

University of Wollongong - Research Online

Thesis Collection

Title: Contribution to securing wireless mesh networks

Author: Shams Ud Din Qazi

Year: 2009

Repository DOI:

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Research Online is the open access repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

University of Wollongong Thesis Collections

University of Wollongong Thesis Collection

University of Wollongong

Year 2009

Contribution to securing wireless mesh networks

Shams Ud Din Qazi
University of Wollongong

Qazi, Shams UD, Contribution to securing wireless mesh networks, MCompSc-Res thesis, School of Computer Science and Software Engineering, University of Wollongong, 2009.
<http://ro.uow.edu.au/theses/792>

This paper is posted at Research Online.
<http://ro.uow.edu.au/theses/792>

NOTE

This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.



Contribution to Securing Wireless Mesh Networks

A thesis submitted in fulfillment of the
requirements for the award of the degree

Masters by Research

from

UNIVERSITY OF WOLLONGONG

by

Shams Ud Din Qazi

School of Computer Science and Software Engineering
June 2009

© Copyright 2009

by

Shams Ud Din Qazi

All Rights Reserved

Dedicated to
My Parents

Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

Shams Ud Din Qazi
June 3, 2009

Abstract

A wireless mesh network (WMN) comprises of mesh access points (MAPs)/mesh routers and mesh clients (MCs), where MAPs are normally static and they form the backbone of WMNs. MCs are wireless devices and dynamic in nature, communicating among themselves over possibly multi-hop paths, with or without the help of MAPs. Security has been a primary concern in order to provide protected communication in WMNs due to the open peer-to-peer network topology, shared wireless medium, stringent resource constraints and highly dynamic environment. These challenges clearly make a case for building multi-layer security solution that achieves both wide-range protection and desirable network performance.

In this thesis, we attempt to provide necessary security features to WMNs routing operations in an efficient manner. To achieve this goal, first we will review the literature about the WMNs in detail, like WMN's architecture, applications, routing protocols, security requirements. Then, we will propose two different secure routing protocols for WMNs which provide security in terms of routing, data and users as well.

The first protocol is a cross-layer secure protocol for routing, data exchange and Address Resolution Protocol (ARP) problems (in case of LAN based upon WMNs). Our protocol is a *ticket-based ad hoc on demand distance vector* (TAODV) protocol, a secure routing protocol that is based on the design of the Ad Hoc on demand distance vector (AODV) protocol. Due to the availability of a backbone, we incorporate the Authentication Server (AS) for the issuance of tickets which are further used for secure routing, transfer of public keys and MAC addresses in one single step. By incorporating the public keys, source and destination can easily generate their shared secret key based upon Fixed Diffie-Hellman key exchange protocol for data encryption and decryption. Our protocol is secure against both active as well as passive attacks.

The second proposed protocol is to “achieve user anonymity in WMNs”. This

protocol is also ticket-based protocol. The ticket is issued by Network Operator (NO) which provides user anonymity, user authentication and data confidentiality/privacy throughout the WMN. Our protocol is inspired by the blind Nyberg-Rueppel digital signature scheme. In this protocol NO issues tickets to valid users only and these users can then use these tickets to access Internet or to access services provided by Internet Gateway (IGW). IGW can only verify these tickets whether tickets are valid or not but can not check “Identity of ticket holder”. This way, user anonymity has been achieved along with user authentication and data privacy throughout WMN.

Acknowledgements

First of all, I would like to thanks A/Prof Dr Yi Mu and A/Prof Dr Willy Susilo, my supervisors, for their guidance and constant support during my study. I must evidence their wealth of knowledge in the field of security and cryptography. I also appreciate their efforts in guiding me in the field of network security, especially in the area of cryptography.

I am grateful to University of Sciences and Technology, Pakistan for providing me this opportunity to pursue my higher studies in University of Wollongong by giving financial support.

I would like to thanks all of my research group members especially Xinyi Huang, Wei Wu and Siamak Fayyaz Shahandashti, for their help in learning cryptography. I would also like to thank all staff of Centre for Computer and Information Security Research and the School of Computer Science and Software Engineering.

Finally, I would like to thanks my parents, for their relentless support throughout my entire life with their love and guidance. Without them, I would never be able to have all my achievements.

Publications

1. Shams Qazi, Yi Mu and Willy Susilo. *Securing Wireless Mesh Networks with Ticket-Based Authentication*. 2nd International Conference on Signal Processing and Telecommunication Systems, ICSPCS'2008.

Contents

Abstract	v
Acknowledgements	vii
Publications	viii
1 Introduction	1
1.1 Background	1
1.2 Problem Description	2
1.3 Our Contribution	3
1.4 Thesis Structure	4
2 Wireless Mesh Networks Basics	5
2.1 Introduction	5
2.2 Network Architecture	7
2.2.1 Infrastructure WMNs	9
2.2.2 Client WMNs	10
2.2.3 Hybrid WMNs	11
2.3 Characteristics of WMNs	12
2.3.1 Multi-Hop Wireless Network	12
2.3.2 Support for Ad Hoc Networking	12
2.3.3 Mobility Factor	12
2.3.4 Access of Multiple Networks	13
2.3.5 Dependence of Power Consumption	13
2.3.6 Compatibility with Existing Wireless Networks	13
2.4 Applications of WMNs	13
2.4.1 Broadband Home Networking	14

2.4.2	Community and Neighborhood Networking	14
2.4.3	Enterprise Networking	15
2.4.4	Metropolitan Area Networks	16
2.4.5	Transportation Systems	17
2.4.6	Building Automation	17
2.4.7	Health and Medical Systems	17
2.4.8	Security Surveillance Systems	18
2.5	Routing Protocols	18
2.5.1	Ad-Hoc on Demand Distance Vector (AODV) Protocol	20
2.5.2	Dynamic Source Routing (DSR) Protocol	22
2.6	Security Requirements	24
2.6.1	General Security Requirements	24
2.6.2	Security Requirements for WMNs	27
2.7	Existing Secure Routing Protocols	29
2.7.1	ARAN	29
2.7.2	SAODV	30
2.7.3	SAR	30
2.8	Evaluation of Existing Secure Routing Protocols	32
2.8.1	ARAN	32
2.8.2	SAODV	33
2.8.3	SAR	33
2.9	Summary	33
3	Cryptography Basics	35
3.1	Introduction	35
3.2	Cryptography	36
3.2.1	Secret or Symmetric Key Cryptography	36
3.2.2	Public or Asymmetric Key Cryptography	37
3.3	Diffie-Hellman Key Exchange Protocol	38
3.3.1	Algorithm	39
3.4	Digital Signatures	40
3.4.1	General Scheme	40
3.4.2	Security Requirements for Digital Signature Schemes	42
3.5	Nyberg-Rueppel Signature Scheme	43
3.6	Blind Signatures	43

3.6.1	Functions	44
3.6.2	Protocol	44
3.6.3	Properties	45
3.7	Blinding the Nyberg-Rueppel Digital Signature	45
3.8	Summary	46
4	Ticket based Ad-Hoc On Demand Distance Vector Protocol	48
4.1	Introduction	48
4.2	Protocol Design	49
4.2.1	Notations	51
4.2.2	Setup	51
4.2.3	Proposed Run	52
4.2.4	In Case of New MAP	53
4.2.5	In Case of New MC	54
4.2.6	Communication Between Different MCs	55
4.2.7	Address Resolution Protocol Security	58
4.3	Security Analysis	58
4.4	Summary	60
5	Achieving User Anonymity in WMNs	62
5.1	Introduction	62
5.1.1	Anonymity and Its Importance	62
5.1.2	Application Scenario	63
5.2	Protocol Design	65
5.2.1	Notations	66
5.2.2	Registration of New Mesh Client	66
5.2.3	Ticket Generation Process	67
5.2.4	Proposed Run	69
5.2.5	Ticket Verification Process	72
5.2.6	Ticket Uniqueness Checking	73
5.3	Security Analysis	73
5.4	Summary	75
6	Conclusions	76
A	Glossary	79

List of Tables

1.1	Security issues related to each layer	3
3.1	Diffie-Hellman Key Exchange Algorithm	39
4.1	Certificate	52
4.2	Ticket	53

List of Figures

2.1	Wireless Mesh Network Architecture	6
2.2	Examples of mesh routers: (a) Conventional wireless router [1] and (b) Advanced Risc Machines (ARM)[2]	8
2.3	Infrastructure Wireless Mesh Network Architecture	9
2.4	Client Wireless Mesh Network Architecture	10
2.5	Hybrid Wireless Mesh Network Architecture	11
2.6	WMNs for broadband home networking	15
2.7	WMNs for community networking	16
2.8	Route Discovery in AODV Protocol	21
2.9	Route Discovery in DSR Protocol	23
2.10	Man-in-the-middle attack	27
2.11	Security Aware Routing Protocol	31
3.1	Secret or Symmetric Key Cryptography	37
3.2	Public or Asymmetric Key Cryptography	38
3.3	General Digital Signature Scheme	41
3.4	Verification of Digital Signature	42
4.1	Wireless Mesh Network with Authentication Server	50
4.2	Communication Process in Wireless Mesh Network	56
5.1	ISP using WMN for extension of Internet to users in remote area . .	63
5.2	Military Operation using WMN for communication	64
5.3	Internet extension using WMN	70

Chapter 1

Introduction

1.1 Background

During the last decade, there is rapid increase in popularity and importance of wireless networks due to recent technological advancements in wireless data communication devices, such as wireless LAN Cards, Bluetooth, PDAs and mobile phones etc. Easy installation and low setup cost of wireless networks as compared to wired networks have also amplified the interest of people in wireless communication and now everyone is looking for efficient wireless communication in everyday's life.

