Secret Key Extraction from Wireless Signal Strength in Real Environments

A Dissertation Submitted to

P.E.S COLLEGE OF ENGINEERING, MANDYA

(An Autonomous Institution under Visvesvaraya Technological University, Belgaum)

In partial fulfilment of the requirement
for the award of the Degree

BACHELOR OF ENGINEERING
IN
COMPUTER SCIENCE & ENGINEERING

Submitted by

OBAIDULLAH DANISH (4PS11CS073)
PRAVEEN KUMAR (4PS11CS080)
RAHUL KUMAR (4PS11CS087)
SUNIL KUMAR (4PS11CS119)

Under the guidance of

Mr. M. Jayashankar
Asst. Professor
Dept. of CS&E, PESCE, Mandya

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
P.E.S College of Engineering, Mandya

2014-2015

P.E.S COLLEGE OF ENGINEERING
MANDYA-571401
(An Autonomous Institution Affiliated to VTU, Belgaum)
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Certificate

This is to certify that ***OBAIDULLAH DANISH (4PS11CS073), PRAVEEN KUMAR (4PS11CS080), RAHUL KUMAR(4PS11CS087), SUNIL KUMAR(4PS11CS119)*** has satisfactorily completed the dissertation work entitled ***"Secret Key Extraction from Wireless Signal Strength in Real Environment"*** in partial fulfillment for the award of degree of ***Bachelor of Engineering*** in ***Computer Science & Engineering*** in P.E.S. College of Engineering, Mandya, an Autonomous Institution affiliated to Visvesvaraya Technological University, Belgaum during the year 2014-15. It is certified that all corrections/suggestions indicated in Internal Assessment have been incorporated in the report deposited in the Library. The Project has been approved as it satisfies the academic requirements in respect to project work prescribed for the degree in Bachelor of Engineering.

Signature of Guide
Mr. M Jayashankar
Asst. Professor, Dept. of CS&E,
PESCE, Mandya.

Signature of HOD
Dr. M.C. Padma
Professor, Dept. of CS&E,
PESCE, Mandya.

Signature of Principal
Dr. Sridhar V
PESCE, Mandya

Details of Project Work Viva Voce Examination held			
Sl. No.	**Examiners**		**Date**
	Name	**Signature**	
1.			
2.			

DECLARATION

We, **Obaidullah Danish, Praveen Kumar**, **Rahul Kumar and Sunil Kumar** students of final semester, B.E., Computer Science & Engineering, P.E.S. College of Engineering, Mandya, hereby declare that this dissertation work entitled **"Secret Key Extraction from Wireless Signal Strength in Real Environments"** has been independently carried out by us under the guidance of **Mr. M. Jayashankar,** Assistant Professor, Dept. of Computer Science & Engineering, PESCE, Mandya and submitted in partial fulfillment of the requirement for the award of the degree of **Bachelor of Engineering in Computer Science & Engineering** during the academic year 2014-15.

We further declare that the matter embodied in this dissertation has not been submitted previously for the award of any degree to any other university.

Place : Mandya

Date :

Obaidullah Danish (4PS11CS073)

Praveen Kumar (4PS11CS080)

Rahul Kumar (4PS11CS087)

Sunil Kumar (**4PS11CS119**)

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany successful completion of any task would be incomplete without the mention of people who made it possible. We take this opportunity to express our sincere gratitude to all those who have helped us in this project.

We have immense pleasure in expressing our thanks to **Dr. Sridhar V**, Principal, PESCE, Mandya for providing all the facilities for the successful completion of the project.

It is our great privilege to express our sincere and heartfelt thanks to our Head of the Dept. **Dr. Padma M C** Department of Computer Science & Engineering, for her constant encouragement, valuable suggestions and support in bringing out this dissertation successfully.

We would like to express my heartfelt gratitude to our guide **Mr. M Jayashankar**, Assistant Professor, Dept. of Computer Science & Engineering for their encouragement and help through the tenure of the project.

Also, We would like to express our gratitude to all the teaching and non-teaching staff for their kind co-operation and support during the course of our project work. Finally we would like to thank our parents and all our friends for their constant support.

Obaidullah Danish (4PS11CS073)

Praveen Kumar (4PS11CS080)

Rahul Kumar (4PS11CS087)

Sunil Kumar (**4PS11CS119**)

ABSTRACT

We evaluate the effectiveness of secret key extraction, for private communication between two wireless devices, from the received signal strength (RSS) variations on the wireless channel between the two devices. We use real world measurements of RSS in a variety of environments and settings. The results from our experiments with 802.11-based laptops show that in certain environments, due to lack of variations in the wireless channel, the extracted bits have very low entropy making these bits unsuitable for a secret key and an adversary can cause predictable key generation in these static environments, and in dynamic scenarios where the two devices are mobile, and/or where there is a significant movement in the environment, high entropy bits are obtained fairly quickly. Building on the strengths of existing secret key extraction approaches, we develop an environment adaptive secret key generation scheme that uses an adaptive lossy quantizer in conjunction with Cascade-based information reconciliation and privacy amplification. Our measurements show that our scheme, in comparison to the existing ones that we evaluate, performs the best in terms of generating high entropy bits at a high bit rate. The secret key bit streams generated by our scheme also pass the randomness tests of the NIST test suite that we conduct. We also build and evaluate the performance of secret key extraction using small, lowpower, hand-held devices—Google Nexus One phones—that are equipped 802.11 wireless network cards and we evaluate secret key extraction in a multiple input multiple output (MIMO)-like sensor network testbed that we create using multiple TelosB sensor nodes. We find that our MIMO-like sensor environment produces prohibitively high bit mismatch, which we address using an iterative distillation stage that we add to the key extraction process.

CONTENTS

CHAPTER	PAGE NO
1. INTRODUCTION	**1**
2. LITERATURE SURVEY	**4**
2.1 Converting Signal Strength Percentage to DBM Values	4
2.2 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications	4
2.3 Wireless Secret Key Generation Exploiting Reactance - Domain Scalar Response of Multipath Fading Channels	5
2.4 Robust Key Generation from Signal Envelopes in Wireless Networks	5
2.5 Experimental Quantum Cryptography	6
3. SYSTEM ANALYSIS	**7**
3.1 Existing system	7
3.2 Proposed system	8
4. SYSTEM REQUIREMENT SPECIFICATION	**9**
4.1 Hardware Requirements	9
4.2 Software Requirements	9
5. SYSTEM DESIGN	**10**
5.1 Architecture	
5.2 Data Flow Diagram	12
5.2.1 Level 0	12
5.2.2 Level 1	12
5.2.3 Level 2	13
5.2.4 Level 3	14
5.3 Use Case Diagram	15
5.4 Sequence Diagram	16
5.5 Class Diagram	17

6. METHODOLOGY **18**

6.1 Components of RSS-Based Secret Key Extraction 18

6.1.1 Quantization 18

6.1.2 Information Reconciliation 19

6.1.3 Privacy Amplification 19

6.2 Existing Approaches 20

6.2.1 Entropy 20

6.2.2 Bit Mismatch Rate 20

6.2.3 Secret Bit Rate 20

7. IMPLEMENTATION **21**

7.1 Modules 21

7.1.1 Node Design 21

7.1.2 Route Request 22

7.1.3 Route Response 22

7.1.4 Key Generation 22

7.1.5 Encryption 22

7.1.6 Message Transfer Agent 22

7.1.7 Receiver 23

7.1.8 Decryption 23

8. TESTING **24**

8.1 Unit Testing 24

8.2 Functional Testing 24

8.3 System Testing 25

8.4 Performance Testing 25

8.5 Integration Testing 25

8.6 Acceptance Testing 26

CONCLUSION **28**

FUTURE ENHANCEMENTS **29**

REFERENCES **30**

SNAP SHOTS **31**

CHAPTER 1

INTRODUCTION

Secret key establishment is a fundamental requirement for private communication between two entities. Currently, the most common method for establishing a secret key is by using public key cryptography. However, public key cryptography consumes significant amount of computing resources and power which might not be available in certain scenarios (e.g., sensor networks). More importantly, concerns about the security of public keys in the future have spawned research on methods that do not use public keys.

Quantum cryptography is a good example of an innovation that does not use public keys. It uses the laws of Quantum theory, specifically Heisenberg's uncertainty principle, for sharing a secret key between two end points. Although quantum cryptography applications have started to appear recently they are still very rare and expensive. A less expensive and more flexible solution to the problem of sharing secret keys between wireless nodes (say Alice and Bob) is to extract secret bits from the inherently random spatial and temporal variations of the reciprocal wireless channel between them. Essentially, the radio channel is a time and space varying filter that at any point in time has the identical filter response for signals sent from Alice to Bob as for signals sent from Bob to Alice.

