**Secure and Reliable Data Forwarding Against Blackhole and Wormhole Attacks in Mobile Ad hoc Networks**

By

**Mazharul Islam**

Roll: 1807102

A thesis submitted in fulfilment of the requirements for the degree of

“Bachelor of Science in Computer Science and Engineering”

**Supervisor:**

**Professor Dr Kazi Md. Rokibul Alam**

Professor

Department of Computer Science and Engineering

Khulna University of Engineering & Technology, Khulna Signature

Department of Computer Science and Engineering

Khulna University of Engineering & Technology

Khulna 9203, Bangladesh

December, 2023

**Acknowledgement**

All the praise to the almighty Allah, whose blessing and mercy succeeded me to complete this work fairly. I gratefully acknowledge to our highly esteemed teacher and My supervisor, Professor Dr Kazi Md. Rokibul Alam sir, Professor, Department of Computer Science and Engineering, Khulna University of Engineering & Technology (KUET), for his excellent advices, guidance and right directions without which this thesis may not have reached a state it is in now. I would like to thank my seniors who inspired us to implement different Ideas throughout this project. We would also like to thank our friends for their association also.

Any constructive comments, suggestions, criticism from teachers as well as seniors will be highly appreciated and gratefully acknowledged.

**Authors**

**Mazharul Islam**

**Abstract**

MANETs consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. They form a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes. For the highly dynamic behaviour and due to mobile nodes, threats from compromised nodes inside the network, limited physical security, scalability and lack of centralized management MANETs is more vulnerable. So, Ensuring Security is must and also challenging for node-to-node communication. Black hole attacks are very dangerous and is not considered by any routing protocol, instead most of the routing protocols don’t concern about network security. Any malicious node can practically drop data instead of forwarding them. Hence a new method is proposed for reliable data forwarding in MANETs during Blackhole attacks based on ad-hoc on-demand multipath distance vector (AOMDV) protocol. Message is divided in some parts and sent. At the receiver end using homomorphic encryption to sum up the encrypted message. The performance is measured by analysis of throughputs, packet delivery ratio etc on different key size. It is more reliable and secure more than general AOMDV, while AOMDV is vulnerable with the intrusion of malicious nodes and can avoid blackhole attacks as well as wormhole attacks.

**Contents**

**PAGE**

Title Page i

Acknowledgment ii

Abstract iii

Contents iv

Lists of Tables vii

Lists of Figures viii

**CHAPTER I Introduction 1**

1.1 Background 1

1.2 Requirements 2

1.3 Problem Statement 2

1.4 Objectives 4

1.5 Unfamiliarity 4

1.7 Project Planning 5

1.6 Organization 5

**CHAPTER II Related Works 6**

Related Works 5

**CHAPTER III Required Tools 9**

3.1 Dynamic Routing Protocols 9

3.1.1 Route Discovery 9

3.1.2 Route Reply 9

3.1.3 Route Maintenance 9

3.2 Ad Hoc On-demand Distance Vector Routing (AODV) 10

3.3 Ad Hoc On-demand Multipath Distance Vector routing (AOMDV) 10

3.4 Homomorphic Encryption 11

3.5 Enhanced Homomorphic Cryptosystem (EHC) 11

3.5.1 Secret Key Generation 12

3.5.2 Encryption 12

3.5.3 Decryption 12

3.5.4 Homomorphic Characteristic of EHC 12

**CHAPTER IV Proposed Methodology 14**

4.1 Proposed Scheme 14

4.1.1 Assumption 14

4.1.2 Blackhole Attack Avoidance 15

4.1.3 Wormhole Attack Avoidance 17

4.2 Example Scenario 19

4.2.1 Secure Route Discovery 19

4.2.2 Send Message 23

**CHAPTER V Implementation 24**

5.1 Encryption Process 24

5.2 Decryption Process 24

5.3 Algorithm 24

5.3.1 The sender Procedure 24

5.3.2 The Receiver Procedure 25

5.4 Key Exchange Algorithm 26

5.5 Financial Analysis and Budgets 27

5.6 Analytical Model of the Example Scenario 28

**CHAPTER VI Performance Evaluation 30**

6.1 Performance of EHC 30

6.2 Different Authentication methods 30

6.3 Performance Methodology and Performance Metrics 32

6.4 Simulation Results 33

6.4.1 Packet Delivery Ratio 33

6.4.2 Throughput 34

6.4.3 Packet Loss 34

6.4.4 End-to-end Delay 34

**CHAPTER VII Societal, Health, Environment, Safety, Ethical,** 35

**Legal and Cultural**

7.1 Socio-Economic Impact and Sustainability 35

7.1.1 Socio-Economic Impact 35

7.1.2 Economic Impact Assessment 35

7.2 Ethical Considerations 36

**CHAPTER VIII Addressing Complex Engineering Problems and Activities 36**

8.1**.** Mitigation of Blackhole and Wormhole Attacks 37

8.2 Trust Establishment and Management 37

8.3 Resilience to Insider Threats 37

8.4 Dynamic Key Management and Authentication 38

**CHAPTER IX Conclusion 39**

**References** 40

**Lists of Tables**

|  |  |  |  |
| --- | --- | --- | --- |
| Table no. | Description | | page |
| 2.1 | | Comparison between the related works and the proposed scheme | 8 |
| 4.1 | | Comparison of time complexity between proposed scheme and AOMDV scheme | 16 |
| 5.1 | | Comparing the throughput from the simulation | 26 |  |
| 5.2 | | Comparing the throughput from the simulation [studied] | 28 |  |
| 5.3 | | Simulation parameters | 29 |
| 6.1 | | Encryption process time of different cryptosystems when key size is 512 bits | 30 |
| 6.2 | | Encryption process time of different cryptosystems when key size is 1024 bits | 31 |
| 6.3 | | Analysing different authentication methods | 31 |
|  | |  |  |
|  |  | |  |

**Lists of Figures**

|  |  |  |  |
| --- | --- | --- | --- |
| Figure no. | Description | | page |
| 1.1 | | Wormhole attacks in mobile ad hoc network | 4 |
| 1.2 | | Gantt chart for thesis plan | 5 |
| 3.1 | | An example of Dynamic routing protocol | 10 |
| 3.2 | | Ad hoc on demand distance vector routing scenario | 11 |
| 4.1 | | Work flow of the Proposed Scheme | 16 |
| 4.2 | | The procedure of message sending through malicious nodes | 17 |
| 4.3 | | Route discovery example. The initiator node S is attempting to discover a route to the target D. | 20 |
| 4.4 | | An example of proposed scheme where n = 6 | 22 |
| 5.1 | | Queue model for proposed protocol | 28 |
| 6.1 | | Packet delivery ratio | 32 |
| 6.2 | | Throughput as a function of malicious nodes | 32 |
| 6.3 | | Packet loss as a function of malicious nodes | 33 |
| 6.4 | | End-to-end delay as a function | 33 |