University of Science and Technology

College of Post Graduate Studies and Academic Advancement

Thesis submitted in Partial Fulfillment of the Requirements for the Degree of Master of Computer Sciences

A Proposed Detection and Prevention Technique for Black-hole Attacks in AODV MANETs

By:
Ahmed Salih Mohamed

Supervisor :

Dr. Noureldien Abdelrhman Noureldien

December - 2014

Abstract

A mobile ad-hoc networks (MANETs) are composed of equivalent nodes that communicate over wireless links without any central control. And can move randomly. MANETs have no network infrastructure, and are used in many areas because the ease and speed of deployment.

The nodes can cooperate to communicate with each other by sending data packets from source to destination node throw the intermediate node(s) by using routing protocols such as AODV MANETs have limited which is the most popular routing protocol. resources and several vulnerabilities, so mobile ad-hoc networks are defenseless to attacks done by some of the malicious nodes. These attacks can prevent the transmission or reduce the performance of the network. One of these attacks is the Black Hole Attack in which one or more malicious nodes absorbing all the data in the network. As a result the data packets do not reach the destination node and the data will be lost.

The security is essential for such kind of networks, many black hole detection and prevention techniques have been proposed, such as neighborhood-based method, path based

method, fake RREQ scheme, sequence number scheme and watchdog, most of this techniques had a clear security cost in terms of network performance.

In this research, we proposed and simulate an improvement in fake RREQ scheme to detect and prevent the black-hole attack in AODV MANETs in order to reduce the security cost and the results represented to reflect the better performance.

المستخلص

تتألف شبكات المحمول الخاصة من عقد متكافئة تتصل عبر شبكة لاسلكية ليس لديها بنية تحتية دون اي تحكم مركزي . ويمكن لجميع العقد التحرك بشكل عشوائي ، والتي يمكن استخدامها في عديد من المجالات بسبب سهولة وسرعة انتشارها .

يمكن للعقد التعاون للتواصل مع بعضها البعض عن طريق إرسال حزم البيانات من المصدر إلى المستقبل وذلك عبر عقده او مجموعة عقد وسيطه باستخدام أحد بروتوكولات التوجيه مثل بروتوكول AODV والذي يعتبر من اشهر بروتوكولات التوجيه. كما أن موارد هذه الشبكات محدوده وبها العديد من نقاط الضعف مما يجعل منها غير قادرة على التصدي لبعض إختراقات العقد الخبيثة.

هذه الهجمات من الممكن ان تمنع عملية نقل البيانات او تقلل من أداء الشبكة،أحد هذه الهجمات هو الفجوة السوداء والذي يعمل على إمتصاص جميع البيانات المرسلة عبر الشبكة ،ونتيجه ذلك عدم وصول البيانات الى وجهاتها وبذلك تفقد البيانات.

ولذلك فإن الأمن هو ضرورة لهذه الشبكات ، وهنالك العديد من الآليات المستخدمة لإكتشاف ومنع وجود هذا الهجوم مثل إستخدام معلومات عن العقد المجاورة، أسلوب الكشف باستخدام المسار، طريقة الاستعلام عن المسار المزيف ، طريقة رقم التسلسل و طريقة استخدام كلاب المراقبة، معظم هذه الآليات لديها أثر واضح على أداء الشبكة.

في هذا البحث قمنا بتمثيل وتطوير تقنية الاستعلام عن المسار المزيف المستخدمة للكشف عن وجود هذا الهجوم في هذا النوع من الشبكات في سبيل تقليل كلفة الامن وعرضت النتائج لتعكس أداءَ أفضل .

1.1 Introduction

MANET’s (Mobile Ad-hock Networks) have capability to self-manage without any need to predefined infrastructure. In addition MANET’s give their members nodes another feature namely the freedom of rooming that is all nodes in MANET’s will be unrestricted to be in specific location in the network. MANET’s can be applicable in many potential areas when it is not possible to set up a fixed infrastructure like: Military environments, Emergency operations, Civilian environments and Personal area networking[1].

To make the connection between the MANET’s nodes in the absence of centralization the nodes act as host and router as well, to supports this kind of connectivity new routing protocols were developed like: AODV (Ad-hock On-demand Distance Victor), DSDV (Destination-Sequenced Distance-Vector), OLSR (Optimize Link state Routing) and DSR (Dynamic Source Routing)[1].

MANET’s facing many security challenges that inherit from wireless transmission media which is used as a link between nodes and the highly dynamic topology. The use of wireless transmission media make MANET’s exposed to a many types of attacks that targets a confidentiality of data such as IP-spoofing, on the other hand the highly dynamic topology make implementation of some traditional security mechanism difficult[2].

1.2 Research Question

There are a many black hole detection and prevention techniques were proposed to make MANET’ s able to defend against black-hole attack. Most of proposed solutions have a clear cost in terms of network performance. Can we enhance a black-hole detection and prevention technique in order to mitigate this cost on the network performance?

1.3 Research Objectives

The main objective of this research is to investigate the current black hole attack detection techniques in order to develop or improve an efficient new detection technique.

1.4 Research Methodology

In this research we use an analytical approach to understand MANET’ s vulnerabilities and how can be exploited by many types of attacks and especially by black-hole attack. A deep analysis of black hole attack is carried out. Simulation approach to improve the fake RREQ black-hole detection method complements the analytical approach.

1.5 Results

In this research a new black-hole prevention and detection technique in AODV network was developed. The simulation results show that the new solution provides security to AODV against black-hole attack and improves the network performance in terms of packet delivery ratio and throughput.

1.6 Thesis Organization

The rest of this thesis is organized as follows: chapter 2 surveys MANET’ s attacks, chapter 3 details black hole attack, chapter 4 is dedicated to current black-hole detection techniques and the proposed technique and finally conclusion and future work is given in chapter 5.