Ain Shams University
Faculty of Engineering
COMPUTER AND SYSTEMS ENGINEERING DEPARTMENT

A Secure Routing Protocol for Mobile Ad-Hoc Networks

by
Amin Abdel-Wahab Amin Sorrour
B.Sc.

A THESIS
SUBMITTED IN PARTIAL FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF MASTERS OF
SCIENCE IN ELECTRICAL ENGINEERING

DEPARTMENT OF COMPUTER AND SYSTEMS ENGINEERING

Supervised By

Prof. Dr. Yasser Hesham Dakroury
Dr. Hassan Shehata Bedour
Dr. Shaimaa Arafat

Cairo, Egypt
2006

List of Symbols, Abbreviations and Nomenclature

Abbreviation	Meaning
AODV	Ad hoc On-demand Distance vector
CBR	Constant Bit Rate
DARPA	Defense Advanced Research Projects Agency
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
Forwarding Group	A group of nodes participating in multicast packet forwarding.
GLOMOSIM	GLObal MObil information system SIMulator
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
MAC	Message Authentication Code
MANET	Mobile Ad hoc NETwork
Member Table	The table maintained by multicast receivers containing information of multicast sources for each multicast group it is associated with.
Multicast mesh	The topology defined by the link connection between forwarding group members
Neighbor node	Nodes that are within the radio transmission range.
Node	A device that implements IP.
PARSEC	PARallel Simulation Environment for Complex systems
PDA	Personal Digital Assistant
Routing table	Table maintained by each node containing route information (e.g., next hop node) of existing active routes.
TORA	Temporally Ordered Routing Algorithm
TTL	Time To Live

مستخلص

الاسم: أمين عبد الوهاب أمين سرور

عنوان الرسالة: بروتوكول لتأمين المسار فى شبكات الحاسبات الجواله ذات الأغراض المؤقته

رسالة ماجستير فى الهندسة الكهربية (هندسة الحاسبات والنظم)

جامعة عين شمس – كلية الهندسة

فى مجال شبكات الحاسب تعرف الشبكات الارتجالية بأنها عبارة عن شبكات مؤقته تستخدم لربط عدة مستخدمين بدون الحاجة لتحكم مركزى، فكل حاسب بالشبكة يكون له القدرة على العمل كمضيف ومحدد مسار كما يكون عنده الاستعداد لتمرير الرسائل للحواسب الأخرى.وقد نشات عدة بروتوكولات تحديد مسار ذو فاعلية تؤدى هذه الخدمه منها بروتوكول ال DSR لذا فإننا فى حاجة إلى بروتوكول يضمن سرية تحديد هذا المسار .

أهم الصعاب التى واجهت هذا العمل هى ديناميكية الترابط الناتجة عن حركة الحواسب حيث يمكن للحواسب أن تغير من موقعها على فترات متقاربة مما يجعلنا فى حاجة إلى بروتوكول يمكنه التعامل مع التغير فى ترابط الشبكة. إن الحواسب يمكن أن تكون أجهزة حاسب محمولة أو المساعد الرقمى الشخصى (PDA) والتى غالبا ما تعانى من نقص فى قدرة معالجاتها، أو سعة التخزين بها،أو مصادر الطاقة، أو مجال الإرسال. لذا يجب أن يقوم البروتوكول بتقليل كم الرسائل المستخدمة لتحديث المسارات.

فى هذا البحث تم اختيار بروتوكول Ariadne وهو بروتوكول يعتمد على ال[DSR] فى تحديد مسار بين مرسل واحد وعدة مستقبلين حيث يتم تحديد المسارات بينهم على مرحلتين، مرحلة الإستفسار (Request phase) ومرحلة الاستجابة (Reply phase). يتم تكرار هاتين المرحلتين بصفة مستمرة باضافة ادوات السريه لتامين المسار المطلوب .

وقد تم تحقيق برتوكول Ariadne الا انه وجد عرضه للاختراق من worm attacking وقد قمنا باقتراح لحل هذه الثغره وذلك باضافه عنوان كل مضيف الى المسار مع حذف عنوان المضيف

السابق بدلا من الاحتفاظ به كما فى بروتوكول Ariadne مما يجعل ال compromise node لايرى نظيره الذى يمكنه من الاختراق.