Communication in networks occurs by transmission of data packets from source to destination along some certain paths known as 'routes'. Finding the best possible path for data transmission over the network is known as routing. Routing is based upon routing protocols which use metrics to evaluate the best available path for a packet to travel from source and destination. A metric is a standard of measurement, such as path bandwidth, which is used by routing algorithms to determine the optimal path to a destination. To enable the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information [24].

Hence, routing is one of the important factors in data transmission from source to destination. Therefore, if routing information is maliciously tailored during communication process, then the routing protocol will not be able to ensure correct data delivery from source to destination. Attacks against routing protocols [37] generally can be categorised into one of two main categories:

- Routing-disruption attacks: The attacker attempts to cause legitimate data packets to be routed in dysfunctional ways.
- Resource-consumption attacks: The attacker injects packets into the network

in an attempt to consume valuable network resources such as bandwidth or to consume node resources such as memory (storage) or computation power.

Wireless networks lack efficient and scalable security solutions because their security is easier to be compromised because of following characteristics: i) vulnerability of channels and nodes in the shared wireless medium; ii) dependence upon neighbors; iii) dynamic change of network topology. All of these factors offer intruders to obtain access into the network and participate in communication. In order to prevent routing operations from being interrupted, security features like confidentiality, authentication, integrity and authorization are necessary to be implemented [45].

To implement above mentioned security features in wireless networks, some cryptographic primitives are suitable like encryption, digital signatures, certificates etc. However, implementation of these cryptographic primitives in wireless networks is not straightforward.

1.2 Problem Description

With the capability of self-organization, self-configuration, infrastructure and support to other networks (wired or wireless), Wireless Mesh Networks (WMNs) become an exciting research area and a popular commercial application of the ad hoc networks. But security is still an important research area in the field of WMNs because of shared wireless medium, infrastructure and dependence on other nodes for routing/data transfer.

The ultimate goal of the security solutions for WMNs is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mesh clients. In order to achieve these goals, the security solution should provide complete protection spanning the entire protocol stack.

Table 1.1 identifies the security issues in each layer [73].

As mentioned in Table 1.1, different network layers suffer from different type of security issues. At application layer, security against viruses, worms and malicious codes is required to implement. At transport layer, user authentication and end to end (from source to destination) data security is required, which can be implemented with the help of encryption. Routing protocols and forwarding protocols are running on network layer, therefore, security for routing protocols is needs to implemented at network layer. At link layer, protection for wireless MAC protocol and link-layer

Layer	Security Issues
Application	Prevention, detection of viruses, worms, malicious codes
Transport	Authentication and end to end data security through encryption
Network	Security of routing protocols and associated parameters
Link	Protecting the wireless MAC protocol and providing link-layer security support
Physical	Preventing signal jamming, denial of service attacks and other active attacks

Table 1.1: Security issues related to each layer

protocol is required. At the end, at physical layer, security against signal jamming and denial of service attacks is required.

We can use different antivirus softwares to prevent our Mesh Clients (MCs) against the attacks for application layer, whereas, for transport, network and link layer attacks, we need to design a cross-layer security protocol which provides authentication, data integrity, anonymity, secured address resolution protocol (security against Denial of Service (DoS), ARP Poisoning, ARP Spoofing etc) and secured routing information.

1.3 Our Contribution

In this thesis, we address security issues related to data exchange, routing and link layer (Address Resolution Protocol security problems) and anonymity for MCs in WMNs. In our first protocol, we propose a cross-layer secure ticket-based protocol which is based upon Ad-Hoc on Demand Distance Vector (AODV) protocol that covers secure routing, authentication, integrity, exchange of public keys and ARP. This would facilitate the users to exchange parameters during the route establishment session and these parameters would subsequently be used to ensure confidentiality and integrity of data exchange later on. With the help of our proposed protocol, network traffic can be reduced since there is no need to broadcast any ARP request for finding the MAC address of destination, since the MAC address is already part of ticket which is received by source during the routing discovery process and this ticket is also trusted because it is signed by Authentication Server.

In our second protocol, we propose a secure protocol which provides anonymity

to MCs in the network. In this protocol, Internet gateway cannot check the identity of MC but can only verify that whether this MC is valid user or not, if it is valid user then its Internet request is processed accordingly and reply is sent back to MC in secure way. Our secured protocols are based upon ticket-based solutions which are suitable for different WMNs applications like defense operations, disaster recovery or internet service extension and mobility support etc.

1.4 Thesis Structure

The rest of the thesis is organised as follows:

- In Chapter 2, we briefly discuss the basics of wireless mesh networks including network architecture, characteristics, applications and their routing standards. we also discuss the existing routing protocols for WMNs and address resolution protocol. Finally, we discuss security requirements for WMNs in terms of routing and address resolution protocols. In addition, we also review the secure routing protocols which exist in the literature and examine the security features they provide.
- In Chapter 3, we discuss all the cryptographic primitives that will be used throughout this thesis. we provide formal definitions for the cryptographic techniques covered in this thesis. we also review the algorithms for some significant schemes to acquire a clearer understanding.
- In Chapter 4, we present our first Ticket-based Ad-Hoc On Demand Distance Vector Protocol. In this Chapter, we discuss its design including setup, proposed run and different scenarios of communications between MCs. Finally, we present its security analysis and also comparison with other existing security protocols.
- In Chapter 5, we present our second protocol to achieve anonymity in WMNs based upon fair electronic cash scheme. In this Chapter, we discuss its design including setup, proposed run and verification process. Finally, we present its security analysis in detail.
- Chapter 6 is the conclusion, where we summarise the contribution of this thesis, and propose future research directions.

Chapter 2

Wireless Mesh Networks Basics

2.1 Introduction

With the passage of time, Internet is rapidly evolving into a global and ubiquitous communication network infrastructure. Traditionally, it is wired Internetwork and serves as a network computing environment only for stationary computers. Nonetheless, in the recent years, the tremendous increase in the number of portable computing devices like laptop computers, palmtop computers, PDAs etc, raised big demand for a mobile computing environment that incorporates both wireless and wired networking technologies concurrently.

In the traditional wireless ad hoc networks, freely moving nodes can participate in the network without requiring any pre-built infrastructure. In some cases, like military operations, disaster recovery or Internet service extension, instant network organization and mobility support are important. Therefore, with the capability of self-organisation, self-configuration, infrastructure and support to other networks (wired or wireless), WMNs have attracted more attention as an alternative for large-scale deployment of metropolitan area wireless networks. Thus, wireless mesh network has become an exciting research area and a popular commercial application of the ad hoc networks [45].

Wireless mesh networks comprise of a number of fixed mesh routers that act as a wireless infrastructure and mobile mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. The multi-hop wireless connectivity among these routers can reduce the significant cabling cost for building infrastructure while supporting Internet access to the users [15]. A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among

themselves (creating, in fact, an ad hoc network). This feature brings many advantages to WMNs such as low up-front cost, easy network maintenance, robustness, and reliable service coverage. Figure 2.1 depicts the basic architecture of Wireless Mesh Network which includes Mesh routers, Mesh clients, connectivity with the Internet and servers.

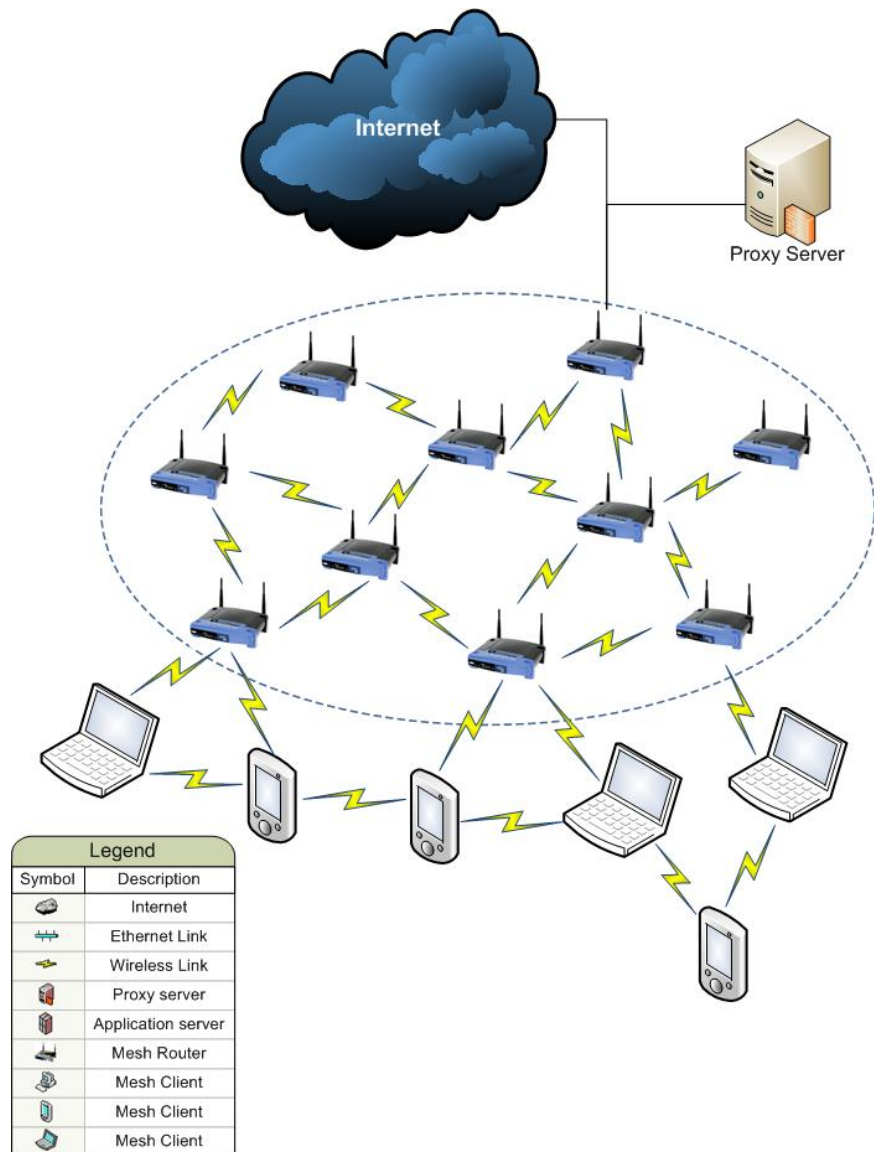


Figure 2.1: Wireless Mesh Network Architecture

A variety of mesh products and technologies have driven international standardisation activities to develop wireless mesh standards because WMN is a promising

