

# الآية

قال تعالى:

ذُرِّيَّتٍ مِّنْ دُونِكَ لَا يَرْجُونَ رَحْمَتَكَ مِنْ دُونِ رَحْمَتِكَ  
وَهُمْ فِيهَا يُنْفَكُونَ  
كُلٌّ كُنِي هَلْ لِي يَم

صدق الله العظيم

الآية (76) من سورة يوسف

## الإهداء

الحمد لله الذي وفقني لإنجاز هذا العمل، الذي أدين به إلى من أوصاني بهما القرآن.  
إلى أجمل ما في الوجود:

❖ إلى من علمتني خالص العطاء ومن كانت شمعة تحترق لتنير دربي، ومن كانت

تسقيني دعاءً وعطاءً، ربها الله وحماها إلى

"أمي"

❖ إلى سدي في مشواري، إلى الذي علمني حب الخير، وبعلي أعراف معني

التحدي والمثابرة. وما وصلت لإنجاز هذا العمل إلا بعون الله ثم عونك، جزاه الله كل

خير، إلى

"أبي"

## الشكر

مصدقاً لقوله صلى الله عليه وسلم "من استعاذ بالله فأعيذوه ومن صنع إليكم معروفاً فكافئوه وأدعو له حتى تروا أنكم كافأتموه". وعلى هذا:

أتقدم بالشكر الجزيل إلى مشرفي الدكتور الفاضل محمد عوض الشيخ الأستاذ العالم والإنسان، على ما قدمه لي من عون ومساندة في مراحل إعداد البحث حتى إنجازه، وعلى ما قدمه من النصح والإرشاد.

وأتقدم بالشكر أيضاً للدكتور يحيى عبدالله والدكتور سامي شريف اللذان شرفاني بقبولهما نقاش وإجازة هذا البحث.

كما أتقدم بالشكر الجزيل لأساتذتي أعضاء هيئة التدريس في برنامج الماجستير الذي تشرفت بالإلتحاق به، على الجهود التي بذلوها في توفير الأجواء الأكاديمية المناسبة.

والشكر أجزله لكلية علوم الحاسوب وتقانة المعلومات- جامعة السودان، وكل العاملين بها.

وأتقدم بالشكر كذلك لإخواني ولجميع الأصدقاء والزملاء الذين ساعدوني على إنجاز البحث.

## المستخلص

شبكة Adhoc الجواله (MANET) من الشبكات المستخدمة بكثرة في مجال الإتصالات، بالرغم من وجود مشكلة تطبيق السرية في عمليات إرسال البيانات وتوجيهها للمسارات. الشبكة تتكون من مجموعة من الأجهزة أو العقد (nodes) الجواله، وهي تستخدم الإتصال اللاسلكي في التخاطب مع بعضها بطريقة غير منتظمة (Ad hoc). في هذا النوع من الشبكات نحتاج لبروتوكول توجيه يكون مختلف عن بقية الشبكات الأخرى. فهناك العديد من العقد التي يمكنها الإرسال في نفس اللحظة مما يتسبب في وجود التصادمات، بالإضافة إلى أن عملية الأرسال يتم بثها (Broadcast)، وبذلك يمكن لكل العقد المشاركة في الشبكة سماع ذلك الإرسال. حالياً يوجد بروتوكولات توجيه لشبكات MANET تلي تلك الإحتياجات. ولكن ومع عدم وجود مركزية في الشبكة أصبح من الضرورة وجود آلية لسرية إرسال البيانات. هنالك العديد من المقترحات التي قُدمت لتوفير السرية لبروتوكولات التوجيه في شبكات (MANET Mobile Adhoc Network)، ولكن معظمها لم يراعي أهمية الموثوقية والتحقق من العقد، وأيضاً محدودية الطاقة لدى العقد المشاركة في شبكات MANET. لذلك تم إقتراح بروتوكول توجيه ليحل مشكلة السرية في شبكات MANET، مراعيّاً توفير السرية للعقد ذات الإمكانيات المحدودة، عن طريق إستخدام آلية التوقيع الإلكتروني (digital signature).

