. The dealer at the source side is used to divide the data into multiple parts and allocates them in to different paths. And the second algorithm combiner is used to gather the data parts from the paths and reconstruct the message from the K secret and from the T data parts received at the destination. The combiner will only re-compute the data message if and only if it got T data parts.

Here in the Enhanced SPREAD we are using the Shamir's Lagrange interpolating polynomial method. This is one of the secret sharing methods. The source node initially gets the i^{th} path i.e., P_i's share S_i by processing a polynomial degree (T-1).

$$f(x) = (K+d_1x+d_2x^2+d_{T-1}x^{T-1}) \bmod p$$

$$at\ x = i\ (i=1, 2, 3, \ldots, N) :$$

$$P_i \rightarrow S_i = f(i)$$

Here $d_1, d_2, \ldots, d_{T-1}$ are randomly selected coefficients, also p is randomly taken prime number which is larger than the all other coefficients and this must be presented with both dealer and combiner. The secret of the message K is also denoted with the coefficient "a_0".

At the destination side (combiner), by taken the T data parts, $f(i_1), f(i_2), \ldots, f(i_T)$, the original data f$(x)$ can be recover by the Shamir's Lagrange interpolation.

$$f(x) = \sum_{j=1}^{T} S_{ij} \cdot l_{ij}\ (x) \bmod p$$

Where

$$l_{ij}\ (x) = \prod_{k=1,\, k \neq j}^{T} \frac{x - i_k}{i_j - i_k}$$

By calculating the $f(0)$, the secret K can be recovered. This is a very efficient algorithm with the time complexity (O (T log 2 T)).

Larger the (T, N) will not be more in our Enhanced SPREAD technique. For the practical implementation of Enhanced SPREAD, the straight forward quadratic algorithms are quite enough. The secret share of the can be applied as block-by-block.

This is a basic and fundamental technique is to perform encryption to the data. Here in the Enhanced SPREAD technique we are using the Blow Fish Algorithm (BFA) to protect the data from the intruders and to hide the original message. The bandwidth is the basic constraint in the wireless networks. The bandwidth is to be reduced in this wireless environment. To reduce the bandwidth in our Enhanced SPREAD more and more coefficients has to be allocated to the data parts or data blocks. Those are $d_0,d_1,d_2,\ldots,d_{T-1}$. All the blocks of the data shares in the secret sharing process is show in the below figure.

3.3.3 OPTIMAL SHARE ALLOCATION

Here in the Enhanced SPREAD the main constraint is the security. Providing the security to the data is our main aim for this security purpose we are using (T, N) secret sharing algorithm. The network layer is mainly responsible for transferring the data from one hop to another hop. The network layer is to find the disjoint nodes in the route initially to protect the data more. If any disjoint node is compromised then every data that is travelling from that disjoint node can be compromised. Let us consider there are "M" disjoint paths that are present in the network. Denoted with the vector "p' i.e., $p=[p_1,p_2,p_3,\ldots..,p_M]$ and security characteristics are denote to this paths is with p_i, [i=1,2,….M]. p_i are the nodes that says the probability of compromised nodes.

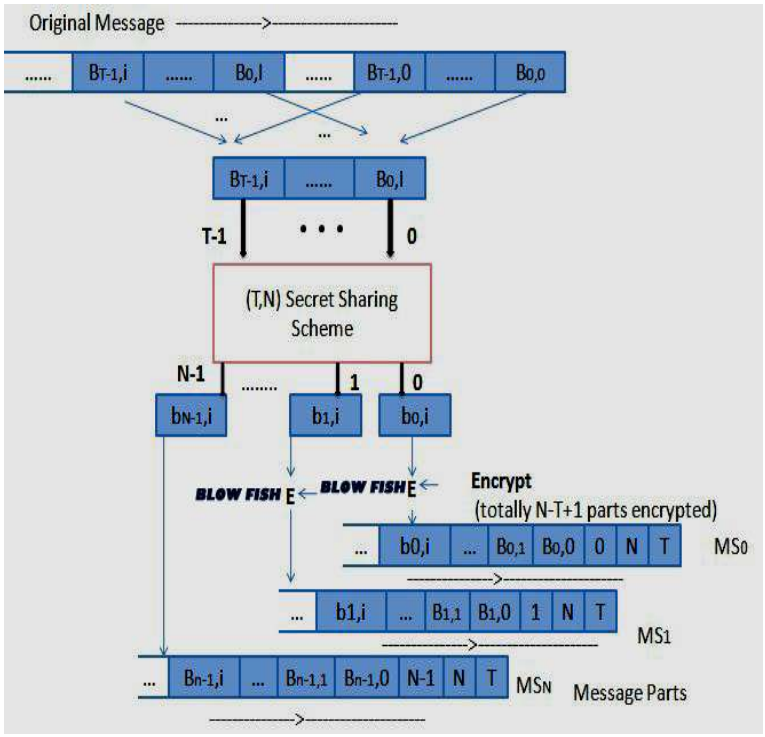

Figure 3.3: (T, N) Secret Sharing Scheme using Blowfish Encryption.

If the N=T then the original data can be easily recovered from the T shares of the data. If (N>= M) or N=N then the data is fully secured i.e., maximum security is assigned. Here we are using the Blow Fish block cipher encryption algorithm which is more advanced algorithm which uses 64 bit block size and variable key size up to 448 bits long and gives well and optimal results than the CBC (Cipher Block Chaining) algorithm.

3.3.4 MULTIPATH ROUTING

The main challenge in the ad-hoc network is routing. This routing carries many functions those are nodes should be properly connected, the data should be delivered correctly to the destination node, malicious node should be identified, routing information should be updates every time and must handles the disjoint nodes in the network. Here in our Enhanced SPREAD we are using the mulitipath routing protocol named as on-demand routing protocol which is very effective and efficient routing protocol in the ad-hoc environment. The on-demand routing protocol is also used to handle the disjoint nodes in the network. Which is also maintains the link cache organization to update the route and also to gives the reply to the source node time to time. This link cache is maintains the minimum hop count and minimum propagation delay. Here we also uses the Dijsktra's shorest path process to get the minimum hop count.

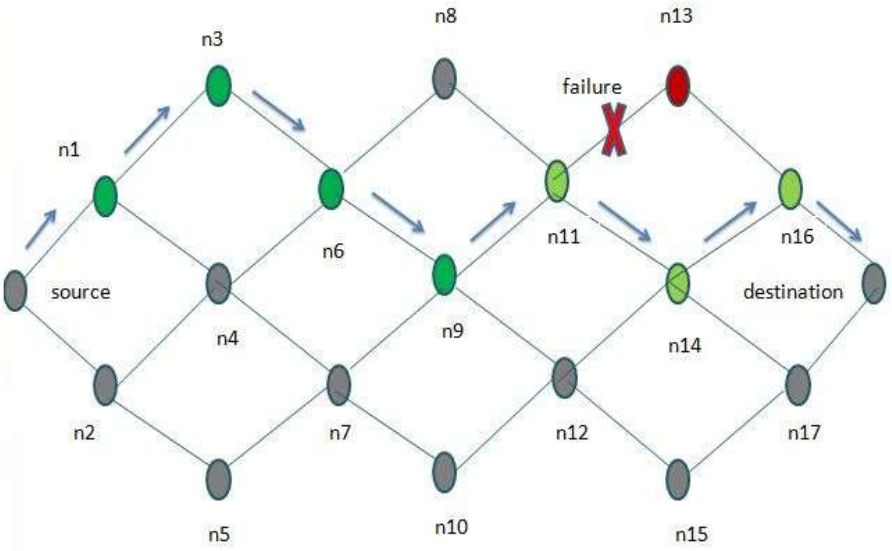

Figure 3.4: Multipath Routing in Enhanced SPREAD.