wireless technology for numerous applications [33], e.g., broadband home networking, community and neighborhood networks, enterprise networking, building automation, etc. It has gained significant attention as a possible way for cash strapped Internet service providers (ISPs), carriers, and others to roll out robust and reliable wireless broadband service access in a way that needs minimal up-front investments. With the capability of self-organization and self-configuration, WMNs can be deployed incrementally, one node at a time, as needed. The reliability and connectivity for the users are directly proportional to the number of nodes. As more nodes are installed, reliability and connectivity have increased accordingly.

Deployment of WMN does not attract major difficulties, since all the required components including equipment, routing and other protocols are already available which are being used by ad hoc networks. These existing routing protocols for ad hoc networks and IEEE 802.11 MAC protocols [41] can be used, although there are still several challenges and issues preventing WMNs to be widely deployed in large scales. The first major issue is, the performance (throughput, delay, or packet loss rate) of WMNs drops sharply with increasing number of wireless hops the packets traverse through. To overcome this problem research is being carried out on, the multi-radio and multi-channel technique [11, 64]. The second major issue is the lack of an integrated cross-layer solution to provide security in WMNs at different layers. Without a well designed security solution, WMNs are vulnerable to various types of internal and external attacks that may cause significant inconvenience to the users and operators [75].

2.2 Network Architecture

WMNs mainly consist of two types of nodes:

1. Mesh Access Points (MAPs)/Mesh routers
2. Mesh Clients (MCs)

In order to support mesh networking, a wireless mesh router contains additional routing functions, besides the normal routing capabilities required by a conventional wireless router. To further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. In a comparison with a conventional wireless

router, a wireless mesh router can achieve the same coverage area with much lower transmission power with the help of multi-hop communications support. Optionally, the medium access control (MAC) protocol in a mesh router is enhanced with better scalability in a multi-hop mesh environment [9].

Similar hardware platform is used to built mesh and conventional wireless routers, but some of the mesh routers can be built based on dedicated computer systems (e.g., embedded systems), as shown in Figure 2.2. They can also be built based on general-purpose computer systems (e.g., laptop/desktop PC).

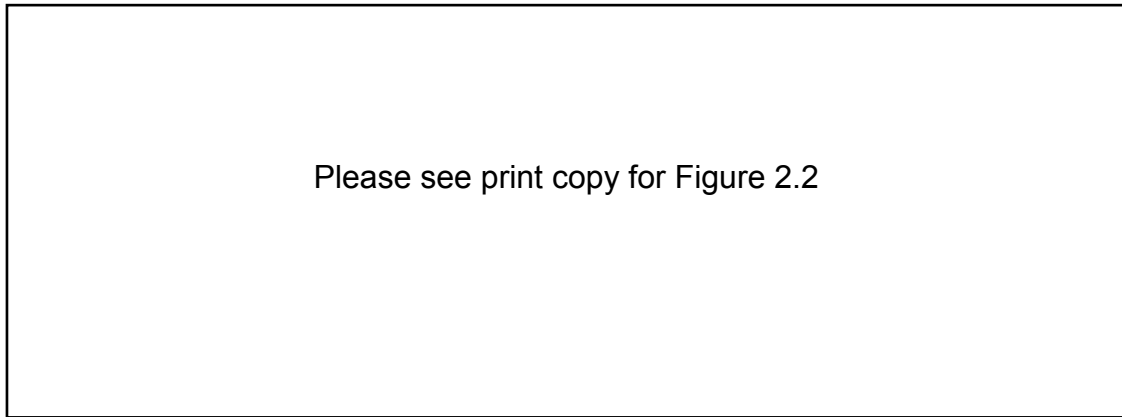


Figure 2.2: Examples of mesh routers: (a) Conventional wireless router [1] and (b) Advanced Risc Machines (ARM)[2]

Mesh clients also required necessary functions for mesh networking, and thus, can also work as a router, but can not perform gateway or bridge functions. As compared to mesh routers, mesh clients usually have only one wireless interface. Therefore, the hardware platform and the software for mesh clients can be much simpler than those for mesh routers. A large number of devices can be used as mesh clients as compared to mesh routers. They can be a laptop/desktop PC, pocket PC, PDA, IP phone, RFID reader, BACnet (building automation and control networks) controller, and many other devices.

WMNs can be classified into following three main groups based on the functionality of the nodes:

1. Infrastructure WMNs
2. Client WMNs
3. Hybrid WMNs

2.2.1 Infrastructure WMNs

In this type of WMNs, infrastructure for mesh clients is built with the help of mesh routers. The WMN infrastructure can be built using various types of radio technologies, in addition to the mostly used IEEE 802.11 technologies. The mesh routers form a mesh of self-configuring, self-healing links among themselves. Mesh routers enabled with gateway functionality can be connected to the Internet and other existing wireless/wired networks.

Conventional clients with Ethernet interface can also be connected to mesh routers via Ethernet links. For conventional clients with the same radio technologies as mesh routers, they can directly communicate with mesh routers. If different radio technologies are used, clients must communicate with the base stations that have ethernet connections to mesh routers. Figure 2.3 depicts the architecture of infrastructure WMNs.

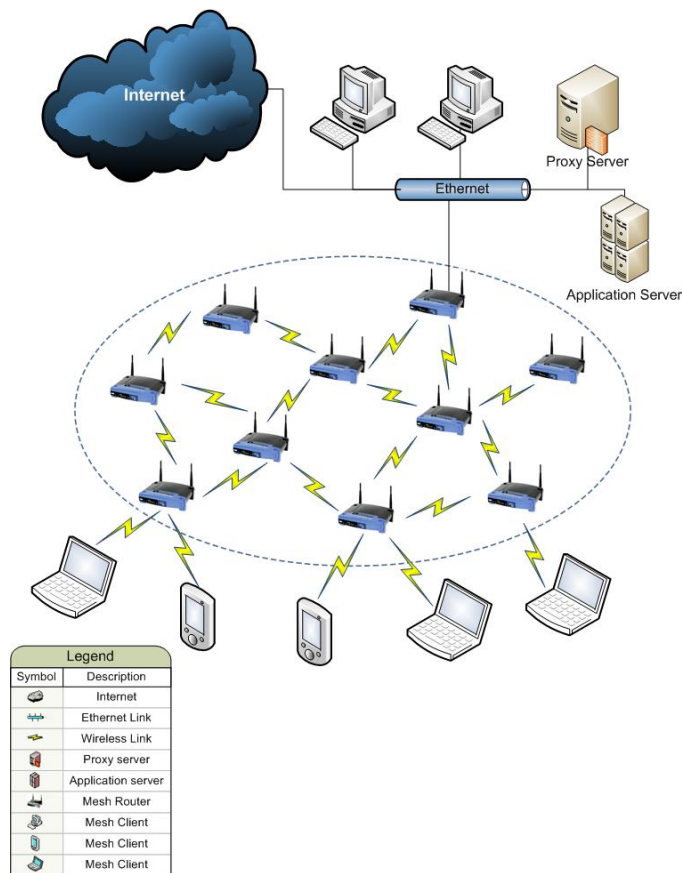


Figure 2.3: Infrastructure Wireless Mesh Network Architecture

Infrastructure WMNs are the most commonly used. For example, community and neighborhood networks can be built using infrastructure meshing. The mesh routers are placed on the roof of houses in a neighborhood, which serve as access points for users inside homes and along the roads. Typically, two types of radios are used in the routers, i.e., for backbone communication and for user communication, respectively. The mesh backbone communication can be established using long-range communication techniques including directional antennas.

2.2.2 Client WMNs

In this type of WMNs, mesh clients constitute the actual network to perform routing and configuration functionalities as well as providing end-user applications to customers. Hence, a mesh router is not required in these types of networks. The basic architecture of client WMNs is shown in Figure 2.4.