في هذا البحث تم توفير آلية سرية ضرورية وفعالة لعمليات إرسال وتوجيه الحزم في شبكات MANET. وفيه تم توليد وحساب التوقيع الإلكتروني مرة واحدة (one time computational scheme)، مما يقلل العبء الإضافي على العقد. في تصميم البروتوكول تم إستخدام خوارزمية MD5 لتوليد التوقيع الإلكتروني، مع الأخذ في الإعتبار الموارد المحدودة للعقد المشاركة في شبكات MANET؛ من حيث محدودية الطاقة المبدولة لحساب التوقيع الإلكتروني، وكذلك محدودية الذاكرة التخزينية، بالإضافة محدودية نطاق الإرسال.

يتم إضافة التوقيع الإلكتروني الخاص بالعقدة عند أول رسالة ترحيب تصدرها بعد دخولها للشبكة. حيث تقوم بقية العقد بتخزين ذلك التوقيع؛ لإستخدامه فيما بعد للتحقق من هوية تلك العقدة. ويتغير ذلك التوقيع كلما تغير موقع العقدة (تبعاً لتغيير الرقم التسلسلي للعقدة). والذي يلزم أن تعيد العقدة بث رسالة ترحيب جديدة، لتعلن لبقية العقد عن مكانها الجديد وكذلك توقيعها الجديد.

# Abstract

Adhoc mobile network (MANET) networks is popular and widely used in telecommunications, despite the existence of security problems of confidential data and direct routes. MANET Network consists of a set of mobile nodes, with wireless interface, communicates with non-regular (Adhoc) manner. The type of networks needs a protocol different from the other networks. Many nodes can send at the same moment, which may cause the collision. In addition to using broadcast in sending messages allow every node participating in the network to hear the transmission. There are many protocols that meet MANET needs. Because the absence of a centralize infrastructure in the MANET network; it is necessity to find a mechanism for confidential data, and secure transmission.

There are many researches propose the confidentiality of MANET's routing protocols, most of them did not take into account the importance of authentication and verification of the nodes. In the other hand, it doesn't take into account the limited energy of the MANET's participating nodes. We need a proposal to secure AODV protocol for solving the problems of MANET's security, at the same time the limited power, providing confidentiality, by using the digital signature.

This thesis provide a confidential and security mechanism, and provide effective processes to send packages into the networks MANET. It used one time computational scheme to calculate the digital signature, which reduce the overhead of calculation and generation of signature.

This thesis used MD5 algorithm, in order to generate a digital signature. Taking into account, the limited resources of the MANET participation nodes, such as: the limit of the energy, the limit of memory storage, and the limit of transition range.

A digital signature has been added to each Hello message issued by the nodes, after entering the network. This signature will be used later by other nodes, to verify the identity of the node.

## فهرس المحتويات

الصفحة	الموضوع	الباب
	المقدمة	الباب الأول
1	..... الملخص	1.1
1	..... المقدمة	1.1
2	..... تعريف المشكلة	1.3
2	..... الأهداف	1.4
	مفاهيم أساسية	الباب الثاني
	<b>الشبكات اللاسلكية غير المنتظمة الجواله (MANET)</b>	<b>2.1</b>
4	..... التوصيف	2.1.1
5	..... خصائص شبكات اللاسلكية غير المنتظمة الجواله (MANET)	2.1.2
6	..... إستخدام الشبكة اللاسلكية غير المنتظمة الجواله (MANET)	2.1.3
6	..... تمرير الحزم في الشبكة اللاسلكية غير المنتظمة الجواله (MANET)	2.1.4
	<b>بروتوكول توجيه الموجهات عند الطلب في الشبكات غير المنتظمة (AODV)</b>	<b>2.2</b>
9	..... التوصيف	2.2.1
10	..... جدول المسارات (Routing Table)	2.2.2
11	..... طريقة عمل بروتوكول توجيه الموجهات عند الطلب في الشبكات غير المنتظمة (AODV)	2.2.3
11	..... إكتشاف المسار (Route Discovery)	2.2.3.1
11	..... صيانة المسار (Route Maintenance)	2.2.3.2
12	..... خصائص بروتوكول توجيه الموجهات عند الطلب في الشبكات غير المنتظمة (AODV)	2.2.4
	<b>بيئة المحاكاة OMNET++ Simulation</b>	<b>2.3</b>
13	..... نبذة عن بيئة النمذجة OMNET++ Simulation	2.3.1
14	..... أهم مزايا OMNET++	2.3.2

