IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 6)

Available online at: www.ijariit.com

To enhance the privacy protection in mobile Ad-hoc network using JBATS protocol

Arun Kumar S.
arunkumars@sapthagiri.edu.in
Sapthagiri College of Engineering , Bengaluru, Karnataka

Swetha S.
swethaanju23@gmail.com
Sapthagiri College of Engineering , Bengaluru, Karnataka

Jayashree C. Y.
jayashreecy@gmail.com
Sapthagiri College of Engineering , Bengaluru, Karnataka

Thriveni L.
tgowda164@gmail.com
Sapthagiri College of Engineering , Bengaluru, Karnataka

Bhuvanashree V.
bhuvanashree79@gmail.com
Sapthagiri College of Engineering , Bengaluru, Karnataka

Renu R.
renurudramurthybt@gmail.com
Sapthagiri College of Engineering , Bengaluru, Karnataka

ABSTRACT

In Wireless Network, the privacy protection in the network is the prominent issue. Many protocols used to give privacy protection for the network and it uses the encoding and decoding approach to pass the data between one node to other node in a secure way. The cellular network will monitor the sensitive information in a protected way and also it is involved in the secure transmission of data. The JBATS protocol will give better security in the network and it uses the encoding and decoding approach. This project mainly focuses on the protection for the JBATS protocol. The main aim of the project is to provide complete security compared to other similar protocol. The JBATS Protocol for mobile Ad-hoc network enhances the stronger privacy protection in the network. When compared with other protocol, JBATS (Just before Accepting and Transacting, Securing the data) provides effective performance includes the cost of computing, the delay between from one end to another end, and dropping of packets.

Keywords*— AODV, DSR, JBATS*

1. INTRODUCTION

In a network, security is a most important factor. The JBATS is very important and it uses the combination of signature for route discovery. In this network, each node is assigned with some signature keys. The JBATS protocol is executing in two ways that are the establishment of keys and finding the best route for the network. In this, all the nodes and intermediate nodes focus on establishing a key. After establishing a key, the required information is transferred to the desired destination. Key process establishment, the route request message is transferred to the destination. After this route request message reaches the destination node and it will decrypt the message and create a session key and pseudonym key and send it to the destination. After sending the message the sender will receive the reply message from the destination and again it will send the data to another destination node. Here this network is having control packets and data packets and they look randomly. The proposed system is used to establish a key with each of its neighbours, and it uses some of the keys to encrypt the whole packet or the data to the corresponding neighbour. Receiving side neighbour can check whether the encrypted packet is used for trial or not, and the decryption from the different nodes. All messages are secured from the outside packets. This process contains node linkage between any two messages and it is checked whether they are from the same source node or from the other nodes and they are also protected. If anyone node is involved in route discovery or packet forwarding, so they having the same source node, destination node, and any of the intermediate node.it is not aware of other malicious nodes.

1.1 Motivation

In Ad-hoc network the privacy plays a vital role. The main aim of this project is to give the strongest privacy protection to the network via the JBATS protocol.

1.2 Our work

The project focuses on the security and compares to other protocols the JBATS protocol will provide full protection for the network. JBATS protocol achieves the best protection for the network and it uses the specialized key to establish a key between the nearest nodes.

Some of the contributions are as follows:

- Maintain confidentiality for the transmission of data.
- Keep data secure from unauthorized users.
- Support for the establishment of keys for the data transfer.
- To support pseudonym.
- It secures a data that is being accessed by the attacker which will access and modify the data that is transmitted from the sender node to the receiver node via an intermediate node while transmitting a data between nodes.

2. RELATED WORK

2.1. Research on network security

The Network security adopts a number of policies and rules to allow only the accessed users, unidentified users. The security involves the trusted persons to access the data, and which can be controlled by the network administrator. Here the users can have the choice to choose passwords and other trusted data so that the users will have access to that data. The simplest way o to protect network infrastructure is by giving a variety of named and passwords. Network security plays a very important role in the category that is networked in computer and security information. The system administrator will handle the network security process. Here network can manage the other related tools in the security which includes software and network hardware is used to protect a network and the resources.

2.2. Research on network routing protocol

A Routing protocol describes, how the routers will communicate with each other. The Routing protocol first shares the information to the immediate neighbours and then overall network. This type of routers will gather information which includes the network information. The Router will maintain a separate routing table which keeps track of routing information in the network. IP Routing process is defined as the moving of packets between different networks. The Routing Protocol will share routing information updates so that it contains the network related information and that information will be stored in the routing table. The Routing table will check the possible route for the packets. This router needs an intermediate node to switch the packets between them. Routers interfaces are associated with each different network. Routers are used to make switching decisions.

2.3. Research on existing protocol

The existing protocol is used to complete valid routers along each pair of nodes in a network to transfer with each other on any time. The goal of the network is to guarantee a valid routing protocol through all the schedule with lowermost price and accuracy. This conventional proactive protocol sometimes recomputed with their table, but due to their intrinsic nature based on their direct paths, they choose the lengthier links that ensure quicker routing. But they are agreeable to quick breakings as devices are moves around. Referencing this shortest day definitely allows a good tracking of the topology's variations and best routes for data transmission.

Some of the existing protocols used in the proposed systems are:

- DES (Data encryption standard) and AES (Advanced encryption standard) protocols for improving presentation which includes costs, delay, packet falling in the existence of an intermediate node.
- An AODV (Ad hoc On-demand distance vector) is a mobile ado network for routing protocol and other wireless ad hoc networks.
- An RSA (Rivets aid Shamir Leonard Adelman) is an asymmetric cryptographic algorithm. **RSA** is a cryptographic system for public-key encryption, and it is commonly used for acquiring delicate data, particularly when being directed over an uncertain network such as the Internet.

3. INPUT AND OUTPUT DESIGN SPECIFICATIONS

3.1 Input Design

Initially, the input is the basic data that is used for the output production. The input design will act as an interface between the user and the information system. When input design is developing, the developer's needs to consider input devices which include PC, Mobile. Therefore, the system quantity of output depends on the input device chosen. Development of etc.…input design should include the following properties:

- It should make sure that it manages major purpose such as data storage and data retrieval.
- It makes sure about what data has to be given as input.
- It makes complete user attention.
- It makes simple and more consistent.

3.2 Objective

1. Input design consists of a number of methods or functions to remove simple input errors by the users. It guides us by showing the correct way of getting the information from the system.
2. They check the trial for data entries and other functions are initiated by using transaction logs, so they can record all the changes which can be done in the database and provide high security and its recoveries all the data in case of any failure.
3. The functions of this process are :
   - To create an input data and form all procedures.
   - To lower the volume and create a layout that is easy to follow.
   - To check the functions for data when entered and develop effective input controls.