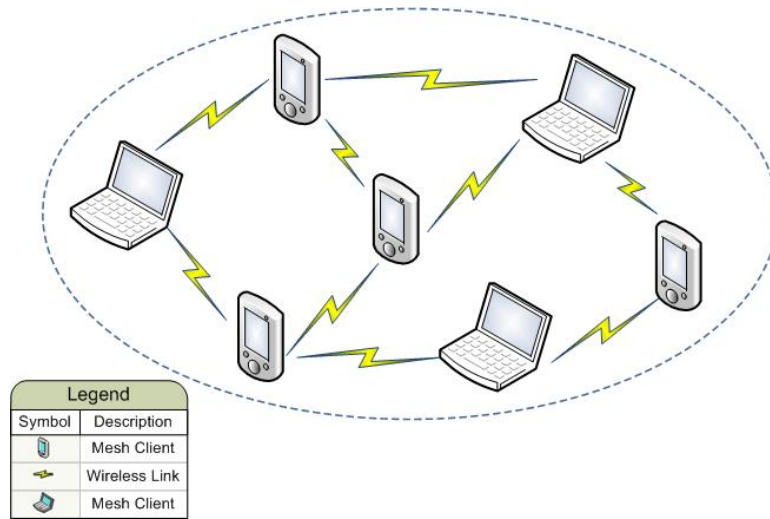


Figure 2.4: Client Wireless Mesh Network Architecture

In Client WMNs, a packet destined to a node in the network hops through multiple nodes to reach the destination. Client WMNs are usually formed using one type of radios on devices. Moreover, the requirements on end-user devices is increased when compared to infrastructure meshing, since, in Client WMNs, the end-users must perform additional functions such as routing and self-configuration.

2.2.3 Hybrid WMNs

In this architecture, both infrastructure and client WMNs are combined to explore the benefits of both as shown in Figure 2.5. Mesh clients can access the network either mesh routers or directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, and other wired/wireless networks; the routing capabilities of clients provide improved connectivity and coverage inside the WMN. The hybrid architecture will be the most applicable case in our opinion.

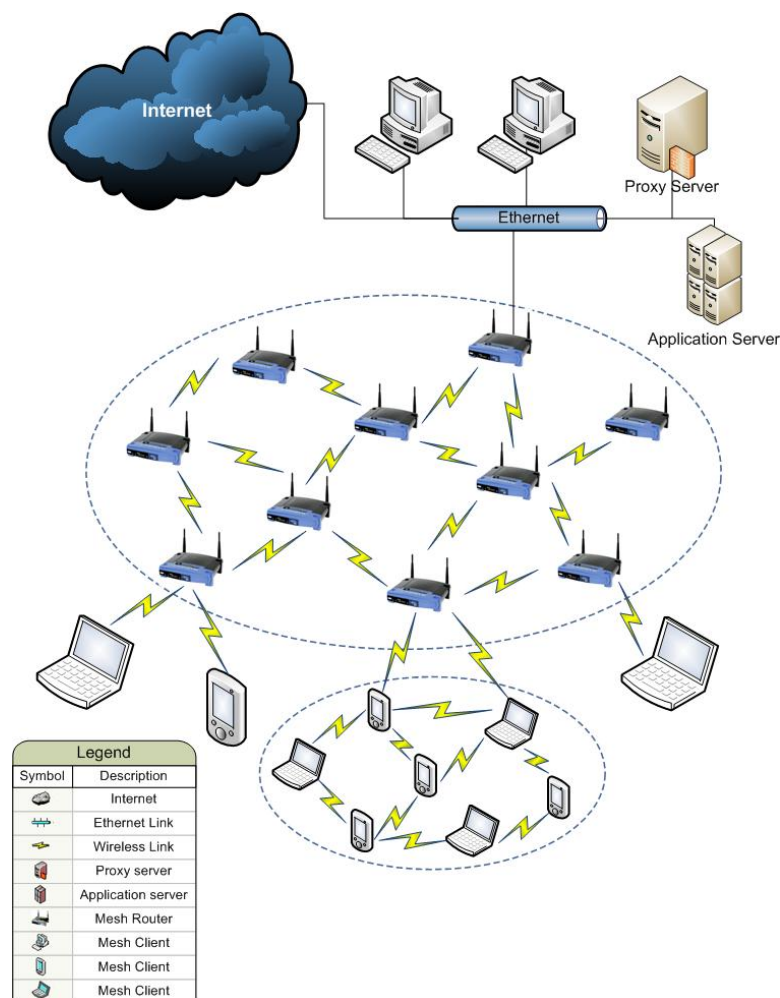


Figure 2.5: Hybrid Wireless Mesh Network Architecture

2.3 Characteristics of WMNs

There are many reasons to consider the use of WMNs because of their characteristics. Based on their characteristics, WMNs are generally considered as a type of ad-hoc networks. Some of the important characteristics of WMNs are discussed in later section.

2.3.1 Multi-Hop Wireless Network

Two main objectives for the development of WMNs are to extend the coverage range of current wireless networks without compromising the channel capacity and to provide non-line-of-sight (NLOS) connectivity among the users without direct line-of-sight (LOS) links [9]. To meet these requirements, the mesh-style multi-hopping is vital [44], because it will achieve higher throughput without sacrificing effective radio range via shorter link distances, less interference between the nodes, and more efficient frequency re-use[9].

2.3.2 Support for Ad Hoc Networking

WMNs enhance network performance and provide support to ad hoc networking, because of flexible network architecture, easy deployment and configuration (self-forming, self-healing, and self-organization), fault tolerance, and mesh connectivity. Due to these features, WMNs have low upfront investment requirements, and the network can grow gradually as needed.

2.3.3 Mobility Factor

Mesh routers usually have minimal mobility, while mesh clients can be stationary or mobile nodes. Mobility is the most challenging and important characteristic. Emulate motion of clients with respect to mesh nodes, motion of mesh nodes with respect to other mesh nodes, and multiple clients moving at the same time affects the performance of WMNs. Different velocities of motion such as people walking and mesh nodes on buses and trains should also affect the performance of WMNs [19].

2.3.4 Access of Multiple Networks

WMNs provide support to access both Internet and peer-to-peer (P2P) communications at the same time [43]. In addition, the integration with other wireless networks and providing services to end-users of these networks can also be supported through WMNs.

2.3.5 Dependence of Power Consumption

Mesh routers usually have minimal mobility, therefore, there is less constraints on power consumption for mesh routers. However, mesh clients may require power efficient protocols because of dynamic nature. As an example, a mesh-capable sensor [61] requires its communication protocols to be power efficient. Thus, the MAC or routing protocols for mesh routers may not be appropriate for mesh clients such as sensors, because power efficiency is the primary concern for wireless sensor networks [8, 7].

2.3.6 Compatibility with Existing Wireless Networks

WMNs built on existing IEEE 802.11 technologies [71] are compatible with IEEE 802.11 standards in the sense of supporting conventional WiFi clients with mesh capability. Such WMNs also need to be inter-operable with other wireless networks such as WiMAX [40] and cellular networks.

2.4 Applications of WMNs

The main motivation behind the research and development of WMNs is because of several applications which are supported by WMNs while at the same time these applications cannot be supported directly by other wireless networks such as cellular networks, ad hoc networks, wireless sensor networks, standard IEEE 802.11, etc [9]. Some of the interesting and important applications of WMNs are discussed in later sections.

2.4.1 Broadband Home Networking

WMNs are well-suited for broadband home networking and wireless mesh routers with mesh connectivity established among them instead of access points. Therefore, the communication between these nodes becomes much more flexible and more robust to network faults and link failures.

WMNs also solve the problems related to WLANs like dead zones can be eliminated by adding mesh routers, changing locations of mesh routers, or automatically adjusting power levels of mesh routers. Communication within home networks can be realized through mesh networking without going back to the access hub all the time like in the case of WLANs. Thus, network congestion due to backhaul access can be avoided.

In this application, wireless mesh routers have no constraints on power consumptions and mobility. Thus, protocols proposed for mobile ad hoc networks [22] and wireless sensor networks [8, 7] are too cumbersome to achieve satisfactory performance in this application. On the other hand, WiFi's are not capable of supporting ad hoc multi-hop networking. As a consequence, WMNs are more suitable for this application. An example of broadband home networking with the help of WMNs is depicted in Figure 2.6.

2.4.2 Community and Neighborhood Networking

The basic architecture of community networking to access network is based on cable or Digital Subscriber Line (DSL) connected to the Internet, and the last-hop is wireless by connecting a wireless router to a cable or DSL modem. Drawbacks related to this type of networks are:

- The main drawback of this type of network is that all traffic must flow through Internet, even if communication is between a community or neighborhood. This means network resources utilization increased insignificantly.
- Distance area in between houses is not covered by wireless services.
- An expensive but high bandwidth gateway between multiple homes or neighborhoods may not be shared and wireless services must be set up individually. As a result, network service costs may increase.

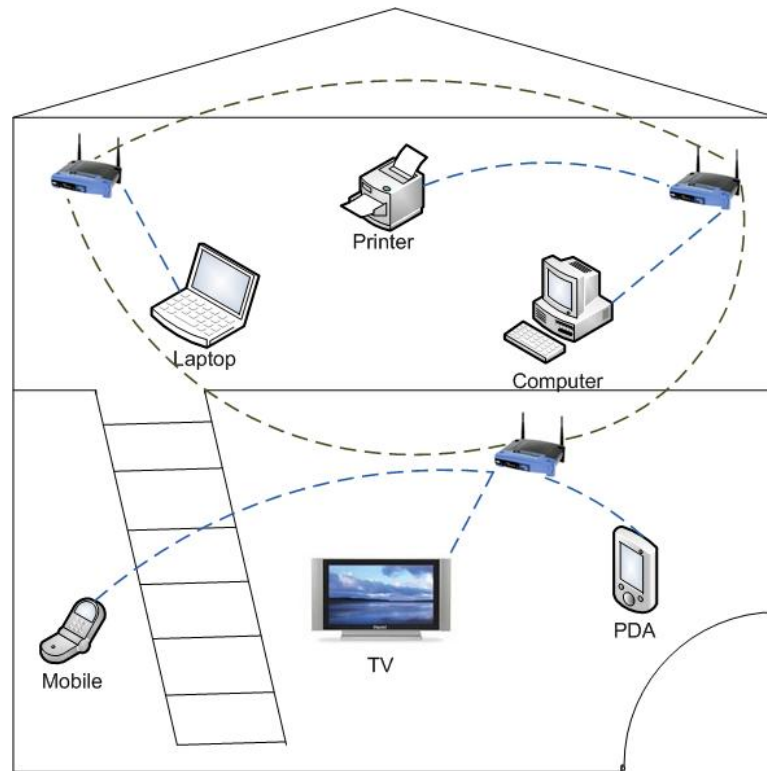


Figure 2.6: WMNs for broadband home networking

- Only a single path may be available for one home to access the Internet or communicate with neighbors.

