UNIVERSITI PUTRA MALAYSIA

PERFORMANCE EVALUATION OF MANET IN PRESENCE OF BLACK HOLE NODES

SAIF MAHMOOD DHAHIR

FSKTM 2017 21

PERFORMANCE EVALUATION OF MANET IN PRESENCE OF BLACK HOLE NODES

BY

SAIF MAHMOOD DHAHIR

Thesis Submitted To the Scholl of Graduate Studies, University Putra Malaysia In Fulfillment Of the Requirement for the Degree of Master of computer Science, Field of Distributed Computing

JANUARY 2017

COPYRIGHT

APPROVAL FORM

This project report was submitted to University Putra Malaysia and has been accepted as in partial fulfillment of the requirement for the degree of Master of Computer Science.

Members of the project report examination committee were as follows:

Mr. Ahmad Alauddin Arffin
Faculty of computer science and IT technology
University Putra Malaysia
(Supervisor)

Raja Azlina Raja Mahmood

Lecturer

Faculty of computer science and IT technology
University Putra Malaysia
(Supervisor)

DEDICATION

This thesis is dedicated to my parents for their endless love, support and encouragement.

Abstract of thesis presented to the Senate of University Putra Malaysia in Fulfillment of the Requirement for the Degree of Master of Computer Science

PERFORMANCE EVALUATION OF MANET IN PRESENCE OF BALCK HOLE NODES

By

SAIF MAHMOOD DHAHIR

JANUARY 2017

Chairman : Ahmad Alauddin Ariffin
Faculty : Computer Science and Information Technology

Abstract

Mobile ad-hoc network (MANET) is a standout amongst the most dynamic exploration subjects amid the earlier years. Mobile Ad-hoc networks are wireless, self-configurable as well as infrastructure-less networks which, can help in communicating information from one node to another using the intermediate nodes as a router. As the devices have mobility here, the network is dynamic in nature and it is quite often to re-establish the connection again and again. Because of the environment of ad-hoc network, dynamic, infrastructure-less and self-organizing, MANETs are vulnerable to several kinds of attacks and the black hole is one of the network layer attacks. In this type of attack, the black hole node uses the maximum destination sequence number to lure the sender node, to send packets via the shortest path, so that it will drop or alter the packets intentionally instead of sending them to the destination. Thus, the black hole nodes will reduce the network performance. The major goal of our project is to evaluate the performance of MANETs with and without the black hole node. Network simulator NS2.34 used for the simulation of the network within three different number mobile nodes (50, 150, and 165). The parameters used for evaluating the network performance are packet delivery ratio, an end-to-end delay, throughput and packet drop. The evaluation of two different scenarios using AODV routing protocol such as varying the number of black hole nodes and different mobility speed of the nodes. The analysis of generated trace files can be performed with the help of awk script. And then we will apply an algorithm that can offer better performance evaluation of the MANET compare to previous work[1].

Keyword: black hole attack, AODV routing protocol, MANETs, performance metrics.

Acknowledgements

First, all thanks, praises, and gratitude to the omnipotent Allah, who have favored me with the valuable bounties during my life and have given me the physical and mental power that empowered me to be what I am. I would like to express my deep gratitude after God almighty in the accomplishment of this thesis to my supervisor AHMAD ALAUDDIN ARIFFIN for his time, encouragement, exceptional support, guidance, and fruitful discussion. I would like also to thank Dr. NOORHAYATI MOHD ALI for all for her support and important information throughout my journey. Big thanks to my thesis committee for their effort to review my work and provide me with their comments. I would also like to thank all the of my faculty members and colleagues, supporting staff members of the Department of Computer Science and the School of Graduate Studies at university Putra Malaysia. Finally, I would eternally thankful to my parents for their encouragement, help and for their psychological and material support during these two years. I would like to dedicate this success to my dear father who provided me moral and material support during this period even though he suffers from brain cancer. Without them, I would not be here today. My God offers wellbeing and bliss to all of them.

