THE EFFECT OF EAVESDROPPING AND WORMHOLE ATTACKS ON MOBILE AD HOC NETWORK

A Thesis submitted to
College of Arts and Sciences (Applied Sciences)
In Partial fulfillment of the requirements for the degree
Master of Science (Information Technology)
University Utara Malaysia

By

Nadher Mohammed Ahmed Al-Safwani

0·20

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

NADHER MOHAMMED AHMED AL-SAFWANI
(800321)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

THE EFFECT OF EAVESDROPPING AND WORMHOLE ATTACKS ON MOBILE AD HOC NETWORK

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **ASSOC.PROF. HATIM MOHAMAD TAHIR**

Tandatangan
(Signature) :

Assoc. Prof. HATIM MOHAMAD TAHIR
College Of Arts & Sciences
Univesiti Utara Malaysia
06010 UUM Sintok, Kedah, Malaysia
Tel: +604-928 4659 Fax: +604-928 4753
H/P: 019-454 9603 e-mail: hatim@uum.edu.my
Website: stafweb.uum.edu.my/hatim

Tarikh
(Date) : 8/11/09

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a Master of Science in Information Technology (MSc. IT) from University Utara Malaysia, I agree that the University library may make it freely available for inspection. I further agree that permission for copying of this project in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or in their absence, by the Dean of College of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to University Utara Malaysia for any scholarly use which may be made of any material from my project.

Request for permission to copy or make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Research and Graduate Studies
Colleges of Arts and Sciences
University Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman
Malaysia

ABSTRACT

Security has become the main concern to grant protected communication between mobile nodes in an unfriendly environment. Wireless Ad Hoc network might be unprotected against attacks by malicious nodes. This project evaluates the impact of some adversary attacks on mobile Ad Hoc network system (MANET's) which have be tested using QualNet simulator. Moreover, it investigates the active and passive attack on mobile Ad Hoc network. At the same time, it measures the performance of MANET with and without these attacks. The simulation is done on data link layer and network layer of mobile nodes in wireless Ad Hoc network. The results of this evaluation are very important to estimate the deployment of the Mobile Ad Hoc nodes for security. Moreover, this study have been analyzed the performance of MANET and perform "what-if" analyses to optimize them.

ACKNOWLEDGEMENT

All praise is due to Allah, Most Gracious, and Most Merciful. Without whose help and mercy, I would not have reached this far.

It would not have been possible for me to complete the course of my master without encourage and support of my family. My first expression of gratitude goes to my parents, wife, brothers, and sisters whose give me the strength to complete this course.

I would like to express my gratitude to my supervisor, Associate Professor Hatim Mohammed Tahir for expertise, gentle guidance, encouragement, critical remarks and advices which ensured that, progress, was continuously maintained. Our discussions since the last three months have contributed to the completion of this work.

I also would like to express my thanks to the University Utara Malaysia, colleagues, and friends to many moments of insight, inspiration, laughter, and for the given support.

Sincere Grateful

Nadher Mohammed A. Al -Safwani

DEDICATION

============================

I would like to dedicate this thesis to my father and mother,
wife, brothers, and sisters who lovely encouraged
and support me through all my study
The motivation for all I do.

============================

TABLE OF CONTENT

CHAPTER 1: INTRODUCTION

CHAPTER 2: LITERATURE REVIEW

CHAPTER 3: RESEARCH METHODOLOGY

CHAPTER 4: FINDINGS AND ANALYSIS OF DATA

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AODV	Ad Hoc on demand Distance Vector
CBR	Constant Bit Rate
DoS	Denial of Service
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
MAC	Medium Access control
MANET	Mobile Ad Hoc Network
NS	Network Simulation
SNT	Scalable Network Technologies
SYN	Synchronize
TCP	Transmission Control Protocol
UDP	User Data Protocol
WLAN	Wide Local Area Network

CHAPTER ONE

INTRODUCATION

1.1 Background

The wireless arena has been growing exponentially in past few decades. We have seen a great advances in network infrastructures as growing availability of wireless applications and the emergence of universal wireless devices like laptops ,PDA ,and cell phone (Papaleo, 2007). Nowadays, mobile users can rely on cellular phone to check emails and browse the internet. For example ,travelers with laptop can use the internet anytime and anywhere (Basagni, Conti, & Giordano, 2004). In the next generation of wireless communication systems, there will be a need for the fast deployment of independent mobile users. Important examples include establishing survivable, efficient, dynamic communication for emergency operations, disaster recovery, and military networks. Such network scenarios cannot rely on centralized and organized connectivity.

There are currently two kinds of mobile wireless networks. The first type is known as infrastructured networks with fixed and wired gateways. Typical applications of this type of “one-hop” wireless network include wireless local area networks (WLANs). The second type of mobile wireless network is infrastructureless mobile network commonly known as the Ad Hoc network or wireless Ad Hoc network (Jin & Jin, 2008).

REFERENCES

Anguswamy, R., Thiagarajan, M., & H.Dagli, C. (2008). Systems Methodology and Framework for problem definition in Mobile ad hoc networks.

Anjum, F., & Mouchtaris, P. (2007). security for Wireless Ad Hoc security

Basagni, S., Conti, M., & Giordano, S. (2004). Mobile Ad Hoc Networking.

Bianchi, A., & Pizzutilo, S. (2008). A Tool for Modeling and Simulating Mobile Ad-hoc Networks.

Bye, R., Schmidt, s., Luther, k., & Albayrak, s. (2008). Application-Level simulation for network security

Caballero, E. J. (2006). Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem.