As shown in Figure 2.7, WMNs can be used to diminish the above disadvantages. WMNs can also enable many applications such as distributed file storage, distributed file access, and video streaming.

2.4.3 Enterprise Networking

WMNs can be used to build all size of networks (small or medium or large) within an office or in an entire building, or among offices in multiple buildings. Wireless networks currently in use are still isolated islands because connections among them have to be achieved through wired Ethernet connections, which is costly solution. Therefore, provision of connectivity between different types of isolated wireless and wired networks within an enterprise is highly expansive as compared to having one type of network throughout the enterprise, which is also not possible. Another important issue in adding more backhaul access modems only increases capacity

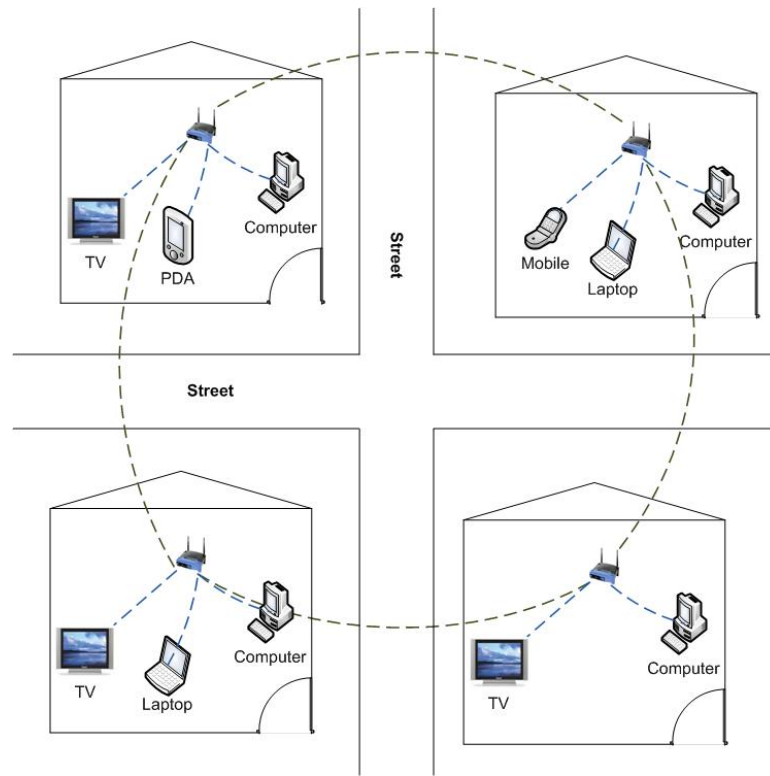


Figure 2.7: WMNs for community networking

locally, but does not improve robustness to link failures, network congestion, performance and cost of the entire enterprise network. Therefore, if the access points are replaced by mesh routers, Ethernet wires can be eliminated. WMNs can grow easily as the size of enterprise expands but WMNs for enterprise networking are much more complicated than at home because more nodes and more complicated network topologies are involved.

The service model of enterprise networking can be applied to many other public and commercial service networking scenarios such as airports, hotels, shopping malls, convention centers, sport centers, etc.

2.4.4 Metropolitan Area Networks

WMNs can also be used for metropolitan area networks and provide several advantages like, the physical-layer transmission rate of a node in WMNs is much higher than that in any cellular networks. For example, an IEEE 802.11g node can transmit at a rate of 54 Mbps. Moreover, wireless mesh MAN is an economic alternative to

broadband networking, especially in remote or rural or underdeveloped regions as compared to wired networks [9]. Thus, the requirement on the network scalability by wireless mesh MAN is much higher than that by other applications because it covers much larger area than other networks discussed above.

2.4.5 Transportation Systems

With the help of mesh networking technology, we can extend access into buses, ferries, and trains, instead of limiting IEEE 802.11 or 802.16 access to train stations and bus stops. Thus, convenient passenger information services, remote monitoring of in-vehicle security video, and driver communications can be supported. To enable such mesh networking for a transportation system, two key techniques are needed: the high-speed mobile backhaul from a vehicle (car, bus, or train) to the Internet and mobile mesh networks within the vehicle [9].

2.4.6 Building Automation

Nowadays, various electrical devices including power, light, elevator, air conditioner, etc., need to be controlled and monitored within a building. Currently this task is accomplished through standard wired or wireless (WiFi) networks, but wired networks are very expensive solution because of deployment complexity and maintenance, whereas wireless (WiFi) networks also have not achieved satisfactory performance yet, because deployment of WiFi for this application is still rather expensive due to wiring of Ethernet. We can reduce the deployment cost by replacing WiFi access points by mesh routers, and the deployment process is also much simpler due to the mesh connectivity among wireless routers.

2.4.7 Health and Medical Systems

In a hospital or medical center, monitoring and diagnosis data need to be processed and transmitted from one room to another for various purposes. Data transmission is usually broadband, since high resolution medical images and various periodical monitoring information can easily produce a constant and large volume of data. Traditional wired networks can only provide limited network access to certain fixed medical devices. WiFi based networks must rely on the existence of Ethernet connections, which may cause high system cost and complexity. However, these issues

do not exist in WMNs.

2.4.8 Security Surveillance Systems

As security is turning out to be a very high concern, security surveillance systems become a necessity for enterprise buildings, shopping malls, grocery stores, etc. In order to deploy such systems at locations as needed, WMNs are a much more viable solution than wired networks to connect all devices. Since still images and videos are the major traffic flowing in the network, this application demands much higher network capacity than other applications.

WMNs can also be used for other application scenarios including spontaneous (Emergency/Disaster) networking and Peer to Peer communications. For example, in case of an emergency response team and fire fighters where they do not have knowledge of environment and placement of network. Therefore, in this case, a WMN can be quickly established by simply placing wireless mesh routers in desired locations. For a group of people holding devices with wireless networking capability, e.g., laptops and PDAs, P2P communication anytime anywhere is an efficient solution for information sharing. WMNs are capable to meet this demand. These applications illustrate that WMNs are a superset of ad hoc networks, and thus can accomplish all functions provided by ad hoc networking [9].

2.5 Routing Protocols

Routing is the basis for communication within any network, therefore, use of efficient and secure routing protocol are necessary in both wired and wireless networks. As these networks are distinct in nature, therefore, different routing protocol are required to be used, according to the nature of network.

Since WMNs share common features with ad hoc networks, the routing protocols developed for MANET can be applied to WMNs [9]. For example, mesh routers of Firetide Networks [4] are based on reverse-path forwarding (TBRPF) protocol [56], Microsoft mesh networks [6] are based on dynamic source routing (DSR) [42], and many other companies mentioned in [5] are using ad hoc on-demand distance vector (AODV) routing [59].

The distinct nature of MANET results in the development of different routing protocols [35, 42, 65, 59, 49, 60]. Generally, these protocols are categorized into

three main groups:

1. Table-driven routing protocols (Proactive)
2. On-demand routing protocols (Reactive)
3. Hybrid (Cluster based approach)

In table-driven routing protocols, each participating node maintains tables which contains routing information to every other node in the network. All nodes update their tables in order to maintain a consistent and up-to-date view of the network after a specific time period. When a change occurs in topology, nodes then propagate update messages throughout the network. Then other nodes will be able to update their tables according to the message. Besides, nodes also inform other nodes about their status information by periodically propagating status messages. Through active information exchanging, all the nodes will be able to finally obtain the up-to-date topology information. When there is data to be sent, nodes can simply search their tables and extract the route. This is an proactive approach to conduct routing. This approach is similar to the one used in wired IP networks, for example in OSPF [50]. Proactive routing protocols for MANET are Destination Sequenced Distance Vector (DSDV) [60], Wireless Routing Protocol (WRP) [52] and Clusterhead Gateway Switch Routing protocol (CGSR) [47] etc. The main disadvantages of this approach are respective amount of data is required to be transfer for maintenance and slow reaction on restructuring and failures because every node needs to update its tables and also propagate updated information to others.

In on-demand routing protocols, whenever there is a requirement, then routes are created. In this approach, nodes do not propagate the topology status to each other and maintain the topology information for the whole network. Whenever a node wants to send data to a destination, it invokes a route discovery mechanism by flooding the route request packets to find the suitable route between source and destination. This route will remain valid until a failure on this route is detected. Reactive route determination is used in the Temporally Ordered Routing Algorithm (TORA) [58], the Dynamic Source Routing (DSR) [42] and the Ad-hoc On-demand Distance Vector (AODV) [59] protocols. The main disadvantages of this approach are high latency time in route finding and excessive flooding for route discovery can lead to network clogging.

In hybrid routing protocol, advantages of both proactive and reactive routing protocols combined to get better and efficient routes. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice for one or the other method requires predetermination for typical cases. Zone Routing Protocol (ZRP) [12] is an example of hybrid routing protocol for MANETs. The main disadvantages of such protocols are Advantage depends on amount of nodes activated and reaction to traffic demand depends on gradient of traffic volume.