DECLARATION

Declaration by graduate student I hereby confirm that:

- This thesis is my original work;
- Quotations, illustrations and citations have been duly referenced;
- This thesis has not been submitted previously or concurrently for any other
- Degree at any other institutions;
- Intellectual property from the thesis and copyright of thesis are fully-owned by University Putra Malaysia, as according to the University Putra Malaysia. (Research) Rules 2012;
- Written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the University Putra Malaysia (Research) Rules 2012;
- There is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the University Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the University Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ____________________ Date: ________________

Name and Matric No.: ____________________________________

LIST OF ABBREVIATIONS

AODV	Ad-Hoc on Demand Routing Vector
MANETS	Mobile Ad-Hoc Network
RREP	Route Reply
RREQ	Route Request
RERR	Request route error
DN	Destination node
SN	Source node
MN	Malicious node
CBR	Constant Bit Rate
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
DSR	Dynamic Source Routing
DOS	Denial of Service
NS2	Network Simulator 2
TORA	Temporally Ordered Routing Algorithm
DSDV	Destination-Sequenced Distance-Vector
OLSR	Optimized Link State Routing Protocol

LIST OF FIGURE

TABLE OF CONTENTS

CHAPTERS

CHAPTER ONE

INTRODUCTION

1.1 Background

(MANET) is a group of mobile nodes which it has the ability to communicate with each other without any fixed infrastructure, like mobile switching centers or base stations[2]. In MANET, connectivity and communication is complete from node to node by sending the messages through radio broadcast medium. Thus, MANET can be used in military services, battlefields, emergency cases such as floods, earthquake, fire etc. Moreover, each hub in ad-hoc network perform as a router and switch when it requesting for giving data from/to diverse nodes within the network. However, the traditional copper wired network limited bandwidth which it uses for communication. According to the nature and characteristics of MANET which is less infrastructure and self-organized it causes some issues for MANET like service discovery, mobility management, Quality of Services, security, bandwidth constraints etc. [3].Amongst all of these issues, security is one of the most critical research issues in MANET. The security issues might occur in different subjects such as frequent changes of network topology, lack of central monitoring, open medium node mobility etc. In addition, it is vulnerable to numerous types of attack such as impersonation, sinkhole attack, Sybil attack, denial of Service attack, wormhole attack, eavesdropping, Black hole attack etc.[4].

In this project, we will emphasize on the black hole attack which is one of the most severe kinds of attack in MANET. In this type of attack, the malicous node can simply use the highest sequence number of the destination to attract the sender node, to drive the packets via the shortest path. So that, it will drop or alter all packets intentionally instead of forwarding them to the destination.

Routing protocols have been made to determine how routers communicate with each other and how to select routers between any two nodes on the network. Several routing methods have been designed for MANETs such as AODV, DSR or OLSR and so on.[5]

The purpose of this work is to study the effect of black hole attack in two different network scenarios such as a number of black hole nodes, and mobility speed of nodes using AODV routing protocol. Figure 1.1 illustrates the mobile ad- hoc network.

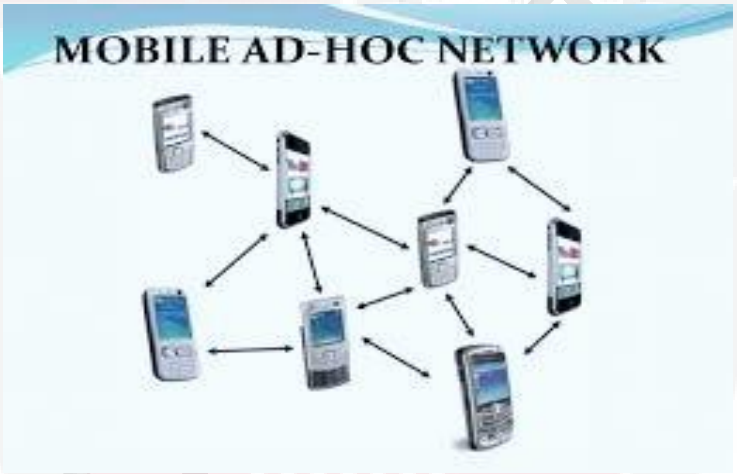

Figure 1.1: Mobile Ad-hoc network

1.2 Organization of this project

The project is consists of five chapters. Chapter 1 describes the introduction, problem statement, research motivation, scope, and objective of the study. Chapter two provides the background of the subject as well as the related work. Chapter 3 describe the methodology of the study. Chapter 4 shows the implementation result and analysis. Finally, we conclude the project, summary of objectives, contribution and future work.