Received signal strength (RSS) is a popular statistic of the radio channel and can be used as the source of secret information shared between a transmitter and receiver. We use RSS as a channel statistic, primarily because of the fact that most of the current of-the-shelf wireless cards, without any modification, can measure it on a per frame basis. The variation over time of the RSS, which is caused by motion and multipath fading, can be quantized and used for generating secret keys. The mean RSS value, a somewhat predictable function of distance, must be filtered out of the measured RSS signal to ensure that an attacker cannot use the knowledge of the distance between key establishing entities to guess some portions of the key.

These RSS temporal variations, as measured by Alice and Bob, cannot be measured by an eavesdropper (say Eve) from another location unless she is physically very close to Alice or Bob. However, due to non-ideal conditions, including limited capabilities of the wireless hardware, Alice and Bob are unable to obtain identical measurements of the channel. This asymmetry in measurements brings up the challenge of how to make Alice and Bob agree upon the same bits without giving out too much information on the channel that can be used by Eve to recreate secret bits between Alice and Bob.

We are using two well-known techniques from quantum cryptography information reconciliation and privacy amplification, to tackle the challenge caused by RSS measurement asymmetry. Information reconciliation techniques leak out minimal information to correct those bits that do not match at Alice and Bob. Privacy amplification reduces the amount of information the attacker can have about the derived key. This is achieved by letting both Alice and Bob use universal hash functions, chosen at random from a publicly known set of such functions, to transform the reconciled bit stream into a nearly perfect random bit stream.

Most of the previous research work on RSS-based secret key extraction is based on either simulations or theoretical analysis. There is a very little research on evaluating how effective RSS-based key extraction is in real environments under real settings. We address this important limitation of the existing research in this paper with the help of wide-scale real life measurements in both static and dynamic environments. In order to perform our measurements and subsequent evaluations, we implement different RSS quantization techniques in conjunction with information reconciliation and privacy amplification.

We first collect measurements under different environments to generically evaluate the effectiveness of secret key generation. We find that under certain environments due to lack of variations in the channel, the extracted key bits have very low entropy making these bits unsuitable for a secret key. Interestingly, we also find that an adversary can cause predictable key generation in these static environments. However, in scenarios where Alice and Bob are mobile, and/or where there is a

significant movement in the environment, we find that high entropy bits are obtained fairly quickly.

Next, building on the strengths of the existing schemes, we develop an environment adaptive secret key generation scheme that uses an adaptive lossy quantizer in conjunction with Cascade-based information reconciliation and privacy amplification. Our measurements show that our scheme performs the best in terms of generating high entropy bits at a high bit rate in comparison to the existing ones that we evaluate.

CHAPTER 2

LITERATURE SURVEY

2.1 TITLE: Converting Signal Strength Percentage to DBM Values

AUTHOR: Joe Bardwell, VP of Professional Services

ABSTRACT

AiroPeek and AiroPeek NX provide a measurement of RF signal strength represented by a percentage value. The question sometimes arises as to why a percentage metric is used, and how this relates to the actual RF energy that is present in the environment. This paper discusses RF technology with sufficient detail to provide a basis for understanding the issues related to signal strength measurement.

2.2 TITLE: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

AUTHORS: Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, SanVo

ABSTRACT

This paper discusses some aspects of selecting and testing random and pseudorandom number generators. The outputs of such generators may be used in many cryptographic applications, such as the generation of key material. Generators suitable for use in cryptographic applications may need to meet stronger requirements than for other applications. In particular, their outputs must be unpredictable in the absence of knowledge of the inputs. Some criteria for characterizing and selecting appropriate generators are discussed in this document. The subject of statistical testing and its relation to cryptanalysis is also discussed, and some recommended statistical tests are provided. These tests may be useful as a first step in determining whether or not a generator is suitable for a particular cryptographic application. However, no set of statistical tests can absolutely certify a generator as appropriate for usage in a particular application, i.e., statistical testing cannot serve as a substitute for

cryptanalysis. The design and cryptanalysis of generators is outside the scope of this paper.

2.3 TITLE: Wireless Secret Key Generation Exploiting Reactance - Domain Scalar Response of Multipath Fading Channels

AUTHORS: Tomoyuki Aono, Keisuke Higuchi, Takashi Ohira, Bokuji Komiyama, and Hideichi Sasaoka

ABSTRACT

We describe a secure communication scheme that uses the random fluctuation of the natural environment of communication channels. Only the transmitter and the receiver share the communication channel characteristics. From reciprocity between a transmitter and a receiver, it is possible for them to share one-time information of their fluctuating channel. This can provide a secret key agreement scheme without key management and key distribution processes. In this paper, we propose a new secret key generation and agreement scheme that uses the fluctuation of channel characteristics with an electronically steerable parasitic array radiator (ESPAR) antenna. This antenna, which has been proposed and prototyped, is a smart antenna designed for consumers. Using the beam-forming technique of the ESPAR antenna, we can increase the fluctuation of the channel characteristics. From experimental results, we conclude that the proposed scheme has the ability to generate secret keys from the received signal strength indicator (RSSI) profile with sufficient independence.

2.4 TITLE: Robust Key Generation from Signal Envelopes in Wireless Networks

AUTHORS: Babak Azimi-sadjadi , Alejandra Mercado , Bulent Yener, et al.

ABSTRACT

The broadcast nature of a wireless link provides a natural eavesdropping and intervention capability to an adversary. Thus, securing a wireless link is essential to the security of a wireless network, and key generation algorithms are necessary for securing wireless links. However, traditional key agreement algorithms can be very costly in many settings, e.g. in wireless ad-hoc networks, since they consume scarce resources such as bandwidth and battery power. Traditional key agreement algorithms

are not suitable for wireless ad-hoc networks since they consume scarce resources such as bandwidth and battery power. This paper presents a novel approach that couples the physical layer characteristics of wireless networks with key generation algorithms. It is based on the wireless communication phenomenon known as the principle of reciprocity which states that in the absence of interference both transmitter and receiver experience the same signal envelope. The key-observation here is that the signal envelope information can provide to the two transceivers two correlated random sources that provide sufficient amounts of entropy which can be used to extract a cryptographic key.

2.5 TITLE: Experimental Quantum Cryptography

AUTHORS: Diplomarbeit von, Henning Weier

ABSTRACT

Whenever information is conveyed or processed, physical systems are involved. If information processing devices continue to get scaled down in size as they have been in the past, they will soon reach dimensions at which classical physics ceases to describe the systems correctly and quantum mechanics comes into play. Since classical systems are usually regarded as simpler, the fact that quantum effects cannot be neglected anymore seems to be disturbing at first glance. Yet, during the last few decades it was discovered that the combination of classical information theory and quantum physics offers amazing possibilities.

CHAPTER 3

SYSTEM ANALYSIS

3.1 Existing Systems

In Existing they using two well-known techniques from quantum cryptography—information reconciliation and privacy amplification, to tackle the challenge caused by RSS measurement asymmetry. Information reconciliation techniques leak out minimal information to correct those bits that do not match at Alice and Bob. Privacy amplification reduces the amount of information the attacker can have about the derived key. This is achieved by letting both Alice and Bob use universal hash functions, chosen at random from a publicly known set of such functions, to transform the reconciled bit stream into a nearly perfect random bit stream. Most of the previous research work on RSS-based secret key extraction, including that of is based on either simulations or theoretical analysis. Other than the recent work that was performed in a specific indoor environment, there is very little research on evaluating how effective RSS-based key extraction is in real environments under real settings.

Various disadvantages have been found while two wireless devices are participating in a private communication, with reference to other surveyed papers some of the major drawbacks are listed below:

- Bits drop probabilistically to maintain a high bit entropy.
- Not Secured.
- Does not use privacy amplification.
- Low output bit rate.
- The goal of this approach is to output a high entropy bit stream so that the output bit stream can be used directly as the shared secret key.

3.2 Proposed Systems

We address the important limitation of the existing research in this paper with the help of wide-scale real life measurements in both static and dynamic environments. In order to perform our measurements and subsequent evaluations, we implement different RSS quantization techniques in conjunction with information reconciliation and privacy amplification. The secret key bit streams generated by our scheme also passed the randomness tests of the NIST test suite that we conducted. In other words, our proposed scheme works against passive adversaries. Even without an authentication mechanism, the Diffie-Hellman secret key establishment scheme has found widespread use in network security protocols and standards (e.g., for providing Perfect Forward Secrecy, Strong password protocols, etc.). We expect that our scheme will provide a strong alternative to the Diffie- Hellman scheme in wireless networks. There is a growing amount of work in authenticating wireless devices based on their physical and radiometric properties.

Advantages that mark the unique nature of the proposed system are listed as follows. These advantages make the systems security get enhanced to a greater level.

- Strong password.
- One key generate at a time.
- More secure than existing system.
- Key transferred in reverse order, so difficult to trace.

