Ain Shams University

Faculty of Computer and Information Sciences

Computer Systems Department

# Efficient Routing Protocol in Mobile Ad hoc Networks

A Thesis submitted to Computer Systems Department,
Faculty of Computer and Information Sciences, Ain Shams University,
in partial fulfillment of the requirements for
the degree of Master of Science in Computer Systems

By

**Abeer Assem Zaky Ghander**

B.Sc. in Computer and Information Sciences,
Demonstrator at Computer Systems Department,
Faculty of Computer and Information Sciences, Ain Shams University.

Under Supervision of

**Prof. Dr. Zaki Taha Fayed**

Professor of Computer Science
Faculty of Computer and Information Sciences, Ain Shams University.

**Prof. Dr. Hossam El-Deen Mostafa Faheem**

Professor of Computer Systems
Faculty of Computer and Information Sciences, Ain Shams University,

**Dr. Eman Shaaban**

Associate Professor of Computer Systems,
Faculty of Computer and Information Sciences, Ain Shams University.

**Cairo 2015**

## Acknowledgement

First and foremost, I have to thank my research supervisors, Prof. Zaky Taha, Prof. Hossam Faheem and Dr. Eman Shaaban. Without their assistance and dedicated involvement in every step throughout the process, this thesis would have never been accomplished. I would like to thank you very much for your support and understanding over the past years.

Finally I want to thank my family and friends for the support along the years. They have always been pushing me to be a successful person in my life and career.

# Abstract

Mobile Ad hoc network MANET is a self-organizing and self-configuring multi-hop wireless network, where the topology of the network changes dynamically. Nodes in these networks cooperate in a friendly manner in order to engage themselves in a multi-hop forwarding behavior.

Security attacks and limited energy are the most critical issues in mobile ad hoc networks. Multi-hop routing, random movement of mobile nodes and other features unique to MANET lead to enormous communication overhead for route discovery and maintenance. Meanwhile, to save energy, some nodes may opt for routing misbehavior such that they take part in routes finding process but do not forward data packets. Detecting and mitigating routing misbehavior, forcing malicious nodes to cooperate, and extending lifetime of the network should be considered in routing decisions in MANET.

This thesis proposes a Power Aware Cooperation Enforcement (PACE) distributed mechanism to help nodes make intelligent routing and forwarding decisions. Its functionality resides between the network and MAC layers of the protocol stack. The proposed distributed mechanism combines the knowledge of misbehaving nodes and link reliability to pick the most reliable path with highest residual energy for routing decision. To enforce malicious nodes to cooperate, other nodes will isolate them from the network by rejecting all their traffics. To evaluate the efficiency of this mechanism, it was integrated with well known AOMDV and DSR MANET routing protocols.

An extensive simulation study was conducted to evaluate and compare the performance of enhanced versions of these routing protocols. We measure the accuracy of detecting malicious nodes, throughput, delay, routing overhead, and residual energy of the MANET with different scenarios.

Integrating PACE mechanism with DSR and AOMDV helped to detect and isolate malicious nodes in the network. Moreover, it obtained safe

routes bypassing malicious nodes in the network without sacrificing the network performance. Additionally, power aware component incorporated into PACE mechanism managed to save nodes energy despite the high energy consumption by PACE mechanism due to the monitoring and overhearing of neighbor nodes requirement.

# Table of Contents

# List of Figures

# List of Tables

## List of Publications

- A. Ghander, E. Shaaban and Z. Fayed, “Performance Analysis of Observation Based Cooperation Enforcement in Ad Hoc Networks”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 2, 79-85, Nov. 2011

- A. Ghander, E. Shaaban, “Power Aware Cooperation Enforcement MANET Routing Protocols”, Submitted to The International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015), Mar. 2015

# Chapter 1 – Introduction

Mobile Ad hoc networking is one of the rapid growing technologies in the field of telecommunication. This chapter introduces mobile ad hoc networking with its advantages and limitations. Routing in mobile ad hoc networks and network applications are identified. The problem statement, objectives, and an overall thesis outline are clarified.

