**CONTENTS**

**CHAPTERS PAGE NUMBER**

1. **INTRODUCTION 1**
2. **PREAMBLE 2**
   1. Existing systems 2
   2. Proposed systems 2
3. **LITERATURE SURVEY 5** 
   1. Vehicular ad-hoc networks 5
   2. Data Encryption Standard (DES) 6
   3. Elliptic curve 8
   4. Elliptic Curve Cryptography (ECC) 9
   5. Java 12
4. **SYSTEM REQUIREMENTS AND SPECIFICATION 19**
   1. Software requirement specification 19
   2. Functional requirement specification 20
   3. Nonfunctional requirement specification 21
   4. Domain requirement specification 21
   5. Hardware requirements 22
   6. Software requirements 22
5. **SYSTEM DESIGN 23**
   1. Introduction 23
   2. Modules 24
   3. Data flow diagram 25
   4. Architecture 27
   5. Use case diagram 28
   6. Sequence diagram 29
   7. Activity diagram 30
   8. Class Diagram 32
6. **IMPLEMENTATION 34**
   1. Introduction 34
   2. Registration module 35
   3. Message transfer and key distribution module 35
   4. Road side unit module 36
   5. Node module 37
   6. Mobile agent module 37
   7. Key generation and message encryption 38
   8. Socket connection module 39
7. **TESTING 42**
   1. Types of tests 42
   2. Test cases 46

**CONCLUSION 51**

**FUTURE ENHANCEMENTS 52**

**REFERENCES 53**

**APPENDIX A 55**

**APPENDIX B 61**

**LIST OF FIGURES**

**FIGURE NUMBER PAGE NUMBER**

3.1 Graphs of curves *y*2 = *x*3 − *x* and *y*2 = *x*3 − *x* + 1 9

3.2 Execution of java program 13

3.3 Java platform 14

3.4 Socket connection request 18

3.5 Socket connection 19

5.1 DFD of registration phase 26

5.2 Communication between sender and receiver 26

5.3 Working of mobile agent 27

5.4 System architecture 28

5.5 Use case diagram 29

5.6 Sequence diagram 30

5.7 Activity diagram 31

5.8 Class diagram of node 32

5.9 Class diagram of RSU 33

**LIST OF TABLES**

**TABLE NAME PAGE NUMBER**

3.1 Java development toolkit 16

5.1 Commonly used methods of the stream mode socket IP 40

7.1 Testing results 45

7.2 Socket connection 47

7.3 Running module 47

7.4 Registering with RSU 48

7.5 Mobile agent 48

7.6 Message sending 49

7.7 Key distribution 49

7.8 Encryption and decryption 50

7.9 Node not registered with RSU 50