CHAPTER 4

SYSTEM REQUIREMENT SPECIFICATION

A System Requirements Specification is a structured collection of information that embodies the requirements of a system. The System Requirements Specification (SRS) document describes all Hardware and Software requirements of the software under production or development.

4.1 HARDWARE REQUIREMENTS

- Processor : Any Processor above 500 MHz
- Ram : 128Mb.
- Hard Disk : 10 Gb
- Compact Disk : 650 Mb
- Input device : Standard Keyboard and Mouse
- Output device : VGA and High Resolution Monitor

4.2 SOFTWARE REQUIREMENTS

- Front End/GUI Tool : Java Swings
- Operating System : Windows
- Tools : JDK 5.0, Jcreator

CHAPTER 5

SYSTEM DESIGN

5.1 SYSTEM ARCHITECTURE

The design process of identifying the sub-systems and establishing a framework for sub-system control and communication is called system architecture design. Here the architecture design consists of 4 nodes which acts as source, destination or intermediate node and all nodes are connected with a router(Wi-Fi).

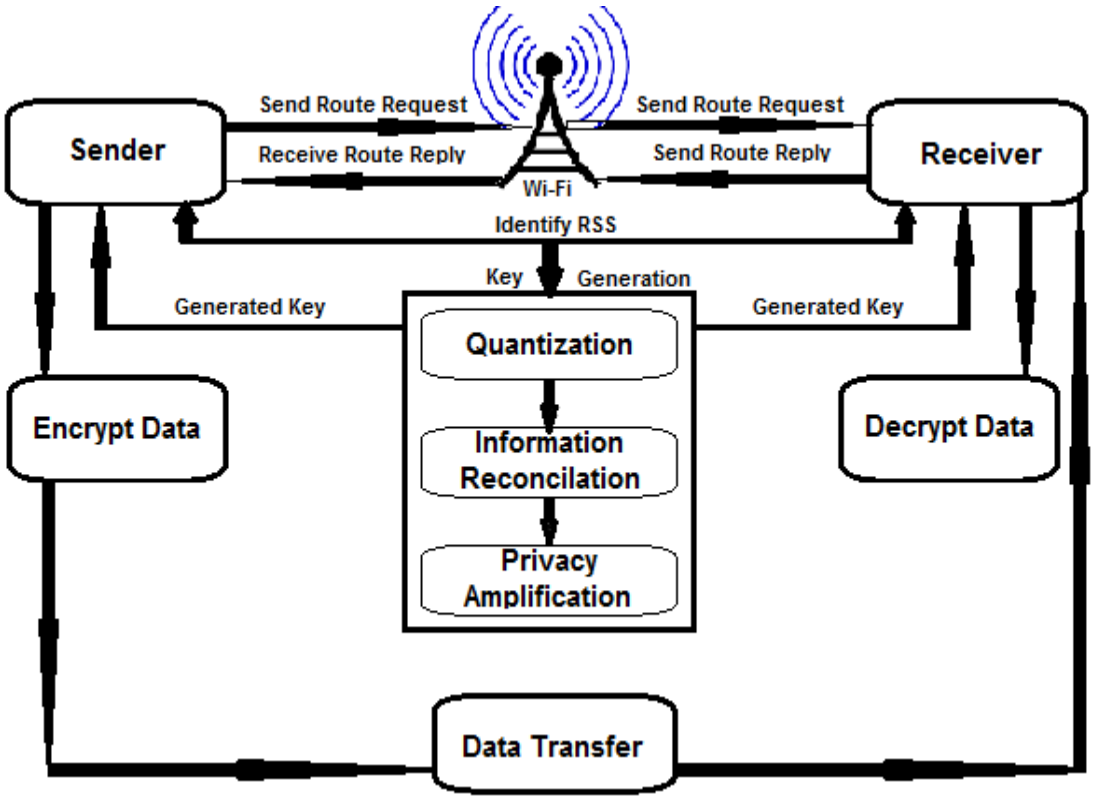


Fig 5.1: System Architecture of Secret Key Extraction

The system architecture mainly describes the system being divided into eight major modules namely, node design, route request, route response, key generation, encryption, message transfer agent, receiver and decryption. The system architecture depicts how the data is being forwarded after the network construction. The network initiation involves the node frame initialization that assigns time frame to each node. Implementation specifically involves the network construction in which the node frame initialization plays a vital role. In node frame initialization, each node that logs in into the system is assigned with the time frame that depicts the mobile nature of the node. Handler node focus on all the monitoring activity of the nodes that are active in the network and also update the necessary details in the database concerned. Encryption is based on the DES algorithm and the particular node selects the file to be encrypted, enters the key and encrypts it and sends to the destination. After the file is encrypted the source sends the encrypted data to the destination, then secret key is generated based on RSS and from the secret key random key is generated. Hash value of the key along with all these combinations are used to make the transmission secured and authenticated.

5.2 DATA FLOW DIAGRAM

5.2.1 Level Zero

Fig 5.2.1: Dataflow Diagram Level 0

- Sender reads the signal strength and generate a 8 bit Secret key.

5.2.2 Level 1

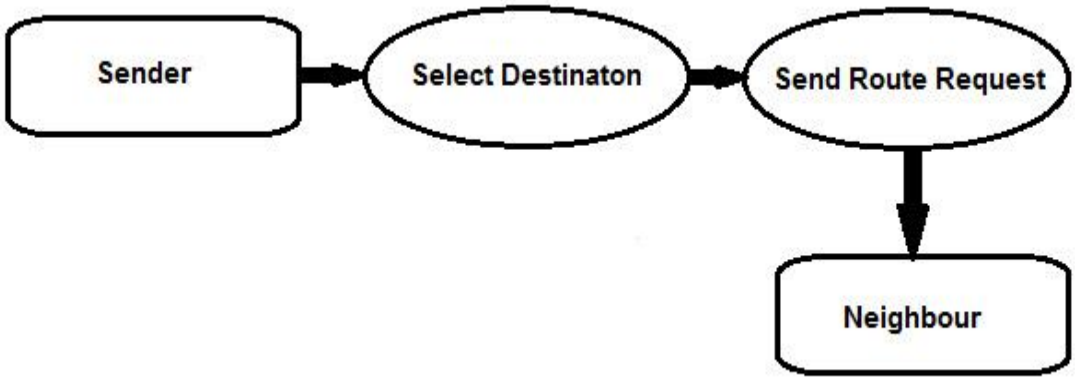


Fig 5.2.2: Dataflow Diagram Level 1

- The sender selects the destination using AODV routing protocol and sends the route request to establish the route path through its neighbour.

5.2.3 Level 2

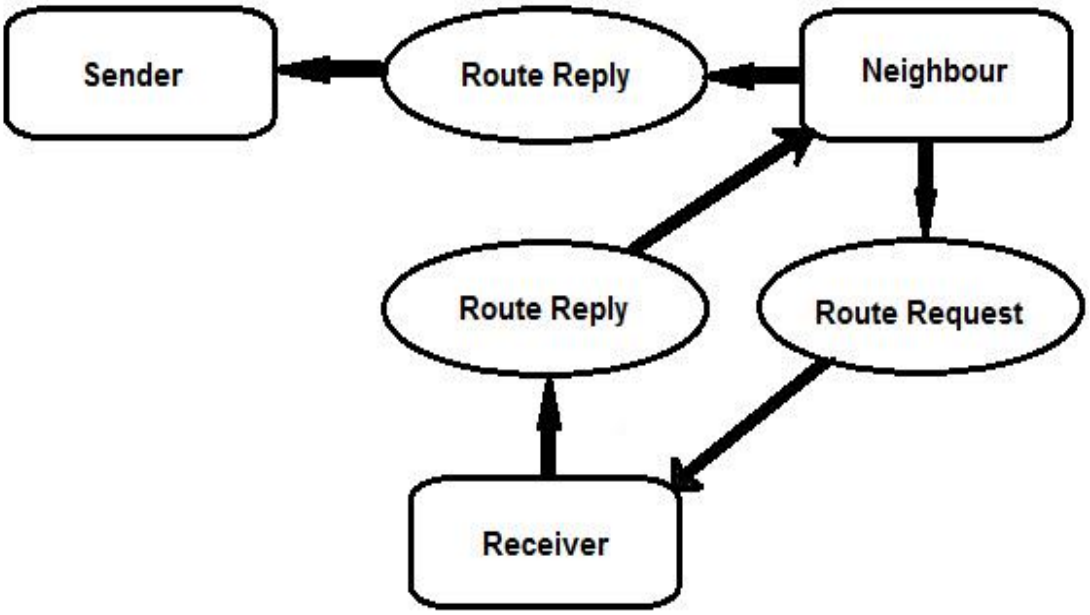


Fig 5.2.3: Dataflow Diagram Level 2

- The neighbour sends the route request to the receiver and the receiver sends the route reply to the neighbour and then finally back to the sender. This establishes the route path between the sender and receiver.