14	خطوات العمل الأساسية في OMNET++ .....	2.3.3
	<b>الدراسات السابقة</b>	<b>الباب الثالث</b>
15	المقدمة .....	
16	بروتوكول توجيه الموجهات ذو السرية الفعالة (SEAD) .....	3.1
17	بروتوكول عقود إيجار الحزمة (Packet Leashes) .....	3.2
18	بروتوكول Ariadne .....	3.3
18	بروتوكول لجنة الرقابة والمستكشف (Watchdog and Pathfinder) .....	3.4
19	بروتوكول توجيه الموجهات الآمن في الشبكات غير المنتظمة (SAODV) .....	3.5
20	بروتوكول سرية حالة الرابط (Secure Link-State) .....	3.6
20	بروتوكول المستشار (Confidant) .....	3.7
20	بروتوكولات أخرى للتوجيه الآمن .....	3.8
	<b>متطلبات السرية في بروتوكول توجيه الموجهات في الشبكات غير المنتظمة (AODV)</b>	<b>3.9</b>
21	أنواع الهجمات على بروتوكول توجيه الموجهات في الشبكات غير المنتظمة (AODV) .....	3.9.1
22	خصائص السرية (Security attributes) .....	3.9.2
	<b>مهددات السرية في بروتوكول توجيه الموجهات في الشبكات غير المنتظمة (AODV)</b>	<b>الباب الرابع</b>
24	<b>هجمات تعديل إتجاه الحركة (Traffic Redirection by Modification)</b>	<b>4.1</b>
24	تعديل الرقم التسلسلي (Modification of Sequence Number) .....	4.1.1
25	تعديل حقل عدد العقد الوسيطة (Modification of Hop Count) .....	4.1.2
25	<b>هجمات إعادة الإرسال (Replay Attacks)</b> .....	<b>4.2</b>
25	هجوم فيضان طلب المسار (RREQ Flooding attack) .....	4.2.1
27	هجوم الثقب (Wormhole attack) .....	4.2.2
28	<b>تشكيل حلقات التوجيه (Formation of Routing Loops)</b> .....	<b>4.3</b>
30	<b>الرسائل الخاطئة بفشل المسار (False Route Error)</b> .....	<b>4.4</b>

	<b>التصميم والحلول المقترحة</b>	<b>الباب الخامس</b>
31	..... الفرضية والمخطط	5.1
31	..... شرح النموذج المقترح	5.2
	<b>التطبيق</b>	<b>الباب السادس</b>
	<b>(Simulation Description) وصف النموذج</b>	
34	..... بيئة نظام المحاكاة	6.1
36	..... خوارزمية MD5	6.2
37	..... نموذج AdhocSim	6.3
37	..... وصف النموذج المقترح	6.4
41	..... طريقة عمل النموذج المقترح	6.5
	<b>الخلاصة والتوصيات</b>	<b>الباب السابع</b>
44	..... الخلاصة	7.1
44	..... التوصيات	7.2
45	.....	<b>المراجع</b>
48	.....	<b>الملاحق</b>

## فهرس الأشكال

رقم الصفحة	موضوع الشكل	رقم الشكل
5	نمذج للشبكة الالسلكية غير المنتظمة الجواله (MANET) مكونه من ثلاث عقد	2-1
25	الهجمات عن طريق التعديل	4-1
26	توسيع حلقة التوجيه	4-2
27	فيضان طلب المسار	4-3
28	هجوم الثقب	4-4
29	حلقة التوجيه أ	4-5
29	حلقة التوجيه ب	4-6
29	حلقة التوجيه ج	4-7
31	النمذج الإفتراضي	5.1
32	الإكتشاف الآمن للمسار	5.2
35	الشاشه الرئيسيه في OMNET++	6-1
35	شاشه النمذج في OMNET++	6-2
36	خصائص العقده في OMNET++	6-3
41	مقطع من شاشه تنفيذ النمذج أ	6-4
42	مقطع من شاشه تنفيذ النمذج ب	6.5
43	مقطع من شاشه تنفيذ النمذج ج	6.6
43	مقطع من شاشه تنفيذ النمذج د	6.7