Here in the above routing diagram, source node initially enters the destination node ip-address then broadcasts the data to its neighboring nodes. All the remaining nodes that are presented in the networks handle this task to deliver the data to the destination node. If any node is failed in the network then the previous node from the failed node will select another route to the destination.

3.3.5 Blowfish Block Cipher Algorithm:

Blowfish Encryption Algorithm: there are many symmetric block ciphers algorithms that are presented in the network security. There is one of the best symmetric algorithms that are presented in the networking named as Blowfish symmetric block cipher algorithm. The blowfish algorithm is generally used to protect the data from the intruders and effectively used in encryption of the data. The blowfish is a good securing algorithm because it is following variable length of key sizes from 32 bits to 448 bits. Blowfish is a block cipher encryption algorithm which is developed in the year of 1993 by the cryptographer named as Bruce Schneier. Blowfish is very fast encryption algorithm and free algorithm than the all existing encryption algorithms. This is totally free algorithm which says that blowfish is a license-free and any user can use this algorithm freely.

There is a feistel network following by the Blowfish algorithm. There is function that is which is used to iterating the encryption function for 16 times and it contains the 64 bits block size. Blowfish algorithm contains the key it can be anything that is up to the 448 bits. If we are going to use large microprocessor the encrypting data is very efficient and before making any encryption the complex initialization phase is necessary. There is no fixed length key for the blowfish block cipher algorithm, this is a variable –key length block cipher. This is one of the most suitable encryption techniques where key doesn't changes. The blowfish is very suitable encryption algorithm in the communications channels and file encryption that performs automatically. This is very much faster than all the encryption algorithms.

The main features of blowfish algorithm explained below.

- This algorithm generally deals with data message in big blocks.
- It consist block size of 64 bits.
- It has a variable key length from32 bit to 448 bits.
- This is very efficient and also uses very normal and simple operations.
- This contains the number of iterations those are changeable, (to avoid from the attack named as brute-force).
- This uses sub-keys, for key which is of one way hash, (by using this is perhaps the security for the larger blocks).
- This blowfish generally does not have the single structure which is decreasing the complexity of thorough search.
- This blow fish contains the very simple and understandable design. This describes that algorithms is feistel and iterated block cipher.

Description of the Algorithm:

The Blowfish contains the variable length of key sizes from 32 bits to 448 bits. This also contains the size of the block cipher with 64 bit. The blowfish algorithm generally contains two parts those are expanding the key and the encryption of the data part. The expansion of the key part generally translates the key into at most 448 bits also into different number 4168 bytes of sub-key arrays.

The encryption of the data is performed by the fiestel structure network that contains 16 rounds. And each and every round depends on the key. That also depended by the permutation and the substitution of key dependent. All the rounds in a feistel structure

perform XOR and the 32 bit word addition. The addition operation contains index with four array data loops for each round.

Sub-keys:

The block cipher algorithm named as blowfish generally contains sub-keys in large number. Before the encryption or decryption has performed these numbers must be computed i.e., pre-computed.

The p array generally contains sub key of 32. Those are denoted with the P1, P2,..., P18.

This is also contains S-boxes numbered with 32 bit , each with entry of 256. Those are denoted below.

$S_{1,0}$, $S_{1,1}$,…….. , $S_{1,255}$;

$S_{2,0}$, $S_{2,1}$,……, $S_{2,255}$;

$S_{3,0}$, $S_{3,1}$,....., $S_{3,255}$;

$S_{4,0}$, $S_{4,1}$,……, $S_{4,255}$.

Encryption of Blowfish:

We already mentioned that blowfish contains 16 rounds in fiestel network.

- Let us consider the input is X, which is 64 bit data block.

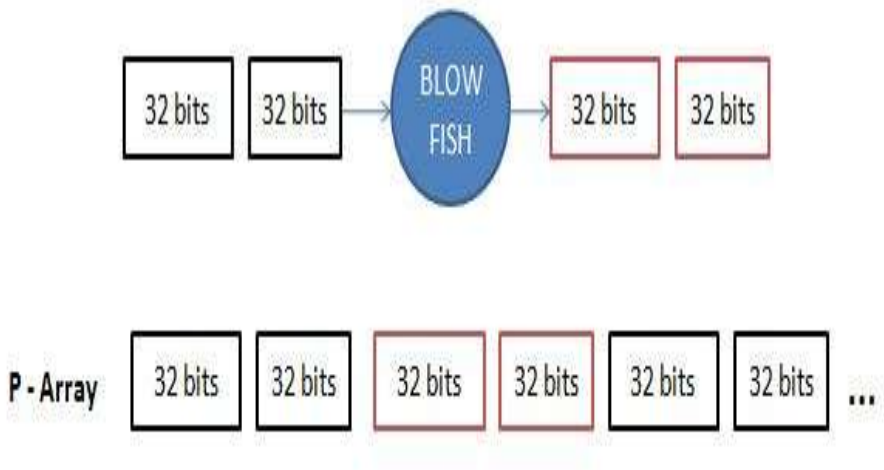

Figure 3.5: 64 Bit Block of P-Array in Blowfish.

This 64 block generally divided in to two parts, each part contains 32 elements of data X_L, X_R.

- Now this executes the loop up to 16 starting from 1 and ends with 16.
- $X_L = X_L$ XOR Pi,
- $X_R = F(X_L)$ XOR X_R.
  Where i start from 0 and ends with 16.
- Now interchange the elements of X_L, X_R.
- Once all the 16 rounds get completed then interchange the elements of X_L, X_R once again to undo the last interchange.
- Next $X_R = X_R$ XOR P17 and $X_L = X_L$ XOR P18.
- Finally combine the elements of X_L and X_R to get the cipher text for the given plain text.

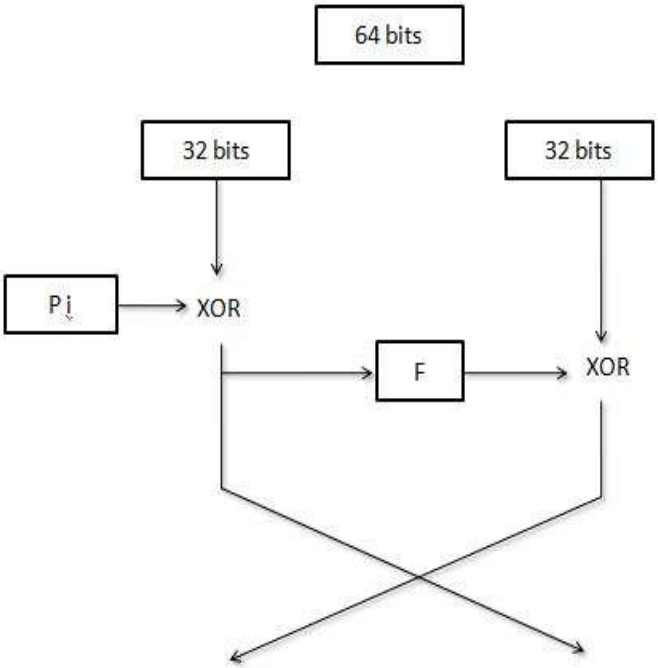

Figure 3.6: 16 Rounds of Blowfish.