5.2.4 Level 3

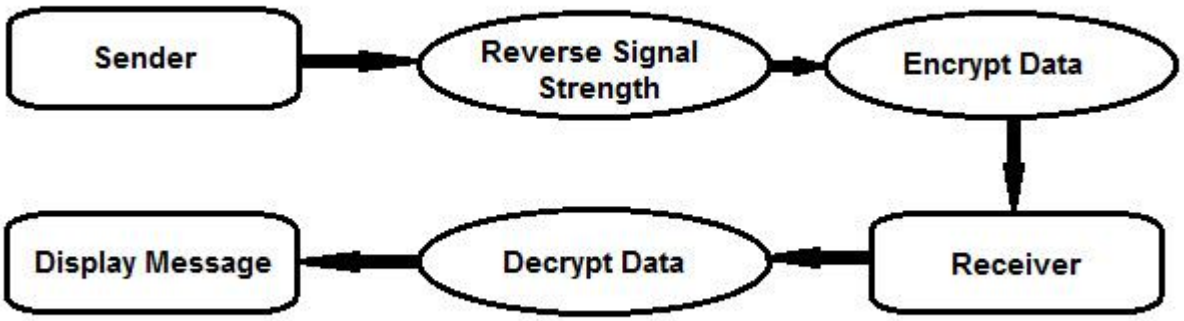


Fig 5.2.4: Dataflow Diagram Level 3

- The sender sends the reverse signal strength along with the message to be encrypted to the receiver where the message is decrypted and then displayed.

5.3 USE CASE DIAGRAM

These internal and external agents are known as actors. So use case diagrams consists of actors, use cases and their relationships. The diagram is used to model the system of the application.

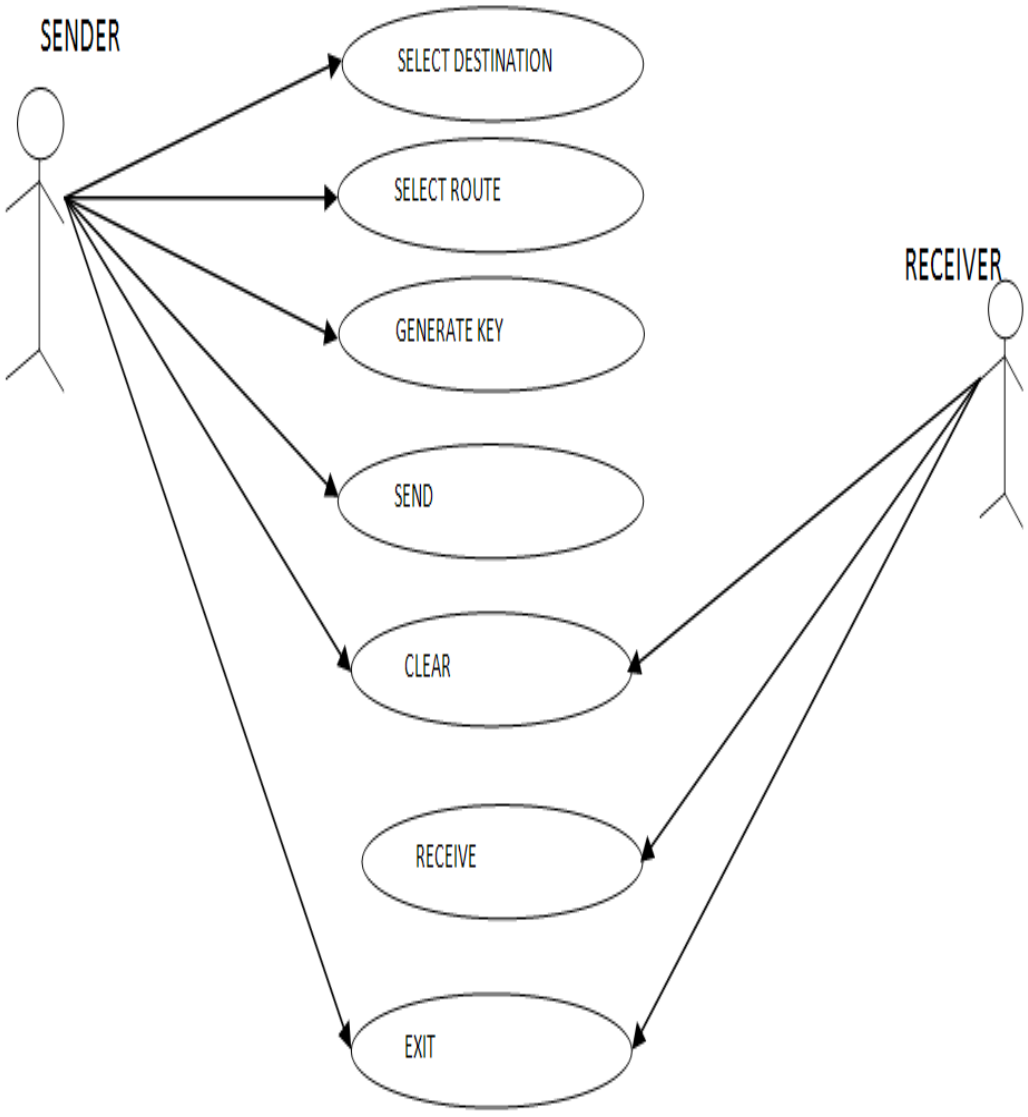


Fig 5.3: Use case diagram for Sender and Receiver

5.4 SEQUENCE DIAGRAM

A sequence diagram is an interaction diagram that details how operations are carried out: what messages are sent and when. Sequence diagrams are organised according to time. The objects involved in the operations are listed from left to right according to when they take part in the message sequence.

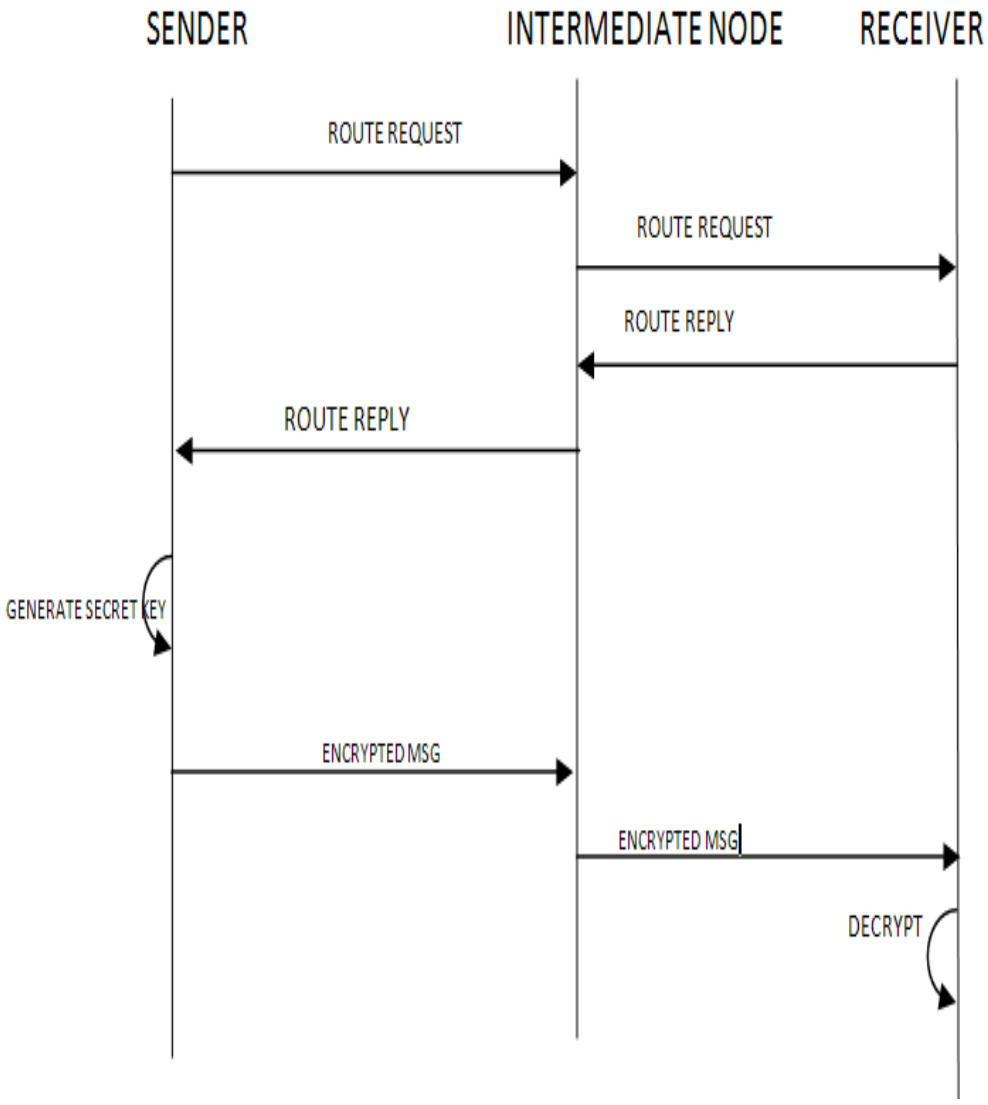


Fig 5.4: Sequence Diagram of Message Passing

5.5 CLASS DIAGRAM

A class diagram is a collection of static modelling elements, such as classes and their relationship, connected as a graph to each other and their contents. This visual representation of objects, their relationship, and their structures is for ease understanding.