3.3 Output Design

The output is the one basic entity which is a most important factor that satisfies the user requirements and it shows information clarity. Most intelligent and accurate quality of output design tries to enhance the relationship of the system which feels the user make decisions. The system should require a proper output and the design of an output plays a major role. While designing an output the developers will recognize the types of output required and consider only the required outputs.

- The main purpose of the developer is to satisfy user requirements and so eliminates the unwanted output.
- To make the output design should meet the user requirements.
- To pass only the required piece of output.
- The data should be delivered to the right person so in such a way that the data should be prepared.
- The output should be available within a given time to make good decisions.

4. MODULES CATEGORIZATION

Five modules have been mainly defined in order to ensure privacy protection and security: Encryption, Route request, route reply, Data transfer, and Decryption categorization.

4.1 Encryption

The encryption process is used by the plaintext to check out the text data is convertible from readable form to an encrypted version so the encrypted data is decrypted only from an entity which is having access to allow a decryption key. It plays a vital role to ensure data protection. This is suited for one node to another node end for the protection of data. This process is usually used to provide the data information over the internet and that is sent for the network to browse the data and it includes passwords, usernames and other personal or private information should be considered. Most of the organization and individuals commonly uses an encryption method to ensure the private data which is stored on a computer, server and another device like hard disk etc. Most companies use an encryption method so that company's data and trade secrets easily maintained where only the authorized person can access or view the which ensures security.

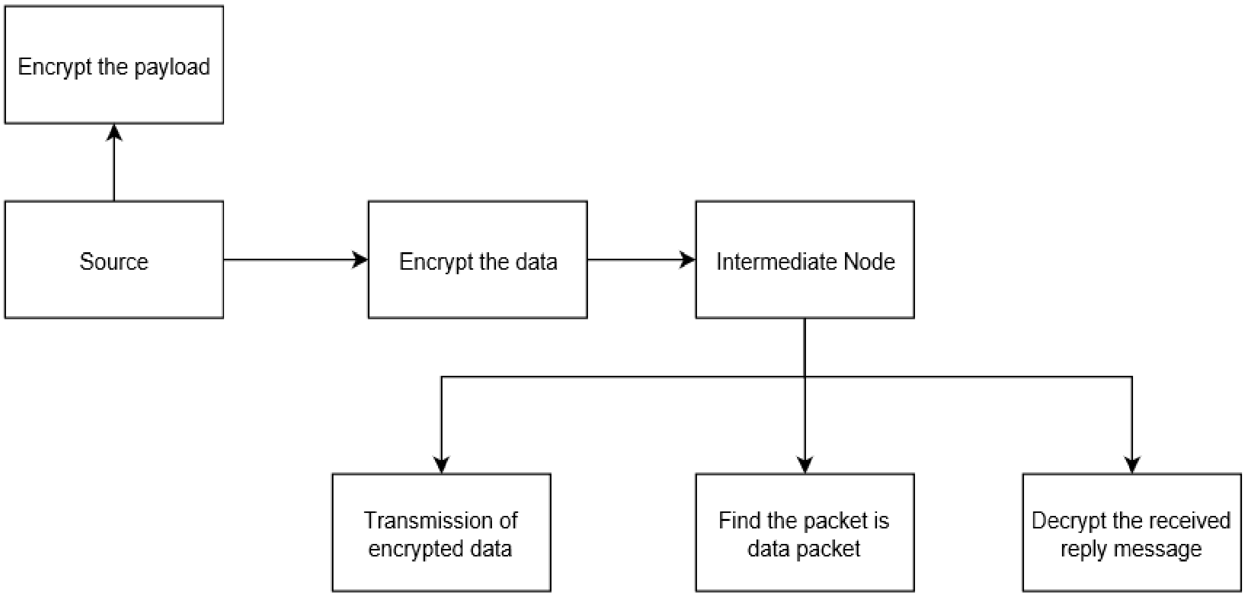

Encrypt the payload
Source
Encrypt the data
Intermediate Node
Transmission of encrypted data
Find the packet is data packet
Decrypt the received reply message

Fig. 1: Data Encryption

4.2 Route request

The sender and the receiver have the intermediate devices in between. Source device will pass a message to the receiver via an intermediate node. Each node will maintain a separate temporary entry for the Sequence Number, Previous Hop and next hop details. Source device sends that request message and it also sends the pseudonym to the next node. Then that intermediate node would find out session key that satisfies pseudonyms of the source. So, the user will make use of session key for decrypting a ciphertext that is sent from sender node.

4.3 Route reply

After the route message reaches the receiver end it decrypts the data. Key, also generates the route reply key and pseudonyms and forward it to the previous node from where it receives the request message until reply message reaches the source it sends through the intermediate nodes.