The Decryption algorithm is performed similarly but P1, P2, P3,…., P18 used in the reverse order.

```
static DWORD bf_P[NPASS + 2] = {
  0x243f6a88, 0x85a308d3, 0x13198a2e, 0x03707344,
  0xa4093822, 0x299f31d0, 0x082efa98, 0xec4e6c89,
  0x452821e6, 0x38d01377, 0xbe5466cf, 0x34e90c6c,
  0xc0ac29b7, 0xc97c50dd, 0x3f84d5b5, 0xb5470917,
  0x9216d5d9, 0x8979fb1b,
};
static DWORD bf_S[4][256] = {
  0xd1310ba6, 0x98dfb5ac, 0x2ffd72db, 0xd01adfb7,
  0xb8e1afed, 0x6a267e96, 0xba7c9045, 0xf12c7f99,
  0x24a19947, 0xb3916cf7, 0x0801f2e2, 0x858efc16,
  0x636920d8, 0x71574e69, 0xa458fea3, 0xf4933d7e,
  0x0d95748f, 0x728eb658, 0x718bcd58, 0x82154aee,
  0x7b54a41d, 0xc25a59b5, 0x9c30d539, 0x2af26013,
  0xc5d1b023, 0x286085f0, 0xca417918, 0xb8db38ef,
  0x8e79dcb0, 0x603a180e, 0x6c9e0e8b, 0xb01e8a3e,
  0xd71577c1, 0xbd314b27, 0x78af2fda, 0x55605c60,
  0xe65525f3, 0xaa55ab94, 0x57489862, 0x63e81440,
  0x55ca396a, 0x2aab10b6, 0xb4cc5c34, 0x1141e8ce,
  0xa15486af, 0x7c72e993, 0xb3ee1411, 0x636fbc2a,
  0x2ba9c55d, 0x741831f6, 0xce5c3e16, 0x9b87931e,
  0xafd6ba33, 0x6c24cf5c, 0x7a325381, 0x28958677,
  0x3b8f4898, 0x6b4bb9af, 0xc4bfe81b, 0x66282193,
  0x61d809cc, 0xfb21a991, 0x487cac60, 0x5dec8032,
  0xef845d5d, 0xe98575b1, 0xdc262302, 0xeb651b88,
  0x23893e81, 0xd396acc5, 0x0f6d6ff3, 0x83f44239,
  0x2e0b4482, 0xa4842004, 0x69c8f04a, 0x9e1f9b5e,
  0x21c66842, 0xf6e96c9a, 0x670c9c61, 0xabd388f0,
  0x6a51a0d2, 0xd8542f68, 0x960fa728, 0xab5133a3,
  0x6eef0b6c, 0x137a3be4, 0xba3bf050, 0x7efb2a98,
  0xa1f1651d, 0x39af0176, 0x66ca593e, 0x82430e88,
  0x8cee8619, 0x456f9fb4, 0x7d84a5c3, 0x3b8b5ebe,
  0xe06f75d8, 0x85c12073, 0x401a449f, 0x56c16aa6,
  0x4ed3aa62, 0x363f7706, 0x1bfedf72, 0x429b023d,
  0x37d0d724, 0xd00a1248, 0xdb0fead3, 0x49f1c09b,
  0x075372c9, 0x80991b7b, 0x25d479d8, 0xf6e8def7,
  0xe3fe501a, 0xb6794c3b, 0x976ce0bd, 0x04c006ba,
  0xc1a94fb6, 0x409f60c4, 0x5e5c9ec2, 0x196a2463,
  0x68fb6faf, 0x3e6c53b5, 0x1339b2eb, 0x3b52ec6f,
  0x6dfc511f, 0x9b30952c, 0xcc814544, 0xaf5ebd09,
  0xbee3d004, 0xde334afd, 0x660f2807, 0x192e4bb3,
  0xc0cba857, 0x45c8740f, 0xd20b5f39, 0xb9d3fbdb,
  0x5579c0bd, 0x1a60320a, 0xd6a100c6, 0x402c7279,
  0x679f25fe, 0xfb1fa3cc, 0x8ea5e9f8, 0xdb3222f8,
  0x3c7516df, 0xfd616b15, 0x2f501ec8, 0xad0552ab,
  0x323db5fa, 0xfd238760, 0x53317b48, 0x3e00df82,
  0x9e5c57bb, 0xca6f8ca0, 0x1a87562e, 0xdf1769db,
  0xd542a8f6, 0x287effc3, 0xac6732c6, 0x8c4f5573,
  0x695b27b0, 0xbbca58c8, 0xe1ffa35d, 0xb8f011a0,
```

Figure 3.7: Blowfish P-arrays and Sub-keys.

Generating the Sub-keys:

Using the blowfish algorithm and calculate the sub-keys.

i. By using the unchangeable string and make initiation of the P- array and later four S – boxes into particular order.

ii. The string should be of the hexadecimal digits of P_i which should be <3 P1 =

iii. 0x14568bc9, P2 = 0x8723dfa1, P3 = 0xedc98564, P4 = 0x55697bd0, etc...

iv. The 64 block of data is divided into two parts. The first part contains 32 bits and a second part contains 32 bits. Then perform XOR operation with P1 with first 32 bits of the key and so on up to the P14.
v. Then perform all zero operation with the sub-keys discussed in the step (i), (ii), (iii).
vi. And output has to be replaced with the strings P1 and P2.
vii. Now the output has to be encrypted that is generated in the step iv, by using the modified sub-keys used in the blowfish algorithm.
viii. Now the output of the step (vi), has to be replaced with P3 and P4.
ix. The process has to complete up to replacing all the P-array and then all the S- boxes respectively, using the output of blowfish algorithm which is continuously changing. Generally we require 512 iterations to generate all the sub-keys.

.

CHAPTER 4
RESULTS AND DISCUSSION

Experimental Work:

Parameters	Settings
Traffic type	CBR
Connection	UDP
X-axis	1200
Y-axis	600
Number of nodes	20
Routing protocol	AODV
Simulation area	1200 X 600
Trace file	AODV.tr
Nam file	AODV.nam
Transmission radius	150
Transmission rate	600 kb
Data packet size	512 kb
Simulation time	90sec
Interval	0.05 sec
MAC protocol	802.11

We have used ns-2.35 as simulation tool. We compared our proposed message security scheme [E-SPREAD] against SPREAD. We have implemented our security scheme on AODV routing protocol. Simulation is done on the algorithm and a trace file is generated. By using trace file with combining awk script we can generate a graph said to be Xgraph, where we can show the difference between the two protocols.