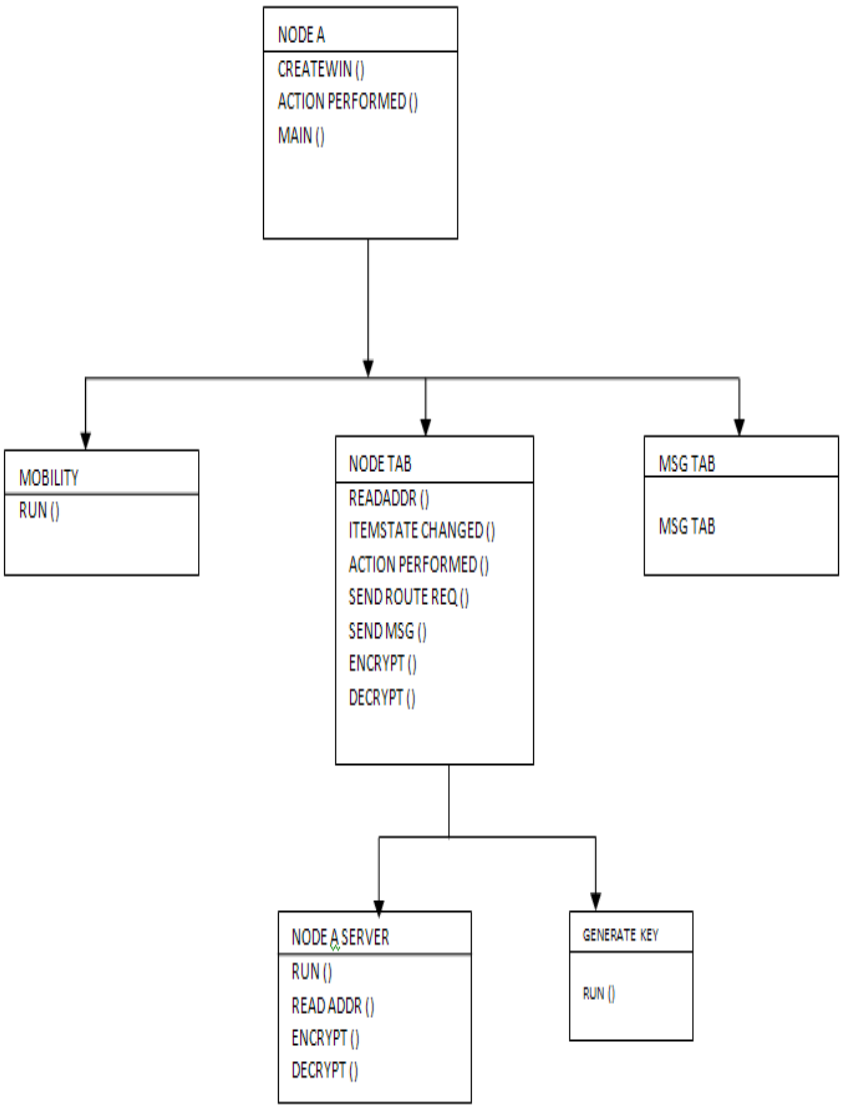


Fig 5.5: Class Diagram of Different Nodes

CHAPTER 6

METHODOLOGY

In this section, we first describe the three components of our wireless RSS-based secret key extraction. Next, we briefly describe two classes of existing quantization approaches. Last, we develop a new approach by combining the advantages of the existing approaches.

6.1 Components of RSS-Based Secret Key Extraction

To establish a shared secret key, Alice and Bob measure the variations of the wireless channel between them across time by sending probes to each other and measuring the RSS values of the probes. Ideally, both Alice and Bob should measure the RSS values at the same time. Typical commercial wireless transceivers are half duplex, i.e., they cannot both transmit and receive the signals simultaneously. Thus, Alice and Bob must measure the radio channel in one direction at a time. However, as long as the time between two directional channel measurements is much smaller than the inverse of the rate of change of the channel, they will have similar RSS estimates. Most of the existing literature on key extraction from RSS measurements either use some or all of the following three steps:

6.1.1 Quantization

As multiple packets are exchanged between Alice and Bob, each of them builds a time series of measured RSS. Then, each node quantizes its time series to generate an initial secret bit sequence. The quantization is done based on specified thresholds. Figure shows a sample RSS quantizer with two thresholds. The values between the lower and upper threshold are dropped, the value greater than the upper threshold is encoded as 1 and the value less than the lower threshold is encoded as 0. For the example in figure the quantizer will output 1010011. The difference in these quantizers mainly results from their different choices of thresholds and the different number of thresholds that they use.

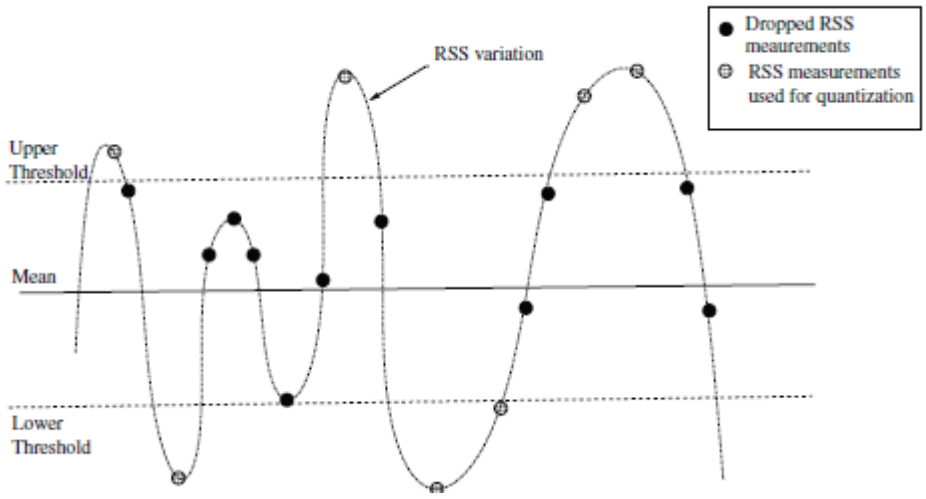


Fig 6.1.1: A sample RSS quantizer. The values between the lower and upper threshold are dropped, the value greater than the upper threshold is encoded as 1 and the value less than the lower threshold is encoded as 0. In this example, the quantizer will output 1010011.

6.1.2 Information Reconciliation

The existing system use Cascade an interactive information reconciliation protocol. In this protocol, Alice permutes the bit stream randomly, divides it into small blocks and sends permutation and parity information of each block to Bob. Bob permutes his bit stream in the same way, divides it into small blocks, and computes parities and checks for parity mismatches.

6.1.3 Privacy Amplification

It is observed that the information reconciliation stage reveals a certain fraction of information to correct the mismatching bits of Alice and Bob. The leaked portion needs to be removed so that an adversary cannot use this information to guess portions of the extracted key. Privacy amplification solves the above two problems by reducing the size of output bit stream. This is achieved by letting both Alice and Bob use universal hash functions. These functions are randomly chosen from a publicly known set, to obtain fixed size smaller length output from longer input streams. Essentially, privacy amplification generates a shorter secret bit stream with a higher entropy rate and a longer secret bit stream with a lower entropy rate. Most of the

popular methods used for privacy amplification are based on the *leftover hash lemma*, a well-known technique to extract randomness from imperfect random sources.

6.2 Existing Approaches

We classify the existing approaches into the following two categories:

Lossy-Quantization-Based Approach

In this approach, bits extracted from the RSS measurements are ropped probabilistically to maintain a high bit entropy. This approach does not use privacy amplification. The goal of this approach is to output a high entropy bit stream so that the output bit stream can be used directly as the shared secret key. This approach has a low output bit rate.

Lossless-Quantization-Based Approach

This approach does not drop any bits but uses privacy amplification to increase the bit entropy. This approach produces a high rate output bit stream. Note that quantization is inherently lossy. However, in this paper lossless quantization corresponds to obtaining 1 bit or more per sample and lossy quantization corresponds to obtaining less than 1 bit per sample. Also note that we compare these different approaches for the quality of the bit streams they generate. This quality is quantified by three performance metrics:

6.2.1. Entropy

Entropy characterizes the uncertainty associated with a random variable. We estimate the entropy of a bit stream using NIST test suite's Approximate entropy test.