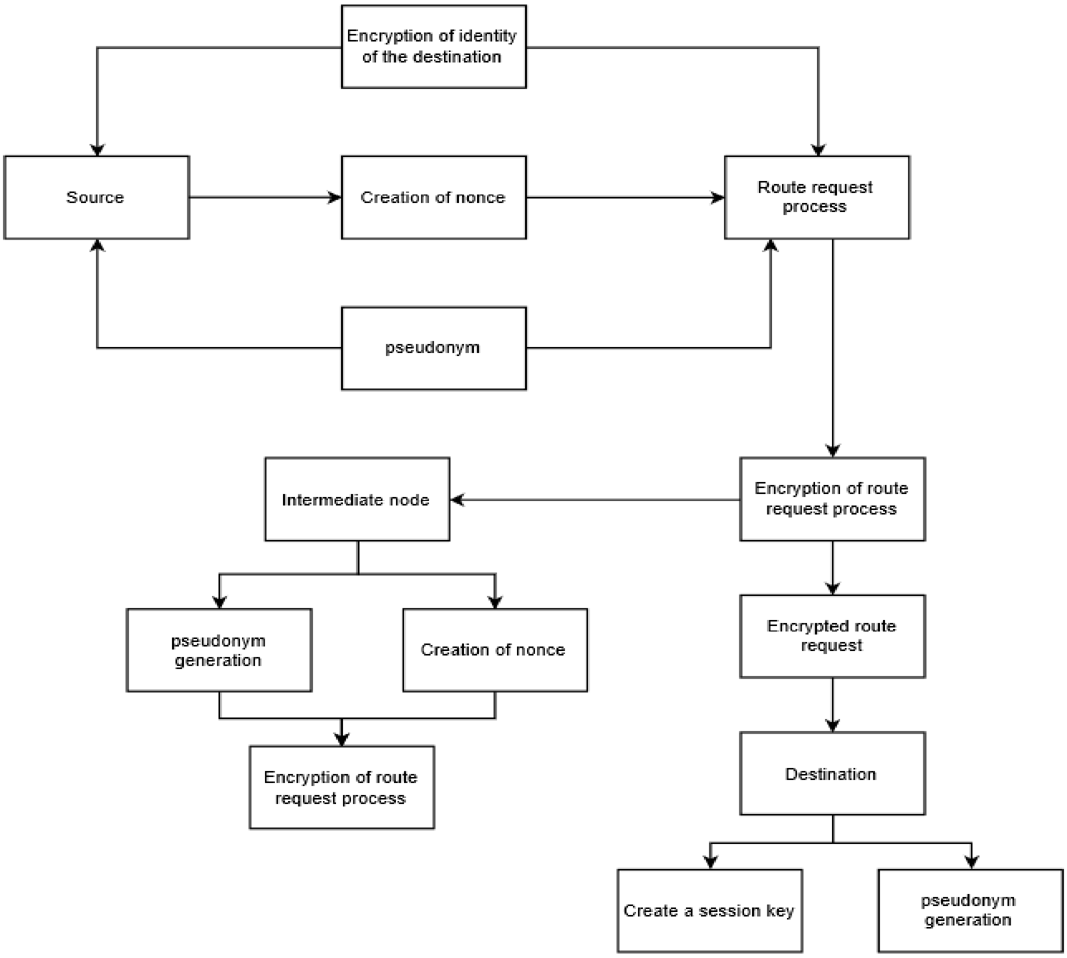


Fig. 2: How the route request is sent to receiver

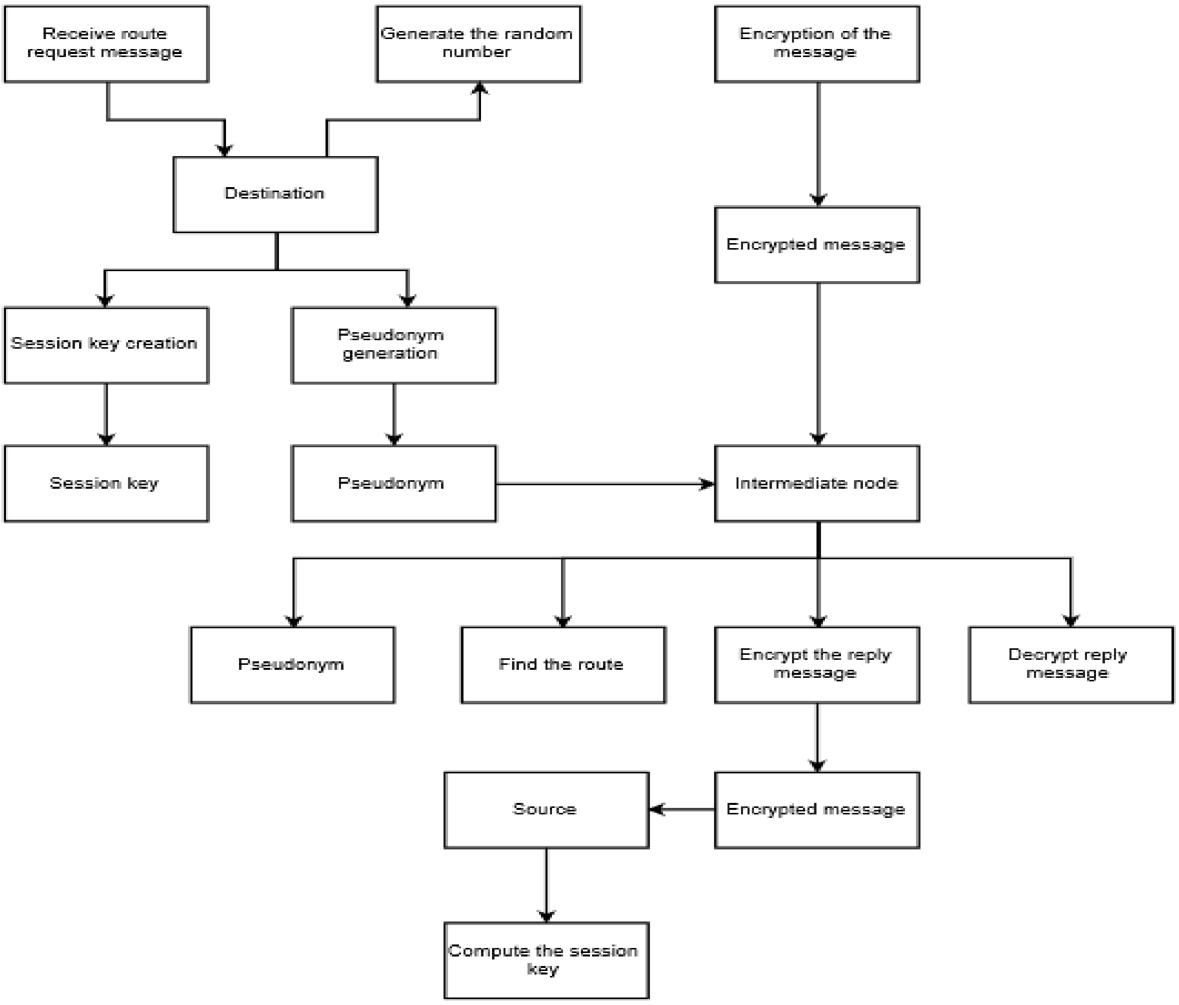


Fig. 3: Route request replied to the sender

4.4 Data transfer

Data transfer is the process passing data from one computer device to another device that is from the source node to the destination node. Data transfer can be done by using computing techniques and technologies. Data is transferred between sources to the destination via the intermediate over the communication channel. The process enables communication and its movements between devices.