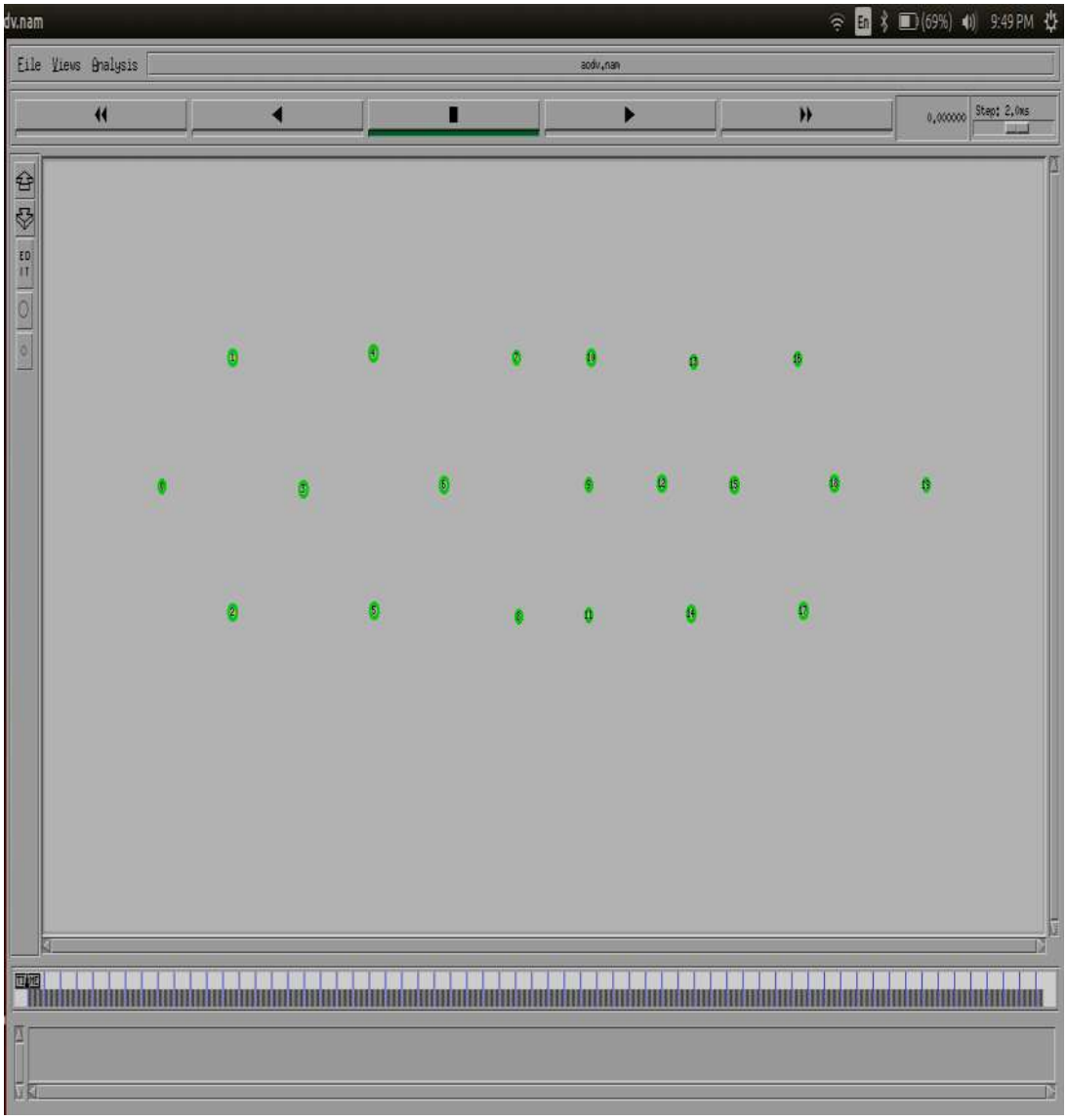

Figure 4.1: Simulation Area.

A trace file is generated by the algorithm to represent how the algorithm works by our routing protocol. Node movements are observed to secure the nodes from the intruders. By the below figure we can observe the node location and packet transferring from node

to node by initial request of RREQ by the nodes. Once the RREQ is the sender is initially started to send all the data from the path from where he get the response. After sending the data, they may be able to lose by the intruders also it may lose by the node movement in the network. If the data is lost by the node movement then the sender has to resend the data, if the data is lost by the intruders or any intrusion is found in the network then we can able to change the paths in the routing protocol.

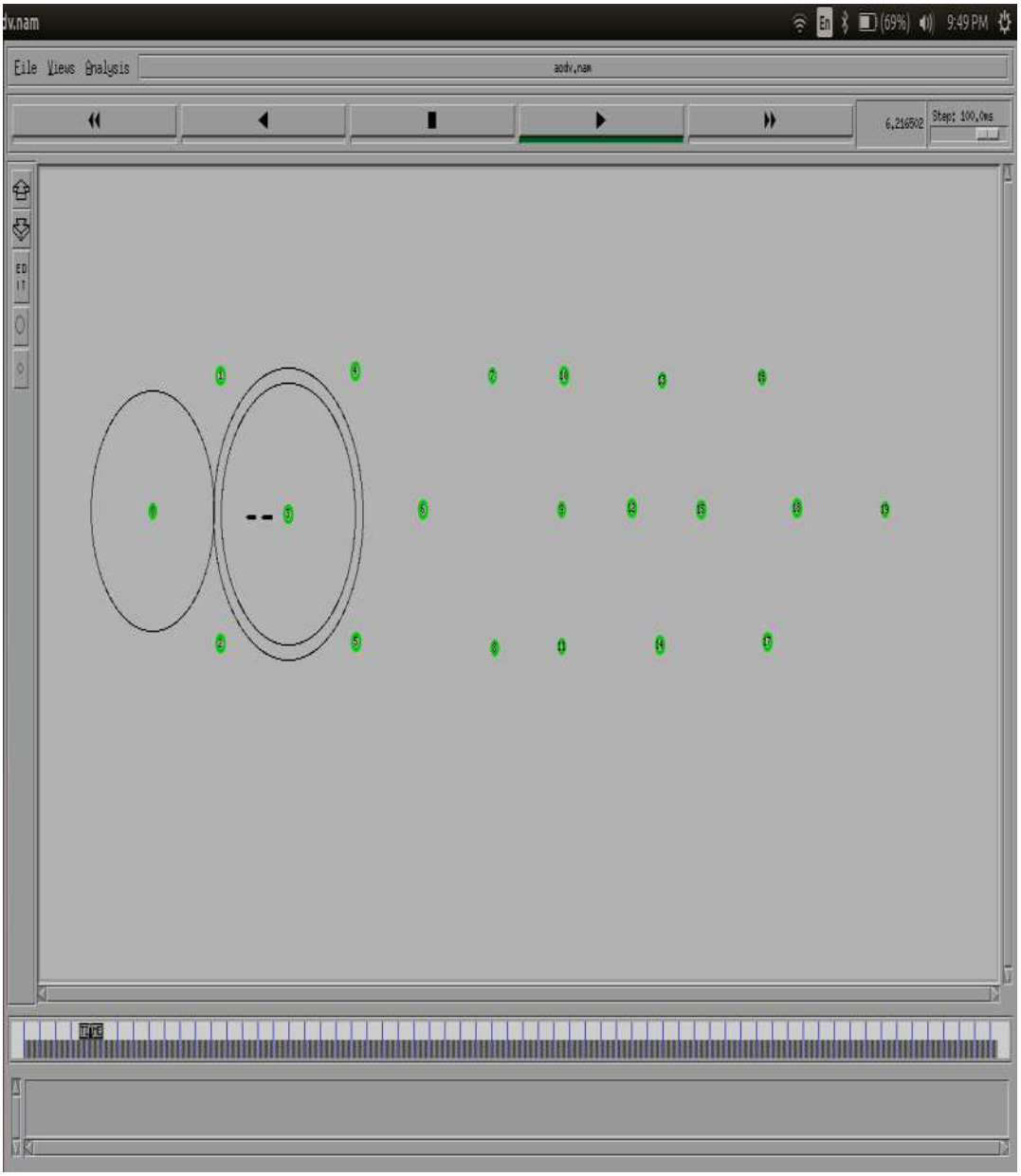

Figure 4.2: Packet Transformation by Request

The below diagram which is explaining about the simulation results which is performing at the time of 64 sec. initially all the nodes are in E-SPREAD are constant at the time of 0 sec, the nodes are going to take the moment at the time of the 10 sec. once we starts the simulation then it follows some route requests and responses and starts getting the routing table information and everything which are usually used to transfer the data from source node to the destination node.