1.3 Problem statement

The network security issues are all associated to malicious nodes or hubs that purposely deteriorate or compromise the network functionality. Mobile ad-hoc network copes different types of security threats i.e. attack that is achieved against them to interrupt the normal performance of the networks. However, many of the researchers have proposed methods and techniques that can prevent and detect the black-hole attack, to build a secure Ad-hoc network in several ways. In black-hole attack malicious node use its routing protocol to know other node that it has shortest path in the direction of destination and the aggressor drop the packet to decrease the amount of information that obtainable to other nodes. This type of attack made intentionally for denial of service type attack. This make destination system unreachable or shutdown in network.

1.4 Research Motivation

Wireless ad-hoc networks improved significant distinguish in wireless connections. Wireless connections made by hubs acting as switches and routers from single mobile node to another in MANET. As ad-hoc network come to widely used, the security case has come to be one of the critical arrangements for the entire times. The Black Hole attack, consider one of the most well-known attack that is the public in the on-demand routing protocols like AODV. Due to AODV protocol lack to devices, a malignant node can achieve several attacks in the network only by acting according to AODV rules.

1.5 Scope and objectives of the study

In this thesis, we will evaluate the effect of single and multiple black hole attacks in MANET by using a reactive routing protocol (ad-hoc on demand distance vector AODV). Then, the simulation will examine the performance of MANET within different number of mobile nodes (50, 150, and 165) within two different network scenarios like a various number of black hole nodes and mobility speed of nodes. The performance of the MANET is done by using network simulator (NS2.24). Additionally, the performance evaluation of MANET without the black hole and a different number of black hole nodes (1-5) as well as different mobility speed 0 – 10 m/s, along with diverse network parameters such as packet delivery ratio, throughput, packet drop, end-to-end delay.

REFERENCES

[1] C. Joseph, P. C. Kishoreraja, R. Baskar, and M. Reji, “Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios,” *Indian J. Sci. Technol.*, vol. 8, no. 29, pp. 1–10, 2015.

[2] K. M. Naseera and C. Chandrasekar, “Prevention of Black Hole Attack Using AOMDV,” *J. Eng. Res. Appl.*, vol. 3, no. 6, pp. 717–722, 2013.

[3] G. S. Mamatha and S. C. Sharma, “A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS,” *Int. J. Comput. Sci. Secur.*, vol. 4, no. 3, p. 275, 2010.

[4] H. K. Akanksha Saini, “Effect Of Black Hole Attack On AODV Routing Protocol In MANET,” *Int. J. Comput. Sci. Technol.*, vol. 4333, no. March, pp. 57–60, 2010.

[5] I. Ullah and S. U. R. Rehman, *Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols*. Ronneby Sweden, 2010.

[6] P. Goyal, V. Parmar, and R. Rishi, “MANET : Vulnerabilities , Challenges , Attacks , Application,” *IJCEM Int. J. Comput. Eng. Manag.*, vol. 11, no. January, pp. 32–37, 2011.

[7] D. S. S. T. Aarti, “Study of MANET: Characteristics, Challenges, Application and Security Attacks,” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 5, pp. 252–257, 2013.

[8] 2Capt. Dr. S Santhosh Baboo Mr. L Raja, “An Overview of MANET : Applications , Attacks and Challenges,” *Int. J. Comput. Sci. Mob. Comput.*, vol. 3, no. 1, pp. 408–417, 2014.

[9] S. R. G. Ruchia A.Kale, “AN OVERVIEW OF MANET AD HOC NETWORK,” vol. 6, no. 2, pp. 223–227, 2013.