. تم استخدام المحاكى Glomosim والذى أعد خصيصا لمحاكاة الشبكات الجوالة الارتجالية. وقد تم تعديل الكود فى برنامج المحاكاة ليتلائم مع اضافه خواص السريه . كما تم توثيق خطوات استخدام المحاكى حيث لايوجد وثائق يعتمد عليها لمعرفة كيفية تشغيلة، وتم كتابة برنامج بلغة C++ لاستخلاص البيانات المطلوبة ومقارنتها ببروتوكول ariadne قبل التعديل وبعده

الكلمات المفتاحية :

سريه الشبكات الجوالة الارتجالية، الشبكات الجواله الإرتجاليه، Ariadne

كلية الهندسة
قسم هندسة الحاسبات والنظم

صفحة العنوان

اسم الباحث : أمين عبد الوهاب أمين سرور
اسم الدرجة : ماجستير فى الهندسة الكهربية
القسم التابع له : هندسة الحاسبات والنظم
اسم الكلية : كلية الهندسة
سنة التخرج : 1982
سنة المنح : 2006

كلية الهندسة
قسم هندسة الحاسبات والنظم

تعريف بمقدم الرسالة

إسم الباحث	: أمين عبد الوهاب أمين سرور
تاريـخ الميلاد	: 1958/12/29
محل الميلاد	: القاهرة
الدرجة العلمية الأولى	: بكالوريوس هندسة الحاسبات والتحكم الآلي
الجهة المانحة لها	: كلية الهندسة – جامعة عين شمس
تاريخ المنح	: يونيو 1982
الوظيفة الحالية	: ضابط مهندس بمصلحة الأحوال المدنية
اسم مقدم البحث	: أمين عبد الوهاب أمين سرور
التوقيع	:
التاريخ	:2006/5/27

كلية الهندسة

قسم هندسة الحاسبات والنظم

رسالة ماجستير

اسم الباحث : **أمين عبد الوهاب أمين سرور**

عنوان الرسالة : **بروتوكول لتأمين المسار فى شبكات الحاسبات الجواله ذات الأغراض المؤقته**

الدرجة : **ماجستير الهندسة الكهربية**

لجنة الإشراف

الاسم	**الوظيفة**
أ.د. ياسر هشام دكروري	أستاذ هندسة الحاسبات – هندسة عين شمس
د. حسن شحاتة بدور	أستاذ مساعد هندسة الحاسبات – هندسة عين شمس
د. شيماء عرفات	مدرس علوم الحاسب-حاسبات ومعلومات عين شمس

تاريخ البحـــث: / /

الدراسات العليا

ختم الإجازة **أجيزت الرسالة بتاريخ**

/ /

موافقة مجلس الكلية **موافقة مجلس الجامعة**

/ / **/ /**

صفحة الموافقة

اسم الباحث: **أمين عبد الوهاب امين سرور**

عنوان الرسالة: **بروتوكول لتأمين المسار فى شبكات الحاسبات الجواله ذات الأغراض المؤقته**

الدرجة: **ماجستير الهندسة الكهربية(هندسه الحاسبات والنظم)**

لجنة الحكم

الأسماء والوظائف **الإمضاء**

الاستاذ الدكتور/ محمد زكى عبدالمجيد
استاذ ورئيس قسم هندسة الحاسبات و النظم– هندسة الأزهر.

الاستاذ الدكتور/ سلمى عبدالقادر غنيم
استاذ هندسة الحاسبات– هندسة عين شمس.

الاستاذ الدكتور/ ياسر هشام دكرورى
استاذ هندسة الحاسبات– هندسة عين شمس.

