بسم الله الرحمن الرحيم

(نَرْفَعُ دَرَجَاتٍ مِّن نَّشَاء وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ )

"سورة يوسف– الآيه 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 الأمن مثل الموثوقيه والسرية، ومراقبة الدخول، وتوفرالسلامة.

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 العقد المتحركه. في هذا البحث اقتراح نهج لتوزيع وإدارة المفاتيح بين العقد باستخدام مفهوم خوارزمية اراس اي .

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

# CONTENTS



**Chapter Three**

# List of Tables

# List of figures

# 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 |