UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF GRADUATE STUDIES AND ACADEMIC ADVANCEMENT

Simulating Black Hole Detection and Prevention Technique in MANET's using Sequence Numbers

A Thesis

Submitted to the College of Graduate Studies and Academic Advancements

In Partial Fulfillment of the Requirement for the Degree of Master of Science in Information Technology

Prepared By:

Mohammed Anwar Mahmoud Badawi

Supervisor By:

Prof. NourEldien Abdelrahman NourEldien

December 2016

Abstract

Mobile Ad-hoc Networks represents a new generation of wireless networks that allows communication among nodes in areas suffering environmental disasters. MANET’s doesn’t rely on a static infrastructure, but rather each mobile node acts as a router and a host simultaneously allowing it to discover routes and forward data packets as well.

To enable such unique features which allows routes creation instantaneously, protocols such as AODV and DSR among others has been developed and implemented to serve MANET’s needs. MANET’s still suffers from a variety of security issues, some of which are related to its wireless nature, while others are exclusives to MANET’s hence the whole process of route discovery and packet forwarding depends on cooperation.

One of the most elaborately discussed attacks on MANET’s is Black Hole attack which absorbs packets before reaching its destination. To mitigate black hole attacks a variety of solutions have been proposed, to detect and prevent the black hole from carrying its malicious behavior. In this research a presentation of one solution, the sequence number filtering detection mechanism is presented, evaluating its effictiveness in mitigating black hole attack using Network Simulator II.

The simulation results shows that the Sequence Number Filtering is able to detect and remove Black Hole attack nodes from ad-hoc network and improve network packet delivery ratio using a simple mechanism to avoid increase of transmission overhead time.

المستخلص

تُمثِل شبكات الهاتف وفق الطلب جيلاً جديداً من الشبكات اللاسلكية ، التي تتيح التواصل بين الخلايا حتى تحت الظروف الصعبة ، لا تعتمد الشبكات الفجائية لعملها على نقاط إتصال ثابتة و إنما تقوم كل خلية لا سلكية بعمليتي إكتشاف المسار و تمرير حزم البيانات. و ذلك بإستخدام مجموعة من بروتوكولات التوجيه التي تم تصميمها خصيصاً لخدمة احتياجات الشبكات الفجائية.

تعاني هذه الشبكات من مجموعة من المخاطر يعود البعض منها لطبيعة عملها اللاسلكية ، بينما البعض الاخر خاص بها فقط ، و أبرز هذه المخاطر هو هجوم الثقب الأسود الذي يقوم بإمتصاص و إسقاط جميع الحزم قبل وصولها لوجهتها الرئيسية. هذا الهجوم تم دراسته بإستفاضة و تم تطوير مجموعة من الحلول التي تسمح بإكتشافه و الحد من خطورته.

نستعرض في هذا البحث أحد هذه الحلول ونقوم بمحاكاته بإستخدام برنامج Network Simulator 2 لتوضيح إمكانيته على ردع هجمات الثقب الأسود ، و نجد من نتائج المحاكاة أن الحل المقترح قادر على إكتشاف خلايا الثقب الأسود و حذفها من الشبكة ، و بذلك تحسين أداء الشبكة دون التأثير سلباً على زمن الإرسال.

1.1 Introduction

MANET's (Mobile ad-hoc networks) represents a new generation of wireless networks that unlike any other wireless network before doesn't rely on a pre-existing infrastructure, but rather each node acts as a host and a router as well creating its own routes on-the-fly through some newly developed routing protocols such as AODV (Ad Hoc On Demand Distance Vector), DSDV (Destination-Sequenced Distance-Vector), OLSR (Optimize Link State Routing) and DSR (Dynamic Source Routing) enabling a unique way of direct communication among these nodes even in areas that lacks the ability to create a central point of access such as military environment, emergency operations fields, and personal area networks [i].

Although quite useful and full of potential MANET's still suffers from common wireless media transmission issues and some new struggles due to the consistently changing topology and dynamic routing nature. Thus making MANET's a target to a variety of attacks some of which are present in traditional wireless networks such as attacks threatening network confidentiality (e.g. IP spoofing, Man In The Middle and Denial of Service attacks), while other attacks targeting MANET's specifically (e.g. Black Hole, Grey Hole, Worm Attacks) [ii].

Black Hole attacks is considered the most threatening MANET attack, and to mitigate such a threat a variety of solutions has been proposed, one of which is Sequence Number Filtering that allows detection and prevention of black hole attack.

To prove the effectiveness of proposed solutions, researchers tend to use simulation tools (e.g. OPNET, OMNET, NS2, etc...) in order to save time and effort needed to test their algorithms functionality. We are using Network Simulator 2 to test a proposed solution, namely the Sequence Number Filtering solution.

1.2 Problem Statement

MANET's faces a great challenge overcoming security vulnerabilities exploitations, some of the aforementioned vulnerabilities were patched and a handful of security countermeasures were introduced to defend against MANET's targeting attacks. Even though one attack in particular the Black Hole attack still prove to be an issue regarding network security, an attack that dramatically affects the performance of the network rendering it totally useless. Although many solutions (techniques and algorithms) were introduced in this field, there's still a strong need for enhanced solution.

1.3 Research Objectives and Questions

This research aims to provide an honest review of one Black Hole detection and prevention technique and test the ability of Sequence Number Filtering Technique ability in mitigating black hole attack negative effects on the mobile ad-hoc network.
The research questions can be stated as follows:

a. What are the major threats and attacks to Mobile ad-hoc networks?
b. What are the proposed detection and prevention techniques for black hole attack?
c. How the Sequence Number Filtering Method is effective in mitigating Black Hole?

1.4 Research Methodology

In this research a study of an existing black hole detection and prevention technique is introduced. To test the Sequence Number Filtering technique we use Network Simulator 2 to simulate a MANET under normal AODV, MANET's under some nodes using a black hole infected AODV (Black Hole-AODV) and MANET's under some nodes affected by Black Hole-AODV, and other nodes using AODV with Sequence Number Filtering solution. The results of simulation are analyzed and plotted using X-Graph tool.

1.5 Thesis Structure

The rest of this thesis is organized as follows: Chapter 2 surveys MANETs Security issues in general and Black Hole Attack in details. Chapter 3 provides the details of research methodology. Chapter 4 surveys black hole detection and prevention techniques.
Chapter 5 includes the simulation of the proposed solution and results of the analysis. Finally chapter 6 represents conclusion and future work.

1.6 Thesis Scope

This research main scope is detection and prevention of single black hole attack in Mobile Ad-Hoc Networks, in the presence of a single malicious node, using Ad-Hoc on Demand Distance Vector (AODV) routing protocol.

---

[i] S. Khalil and N. Abdelrahman, "A Detection and Prevention Algorithm for Single and Cooperative Black hole Attacks in AODV MANETs", Thinkmind.org, 2015.

[ii] Deng, H., Li, W. and Agrawal, D.P., 2002. Routing security in wireless ad hoc networks. IEEE Communications magazine, 40(10), pp.70-75.