## 1.1 Mobile Ad Hoc Networks

A mobile ad hoc network (MANET) is a collection of wireless mobile hosts forming a temporary network without the assistance of infrastructure or centralized administration. Mobile ad hoc networks are self-organizing and self-configuring multi-hop wireless networks, where the topology of the network changes dynamically. This is mainly because of the mobility of nodes. Nodes in these networks cooperate in a friendly manner to engage themselves in a multi-hop forwarding behavior. Thus, the nodes in the network do not only act as hosts, but also act as routers that route the data to and from other nodes in the network.

In mobile ad hoc networks, where there is no infrastructure support and since a destination node might be out of range of a source node transmitting packets, a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. In this type of networks, each node must be able to forward data for other nodes.

Usage of mobile ad hoc networks has several advantages as follows:

- Setting up wireless network is easy and fast.
- Ad hoc networks eliminate the need to put out cables through walls and ceilings.
- Network can be extended to places where it is impossible to establish a wired network.
- Multiple paths increase network reliability.
- Wireless networks offer more flexibility to adapt to changes in the configuration of the network.

Mobile Ad Hoc networks have some problems such as limited wireless transmission range, broadcast nature of the wireless medium, packet losses due to transmission errors and mobility, stimulated change of route, battery constraints and security problems.

One of the fundamental vulnerability of MANETs comes from open peer-to-peer architecture. In case of wired networks there are dedicated routers but in case of mobile ad hoc network each mobile node acts as a router in order to forward packets for one node to other node. In MANETs, with respect to security design point of view, there is a lack of clear line defense. In case of wired networks we have dedicated routers; which perform routing functionalities for devices. Nevertheless, in case of Mobile ad hoc network, each mobile node acts as a router and forward packets for other nodes.

Mobile ad hoc networks have some limitations as follows:

- **Asymmetric links:** Most of the wired networks rely on the symmetry of links, which are always fixed. However, in ad hoc networks, this is not the case, due to the mobility of nodes and constant change of their positions. For example, consider a MANET where node (A) sends a signal to node (B). There is no guarantee for the quality of the connection in the reverse direction from node (B) to node (A).
- **Routing overhead:** In wireless ad hoc networks, nodes often change their location within the network. As a result, some of the routes in the routing tables of nodes are outdated, which introduce unnecessary routing overhead.
- **Dynamic topology:** This is a major problem in MANETs since the topology is not constant. The mobile node might move, hence medium characteristics might change. In ad hoc networks, routing tables should reflect these changes in topology. Also, the routing algorithms need to be adapted. For example, in a fixed network, routing table update takes place every 30 seconds. On the other hand, the update frequency would be very high for ad hoc networks in response to the rate of mobility of the network nodes.
- **Power Resources Limitation**: Mobile nodes depend mostly on batteries which are limited in energy. The energy available for mobile nodes depends on a lot of factors such as the network load, rate of packets sent and failure rate.
- **Security Issues:** MANETs suffer from many security issues due to the nature of the network setup and lack of centralized administration for the network.

- **Computation Capability:** Low-end devices such as PDAs can hardly perform low computations due to this way they usually use asymmetric cryptographic computation which is bit low complex, because mobile devices have very limited energy resources.

## 1.2 Applications of MANETs

MANETs are used in many fields [2]. The need for the mobile ad hoc networks is increasing with the easiness to obtain wireless mobile devices and with the decrease in the costs of such devices.

**Military Sector:** Military equipment now routinely contains some computer equipment. Ad hoc networking would allow the military to take advantage of common place network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.

**Commercial Sector:** Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. This may be due to the destruction of all of the equipment, or perhaps because the region is too remote. Rescuers must be able to communicate in order to make the best use of their energy, but also to maintain safety. By automatically establishing a data network with the communications equipment that the rescuers are already carrying, their job made easier.

**Low Level:** Appropriate low level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft.

**Data Networks:** A commercial application for MANETs includes ubiquitous computing. By allowing computers to forward data for others, data networks may be extended far beyond the usual reach of installed infrastructure. Networks may be made more widely available and easier to use.

**Sensor Networks:** This technology is a network composed of a very large number of small sensors. These can be used to detect any number of properties of an area. Examples include temperature, pressure, toxins, pollutions, etc. The capabilities of each sensor are very limited, and each must rely on others in order to forward data to a central computer. Individual sensors are limited in their computing capability and are prone to failure and loss. Mobile ad-hoc sensor networks could be the key to future homeland security.

