DEVELOPMENT OF A SECURED AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL FOR MANET

BY

OLUKEMI OLAITAN KUPOLUYI
B. Tech. Computer Engineering, LAUTECH, Ogbomoso

A THESIS SUBMITTED TO
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
FACULTY OF TECHNOLOGY,
OBAFEMI AWOLOWO UNIVERSITY,
ILE-IFE, NIGERIA

IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE AWARD OF MASTER OF SCIENCE IN
COMPUTER SCIENCE

2013

AUTHORISATION TO COPY

OBAFEMI AWOLOWO UNIVERSITY, ILE-IFE,
HEZEKIAH OLUWASANMI LIBRARY
POSTGRADUATE THESIS

AUTHORISATION TO COPY

Author: Olukemi Olaitan KUPOLUYI

Title: DEVELOPMENT OF A SECURED AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL FOR MANET

Degree: M.Sc. (Computer Science)

Year: 2013

I, Olukemi Olaitan KUPOLUYI, hereby authorise the Hezekiah Oluwasanmi Library to copy my thesis in part or whole in response to request from individuals and or organisations for the Purpose of private study or research.

Signature of Author and Date

CERTIFICATION

The undersigned hereby certify that this is an original research carried out by Olukemi Olaitan KUPOLUYI with the registration number TP09/10/H/2521 in the Department of Computer Science and Engineering, Faculty of Technology, Obafemi Awolowo University under my supervision.

Dr. E.A. Olajubu

Dr. H.A. Soriyan

DEDICATION

I dedicate this work to God Almighty.

ACKNOWLEDGMENT

I appreciate the Almighty God, for the great privilege of fulfilling my dreams despite all odds.

With so much respect, I graciously acknowledge and appreciate my supervisor, Dr E.A. Olajubu who painstakingly saw me through the success of this research work. His counsel, guidance, support and loving mentorship raised this work to this standard. I appreciate all your effort and may God bless you abundantly.

I also want to sincerely appreciate the Head of Department, Dr H.A. Soriyan, our Postgraduate coordinator, Dr. Ajayi and my other lecturers including Dr. O.A Odejobi, Dr. A.O. Oluwatope, Dr. (Mrs) Awoyelu and Dr. Oluwaranti for their encouragements. Their encouragements really aided me and improved the quality of this work. The Lord will stand by you at all times.

My warm gratitude goes to my good friend and colleague Odega Nwaebuni whose assistance contributed to the success of the work; my colleagues, Bello Olasunkanmi, Sarumi Taye, Obamila Ekundayo to mention a few, for your understanding. I heartily thank all my wonderful and loving friends especially Olayiwola Oluwafolake Esther, Erioluwa Oluyide, Temitope Olorunfemi, Olugbenga Akinade, Ifetayo Ojiwusi Balogun (Mrs.), Bruce Folasade, Agidi Olabode, Ekundayo Abimbola, Opeyemi Oyelami, for your patience, love and care, You are really good friends.

Finally, my profound gratitude goes to my loving parents, for being there for me always. You will live long to eat the fruit of your labour always. I appreciate my siblings for your prayers, kindness, care, love and moral support.

Thank you all.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

This study formulated, simulated and evaluated a trust based security model for Ad Hoc On-Demand distance Vector (AODV) routing protocol. This was with a view to reducing malicious attacks on mobile nodes in Mobile Ad-hoc Networks (MANETs).

A trust based security model was modelled as a three-input, one-output fuzzy inference system (FIS) using the fuzzy inference system toolbox in MATLAB. The model developed was fused into the AODV process model and simulated in Optimized Network Engineering Tools (OPNET). The model used the “minimum” hop count to destination and “most trusted route” techniques to route packets in the network. The performance comparison of the model and AODV was done using media access delay, network throughput and total packets dropped as performance metrics under three experimental scenarios (using network nodes of 20, 25 and 30). The developed model was further compared with an existing protocol Trust Based Reliable Ad-hoc On Demand Distance Vector (TBRAODV) using delay and network throughput as performance metrics under five experimental scenarios (using network nodes of 25, 50, 100, 200 and 300).

The simulation result showed that the model developed outperformed AODV by decreasing the packet dropped and increasing the network throughput. For instance, for the 20 nodes network, the average packet dropped for the developed model was 2.467 while the average packet dropped for AODV was 4.789. The network throughput for the developed model was 46,057bits/sec while it was 44,281bits/sec for AODV. Similarly for the second experiment, the network throughput for the developed model was an improvement over TBRAODV for all scenarios. For instance, for 50 nodes network, the network throughput for the developed model was 669,082.00bits/sec as against 114,559.89bits/sec obtained for Trust Based Reliable AODV. In addition, the delay for the developed model was 0.037sec while that of Trust Based Reliable AODV was 0.650sec.