In general, on-demand approach is more preferable than others because mostly mobile devices are used in MANETs, like laptops, PDAs, mobile phones etc. These devices are usually constrained by their memory size and battery life. Another important factor is availability of bandwidth as compared to wired networks. Therefore, on-demand routing protocols are preferred because there is no need to have large memory to store routing tables. Since there are less number of periodical propagated messages, the bandwidth usage is also reduced and battery life is saved as well by avoiding network-wide propagations.

2.5.1 Ad-Hoc on Demand Distance Vector (AODV) Protocol

AODV [59] is one of the most popular on-demand routing protocol, i.e., routes to the destination are only discovered when required thus avoiding memory overhead and less power. It emerged as an on-demand version of distance vector routing protocol [48], which is based on the classical Distributed Bellman-Ford (DBF) algorithm [25]. A node using AODV does not need to discover and maintain a route to another node until the two nodes need to communicate with each other. The routing messages do not contain information about the whole route path, but only about the source and destination. Therefore, routing messages are not increasing in size. All these features enable AODV to be a suitable routing protocol for MANET.

AODV uses a destination sequence number, which is generated, by the destination itself for each route entry. The destination sequence number ensures loop freedom and if two similar routes to a destination exist, then the node chooses the one with the highest sequence number. AODV uses Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages for route discovery and maintenance.

The routing operations of AODV generally consist of two phases: route discovery and route maintenance. In Figure 2.8, Route discovery is performed through broadcasting RREQ messages. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. RREQ carries Source ID, Destination ID, Source Sequence Number, Destination Sequence Number and a Broadcast ID. When an intermediate node receives a RREQ, it sends a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. The intermediate node also stores the previous node information in order to forward the data packet to this next node towards the destination.

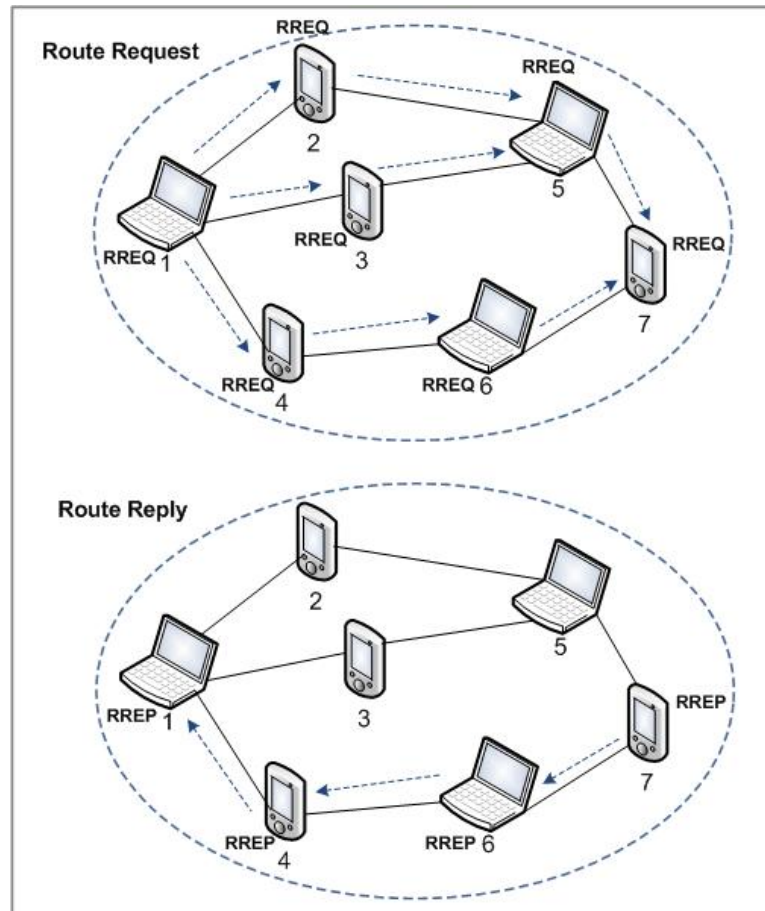


Figure 2.8: Route Discovery in AODV Protocol

When the RREQ reaches the destination, a RREP will be generated by the

destination node as a response to the RREQ. The RREP will be transmitted back to the originator of the RREQ in order to inform the route. If an intermediate node has an active route towards the destination, it can reply the RREQ with a RREP, which is called Gratuitous Route Reply. The intermediate node will also send an RREP to the destination node. The RREP will be sent in reverse route of RREQ if a bidirectional link exists.

Whenever there is a link break in the routing path, the RERR message will be broadcasted by the link break identifying node to the neighbor nodes to update or delete the routes through that node and the source initiates another RREQ broadcast to find fresh routes to the destination.

2.5.2 Dynamic Source Routing (DSR) Protocol

Dynamic source routing (DSR) protocol [42], is an on-demand routing protocol based on the concept of source routing, which means the initiator knows the complete hop-by-hop route to the destination. This specific feature brings efficiency, but also results in the scaling of routing message overhead. To perform DSR, each node is required to maintain a route cache which contains the topology information of the network. The route cache is consistently updated to reflect the current status of the network.

Similar to AODV, this protocol consists of two major phases: route discovery and route maintenance, as shown in Figure 2.9. When a source node originates a packet addressed to a certain destination, the initiator first searches its route cache for a route. If there exists an active route towards the destination, this route will be used. Otherwise, the node generates a route request packet (RREQ) which consists of a data structure called route record listing the IP addresses of all the intermediate nodes. This RREQ will be broadcast to neighbors. The receiving node will have two choices.

1. If it is not the target node of this route discovery, it appends its own address to the route record in the Route Request and propagates it by transmitting it as a local broadcast packet (to its neighbors)
2. If it is the target node, it returns a Route Reply to the initiator, giving a copy of accumulated route record from the Route Request.

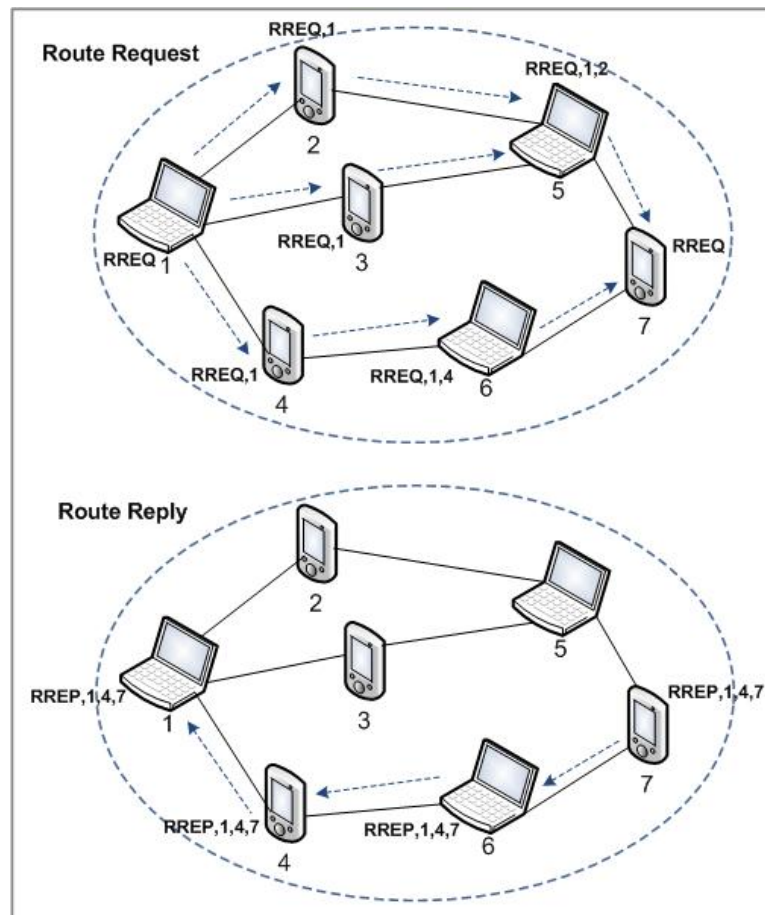


Figure 2.9: Route Discovery in DSR Protocol

This process will be continued until the RREQ packet reaches the destination. The original message is not changed during the transmission (except the RREQ data length field which is a number). The resulting route will be found in the route record.

The data structure of RREQ consists of two fields: IP fields and route request fields. IP fields contains source address, destination address and hop limit. Route request fields contains option type, option data length, identification, target address, and route record. When a RREQ is received, the option data length fields will be increased by 4 and the nodes IP address will be appended to the end of the route record. Other fields will remain unchanged during the whole route discovery process.

In replying the RREQ, the target node generates a route reply packet (RREP) and sends it back to the initiator by two ways. It can simply reverse the sequence

of hops in the route record and use it as the source route on the Route Reply. Otherwise, it searches its own route cache for a route back to the initiator. If such route does not exist, the target should initiate a Route Request back to the initiator.

During transmission, each node on the route is responsible for confirming that data can flow over the link from that node to the next hop. Since periodic routing advertisement is not available, nodes use the acknowledgement (ACK) to provide confirmation that a link is capable of carrying data. The acknowledgement can be required by a node. If the acknowledgement request has been retransmitted for the maximum number of times without being replied, the sender should treat this link as currently broken. It should remove this link from its route cache and should return a Route Error (RERR) to each node that has sent a packet routed over that link since an acknowledgement was last received.

2.6 Security Requirements

WMNs security is easier to be compromised as compared wired networks because of shared wireless medium, dependence upon neighbors for routing and data transfer, dynamic nature of topology and resource constraints including computation, memory and bandwidth. Firstly, general security requirements in terms of wireless networks and then WMNs specific problems will be discussed.