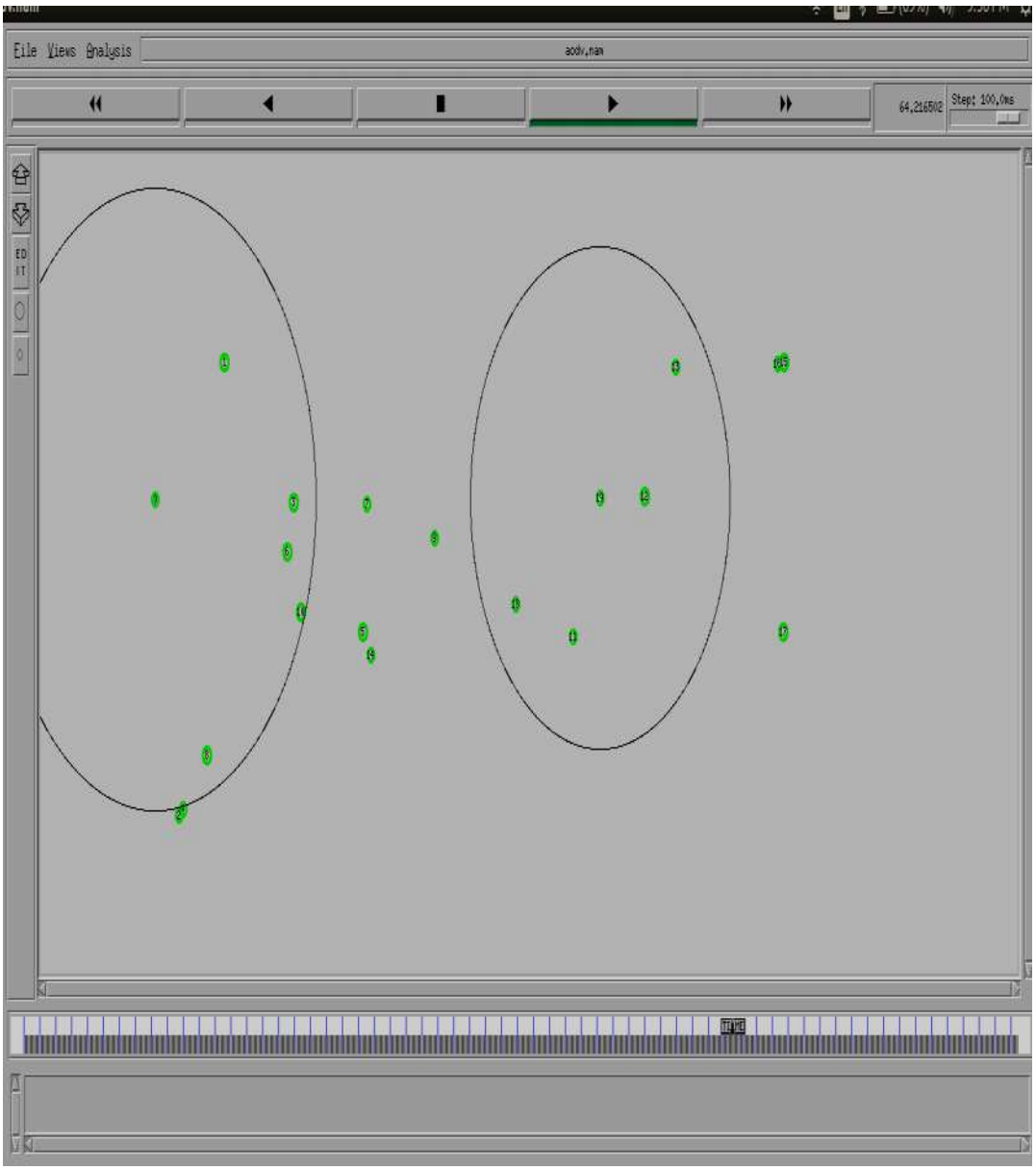

Figure 4.3: Nodes at the time of 64 sec.

Data analysis and Interpretation:

Throughput:

Throughput is defined as number of packets delivered to the destination in a span of time. By comparing with SPREAD, E-SPREAD has the best throughput. As the time and number of nodes increases throughput also increases. Due to the nodes mobility the throughput varies from time to time which is represented in the below graph. When the node moment starts in the network then there is an automatically throughput varies in the network. Compared to the SPREAD throughput the ESPREAD is more good and beneficiary. The green curves in the below graph representing the throughput of the ESPREAD and red color line represents for SPREAD.

