

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ

تَرْفَعُ دَرَجَاتٍ مِّنْ تَشَاءُ وَفَوْقَ كُلِّ ذِي  
( عِلْمٍ عَلِيمٌ )

"سورة يوسف- الآیه 76"

To my Family in Tariqah Burhaniya



# Acknowledgement

First of all I thanks to **AlmightyALLAH** who gave me ability and opportunity to accomplish this study.

I express my gratitude to **Dr\ Ibrahim khider**for the supervision of this thesis. His guidance and valuable suggestions enabled me to successfully end up this work. He always was reachable with welcoming hands during the entire period of this work.

I would like to thank **my family** for their valuable support not only through this thesis but throughout my lives.

My deepest gratitude goes to **my Husband,Mohamed Abd Almonem**, for their Unconditional care and support throughout my life; this thesis .will simply be impossible without him

Last but not the least we would also like to thank **all friends** for their .support and candidness

## ABSTRACT

Networking in vehicles is a promising approach to facilitate road safety, traffic management, and infotainment dissemination for drivers and travelers. Hence it becomes essential to provide security services such as authentication, non-repudiation, confidentiality, access control, integrity, and availability. The possible types of attacks include eavesdropping, denial of service and replay attacks. The security feature being implemented has to be tailor-made to suit the resource constraints imposed by the mobile nodes. In this thesis a propose approach to distribute the key management activities among the nodes by using the concept of the RSA algorithm. The message is encrypted using a public key and the corresponding private key is shared among the participating parties in all of these cases. The efficiency of each of these cases is .demonstrated using the JAVA language

## المستخلص

الشبكات في السيارات هو نهج واعد لتسهيل السلامة على الطرق، وإدارة المرور، ونشر المواد الترفيهية للسائقين والمسافرين. وبالتالي يصبح من الضروري توفير خدمات الأمان مثل الموثوقية والسرية، ومراقبة الدخول، وتوفير السلامة

أنواع الهجمات المحتملة تشمل التنصت، والحرمان من الخدمات وهجمات إعادة التشغيل.

ميزة الأمان التي يجري تنفيذها يجب أن يكون مصممة خصيصا لتتناسب مع قيود الموارد التي فرضها الع قد المتحركه. في هذا البحث اقترح نهج لتوزيع وإدارة المفاتيح بين الع قد باستخدام مفهوم خوارزمية اراس اي

يتم تشفير الرسالة باستخدام المفتاح العام والمفتاح المطابق المشترك الخاص بين الع قد المشاركة في جميع هذه الحالات. ويتم التطبيق وتحليل النتائج باستخدام لغة الجافا

# CONTENTS

I	.....	آ	د	ة
				...
II	.....			Dedication
III	.....			Acknowledgment
IV	.....			Abstraction
V	.....			المستخلص
VI	.....			Contents
VII	.....			List of Tables
VIII	.....			List of Figures
IX	.....			List of Abbreviation

## Chapter One

### Introduction

2	.....	Preface	1.1
5	.....	Objectives	1.2
5	.....	Problem definition	1.3
5	.....	Methodology	1.4
5	.....	Thesis Outline	1.5

## Chapter Two

### Background

8	.....	Introduction	2.1
8	.....	Characteristics of VANETS	2.2
9	.....	High mobility	2.2.1
9	.....	Dynamic topology	2.2.2
9	.....	Wireless communication	2.2.3
10	.....	Delay constraints	2.2.4
10	.....	Geographical addressing	2.2.5
10	.....	Mobility patterns	2.2.6
11	.....	Beaconing	2.2.7
11	.....	2.2.8 Pseudonym change	
12	.....	System Architectures	2.3
13	.....	Applications of VANET	2.4
16	.....	Attacks on vehicular networks	2.5
16	.....	2.5.1 Attacker's model	
17	.....	Basic attacks	2.5.2
19	.....	Security Requirements	2.6
22	.....	Message Security	2.7
23	.....	Security architectures	2.8

## Chapter Three

## Security Methods in VANET

29	.....	Introduction	3.1
33	.....	RSA Algorithm	3.2
34	.....	Public-key encryption	3.2.1
34	.....	Digital signatures	3.2.2
36	.....	Encryption	3.2.3
36	.....	Decryption	3.2.4
36	.....	Public – key cryptosystems	3.2.5
37	.....	Signature	3.2.6
39	.....	security in RSA	3.2.7
40	.....	Summary	3.2.8

## Chapter Four

### Methodology and Results

43	.....	System Model	4.1
46	.....	Mathematical Model	4.2
48	Computer	Model	4.3
	.....		
50	.....	Simulator Environment	4.4
50	.....	Result and Discussion	4.5

## Chapter Five

### Conclusion and Future Work

58	.....	Conclusion	5.1
59	.....	Future Work	5.2
60	.....	References	
62	.....	Appendix	



## List of Tables

2.1	VANET characteristics and their implications.....	11
2.2	VSC Message format.....	26
4.1	.....Simulation Parameters	43

## List of figures

2.1	C2C-CC draft reference architecture.....	13
2.2	Future Vehicular Communication Scenario.....	15
2.3	..... Bogus information attack	18
2.4	.....Illustration of a security architecture	24
4.1	Mobility Node Routing .....	44
4.2	Route discovery .....	45
4.3	Flow chart of vehicular Ad hoc Net work	48
4.4	Flow chart of RSA	49
4.5	Over Head .....	51
4.6	Delay.....	52
4.7	Drop (B).....	53
4.8	Packet Delivery Ratio .....	54
4.9	Throughput .....	55
4.1	Drop (%).....	56
0		

## List of Abbreviation

Vehicular Ad Hoc Network	VANE
Intelligent Transportation Systems	ITS
Onboard Units	OBU
Roadside units	RSU
Roadside – to- Vehicle communication	RVC
Inter-vehicle Communications	IVC
Geographic Broadcast	Geo Cast
Vehicle 2 Vehicle	V2V
Vehicle Safety Communication	VSC
Secure Vehicle Communication	SeVeCom
Media Access Control	MAC
Certificate Revocation List	CRL
Infrastructure Aided Symmetric Solutions	IASS
Time Efficient Stream Loss-to leant Authentication	TESLA
Ron Rivest Adi Shamir and Leonard Adleman	RSA
National Bureau of Standards	NBS
Evolved Packet System	EPS
Ad Hoc On demand Distance Vector	AODV
Constant Bit Rate	CBR
Route Request	RREQ
Rout Reply Packet	RREP