6.3.2. Bit Mismatch Rate

We define the bit mismatch rate as the ratio of the number of bits that do not match between Alice and Bob to the number of bits Extracted from RSS quantization.

6.3.3 Secret Bit Rate

We define secret bit rate as the average number of secret bits extracted per collected measurement. This rate is measured in terms of final output bits produced after taking care of bit losses due to information reconciliation and privacy amplification.

CHAPTER 7

IMPLEMENTATION

7.1 MODULES

A module is a self-contained component of a system which has a well-defined interface to other components of the system. There is typically some degree of substitutability among identical or non-identical modules within a system or between systems.

An interface is a shared boundary or connection between two dissimilar objects, devices or systems through which information is passed. The connection can be physical or wireless.

The modules contained in our project are listed below:

1. Node Design
2. Route Request
3. Route Response
4. Key Generation
5. Encryption
6. Message Transfer
7. Receiver
8. Decryption

7.1.1 Node design

To implement the Project concept, first we have to construct a network which consists of ‘n’ number of Nodes. So that nodes can request data from other nodes in the network. For each node we have to create a Node Frame which contains the Node information, Destination Node field to transfer the data. To create the Frame for each node we use java Swing and AWT. These packages contain many in built classes which can be used for frame design.

7.1.2 Route request

The nodes either run on the same computer or connect through the network. Route request is the module which is used to store all the Nodes information like Node Id, IP address and other information in its database.We use AODV routing protocol to find routes for destination. The route request module is used by sender to send route request to find routes for destination.

7.1.3 Route response

This module is used by receiver to give route reply back to sender when it gets a route request. In route response all possible routes from the source to the destination is shown as the radio buttons.

7.1.4 Key generation

The data will send to the chosen Destination node via the intermediate nodes in the network. While the data is transmitted via intermediate node, they will generate a Key using Key Extraction Algorithm based on Received Signal Strength. The key will be shared to the Source and Destination nodes by the intermediate nodes till the data packets reaches to the Destination Node. In this module we generate the secret key using signal strength of node. If the signal strength increases then we consider it as 1, if it decreases we consider it as 0. Hence a key of eight characters is generated.

7.1.5 Encryption

This module is used by sender to encrypt the message. If the Source nodes wants to the Send the data to the destination node, they will choose the destination node then message is typed in Message Box. Then secret key is reversed and it is given as input to DES algorithm with message. The DES algorithm encrypts message and returns cipher. Once encrypted, the data will send to the Destination node via intermediate nodes. We may able to see the path of the data traveling in the Source/ Destination Nodes frame.

7.1.6 Message transfer Agent

The sender sends the key and cipher to receiver using any one route given by AODV protocol. Here we use java socket programming to connect nodes.

7.1.7 Receiver

The receiver module is used to receive encrypted message and secret key from sender. The receiver node consists of a Received Message Tab, which shows Route (data transmission route), Date & Time (message receiving date & time), Secret Key (identical to the generated key at source node), Encrypted Message (cipher text of the receiving data) and Message (original message after decryption).

7.1.8 Decryption

The decryption process is performed using DES algorithm. The reverse key and cipher is given as input to it. Once the data reaches the destination node mutual verification is attained in the both Source and Destination nodes by sharing the key generated by the intermediate nodes. To implement this concept, we can generate a Random number from the keys shared by the intermediate and verify the key was presented in the Destination Node. If present then other authentication process will be held and the DES returns decrypted message back if it is a valid key if not, then the destination node will not able to the receive data.

CHAPTER 8

TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product it is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

Types of Testing

8.1 Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program input produces valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application. It is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Our goal in unit testing is to isolate each part of the program and show that individual parts are correct in terms of requirements and functionality with respect to the Route request and reply, Key generation, Message encryption, Data Transmission and Message Decryption.

8.2 Functional testing

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Valid Input:	Identified classes of valid input must be accepted.
Invalid Input:	Identified classes of invalid input must be rejected.
Functions:	Identified functions must be exercised.
Output:	Identified classes of application outputs must be exercised.
Systems/Procedures:	Interfacing systems or procedures must be invoked

TABLE 8.2: Functional testing is centered on the following items

8.3 System Testing

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

8.4 Performance Testing

The Performance test ensures that the output be produced within the time limits, and the time taken by the system for compiling, giving response to the users and request being send to the system for to retrieve the results.

8.5 Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Valid Input:	Testing the IP Address for to communicate with the other Nodes.
Process:	Check the route request is sent from sender to receiver.
Process:	Check the key is extracted from signal strength.
Process:	Check the data is encrypted and sent to neighbour.
Process:	Check the encrypted message is received at neighbour

TABLE 8.5: Integration testing for Server Synchronization

8.6 Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

MODULE	GIVEN INPUT	EXPECTED OUTPUT	ACTUAL OUTPUT	RESULT
Sender	Route Request for destination	Possible routes to destination	Possible routes to destination retrieved	OK
Sender	Signal strength	Secret key has to be generated using signal strength	Secret key successfully generated using signal strength	OK
Sender	Message and secret key	Message has to be encrypted using reverse key	Message successfully encrypted	OK
Receiver	Route request from sender	Route reply has to be sent	Route reply successfully sent	OK
Receiver	Message from sender and secret key	Message has to be decrypted using reverse key	Message successfully decrypted	OK

TABLE 8.6: Testing results of all modules

CONCLUSION

In our project we are evaluating the effectiveness of secret key extraction from the received signal strength (RSS) variations in wireless channels using extensive real world measurements in a variety of environments and settings. Our project results will show that bits extracted in static environments are unsuitable for generating a secret key. We will also evaluate that an adversary can cause predictable key generation in static environments. However, bits extracted in dynamic environments shows a much higher secret bit rate. We developed an environment adaptive secret key generation scheme and our measurements showed that our scheme performed the best in terms of generating high entropy bits at a high bit rate in comparison to the existing ones that we evaluated. The secret key bit streams generated by our scheme also passed the randomness tests of the NIST test suite that we conducted. We were able to further enhance the rate of secret bit generation of our scheme by extracting multiple bits from each RSS measurement. The conclusions drawn in this paper, specifically the predictable channel attack, are primarily for key extraction using RSS measurements, and these may not directly apply to key extraction using channel impulse response measurements. We would like to explore this in our future work.

FUTURE ENHANCEMENTS

The following enhancements can be made in order to make this system design more effective and best:

- As our project works on secret key generation, so in future we can include the NIST test suite to improve the randomness of the secret key bit stream.

- We are generating the 8 bit key stream so we can increase the number of bits as well in order to make it less predictable.

- Currently we are working on four nodes connected in ring topology, and further we can increase the number of nodes as per the requirement using efficient topology.

- We can also build and evaluate the performance of secret key extraction using small, low power, hand-held devices like android phones that are equipped 802.11 wireless network card.

REFERENCES

1. T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. IEEE Transactions on Antennas and Propagation, 53(11):3776-3784, Nov. 2005.
2. B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks. In ACM CCS, 2007.
3. Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, SanVo
4. "Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels," IEEE Trans. Antennas and Propagation.
5. "NIST, A Statistical Test Suite for Random and Pseudorandom Number. Generators for Cryptographic Applications," http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501. Pdf.
6. "An Adaptive Quantization Algorithm for Secret Key Generation Using Radio Channel Measurements," New Technologies, Mobility and Security (NTMS), 2009 3rd International Conference.
7. U.M. Maurer, "Secret Key Agreement by Public Discussion from Common Information,"IEEE Trans. Information Theory, vol. 39, no. 3, pp. 733-742, May 1993 .
8. Cryptography and Network Security by Behrouz A. Forouzan, 7th Edition.