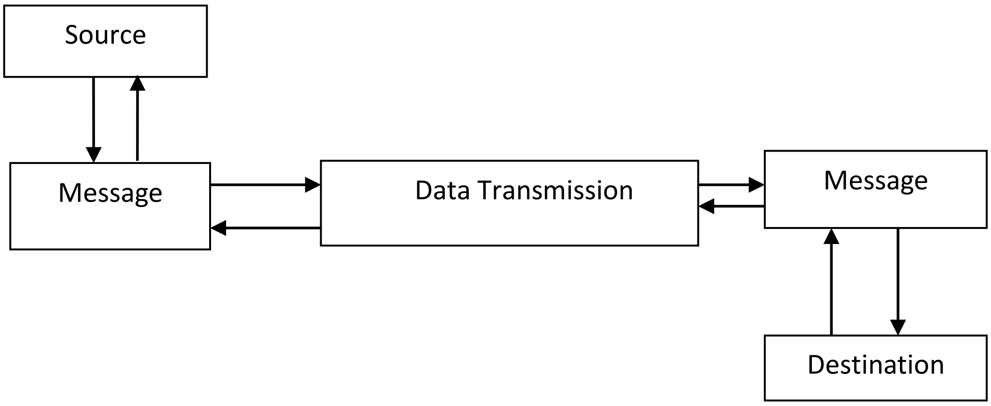


Fig. 4: Data transfer

4.5 Decryption

Decryption method is used for converting from received cipher to plain text so that the device can easily read. It is used to describe a process of manually un-unified data or using some proper codes or keys un-encrypting data. The main theme of the decryption method is to protect the data from unauthorized users so that only the authorized users can access the information so it prevents someone to steal the sensitive information which enhances the security in terms of decrypting data. Most of the companies mainly focus on confidentiality

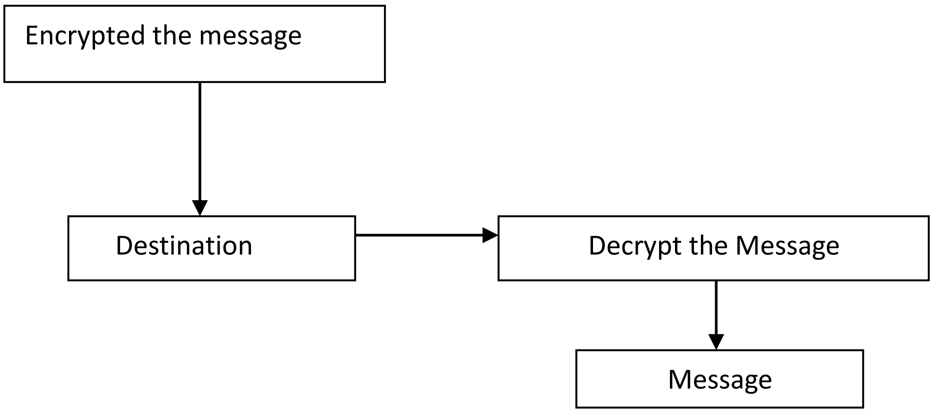


Fig. 5: The received message is decrypted by the receiver

5. ARCHITECTURE

According to the existing routing protocol, privacy protection is the major issue in the network. The JBATS protocol uses encoding and decoding approach for transferring data between sender and receiver node in a protected way. Transmitting the message from one node to another by using an intermediate node and maintaining confidentiality.

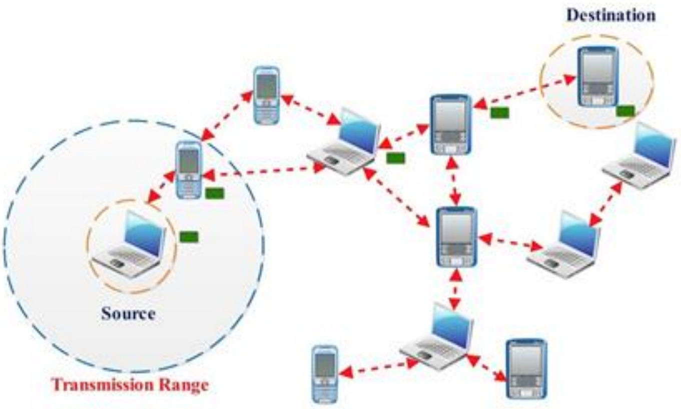


Fig. 6: **Design of JBATS protocol system architecture**

The system architecture shown above summarizes the following steps:

- The user first logs. If the user doesn't have an account, then he must first register to an account by providing the necessary information and the details are stored in the database.
- Once the user logs in him can establish the key. The key is encrypted by the sender and decrypted by the receiver.
- If neighbour node tries to access the data but they can't decrypt the message the only receiver can decrypt the message.
- Type of data would be requested from the sender, reply from the receiver and transferring a data.
- In a request from the sender, first, the message is encrypted by destination ID and send through the intermediate node.
- The neighbour node receives the encrypted ID and tries to decrypt, the received value of the destination it successfully decrypts the message if it is intermediate node cannot decrypt the message.
- In route reply destination is ready to send the message to the source now the source ID is decrypted and sends through the intermediate node.
- In data transfer, the data is encrypted by the sender and send to the receiver.

Contributions to the field:

- The proposed scheme improves security and privacy protection.
- The proposed scheme uses the concept of keys establishment.