تاريخ المناقشة: 7 /9 /2006

جامعة عين شمس
كلية الهندسة
قسم هندسة الحاسبات والنظم

بروتوكول لتأمين المسار فى شبكات الحاسبات الجواله ذات الأغراض المؤقته

رسالة مقدمه للحصول على درجة الماجستير فى هندسة الحاسبات والنظم

مقدمه من

أمين عبد الوهاب امين سرور
بكالوريوس هندسة الحاسبات والتحكم الآلي كلية الهندسة جامعة عين شمس

تحت إشراف

أ.د. ياسر هشام دكروري أستاذ هندسة الحاسبات – هندسة عين شمس

د. حسن شحاتة بدور أستاذ مساعد هندسة الحاسبات – هندسة عين شمس

د. شيماء عرفات حسين مدرس علوم الحاسب-حاسبات ومعلومات عين شمس

القاهره
2006

Abstract

Amin Abdel-Wahab Amin Sorrour

A Secure Routing Protocol for Mobile Ad-Hoc Networks

M.Sc. dissertation

Ain Shams University, 2006

Ad hoc networking is a concept in computer communications, which means that users wanting to communicate with each other form a temporary network, without any form of centralized administration. Each node participating in the network acts both as host and a router and must therefore be willing to forward packets for other nodes. For this purpose an efficient secure routing protocol is needed.

A mobile ad hoc network has certain characteristics, which imposes new demands on the routing protocol. The most important characteristic is the dynamic topology, which is a consequence of node mobility. Nodes can change position quite frequently, which means that we need a routing protocol that quickly adapts to topology changes. The nodes in an ad hoc network can consist of laptops and personal digital assistants (PDAs), and are often very limited in resources such as CPU capacity, storage capacity, battery power and bandwidth. This means that the routing protocol should try to minimize control traffic, and save secure environment such as periodic key for each interval of sending.

Only few researchers addressed the problem of MANET security, in this thesis, we are tested a secure DSR protocol to obtain the best throughput and average end to end delay. DSR is a multicast routing protocol in which routes between source and destinations are determined through a request

phase and a reply phase. We started from an authenticated routing protocol, Ariadne.It was attacked by wormhole attack, we proposed protocol to ***keep only the last MAC value in the route request***, instead of appending the MAC value of each intermediate node in the route, we argue that ***the hash chain has no security value***, so we removed it from route request, and ***use the route messages to exchange a new key*** that will be used till a new one is initiated . The resulting protocol saves a considerable amount of network bandwidth, node efforts, and prevents more attacks.
Glomosim simulator is used to simulate these scenarios. It is especially made to simulate mobile ad-hoc networks. There were some enhancements in the code of the simulator that we done to verify ARIADNE before obtaining the values of our suggestion. And then throughout our work after made a modification, also a C++ code is written to extract required data from the output text file to check the results.

Keywords:
Ad-Hoc Networks, Manet Security, Routing Protocol.

Acknowledgements

I would like to express my gratitude to all those who gave me the possibility to complete this thesis. This would actually be incomplete without a mention of the support given to me by my advisors **Prof. Dr. Yasser Dakroury , Dr Hassan Shehata Beador and Dr. Shaima Arafat** who saved no effort in making this work a success, they had helped me a lot during the preparatory and other subsequent phases of this project. They always found time whenever I needed an intelligent discussion. They are acknowledged for feedback and constructive criticism.

I would like to acknowledge **Prof.Dr. Adeeb Ghonimy** for his invaluable help and support.

Statement

This dissertation is submitted to Ain Shams University for the degree of M.Sc. of Electrical Engineering from the Computer and Systems Engineering Department.

The work included in this thesis was out by the author at the Computer and Systems Engineering Department, Faculty of Engineering, Ain Shams University.

No part of this thesis has been submitted for a degree or qualification at other university or institution.

Date : 27 / 5 / 2006

Signature :

Name : Amin Abdel-Wahab Amin Sorrour

Ain Shams University
Faculty of Engineering
Computer and Systems Department

Thesis Title : A Secure Routing Protocol for Mobile Ad-Hoc Networks.

Name :Amin Abdel-Wahab Amin Sorrour

Degree: Master of Science in Electrical Engineering (Computer and Systems Engineering)

Abstract

Ad hoc networking is a concept in computer communications, which means that users wanting to communicate with each other form a temporary network, without any form of centralized administration. Each node participating in the network acts both as host and a router and must therefore be willing to forward packets for other nodes. For this purpose an efficient secure routing protocol is needed.

A mobile ad hoc network has certain characteristics, which imposes new demands on the routing protocol. The most important characteristic is the dynamic topology, which is a consequence of node mobility. Nodes can change position quite frequently, which means that we need a routing protocol that quickly adapts to topology changes. The nodes in an ad hoc network can consist of laptops and personal digital assistants (PDAs), and