Sites Referred:

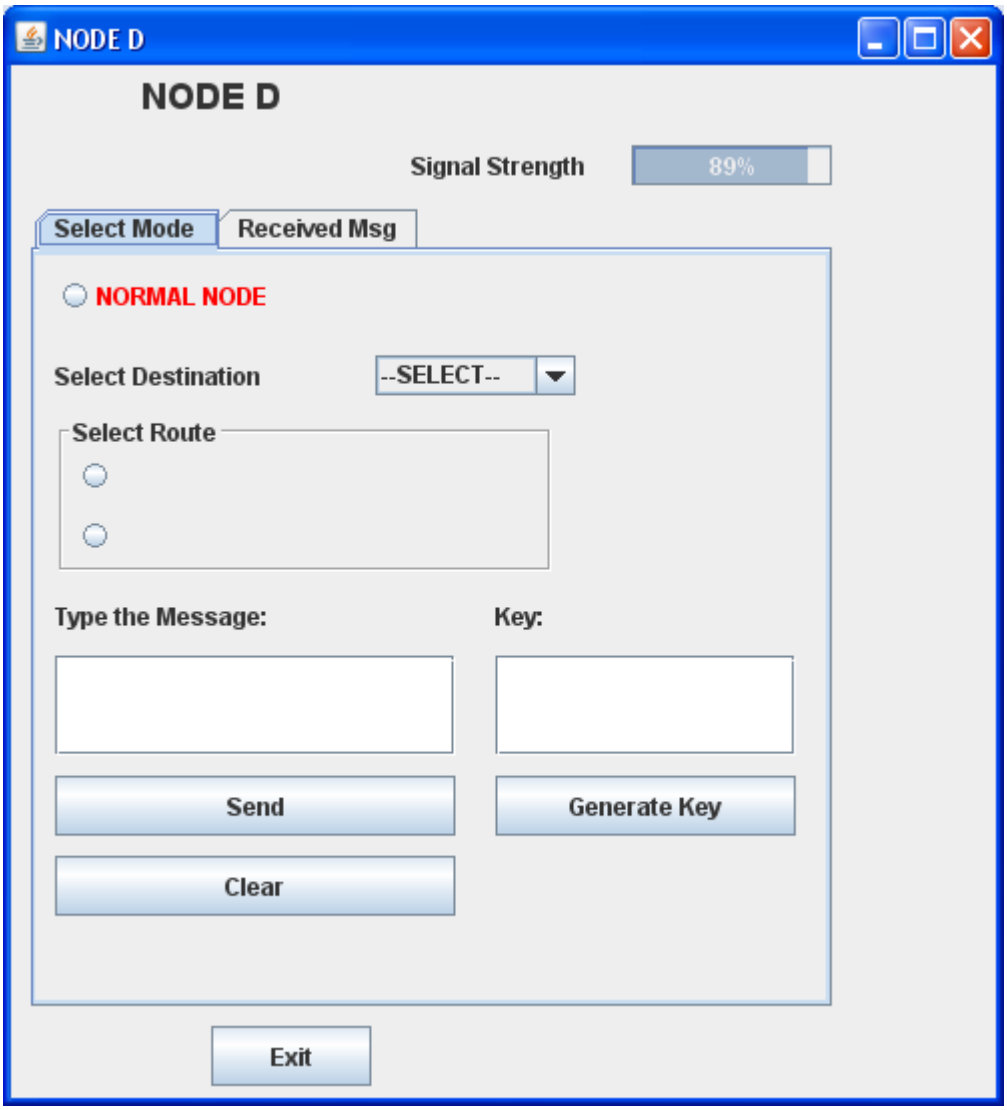
1. http://en.wikipedia.org/
2. http://www.google.com/
3. http://www.secretkeyextraction.com/

SNAP SHOTS

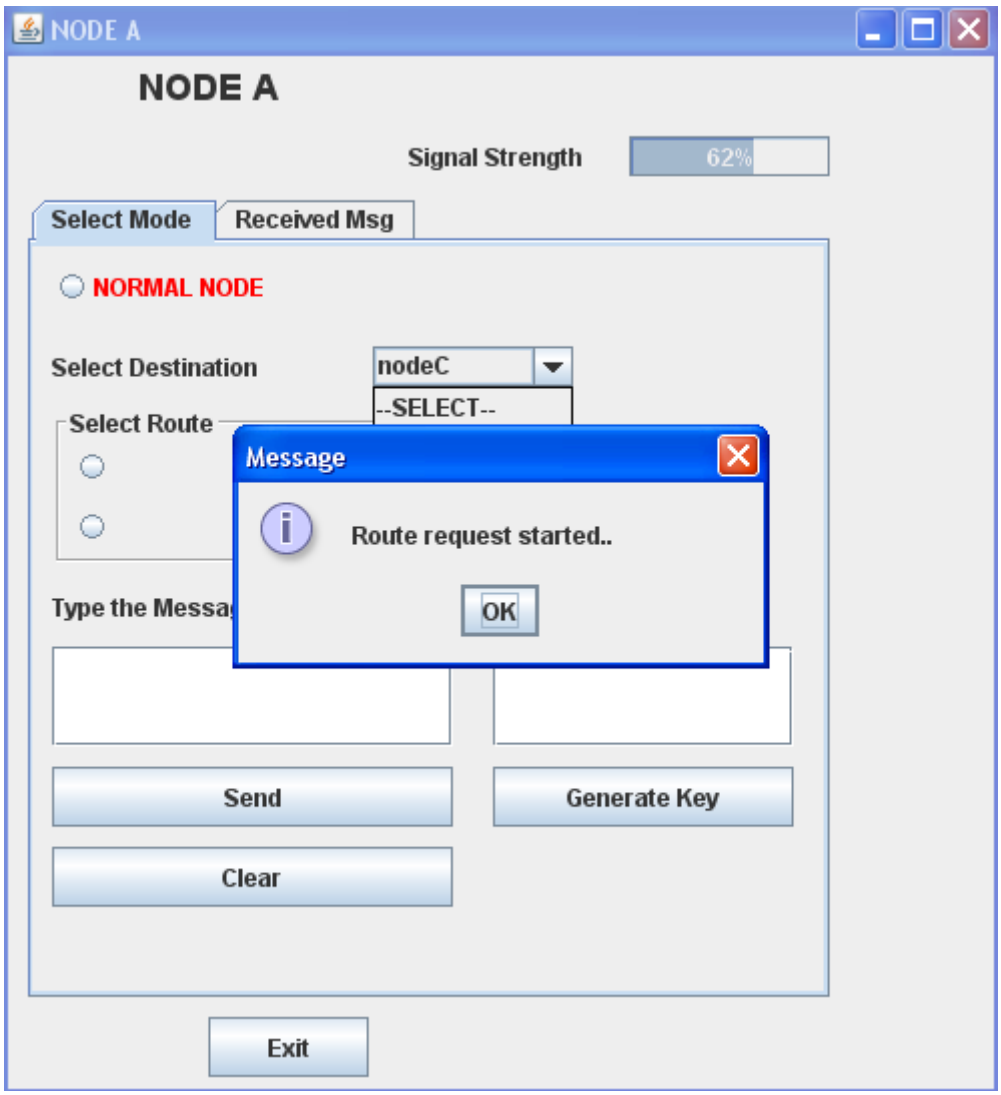
Node A designed using java swing.

Node B designed using java swing.

Node C designed using java swing.



Node D designed using java swing



Route Request

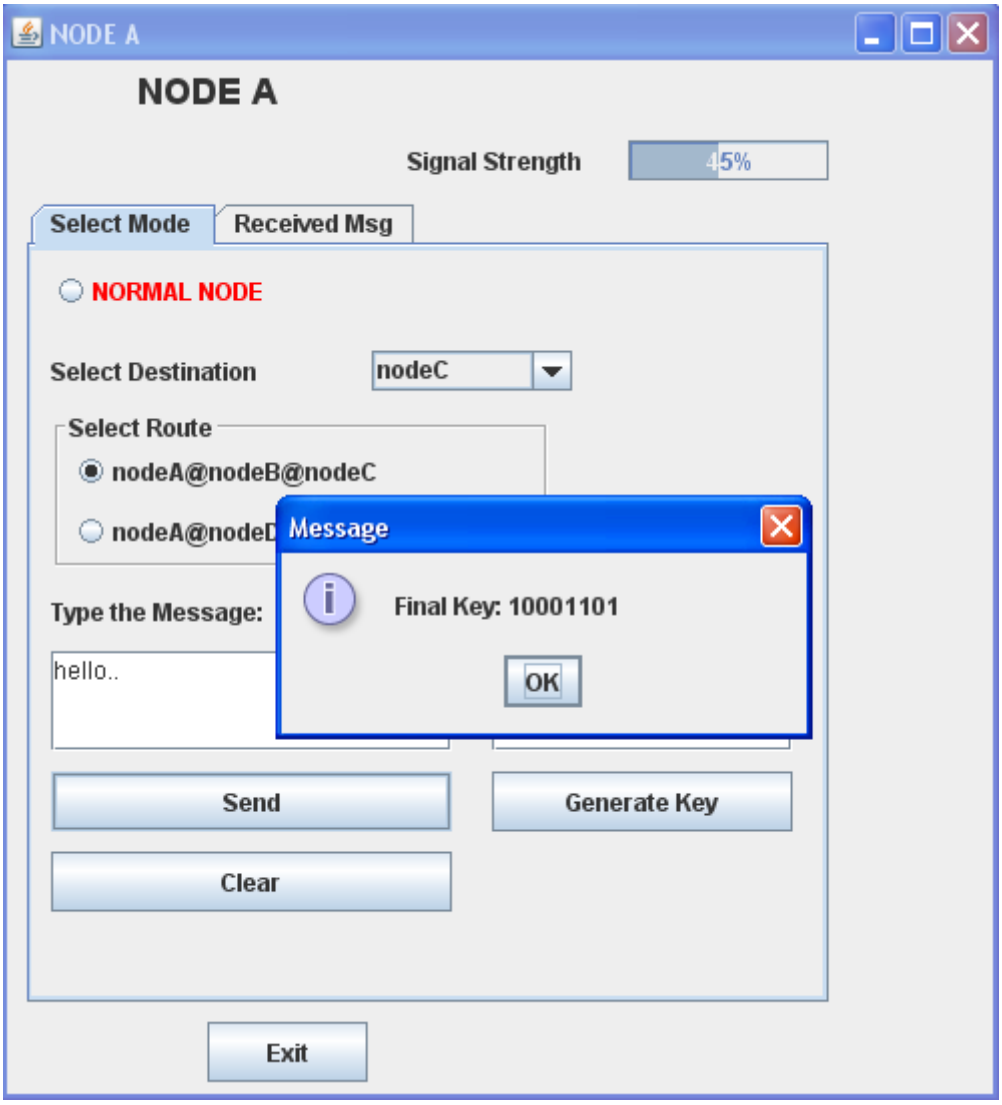
- This screenshot shows the selection of the destination node (node C) after which the route request is started to establish the route path between sender and receiver.

