

Improved Reliable Data Forwarding Using Homomorphic Encryption Against Blackhole Attack in Mobile Ad hoc Networks

By

Mazharul Islam

Roll: 1807102

A thesis submitted in partial 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

August, 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 simulating the scenario in NS2 calculating throughputs, packet delivery ratio etc. It is more reliable than General AOMDV, while AOMDV is vulnerable with the intrusion of malicious nodes.

Contents

	PAGE
Title Page	i
Acknowledgment	ii
Abstract	iii
Contents	iv
Lists of Tables	vi
Lists of Figures	vii
CHAPTER I Introduction	1
1.1 Background	1
1.2 Requirements	2
1.3 Problem Statement	2
1.4 Objectives	3
1.5 Unfamiliarity	3
1.7 Project Planning	3
1.6 Organization	4
CHAPTER II Related Works	5
Related Works	5
CHAPTER III Required Tools	9
3.1 Ad Hoc On-demand Distance Vector Routing (AODV)	9
3.2 Ad Hoc On-demand Multipath Distance Vector routing (AOMDV)	9
3.3 Enhanced Homomorphic Cryptosystem (EHC)	9
CHAPTER IV Proposed Methodology	11

4.1 Secret Key Generation	11
4.2 Encryption	11
4.3 Decryption	11
4.4 Proposed Scheme	11
4.5 Example Scenario	13
4.5.1 Encryption Process	14
4.5.2 Decryption Process	14
4.6 Proposed Algorithm	14
4.6.1 The Sender Procedure	14
4.6.2 The Receiver Procedure	15
4.7 Financial Analysis and Budgets	16
4.8 Socio-Economical Impact and Sustainability	17
4.8.1 Socio-Economic Impact	17
CHAPTER V Simulation	18
5.1 Analytical model of the example scenario	18
CHAPTER VI Performance Evaluation	20
6.1 Performance Methodology and Performance Metrics	20
6.2 Simulation Results	21
6.2.1 Packet Delivery Ratio	21
6.2.2 Throughput	22
6.2.3 Packet Loss	22
CHAPTER VII CONCLUSION	23
Conclusion	23
References	24

Lists of Tables

Table no.	Description	page
2.1	Comparison between the related works and the proposed scheme	7
4.1	Comparison of time complexity between proposed scheme and AOMDV scheme	16
5.1	Comparing the throughput from the simulation	19
5.2	Simulation parameters	19

Lists of Figures

Figure no.	Description	page
1.1	Gantt chart for thesis plan	4
3.1	Ad hoc on demand distance vector routing scenario	9
4.1	An example of proposed scheme where $n = 6$	13
5.1	Queue model for proposed protocol	18
6.1	Packet delivery ratio	20
6.2	Throughput as a function of malicious nodes	20
6.3	Packet loss as a function of malicious nodes	21
6.4	End-to-end delay as a function	21