5.1. Block diagram

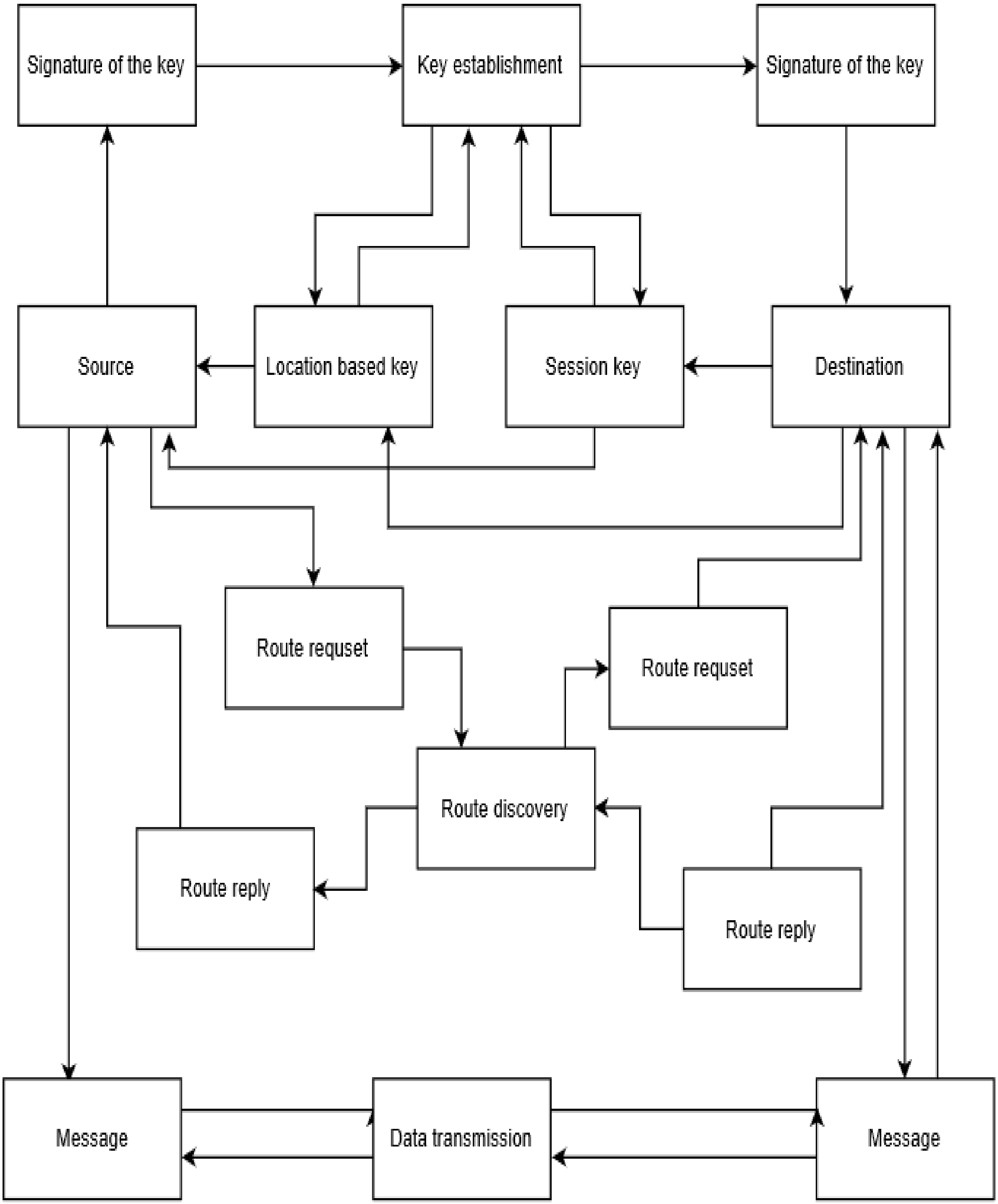


Fig. 7: Block diagram of data transmission using JBATS protocol

6. SYSTEM DESIGN

6.1 Data-flow diagram

If the user doesn't have an account, then he must first register to an account by providing the necessary information and the details are stored in the database. Once the user logged in, the user can establish the key. The key is encrypted by the sender and decrypted by the receiver. If neighbour node tries to access the data but they can't decrypt the message the only receiver can decrypt the message. Both the node and neighbour node can transfer the session key and the neighbour node produces the key and directs it to the node. In data transfer, the data is encrypted by the sender and send to the receiver.

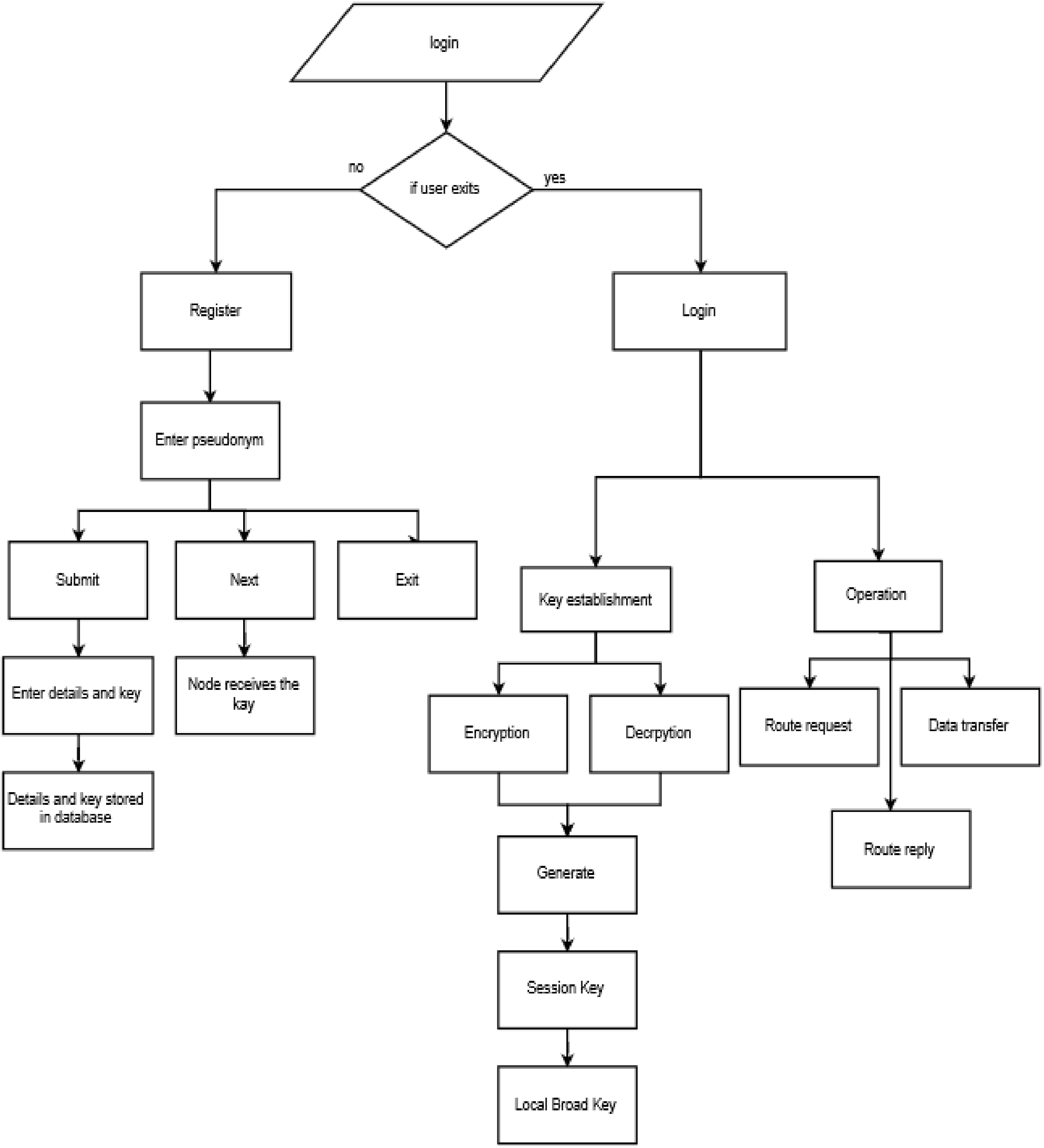


Fig. 8: The data-flow diagram representing the protection of data and security

6.2 UML diagrams

It stays used in the area of software engineering. This was used for developing and modeling language (C, C++, etc..,) in software engineering, and we can visualize the design of a system using UML.

- UML diagram makes the user understand easily
- The creation of UML was originally motivated for designing notational systems and approaches to software design.
- UML defines the notation, semantics and syntax for diagrams while designing.
- UML as some rules for designing for example object constraint language (OCL), object-oriented language (OOL).
- UML support complex level progress concepts such as collaborations, frameworks, patterns, and components.

