Thesis Overview

UMPIRING SECURITY MODELS FOR MANETS

Ayyaswamy Kathirvel
PhD Thesis
Faculty of Information and Communication Engineering
Anna University
October 2010
ayyakathir@gmail.com

In recent times wireless mobile networks have caught increased attention and imagination of end users from all walks of life. The main goal of wireless mobile networks is to enable an end user to transmit data in wireless links in the absence of fixed infrastructure or centralized administrator.

Wireless Mobile Ad hoc Networks (MANET) allow a group of communicating nodes to set up and maintain a network among themselves without the reliance on a fixed base station or a wired backbone network. From the applications point of view, Wireless Mobile Ad hoc Networks are very useful for situations that require quick establishment of infrastructureless network, such as responses to September 11 attacks or the 2004 tsunami calamities in several parts of the world. Ensuring adequate security is an important aspect in such applications.

Secured communications have emerged as one of the most researched areas in the field of wireless mobile ad hoc networking. For popular Internet, dedicated routers controlled by the Internet Service Providers (ISPs) exist. However in wireless mobile ad hoc networks nodes must act both as regular Mobile Nodes and also as routers for other Mobile Nodes. In the absence of dedicated routers, providing security becomes a challenging task in ad hoc networks. Traditional routing protocols for wireless mobile ad hoc networks fail to provide the required security mechanism.

Prominent existing wireless mobile ad hoc routing protocols, such as Ad Hoc On Demand Distance Vector (AODV) routing protocol, Dynamic Source Routing (DSR) protocol, typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by intentionally disobeying the protocol specifications.

In wireless mobile ad hoc networks, packet delivery is achieved through two closely related network-layer operations: ad hoc routing and packet forwarding. As a result any security solution should encompass the protection of both. Protecting the network layer operations such as routing the control messages and data packet forwarding, from malicious attacks is an important and challenging issue in both wired and wireless mobile networks and the issue becomes even more challenging in the case of wireless mobile ad hoc network. Malicious nodes may disrupt routing algorithms by transmitting a false hop count; by dropping data packets and by routing the packets through unintended routes and so on.

The work presented in this thesis attempts to improve the performance of wireless mobile ad hoc networks by protecting the network layer. Five studies are presented.

The first study randomly selects a finite number of nodes in the network population as malicious nodes. Incorporating the Salvaging Route Reply (SRR) mechanism on the prominent On-demand Distance Vector (AODV) routing protocol, it investigates the resultant performance improvement.

The second study attempts to protect the network layer from the malicious attacks, by defining a Self Umpiring System for Security (Self_USS). Self_USS does not apply any cryptographic techniques on the routing the control messages and packet forwarding messages. Instead, it protects the wireless mobile ad hoc network by detecting and quarantining the malicious nodes. In this system each node is issued with a token at the inception.

The token with green flag is a permit issued to each node, which confers it, the freedom to participate in all network activities. Once a malicious node is deducted by its designated umpire, umpire node reacts by changing the status bit to red flag and thus depriving it of its right to access all the network activities. With red flag on, the culprit node is prevented from participating in the network.

The third study is to enhance the performance of Self Umpiring System for Security (Self_USS) with the incorporation of Salvaging Route Reply mechanism. The nodes with routing misbehaviour, during route reply phase maliciously give a wrong hop count. Such nodes are flagged off from the network by the umpire, thus permitting salvaging route reply packet commence immediately.

In the fourth Study, a Triple Umpiring System (TUS) for security is proposed to protect the network layer from the malicious attacks. In this system each node's behaviour from source to destination is closely monitored by a set of three umpires, and malicious node is detected by its designated umpires. The set of three umpires act collectively to detect and quarantine the malicious node.

In the last study, we have proposed two enhancements to the basic TUS. With Enhanced Triple Umpiring System for Security (ETUS), if the nodes behave maliciously during route reply phase, they will be flagged off from the network by the umpire and salvaging route reply packet commences immediately. The second enhancement corresponds to the data forwarding phase. During packet forwarding, once the guilty node is flagged off with a red flag, the remainder part of the message transfer is completed by umpires switching their roles. When a guilty node is identified and flagged off the communication link is cut. The corresponding neighbouring umpires switch their roles; throw off their umpiring coats and give a helping hand in continuation of the message transmission.

QualNet, a scalable simulator for wireless network system provides a comprehensive environment for designing any protocol and analyzing its performance. Simulations have been performed corresponding to the five studies on the QualNet simulator, and the results validate the studies.

ACKNOWLEDGEMENT

First and foremost I wish to express my deepest gratitude to my supervisor **Dr. R. Srinivasan**, Professor, Department of Computer Science and Engineering, B.S. Abdur Rahman University, Chennai, for his excellent guidance, inspiration, everlasting encouragement, untiring support, critical editing of the manuscript, enthusiastic advise and moral support throughout the course of investigation. With great pleasure I render my respectful thanks. I sincerely thank **Dr. K.M. Mehata**, the Head of the Department and Dean, School of Computer and Information Sciences, B.S. Abdur Rahman University, Chennai, for the insightful and cheerful discussions. I am thankful to the members of the doctoral committee, **Dr. V. Rhymend Uthariaraj**, Anna University and **Dr. Ranjani Parthasarathi**, Anna University.

I thank the Director, Dean, Advisor and Principal of Karpaga Vinayaga College of Engineering and Technology and the staff of Department of M.E Computer Science and Engineering, for all their help and support. I thank my parents **Mr. S. Ayyaswamy** and **Mrs. A. Indurani**, my wife **Mrs. K. Mohanambal**, my son **A.K. Naren** and my daughter **A.K. Keerthana**, for all their sacrifices. I give thanks to Him – of whom, through Whom, and unto Whom are all things; in Him all things hold together.

Ayyaswamy Kathirvel
ayyakathir@gmail.com