Route Option

- The possible route path from sender to receiver is shown in select route.

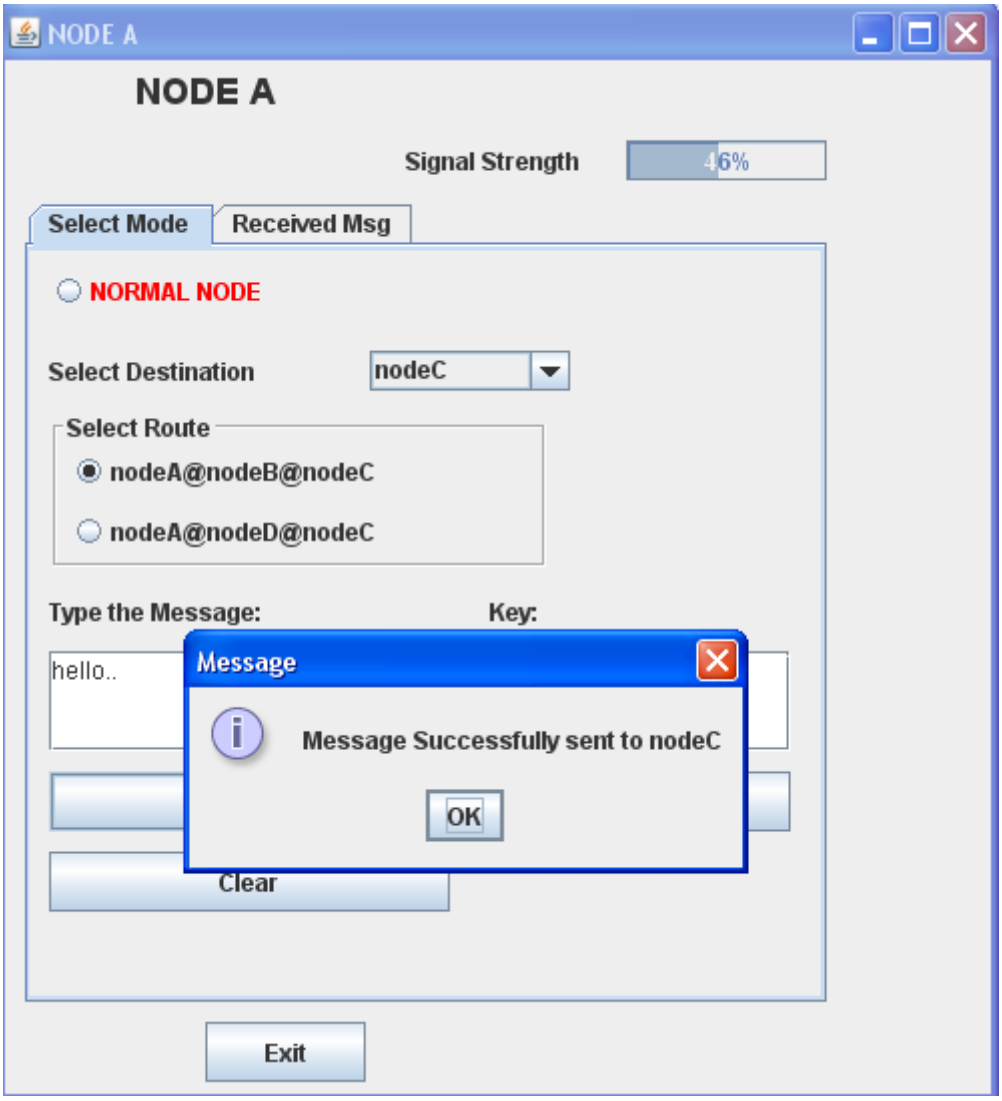
Route Selection

- One of the possible route path is selected. Message is typed in message box and 8 bit secret key is generated.



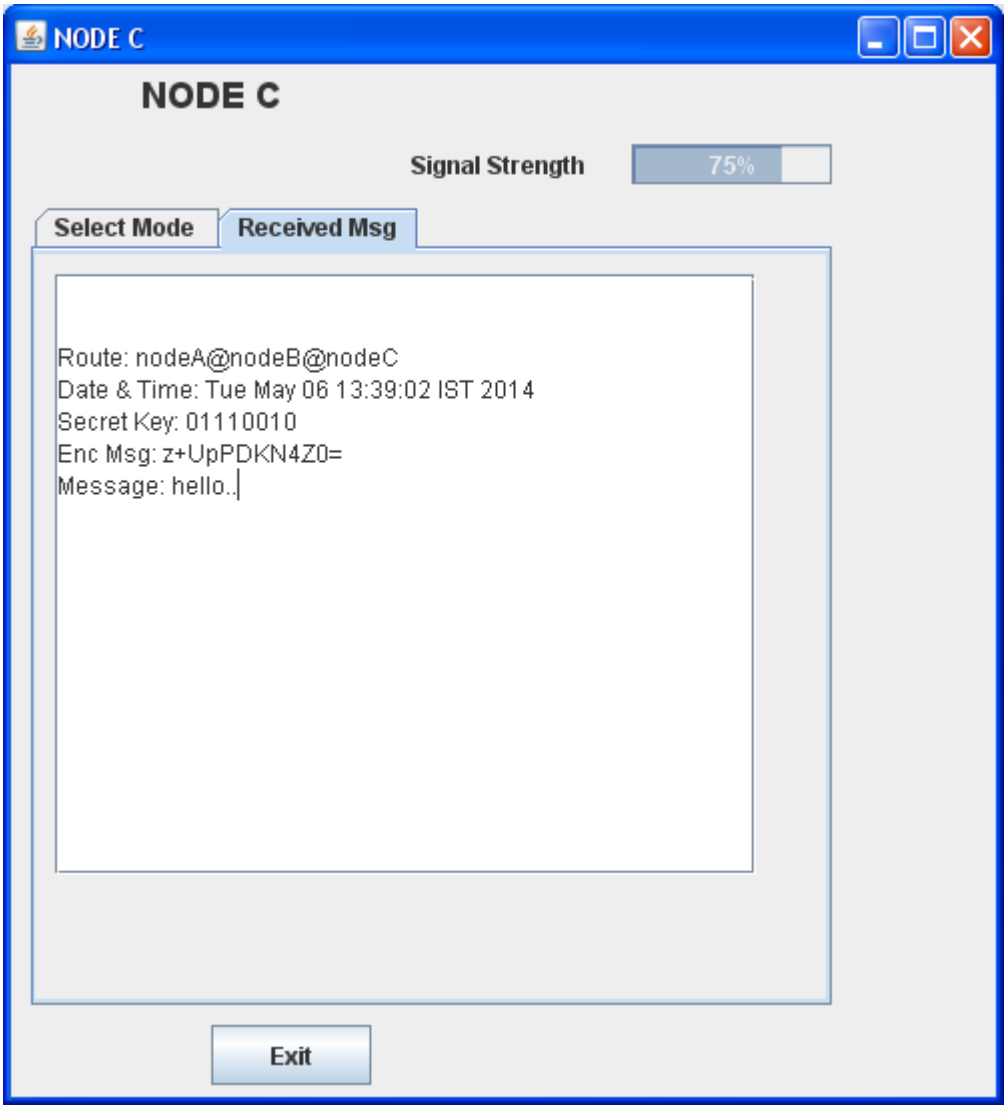
Key Generation

- Finally the reverse secret key or hashed key is generated.



Message Sent

- The send button is clicked to send the message. The dialogue box appears which shows that message is send to required destination.



Message Received

- The received message is shown in the received message field of destination node.