6.3 Use case diagram

Use case diagram is a kind of behaviour figure defined and produced by the user from a use-case study. It provides a graphical view of the system functionality in terms of actors; their goal is dependences among the use-case. The main resolution of use case figure is the system functionality is performed by which actor. Characters of the actors in the system can be understood easily.

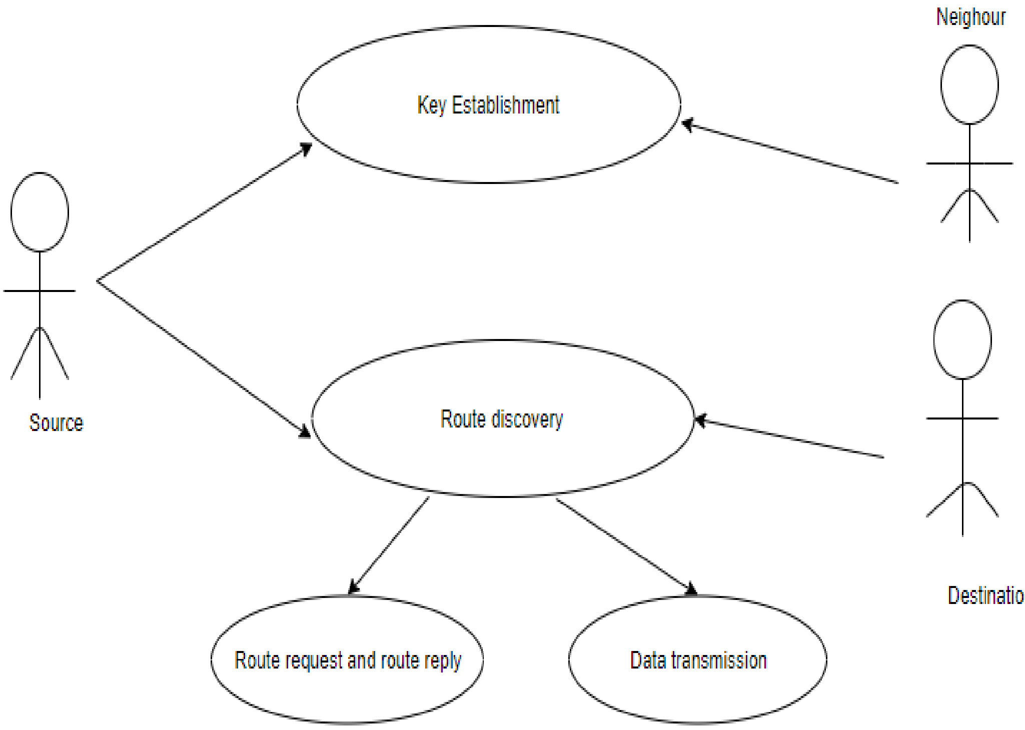


Fig. 9: A use case diagram depicting the functions that are performed by the corresponding actors

6.4 Class diagram

A class figure is a structure figure which cannot be changed .class diagram represents the system's attributes, method, and the relationships between the classes. The class diagram is the structure chunk of object-oriented modelling. It uses together conceptual modelling and detailed modelling. Conceptual modelling of the regular application, and complete modelling converting the models into programming code. The class figure describes attributes and class operations. Class diagram most commonly used in modelling of the object-oriented system.

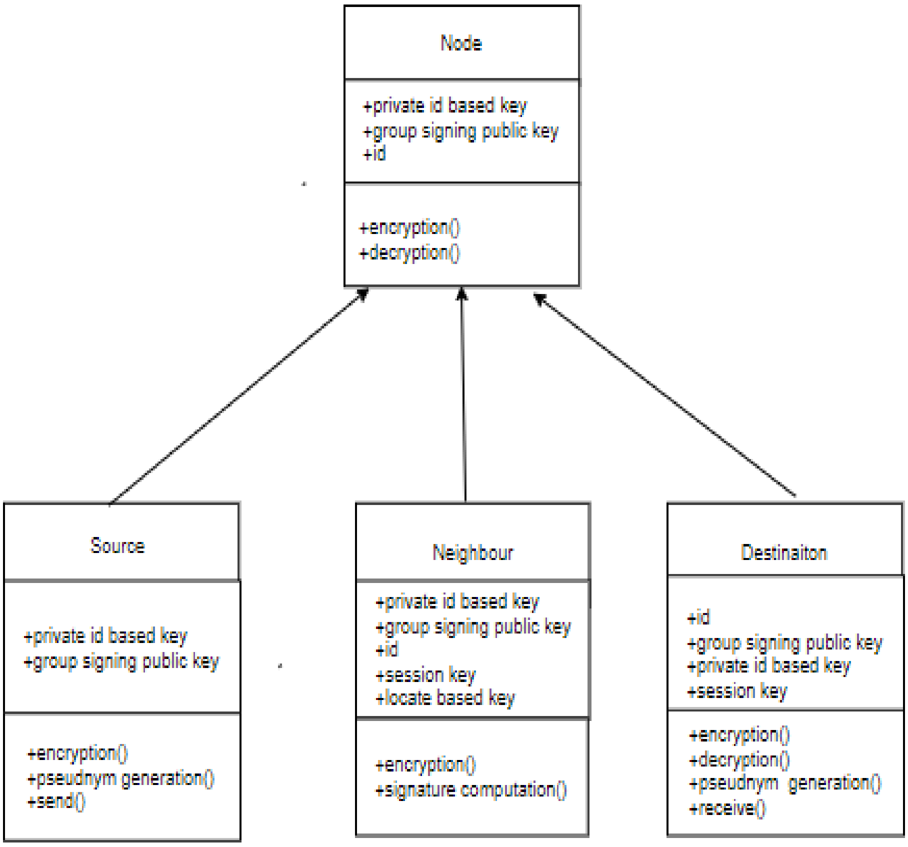


Fig. 10: A Class Diagram representing the various classes, attributes, and operations with respect to our model

6.5 Sequence diagram

A sequence figure is a kind of communication between the figure and the processes that display how the procedures work with one another and in which direction. It is the construction of a Message Sequence Chart. A sequence figure displays the connections decided with respect to time. Sequence diagrams normally related by the use-case realization in the Logical View of the system below progress. The Sequence Figure replicas the combination of objects based on time order. It displays how the object interacts by other in a specific structure of use-case.