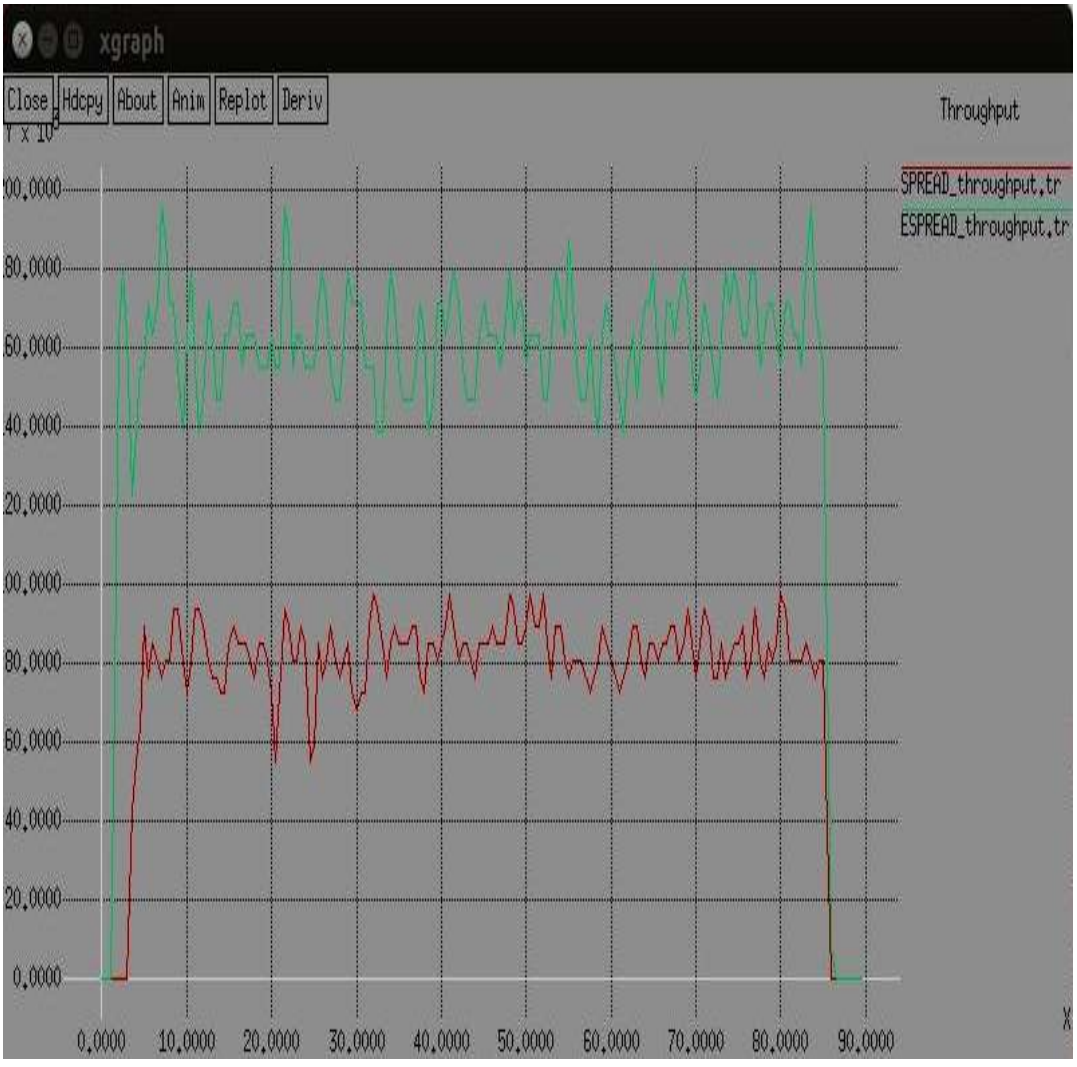

Figure 4.4: Throughput.

Packet Loss:

As there is a huge traffic in the network, there will be loss of data due to congestion at the nodes in the network. If the congestion occurs then there will be huge packet loss. By comparing with SPREAD, E-SPREAD has less packet loss which is shown in the following graph. The SPREAD and ESPREAD is always making differ in the every calculation because ESPREAD is faster and secured and advanced encryption algorithm than the SPREAD technique. For this reason we are getting the less packet loss in the ESPREAD compared to the SPREAD.

Figure 4.5: Packet Loss.

End to End Delay:

If the traffic in the network increases then the delivery of the packets are also may take delay. Because more usage of the route, number of intermediate nodes participating to make the data deliverable. As there are many nodes in the network there will be huge data traffic by the data transfer from the nodes. As the nodes do not have fixed topology then delay will be increased. E-SPREAD has the best end to end delay than SPREAD which means it have less delay.

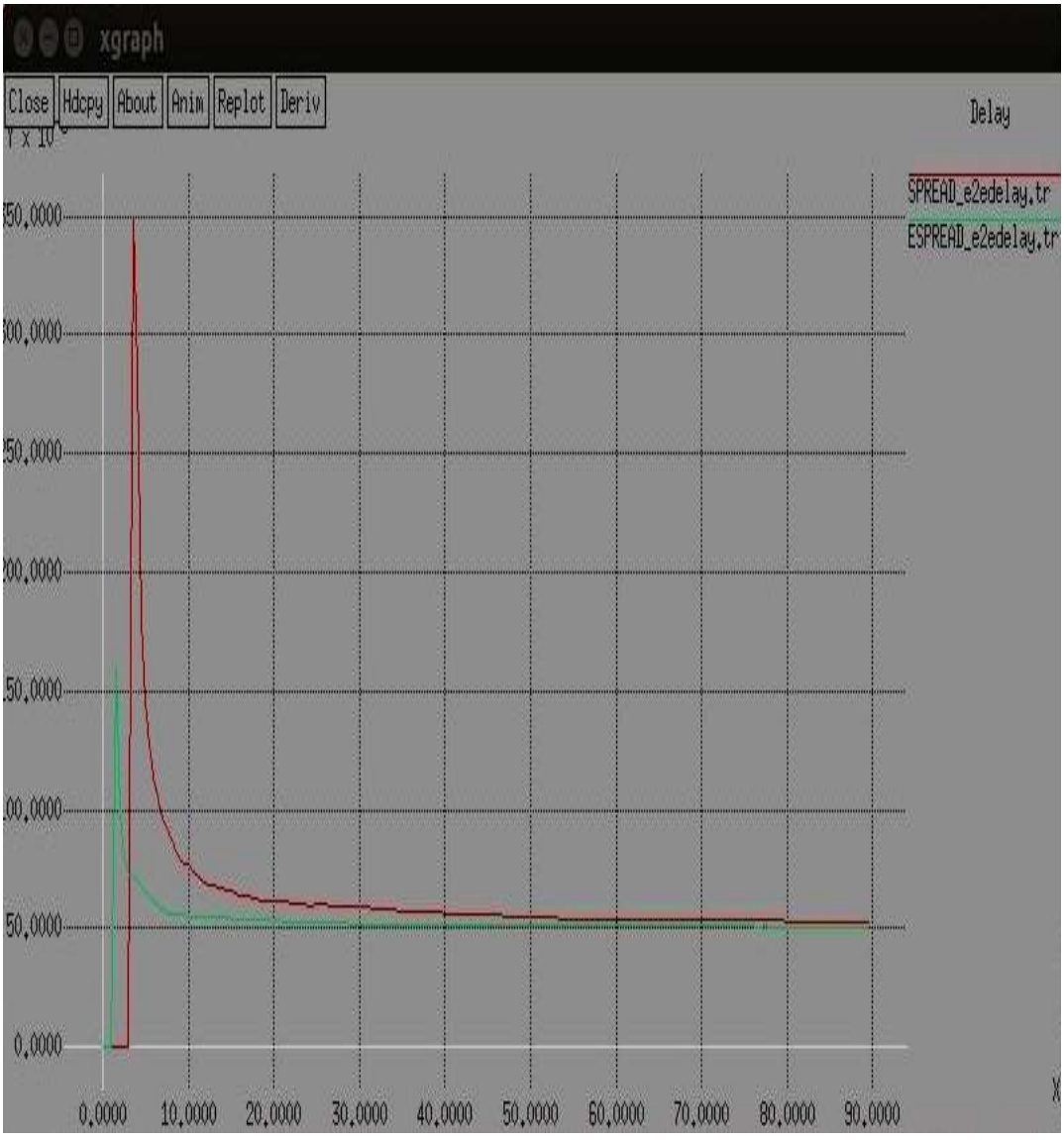

Figure 4.6: End to End Delay.

Energy Deviation:

As there were many nodes in network the nodes uses power to process. The consumption of power by the nodes can vary from node to node. We can see the energy deviation of nodes at various time slots and we can know the average energy consumption nodes in the network. Since we are using the block cipher algorithm in the ESPREAD the data is going to delivered in the format of blocks, while we are sending the small amount of the data block it obliviously reduce the load on the network also reduce the power consumption of the process.