It was therefore concluded that the developed model performed optimally better than both the unsecured AODV and Trust Based Reliable AODV (TBRAODV) with minimized packet dropped and increased network throughput.

CHAPTER ONE

INTRODUCTION

1.1 Background

The rapid proliferation of wireless networks, the continual increase in computing power and the tremendous growth of the Internet have changed the way the society manages information and information services. Computing today is becoming pervasive and wireless technologies are playing an important role in allowing devices like cellular phones and handhelds to wirelessly communicate with other devices and spontaneously forming short-range, short-term, ad-hoc networks.

All complex ecosystems; biological like the human body, natural like a rain forest, social like an open-air market, or socio-technical like the global financial system or the Internet, are interconnected (Bruce, 2012). Individual unit within those ecosystems are interdependent, each unit does its part and relies on the other units to do their parts as well. Also, all complex ecosystems contain parasites, within every interdependent system; there are individuals who try to subvert the system to their own ends. Every entity in a system needs to be able to trust that the entities it interacts with will corporate. Somehow, the entity does not trust completely or blindly but should be able to develop a confidence or be reasonably sure that its trust is well founded and other entities will be trust worthy in return (Bruce, 2012).

A mobile ad hoc network is an example of a complex ecosystem. It is a collection of wireless mobile nodes communicating with each other without the aid of a fixed infrastructure. Its unique characteristics like open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes makes it more vulnerable to attacks. In spite of the convenience that comes with being able to speedily deploy mobile ad-hoc networks and being mobile, they are vulnerable to malicious attacks. The lack of infrastructure and organizational environment offer special opportunities to attackers. Attackers may intrude into the network through malicious nodes because the topology of the network is highly dynamic as nodes frequently join or leave the network, and roam in the network (Madhavi and Kim, 2008).

Centralized security management appears impossible because of the scale of the system, the large number of potential users and sizable resources. Considering the size of the system, collaboration among strangers is unavoidable. The security objectives of both Mobile Ad hoc Networks and traditional networks are considered to be the same such as availability, confidentiality, integrity, authentication, and non-repudiation, however security issues involved in mobile ad hoc networks are quite different due to the 'mobile' and 'ad hoc' constraints (Sen *et al.*, 2008). Therefore for proper functioning of the network cooperation between nodes is required. Here cooperation refers to performing the network functions collectively by nodes for benefit of other nodes but because of open infrastructure and mobility of nodes; nodes might not cooperate resulting in a serious degradation in the network performance (Ukey and Chawla, 2010).

Routing algorithms for MANET have been designed with the assumption that all nodes cooperate. However a node may decide not to cooperate or misbehave by agreeing to forward packets and then fails to do so, because it is malicious, selfish, overloaded or broken. A malicious node launches a denial of service attack by dropping packets. A selfish node does not want to spend its remaining battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets. A broken node might have a software fault that prevents it from forwarding packets. Misbehaving nodes can be a significant problem. Therefore, the focus of this work is to develop a secured routing protocol by adding a notion of trust to the existing Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol, thereby making sure that only trusted routes are used as forwarding paths. Trust is the firm belief in the competence of an entity to act dependently, securely and reliably within a specified context (Kagal *et al.*, 2002). This work therefore optimized Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol to choose a forwarding path consisting of nodes that can be trusted to forward packets and not drop them thereby acting dependently, securely and reliably in the network.

1.2 Statement of the Problem

The present Ad-Hoc On-Demand Distance Vector (AODV) Routing Protocol is vulnerable to malicious attacks since no security feature is embedded. This study developed a secured routing protocol to achieve protection and high network performance.

1.3 Justification

Mobile Ad hoc networks bank on the cooperation of the nodes participating in the network to forward packets for each other. A node might decide not to cooperate to preserve its resources while using the resources of other nodes in the network to forward its own packet thereby degrading the network performance and cooperating nodes may find themselves unfairly loaded if too many nodes exhibit this behaviour (Bansal and Baker, 2003). The proposed protocol mitigates against routing misbehaviour in Mobile Ad hoc networks, encourages nodes to cooperate to increase their trust value and increase network performance.

1.4 Aim of the Study

This study developed a trust enhanced security model for Ad hoc On-Demand Distance Vector routing protocol for Mobile Ad hoc Networks.