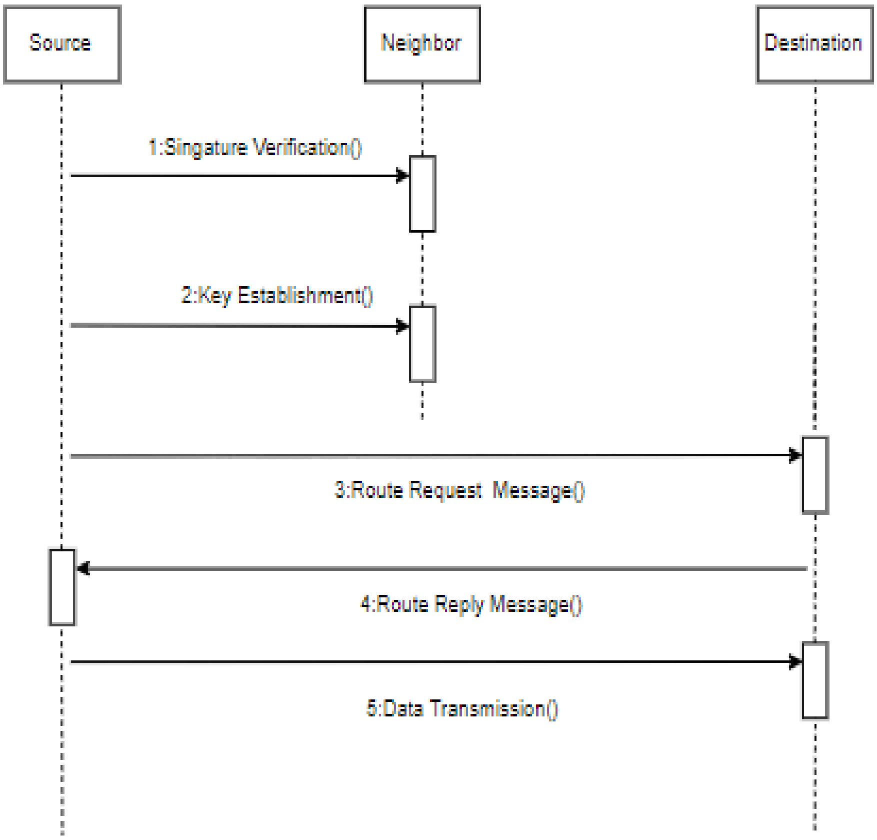


Fig. 11: A Sequence diagram depicting how the control flows through the various sections of our system

6.6 Activity Diagram

This diagram is similar to data flow diagram that is step by step actions and movements with care for the option. Activity diagram can be used to explain the business and working step-by-step workflows of components in a system. Activity diagram displays the general movement of control.

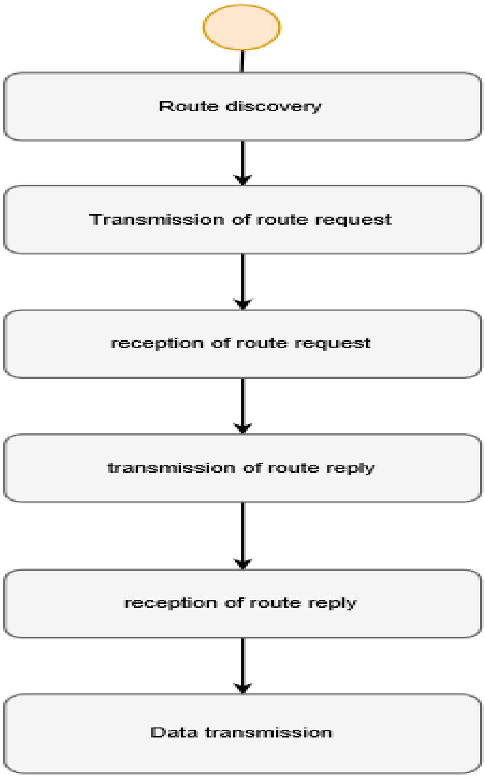

Route discovery
Transmission of route request
reception of route request
transmission of route reply
reception of route reply
Data transmission

Fig. 12: An Activity diagram representing the workflow of the components in our system

7. RESULTS

The result is evaluated using data from the MySQL database. We make use of a database to know the details of the destination node and neighbour node while sending the data or packet. We will provide strong privacy and security in presence of malicious node even the neighbour node cannot decrypt the data. The only destination node can decrypt the data. The encrypted message is sent to the destination and they share the group signature and key. The JBATS protocol is more efficient, reliable and flexible compared to other protocols.

