الآية

قال تعالى:

"نَرْفَعُ دَرَجَاتٍ مَّن نَّشَاءُ وَفَوْقَ
كُلِّ ذِي عِلْمٍ عَلِيمٌ"

صدق الله العظيم

الآية (76) من سورة يوسف

الإهداء

الحمدلله الذي وفقني لإنجاز هذا العمل، الذي أدين به إلى من أوصاني بهما القرآن.

إلى أجمل مافي الوجود:

❖ إلى من علمتني خالص العطاء ومن كانت شمعة تحترق لتنير دربي، ومن كانت تسقيني دعاءاً وعطاءاً، رعاها الله وحماها إلى

"أمي"

❖ إلى سندي في مشواري، إلى الذي علمني حب الخير، وجعلني أعرف معنى التحدي والمثابرة. وما وصلت لإنجاز هذا العمل إلا بعون الله ثم عونه، جزاه الله كل خير، إلى

"أبي"

الشكر

مصداقاً 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 يحي عبدالله والدكتور سامي شريف اللذان شرفائي 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 الجوالة (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) الجوالة، وهي تستخدم الإتصال اللاسلكي في التخاطب مع بعضها بطريقة غير منتظمة (Ad hoc). في هذا النوع من الشبكات نحتاج لبروتوكول توجية 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 توجية لشبكات MANET تلبي 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 التوجية 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، مراعياً 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 وتوجية 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 المبذولة 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؛ لإستخدمه 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

فهرس الأشكال