2.6.1 General Security Requirements

Networking either wired or wireless always suffers from different type of security threats [16], which are categorized as under:

- External Attacks: are committed by parties that are not legally parts of the network.
- Internal Attacks: are originated from inside a particular network.
- Passive Attacks: These attacks do not involve any disruption of the services, they are merely intended to steal information and eavesdrop on communication within the network.
- Active Attacks: actively alter the data, with the intension of overloading the network, obstructing the operation or cut off certain nodes from their neighbors so that they cannot use the network serviced effectively anymore.

External attacks can be prevented with the help of a firewall or proxy server whereas, detection of internal attacks is much more difficult because these are performed by network peers. These attacks are usually originated from compromised nodes malicious behaviors. Passive attacks do not disturb routing operations, but they are usually the first step of launching other active attacks. By eavesdropping communication, attackers may be able to learn the topology information, such as which node is the bottleneck of the network, and then launch attacks against that node. There are also some sophisticated attacks, exploiting design flaws of basic routing protocols, including black hole [10] and rushing attacks [39]. Some other common attacks which suffer routing and communication in wireless and wired networks are as under:

- Attacks by modification of routing information: This kind of attacks [35, 66] are performed by modifying the routing information. In wireless routing, network topology is maintained by flooding routing information through out the network. Any wrong updation or alteration in these messages will cause topology change, which effects the network communication. Current ad hoc routing protocols generally assume that nodes will not alter the routing message fields, which makes this kind of attack extremely easy to be launched.
- Attacks by spoofing: Spoofing [35, 66, 16, 23] means an attacker assumes the identity of another node, thus receiving messages that are directed to original node that identity it fakes. This kind of attack is commonly known in wired network, but becomes more serious in wireless networks. Because current ad hoc routing protocols do not authenticate the source IP address, attackers can easily masquerade other nodes. It is usually the first step to intrude a network so as to carry out further attacks to disrupt operations.
- Attacks by fabrication: These attacks are usually conducted by generating false routing messages, trying to disturb network topology [35]. It is regarded as route misbehavior, which is very difficult to detect. AODV and DSR are especially vulnerable to this kind of attack. In AODV, a malicious node can prevent communication between any two nodes by flooding spoofed RRER messages along the path. RRER messages claim that the next hop of the originator is currently unavailable. Any nodes receiving this message will mark this link as broken. Further, a malicious node can continue sending spoofed

RRER if the link is re-established, resulting in complete isolation of a targeting node.

- ARP attacks: In WMNs ARP request message is a broadcast message according to the basic ARP mechanism similar to other wired LAN networks, which results in the well-known broadcast storm problem [54] that is really harmful. In case of ARP, there are also some other security threats which also need to be diminished for smooth communication in WMNs. Man-in-the-middle, ARP spoofing and ARP poisoning [32] are the most dangerous attacks of MAC layer protocols. To minimize the number of ARP packets being broadcast, operating systems keep a cache of ARP replies. When a computer receives an ARP reply, it will update its ARP cache with the new IP/MAC mapping. As ARP is a stateless protocol, most operating systems will update their cache if a reply is received, regardless of whether they have sent out an actual request. ARP spoofing involves constructing forged ARP request and reply packets. By sending forged ARP replies, a target computer could be convinced to send frames destined for computer A to instead go to computer B [13, 31]. When done properly, computer A will have no idea that this redirection took place. The process of updating a target computer's ARP cache with a forged entry is referred to as "poisoning". However, using ARP spoofing, "man-in-the-middle (MITM)" attack can be launched in the network. When a MITM is performed, a malicious user inserts his computer between the communication path of two target computers. The malicious computer will forward frames between the two target computers so communications are not interrupted [54]. The attack is performed as follows (where C is the attacking computer, and A and B are targets):

- C poisons the ARP cache of A and B.
- A associates B's IP with C's MAC.
- B associates A's IP with C's MAC.
- All of A and B's IP traffic will then go to C first, instead of directly to each other.

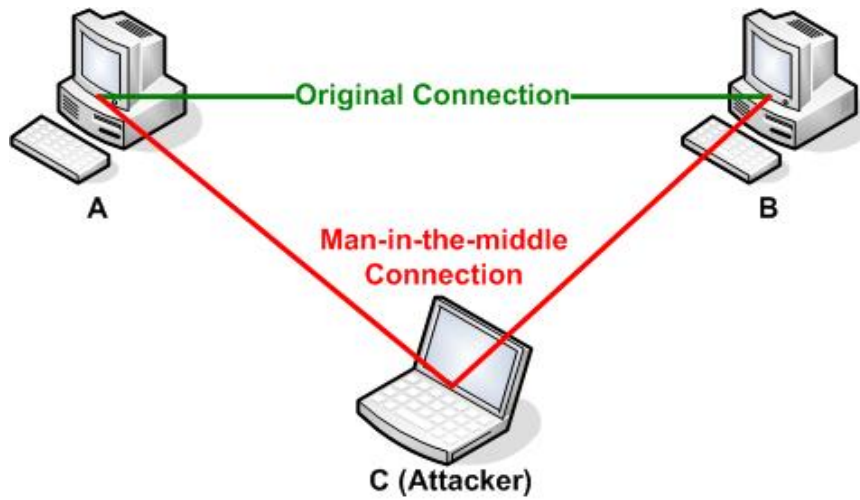


Figure 2.10: Man-in-the-middle attack

2.6.2 Security Requirements for WMNs

High level security issues for WMNs are basically identical to security requirements for any other communication system, but we have identified following security requirements for WMNs on the basis of threats discussed in previous section:

- **Availability:** Availability ensures the survivability of network services despite attacks. Availability does not come to mind as a security concern as quickly as do confidentiality and integrity. But the assurance of availability is very much a security issue. Long-term Denial of Service (DoS) attacks can severely hinder a networks ability to continue. In fact, DoS is often a successful tactic of network services warfare. Moreover, the processes required to prevent or mitigate the effects of loss of availability are very much within the realm of security methodology, because the basic concept of availability assures that authorized persons have uninterrupted access to the information in the system at hand. The availability in a WMN can be compromised by following ways.
- **Confidentiality/Privacy:** The concept of confidentiality is the assurance that sensitive data is being accessed and viewed only by those who are authorized to see it. Whether the data contains trade secrets for commercial business, secret classified government information, or private medical or financial records, confidentiality implies that data is protected from breaches from unauthorized persons and the damage that would be done to the organization, person, and

governmental body by such breaches. Though breaches to confidentiality are not as well-publicized as denial-of-service (DoS) attacks (which are primarily aimed at compromising availability), they can have serious implications to a network services competitiveness, a missions success, and/or personal privacy and safety. For confidentiality, authenticity needs to be implemented first. It is pointless to attempt to protect the secrecy of a communication without first ensuring that one is talking to the right principal.

- **Integrity:** The concept of integrity ensures that the contents of data or correspondences are preserved intact through the transfer from sender to receiver. Integrity embodies the guarantee that a message sent is the message received, that is, it was not altered either intentionally or unintentionally during transmission. Attack on Integrity is usually done in two ways: by the intentional alteration of the data for vandalism or revenge or by the unintentional alteration of the data caused by operator input, computer system, or faulty application errors.
- **Anonymity:** This means that user identity should remain anonymous throughout the network while communicating with other nodes.
- **Authentication:** Authenticity enables a node to ensure the identity of the peer node it is communicating with. Without authenticity, an adversary could masquerade a node, thus gaining unauthorized access to resources and sensitive information and interfering with the operation of other nodes. With the implementation of the concepts such as ubiquitous system, the abundance of networking nodes is reasonable. All these nodes should have an authentic communication within the network. The usual authentication mechanisms involve a centralized system which administers restriction on the basis of access list or capability certificates.
- **Authorization:** It ensures that whether specific user is authorized to do specific task or not.
- **Availability:** It ensures that the desired network services are available to authorized users in case of denial of service attack.
- **Accounting:** It ensures the measurement process for resources used by the user for billing information.

2.7 Existing Secure Routing Protocols

To address security concerns, several secure routing protocols have been proposed: Secure Efficient Distance Vector Routing (SEAD) [36], Ariadne [38], Authenticated Routing for Ad hoc Networks (ARAN) [26], Secure Ad hoc On-Demand Distance Vector Routing (SAODV) [74], Security Aware Routing (SAR) [62]. We have discussed ARAN, SAODV and SAR protocols in detail because these are also based on AODV protocol same like proposed protocol presented in chapter 4.

2.7.1 ARAN

Authenticated Routing for Ad hoc Networks (ARAN) routing protocol is based on Cryptographic Certificates and relies on a central trusted Certification Server (T). Every node entering into the network has to get a certificate signed by T. The certificate contains the IP address of the node, its public key, and time stamp when the certificate was issued and when it will expires.