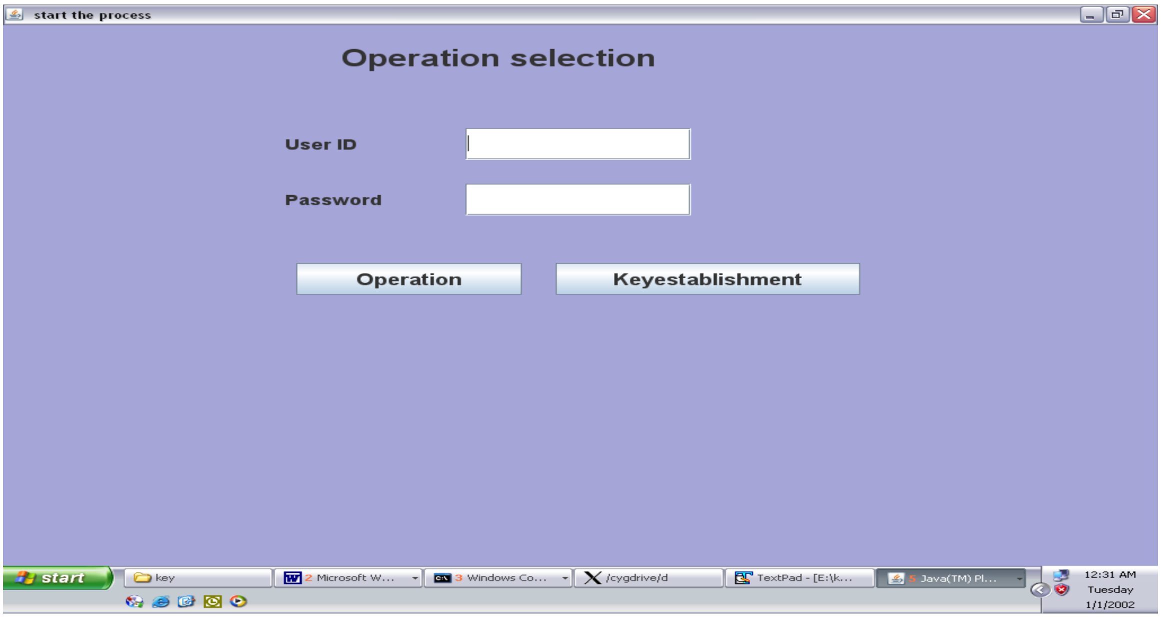
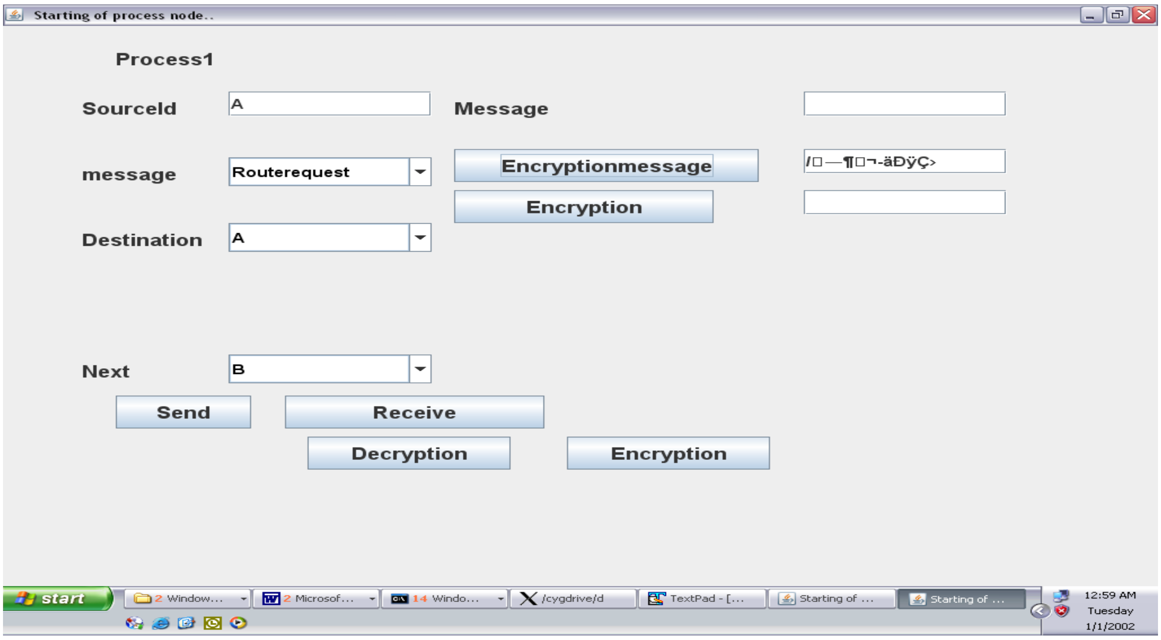


Fig. 13: Selection of operation



SourceId A

Message

message Routerequest

/□—¶□¬-äÐÿÇ>

Destination A

Next B

Fig. 14: Selects the type of message and encrypts that message and send it to the neighbour node. After selecting the type of message and it will select the next node after neighbour press the Decrypt Button node press the Encryption message button

8. CONCLUSION

It keeps mobility information in a protected way. The data is encrypted and decrypted in JBATS routing protocol. First, we send a route request message and receive a response then we send a route reply message after we get the response form the destination, we send the data. The design of JBATS protocol offers the strongest privacy protection in the Network. The JBATS protocol not only focuses on providing complete security, but it also secures from the external attacks.

9. REFERENCES

[1] Diti priya Sinha, Uma Bhattacharya and Rituparna Chaki, "RSRP: A Robust Secure Routing Protocol in MANET", International Journal of Scientific Research in Computer Science and Information Technology, vol.39, no.2, Jan.2017.

[2] Mohamed Amine Abdi, Abdelfettah Belghith and Khalil Drira, "SARP: Synchronous Adaptive Routing Protocol for MANTETs", Indonesia Journal of Electrical Engineering and computer science, vol.21, no.1, Mar.2017.

[3] Dr K Rama Krishna Reddy "Improved Protocol Design with Security over MANET", International Journal of Scientific Research in Computer Science and Information Technology, vol. 3, no.1, 2018

[4] Venkat Prasad and S.Magesh, ”A Survey on Encryption Algorithm Using Modern Techniques”, Indonesia Journal of Electrical Engineering and computer science, vol.117, no.16, 2017.

[5] Hu, Y. C., Johnson, D. B., & Perrig, A., SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Ad Hoc Networks Journal Elsevier, 1, 1, 2003, 175-192.

[6] P. Samar, Z. Haas, Strategies for broadcasting updates by proactive routing protocols in mobile ad hoc networks, IEEEMILCOM 2002, Anaheim, CA, USA.

[7] M.G.G. Pei, T. Chen, Fisheye state routing in Mobile Ad hoc Networks, in ACM SIGCOMM’94 Conference on Communications Architectures, Protocols and Applications.

[8] Amthan, A., & Baradwaj, B. A., Secure Routing Scheme in MANETs using Secret Key Sharing, International Journal of Computer Applications, 22,1, 2011.

[9] Dang, L., Xu, J., Li, H. & Dang, N., and DASR: Distributed Anonymous Secure Routing with Good Scalability for Mobile Ad Hoc Networks, Proceedings of 5th IEEE Asia-Pacific Services Computing Conference. Hangzhou, China: IEEE Computer Society, 454-461, 2010.

[10] Grobler, T. L., & Penzhorn, W. T., Fast Decryption Methods for RSA Cryptosystem, 7th AFRICON Conference. Paris, France: IEEEXPLORE, 2004.

[11] Hu, Y. C., Johnson, D. B., & Perrig, A., SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Adhoc Networks. Ad Hoc Networks Journal Elsevier, 1, 1, 2003, 175-192.

[13] Nagesh Kumar, Jawahar Thakur, Arvind Kalia on “Performance Analysis of Symmetric Key Cryptography Algorithms: DES, AES and Blowfish —in An International Journal of Engineering Sciences ISSN: 22296913 Issue Sept 2011, Vol.4, pp.28-3

BIOGRAPHY

Arun Kumar S.
Assistant Professor
Department of Computer Science Engineering
Sapthagiri College of Engineering , Bengaluru, Karnataka

Swetha S.
Student
Department of Computer Science Engineering
Sapthagiri College of Engineering , Bengaluru, Karnataka

Jayashree C. Y.
Student
Department of Computer Science Engineering
Sapthagiri College of Engineering , Bengaluru, Karnataka

Thriveni L.
Student
Department of Computer Science Engineering
Sapthagiri College of Engineering , Bengaluru, Karnataka

Bhuvanashree V.
Student
Department of Computer Science Engineering
Sapthagiri College of Engineering , Bengaluru, Karnataka

Renu R.
Student
Department of Computer Science Engineering
Sapthagiri College of Engineering , Bengaluru, Karnataka