Caro, G. A. D. (2003). Analysis of simulation environments for mobile ad hoc networks.

Carrillo, L., Marzo, J. L., VILÀ, P., & VILÀ, P. (2004). MAntS-Hoc: A Multi-agent Ant-based System for Routing in Mobile Ad Hoc Networks.

Çayırcı, E., & Rong, C. (2009). Security in Wireless Ad Hoc and Sensor Networks.

CCapkun, S., Hubaux, J. P., & Buttya´n, L. (2006). Mobility Helps Peer-to-Peer Security.

Chan, H., & Perrig, A. (2003). Security and Privacy in Sensor Networks.

Choi, S., Kim, D.-y., Lee, D.-h., & Jung, J.-i. (2008). WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks.

Demetrios, Z.-Y. (2001). A Glance at Quality of Services in Mobile Ad-Hoc Networks.

djenouri, D., khelladi, L., & Badache, N. (2005). A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks.

Erciyes, K., Dagdeviren, O., & Cokuslu, D. (2006). Modeling and Simulation of Wireles sensor and Mobike Ad Hoc Networks

Garrido, P. P., Malumbres, M. P., & Calafate, C. T. (2007). EVALUATION OF 802.11E MODELS UNDER NS-2 AND OPNET MODELER SIMULATION TOOLS IN MANET NETWORKS

Garrido, P. P., Malumbres, M. P., & Calafate, C. T. (2008). ns-2 vs. OPNET: a comparative study of the IEEE 802.11e technology on MANET environments.

Ghaffari, A. (2006). Vulnerability and Security of Mobile Ad hoc Networks.

Hogie, L. (2007). Mobile Ad Hoc Networks: Modelling, Simulation and Broadcast-based Applications.

Hu, Y., Perrig, A., & Johnson, D. B. (2002). Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks.

Jin, C., & Jin, S.-W. (2008). Invulnerability Assessment for Mobile Ad Hoc Networks.

Johston, D., & Walker, J. (2004). Overview of IEEE 802.16 security.

Kargl, F., & Schoch, E. (2007). Simulation of MANETs: A Qualitative Comparison between JiST/SWANS and ns-2.

Karlof, C., & Wagner, D. (2003). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures.

Kurkowski, S., Camp, T., & Colagrosso, M. (2005). MANET Simulation Studies: The Incredibles.

Lin, X.-H., Kwok, Y.-K., & Lau, V. K. N. (2003). Power Control for IEEE 802.11 Ad Hoc Networks:Issues and A New Algorithm.

Liu, J., Fu, F., Xiao, J., & Lu, Y. (2007). Secure Routing for Mobile Ad Hoc Networks.

Michiardi, P., & Molva, R. (2002). Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks.

Mishra, A. (2008). Security and Quality of service in Ad hoc wireless Netoworks.

Mishra, A., Nadkarni, K., Patcha, A., & Tech, V. (2004). Intrusion Detection in Wireless Ad Hoc Networks.

Ning, P., & Sun, K. (2003). How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-Hoc Routing Protocols.

Otrok, H., Paquet, J., Debbabi, M., & Bhattacharya, P. (2007). Testing Intrusion Detection Systems in MANET: A Comprehensive Study.

Papaleo, G. (2007). Wireless Network Intrusion Detection System: implementation and architectural issues.

Ravi, S., Raghunathan, A., & Chakradhar, S. (2003). Embedding Security in Wireless Embedded Systems.

Sabir, A., Murphy, S., & Yang, Y. (2006). Generic Threats to Routing Protocols.

Sarkar, S. K., Basavaraju, T. G., & Puttamadappa, C. (2008). ad hoc mobile wireless networks : principles, protocols, and applications.

Schoch, E., Feiri, M., & Frank Kargl, M. W. (2008). Simulation of Ad Hoc Networks:

ns-2 compared to JiST/SWANS.

Schoch, E., Feiri, M., Kargl, F., & Weber, M. (2008). Simulation of Ad Hoc Networks: ns-2 compared to JiST/SWANS.

Sharma, S., & Gupta, R. (2009). Simulation Study of Blackhole Attack in the Mobile Ad Hoc Networks.

Stajano, F., & Anderson, R. (2004). The Resurrecting Duckling:Security Issues for Ad-hoc Wireless Networks.

Thales. (2007). Implementing Mobile Ad Hoc Networking (MANET) over Legacy Tactical Radio Links.

Turban, E. a. A., J.E (1998). decision support systems and intelligent systems.

Scalable Network Technologies (SNT) . QualNet. http://www.qualnet.com/.

Vinayakray, P. (2002). Security within Ad hoc Networks.

Wang, H., Wang, Y., & Han, J. (2009). A Security Architecture for Tactical Mobile Ad hoc Networks.

Wu, B., Chen, J., Wu, J., & Cardei, M. (2006). A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks.

YianHuang, & Lee, W. (2003). A Cooperative Intrusion Detection System for Ad Hoc Networks.

Yu, S., Zhang, Y., Song, C., & Chen, K. (2005). A security architecture for Mobile Ad Hoc Networks.

Yun, J., Sohn, K., & Yoon, H. (2007). Dynamic Simulation on Network Security Simulator using SSFNET.

Zhang, Y., Huang, Y.-a., & Lee, W. (2005). An Extensible Environment for Evaluating Secure MANET.

Zhou, L., & Haas, Z. J. (1999). Securing Ad Hoc Networks. Cornell University Ithaca, NY 14853.