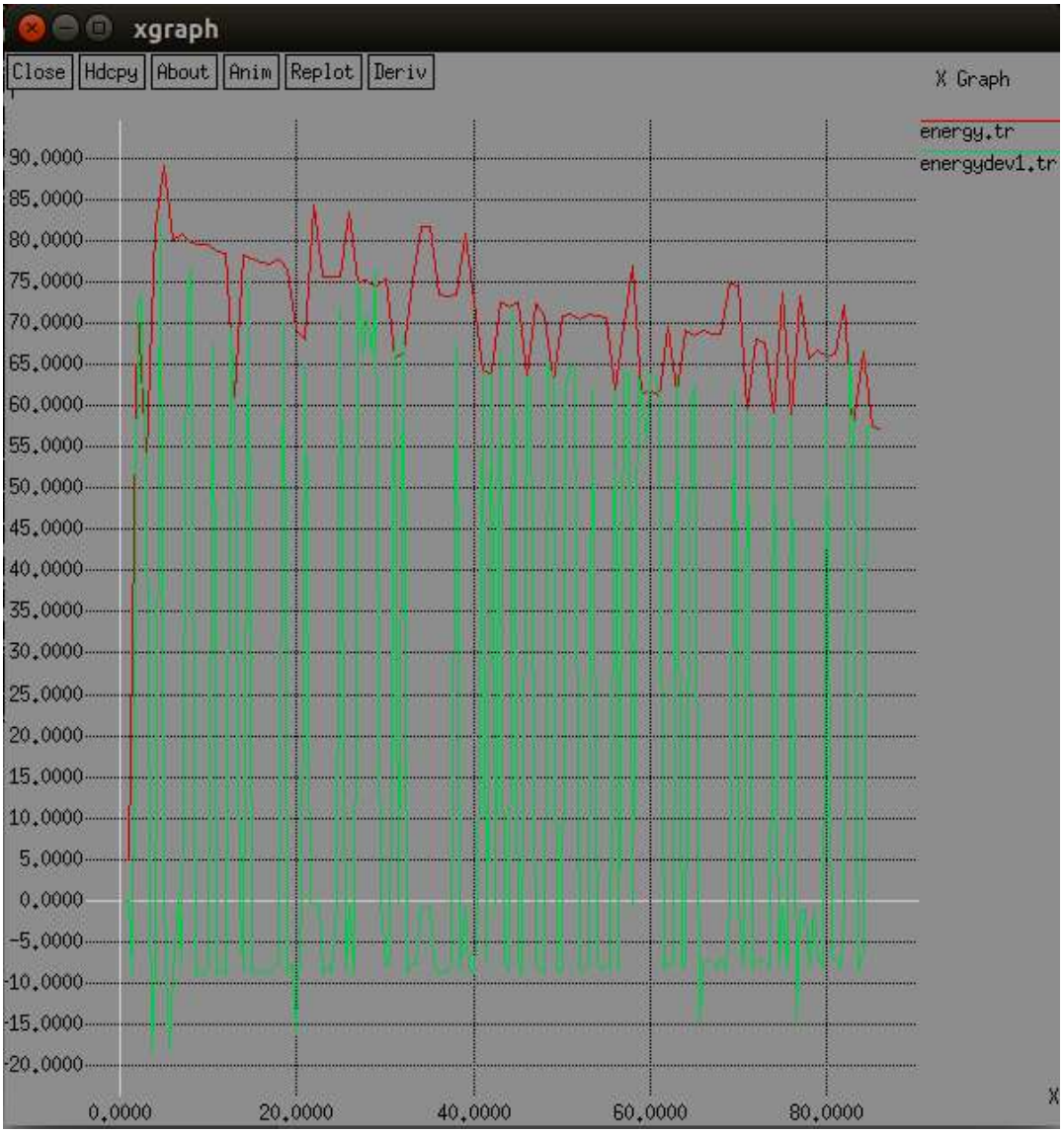

Figure 4.7: Energy deviation

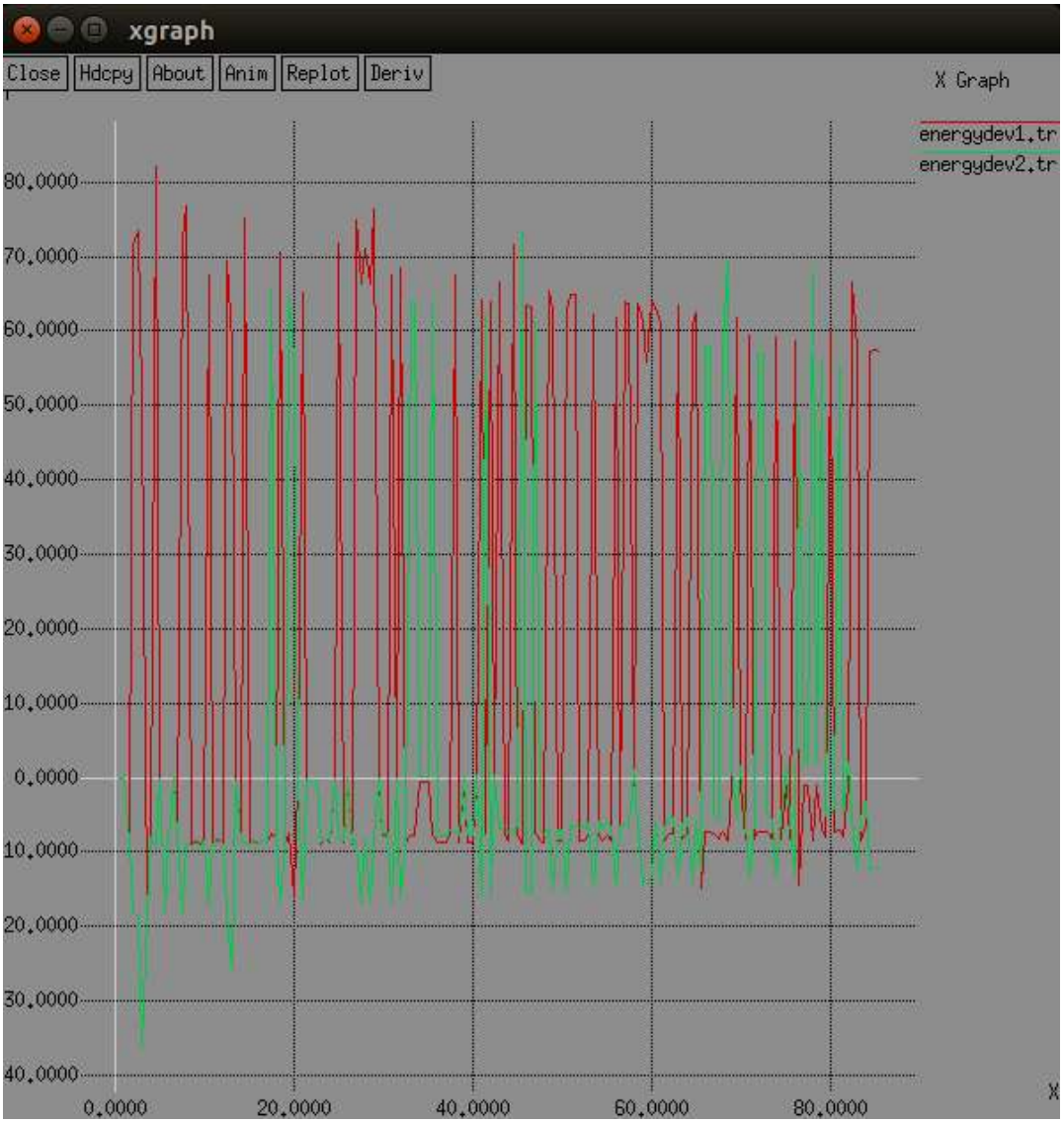

Figure 4.8: Energy Deviation.

Final Node Position and Energy:

After the movement of nodes in the network, the nodes does not have any fixed location, according to the scenario given in the simulation script, the nodes reach their final position by the axis of location and displays consumption of energy by each node in the network .By considering the energy of various nodes average energy of the node consumed is calculated. Also displays the total energy consumed by the nodes in the network. We can observe in the following figure.