## 1.3 Problem Statement

Security attacks and limited energy are the most critical issues in mobile ad hoc networks. Multi-hop routing, random movement of mobile nodes and other features unique to MANET lead to enormous communication overhead for route discovery and maintenance. Meanwhile, to save energy, some nodes may opt for routing misbehavior such that they take part in routes finding process but do not forward data packets. Detecting and mitigating routing misbehavior, forcing malicious nodes to cooperate, and extending lifetime of the network should be considered in routing decisions in MANET. All of these make routing in MANET a very challenging problem, and derives the research work outlined in this thesis.

## 1.4 Objective

The objective of this research is proposing an energy aware routing protocol to protect the network against routing misbehavior. It should help MANET nodes making intelligent routing and forwarding decisions while extending the lifetime of MANET. Moreover it mitigates routing misbehavior and enforces the cooperation of malicious nodes inside the network.

## 1.5 Thesis Outline

In this thesis, the first chapter introduces mobile ad hoc networking with its advantages and limitations. Routing in mobile ad hoc networks and network applications are identified. The problem statement, objectives, and an overall thesis outline are clarified.

The second chapter is a review for typical routing protocols for mobile ad hoc networks, including popular classification methods for the classical MANET unicast and multicast routing algorithms. It includes the popular routing protocols with highlight on DSR and AOMDV.

The third chapter classifies the security attacks, states the types of attacks at each network layer, and identifies the available routing solutions to tackle the security issues in MANETs. It also covers the power issues in mobile ad hoc network. Moreover it gives examples of some modified routing protocols to solve security and power issues. MANETs are highly vulnerable to several types of attacks, due to their open medium, lack of centralized monitoring, management point, and lack of strong line of defense. The different types of attacks have inspired a lot of research work to find mechanisms to defend against these attacks [18].

The fourth chapter proposes a Power Aware Cooperation Enforcement (PACE) distributed mechanism to help nodes make intelligent routing and forwarding decisions.. The proposed distributed mechanism combines the knowledge of misbehaving nodes and link reliability to pick the most reliable path for routing decision. To enforce malicious nodes to cooperate, other nodes will isolate them from the network by rejecting all their traffics. It explains its implementation for well known DSR and AOMDV routing protocols. Data structures and pseudo code for the proposed mechanism are also presented.

The fifth chapter evaluates the efficiency of PACE mechanism. It is integrated with well known AOMDV and DSR MANET routing protocols. An extensive simulation study is conducted to evaluate and compare the performance of enhanced versions of these routing protocols. We measure the accuracy of detecting malicious nodes, throughput, delay, and residual energy of the MANET. We study the effect of varying mobility and percentage of malicious nodes on the performance measures.

Chapter six introduces conclusion and points out future work.

# Chapter 2 - Routing Protocols in MANET

This chapter classifies the classical routing protocols for mobile ad hoc networks. It reviews the popular routing protocols for mobile ad hoc networks unicast and multicast routing algorithms.

## 2.1 Routing Protocol Properties

Routing means how to route a data packet from a source node to a destination node. In the case of MANETs, a packet is necessarily routed through several hops before it reaches the target destination. Since the network relies on multi-hop transmission for the communication, this imposes major challenges for the network layer to determine the multi-hop route over which the data packets can be transmitted between a given pair of source and destination node.

The routing protocol has two main functions: selection of routes for various source-destination pair and delivery of the messages to their correct destination. Movement of nodes in MANETs causes the nodes to go inside and outside of the ranges from one another. As a result, there is a continuous setting up and breaking of links in this network. There are some desirable properties in wireless ad hoc routing protocols that are different from conventional routing protocol like link state and distance vector.

Routing protocols desired properties are listed as follows:

- **Distributed operation:** The protocol should be distributed. It should not be dependent on a centralized controlling node. This is crucial because the nodes in ad hoc networks can enter and leave the network very easily.

- **Loop free:** The routing protocol should be guaranteed to supply routes that are loop-free in order to improve the overall network performance. This avoids any waste of bandwidth or CPU consumption.

- **Demand-based operation:** The protocol shall be a reactive protocol to minimize the control overhead and not to waste the network resources more than necessary. This means that the