[10] S. AL-HUSSEINI, “ON PERFORMANCE EVALUATION OF BLACK HOLE ATTACK IN AD- HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL USING NETWORK SIMULATOR 2,” 2015.

[11] T. M. Mahmoud, A. A. Aly, and others, “A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs,” *Int. J. Comput. Appl.*, vol. 109, no. 6, pp. 27–33, 2015.

[12] S. Gangwar, “Security Threats in Mobile Ad Hoc Networks - A Survey,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 7, no. 1, pp. 74–77, 2016.

[13] S. V. Raghavendran, Naga satish, “Security Challenges and Attacks in Mobile Ad Hoc Networks,” *I.J.Information Eng. Electron. Bus.*, no. September, pp. 49–58, 2013.

[14] S. H. Kauser and P. A. Kumar, “MANET : Services , Parameters , Applications , Attacks & Challenges,” *IJSRSET*, vol. 2, no. 2, pp. 4–9, 2016.

[15] P. K. Gagandeep, Aashima, “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review,” *Int. J. Eng. Adv. Technol.*, no. 5, pp. 269–275, 2012.

[16] S. R. K. and E. kheyrkhah Ali Dorri, “AN ANALYSIS OF SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS,” *Comput. Sci. Inf. Technol. (CS IT)*, pp. 13–25, 2014.

[17] M. K. N. Bharathi M, “Novel Approach for Enhancing the Performance of MANETs Using Reactive Routing Protocols,” *Int. J. Electron.*

Commun. Comput. Eng., vol. 7, no. 1, pp. 12–15, 2016.

[18] N. Saini and L. Garg, "Enhanced AODV Routing Protocol against Black hole Attack," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 6, pp. 847–850, 2014.

[19] J. Kumar, M. Kulkarni, and D. Gupta, "Effect of Black hole Attack on MANET routing protocols," *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 5, p. 64, 2013.

[20] E. Khin and T. Phyu, "IMPACT OF BLACKHOLE ATTACK ON AODVROUTING PROTOCOL," *Int. J. Inf. Technol. Model. Comput.*, vol. 2, no. 2, pp. 9–17, 2014.

[21] H. P. Singh and R. Singh, "A mechanism for discovery and prevention of coopeartive black hole attack in mobile ad hoc network using AODV protocol," in *Electronics and Communication Systems (ICECS), International Conference on*, 2014, pp. 1–8.

[22] B. S. Kakoty, "Simulation and Analysis of Blackhole Attack in MANETs for Performance Evaluation," *nternational J. Latest Trends Eng. Technol. Simul.*, vol. 2, no. 1, pp. 186–192, 2013.

[23] G. Singh and G. Singh, "Detection and Prevention Of Black Hole Using Clustering In MANET Using Ns2," *Int. J. Eng. Comput. Sci.*, no. 7420, pp. 7420–7430, 2014.

[24] R. Kumar, A. Quyoom, and D. N. Gouttam, "To mitigate black hole attack in AODV," in *Next Generation Computing Technologies (NGCT), 2015 1st International Conference on*, 2015, pp. 307–311.

[25] R. R. S. Arun Kumar Singh, "Study and Performance Evaluation of

AODV Protocols under Black Hole Attack in MANET," *Int. J. Adv. Res. Comput. Sci. Manag. Stud.*, vol. 3, no. 9, pp. 132–135, 2015.

[26] A. R. Yaakub and K. I. Ghathwan, "A PARALLEL PREVENTION ALGORITHM FOR BLACK HOLE ATTACKS IN MANET," *Int. Conf. Comput. Informatics*, no. 158, pp. 423–431, 2015.

[27] H. Moudni and M. Er-rouidi, "Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack," 2016.

[28] Teerawat Issariyakul • Ekram Hossain, *Introduction to Network Simulator NS2*. 2009.

[29] K. B. Aware Anand, "Prevention of Black hole Attack on AODV in MANET using hash function," *IEEE*, vol. 978–1–4799, 2014.

[30] K. B. Anand A, "Prevention of Black hole Attack on AODV in MANET using hash function," *IEEE*, vol. 978–1–4799, 2014.