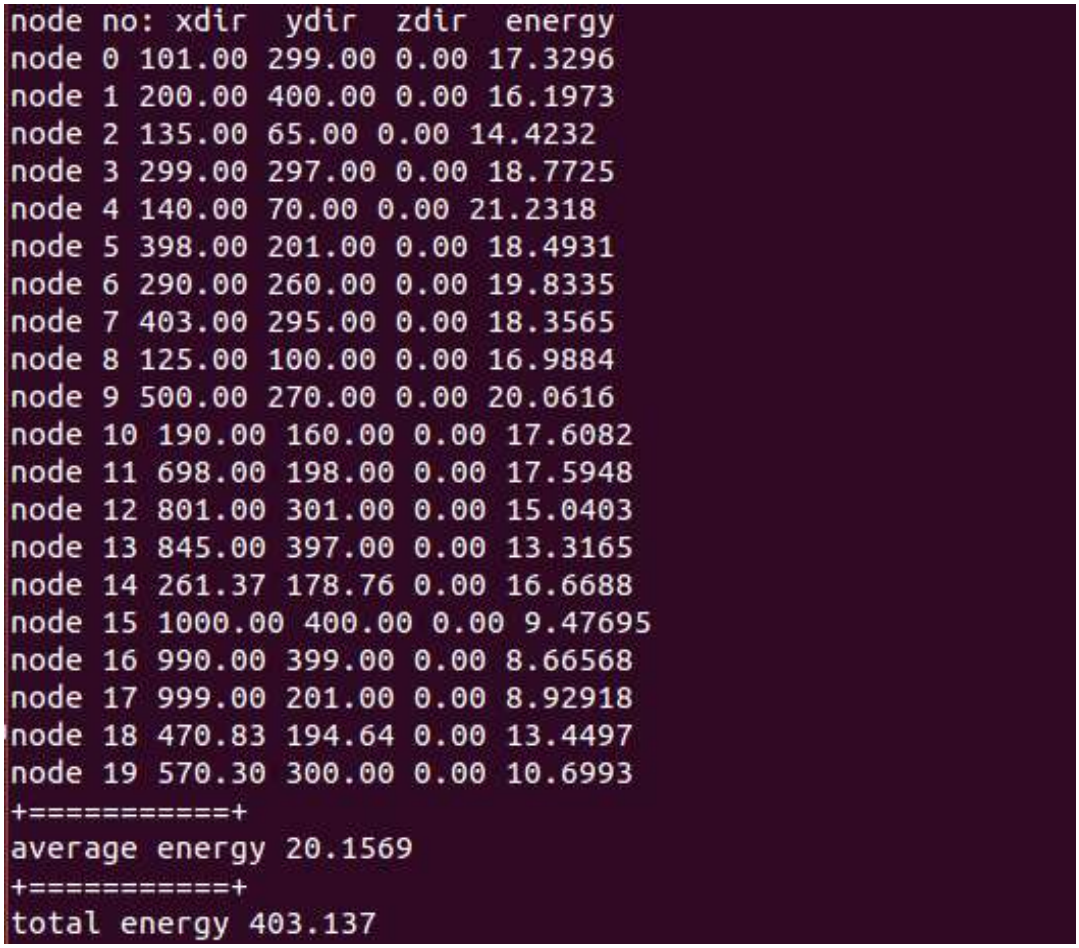

Figure 4.9: Average energy and Total energy of nodes.

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

Here in the Enhanced Security Protocol for Reliable Data Delivery (Enhanced SPREAD). We are using the most recent and powerful block cipher algorithm named as Blow Fish Algorithm which gives good result than the CBC (Cipher Block Chaining). Here in the Enhanced SPREAD we are dividing the data in to multiple shares and then we are passing it to the (T, N) secret sharing scheme which gives more security to the data and if the intruder compromises the small blocks also cannot understand the entire data. These data blocks are transferred through the multipath on-demand routing protocol. To improve the more security environment than the E-SPREAD the researcher has to append the more powerful block cipher technique than the Blowfish algorithm. This Enhanced SPREAD will give more secure data delivery from the source node to the destination node in the mobile ad-hoc networks environment.

CHAPTER 6
LIST OF REFERENCES

I. Research Papers

[1] Ankur Lal, Dr.Sipi Dubey, Mr.Bharat Pesswani CSE, CSVTU [2012].

[2] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994.

[3] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), *Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993)*, Springer-Verlag, 1994, pp. 191-204.

[4] Hani Q.R. Al-Zoubi,Department of Computer Engineering, Mutah University, ad-hoc routing protocols Mutah, Jordan [2012].

[5] J. An and M. Bellare, Constructing VIL-MACs from FIL-MACs: Message authentication under weakened assumptions, Advances in Cryptology { CRYPTO '99, Springer-Verlag, Lecture Notes in Computer Science, Vol. ??, M. Wiener, Ed., pp.(1999).

[6] Jian Liu, Suresh Singh, public key management of network, IEEE members [2001].

[7] Marjan Kuchaki Rafsanjani , Bahador Shojaiemehr ,Department of Computer Science, Shahid Bahonar University of Kerman, Iran. Islamic Azad University. [2012].

[8] Nicklas Beijar, Helsinki University of technology, Finland. [2011].

[9] Narula P, S. K. Dhurandher, S. Misra, and I. Woungang, *"Security in mobile ad-hoc networks using soft encryption and trust based multipath routing"*, Computer Communications, Vol. 31, pp.760-769, 2008

[10] R. Stoleru, H. Wu, H. Chenji. Department of Computer Science and Engineering, A&M University, Texas. [2012].

[11] T. Cormen, C. Leiserson and R. Rivest, *Introduction to Algorithms* (MIT Press, 1990).

[12] T.-C. Wu and T.-S. Wu, Cheating detection and cheater identification in secret sharing schemes, IEE Proc. Comput. Digit. Tech.142(5) (September 1995)

[13] W. Lou and Y. Fang, Predictive caching strategy for on-demand routing protocols in ad hoc networks, Wireless Networks 8(6) (Nov 2002).

[14] Wenjing Lou, Wei Liu, Yanchao Zhang, Yuguang Fang [2012].

II. Websites

[1] http://www.isi.edu/nsnam/ns/tutorial/index.html

[2] http://www.schneier.com/paper-blowfish-fse.html

[3] http://www.users.zetnet.co.uk/hopwood/crypto/scan/cs.html

CHAPTER 7
APPENDIX

A

AODV- Ad-hoc on demand distance vector

B

BER- bit error rate

BFA-bellman ford algorithm

BRP-border-cast resolution protocol

C

CC-congestion control

CBC-cipher block chaining

CWND-context window

D

DoS-denial of service

DSR-dynamic source routing

DSDV- dynamic source distance vector

I

IARP- intra zone routing protocol

IERP- inter zone routing protocol

M

MAC- medium access control

MDS- multi dimensional scaling

MHL- maximum header length

MSDN- mobile secure neighbor discovery

MANET- mobile ad-hoc network

N

NDP- neighbor discovery protocol

P

PRP- proactive routing protocol

R

RRP- reactive routing protocol

RErr- route error

RRep-route reply

RReq- route request

S

SND- source neighbor discovery

SPREAD- secure protocol for reliable data delivery

T

TCP- transmission control protocol

Z

ZRP- zone routing protocol