ARAN protocol in its route discovery sends a Route Discovery Packet (RDP) to its neighbour nodes. RDP includes destination IP (d), Source certificate $Cert(s)$, nonce $N(s)$ which is a time stamp for the packet life and the current time ' t '. And the whole packet is signed by source's private key $K(s)$. $[RDP; IP(d); Cert(s); N(s), t]K(s)$. The IP address of source is contained in its certificate $Cert(s)$. Upon receiving the RDP the neighbor node check the authenticity of the RDP by checking its certificate. If $IP(d)$ matches with it own IP it replies with a REP packet to the source. If not, let ' m ' be the mediating node then it sends the RDP to its next neighbors by signing it with its private key.

$$[[RDP; IP(d); Cert(s); N(s), t]K(s)]K(m); Cert(m).$$

Let ' n ' be the next neighbour node to ' m ' the broadcast Request will look as follows:

$$[[RDP; IP(d); Cert(s); N(s), t]K(s)]K(n); Cert(n)$$

In this process ' n ' after verifying the certificate of ' m ' before sending RREQ it removes ' m 's signature and certificate. The Destination node up on receiving the RREQ it responds with a RREP containing a reverse path derived from the RREQ. The flow will be as follows.

$$[REP; IP(s); Cert(s); N(s), t]K(d)$$

$$[[REP; IP(s); Cert(s); N(s), t]K(d)]K(n); Cert(n)$$

$$[[REP; IP(s); Cert(s); N(s), t]K(d)]K(m); Cert(m)$$

2.7.2 SAODV

Secure Ad Hoc On Demand Distance Vector protocol in its implementation assumes that there is already a central key management system through which every node can obtain public keys. Digital signatures are used to authenticate the fields of the message and hash chains to secure the hop count information. SAODV uses hash chains to authenticate RREQ and RREP flows between neighbor nodes in the route discovery process. A hash chain is formed with a one-way hash function and random seed. Every time a node originates a RREQ or a RREP message, the maximum hop count field is set to the max time to live. The top hash value is calculated using the hash function 'h and the random seed to it. Every time RREQ or RREP are received by a node it verifies the hop count, $[h(\text{max hop}) - \text{hop count time}]$ to check it with the value contained in the top hash value. The intermediate node, after the verification of its integrity and authentication, prepares a RREQ or RREP if it's the destination node. The node applies the hash function to the hash value in the signature extension to account for the new hop. The hash function field indicates which hash function has to be used to compute the hash. When a node first receives a RREQ, it first verifies the signature before creating or updating a reverse route to that host. When the RREQ reaches the destination node, RREP will be sent with a RREP signature extension. When a node receives a RREP, it first verifies the signature before creating or updating a route to that host. Only if the signature is verified, it will store the route with the signature of the RREP and the lifetime.

2.7.3 SAR

SAR is also incorporated security mechanism over AODV. SAR uses security as on of the Key Metrics in its route discovery and maintenance. The framework and attributes of the security metrics use different levels of security for different level of applications. Each node in the network is associated with a level of trust metric, based on which route will be followed according the security requirements of the application. Let us consider the example shown in Figure 2.11.

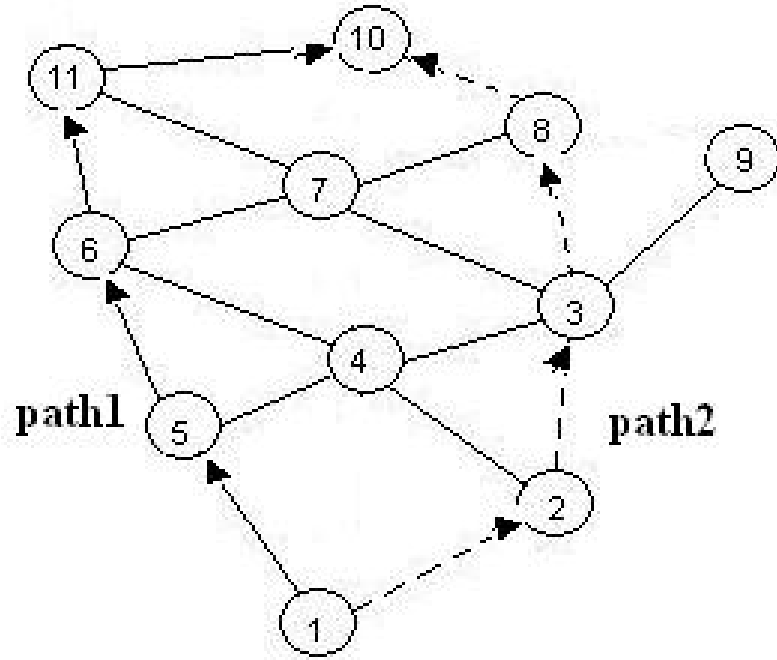


Figure 2.11: Security Aware Routing Protocol

Let us consider that node1 in the network wants to find a route to the node 10. There are two possible ways in the network to establish a route between node 1 and node 10.

Path1: 1-5-6-11-10 and Path2: 1-2-3-8-10.

In the network let us assume that the security metrics of the nodes 2,3 and 8 are less than 5,6 and 11 and they are part of a private network. So based on the security metrics, the SAR protocol chooses the path: 1-5-6-11-10 for routing between node 1 and node 10.

SAR is implemented on the working principle of AODV. In AODV, as earlier explained, in the path discovery phase the source node floods the network with Route Request packet (RREQ). When implemented with SAR, a certain level of security is incorporated into the packet forwarding mechanism. Each packet is associated with a security level and each intermediate node also associated with a security level. Each node can process the RREQ only if they meet the security level of RREQ or higher.

Each of the nodes with a common security level share a common key them. Hence a hierarchical level of security can be maintained. SAR is a trust based security framework. It can be implemented in any basic Ad hoc routing protocol. AODV is widely implemented in current day Ad hoc applications. SAR is mainly implemented over AODV.

2.8 Evaluation of Existing Secure Routing Protocols

In this section, we have presented the evaluation of existing secure routing protocols, implemented over AODV. This evaluation is carried out on the basis of security requirements.

2.8.1 ARAN

ARAN uses public key cryptography and a central certification authority server for node authentication and neighbour node authentication in route discovery.

Denial-of-service attacks are possible with compromised nodes. Malicious nodes cannot initiate an attack due to the neighbor node authentication through certificates. Participating nodes broadcast unnecessary route requests across the network. An attacker can cause congestion in the network, there by compromising the functionality of the network.

Spoofing attacks are prevented by ARAN through node level signatures. Each packet in the network is signed by its private key before broadcasted to the next level and checked for the authentication. So spoofing the identity of node is hampered by ARAN.

Due to the strong cryptographic features of ARAN, malicious nodes cannot participate in any type of attack patterns. Only compromised nodes can participate in any attack pattern.

Tunneling attacks are possible in ARAN. Two compromised neighbor nodes can collaborate to falsely represent the length of available paths by encapsulating and tunneling the routing message between them. Wormhole attack is also possible through two compromised nodes. Table overflow, blackhole attacks are impossible due to node level authentication with signatures.

2.8.2 SAODV

SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts.

Tunneling attacks are possible through two compromised nodes. Warmhole attacks are always possible with compromised nodes in any ad hoc network topology. The use of sequence numbers could prevent most of the possible reply attacks.

2.8.3 SAR

SAR was developed using a trust-based framework. Each node in the network is assigned with a trust level. So the attacks on this framework can be analyzed based on trust level and message integrity. As show below the author [Seung, Prasad, Robin] evaluated the security of SAR in terms of trust level and message integrity.

Trust Level: SAR routing mechanism is based on the behavior associated with the trust level of a user. It is a binding between the identity of the user and the associated trust level. To follow the trust-based hierarchy, cryptographic techniques like: encryption, public key certificates and shared secrets are employed.

Message integrity: The compromised nodes can utilize the information flow in between nodes and reading of packets to launch attacks. It results in corruption of information, confidentiality of the information, and in denial of network services.

2.9 Summary

Wireless mesh networks have been extensively studied in the literature since its evolution. Due to development of wireless equipment and advancements in wireless communication during the last decade, WMNs attracted various commercial and defense applications. Nevertheless, it also increased the responsibility of researchers to provide efficient solutions for the implantation of WMN applications.

Because of highly dynamic nature, shared open medium and infrastructureless network, the major issues in implementation of WMNs are routing (how to find peer nodes and establish links) and security. A lot of routing protocols have been proposed since the inception of WMNs. Among these proposals, AODV and DSR stand out above the rest, becoming the two most popular targets of the research community, as well as any adversaries. Attacks disrupt the normal routing process

by taking advantage of the unsecured communication channel, which presents great threats in the popularisation of WMNs.

The important point is to identify the security problems/threats because without the knowledge of problems/threats, it is impossible to rectify the problems. However, after detailed study of WMNs, we are now able to identify the basic security requirements for WMNs, including: availability, authentication, anonymity, data confidentiality, message integrity and non-repudiation.

In this thesis, we will propose secure routing protocols which cover these security issues for WMNs.

Chapter 3

Cryptography Basics

3.1 Introduction

With the advancement in network (wired/wireless) technologies and Internet, our world become a global village in the terms of communication. However, while using the Internet, along with the convenience and speed of access to information come new risks. Among them are the risks that valuable information will be lost, stolen, corrupted, or misused and that the computer systems will be corrupted. If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home, and may not even be in the same country. They can steal or tamper with information without touching a piece of paper or a photocopier. They can create new electronic files, run their own programs, and even hide all evidence of their unauthorised activity.

The basic security concepts important to information/users on the Internet are confidentiality, authentication, authorization, integrity, availability, and nonrepudiation. To implement these security concepts for the users on the Internet, cryptology is very important like encryption provides confidentiality of messages, digital signatures provide authentication, authorization and integrity of messages as well as users.

In this Chapter, we discuss cryptography primitives that will be used throughout this thesis that include symmetric and asymmetric keys cryptography, Diffie-Hellman key exchange protocol, digital signatures, Nyberg-Rueppel digital signature scheme, blind signatures and blind Nyberg-Rueppel digital signature scheme.

3.2 Cryptography

Cryptography is the science of encrypting and decrypting information. In a typical situation where cryptography is used, two parties (X and Y) communicate over an insecure channel. X and Y want to ensure that their communication remains incomprehensible by anyone who might be listening. Furthermore, because X and Y are in remote locations, X must be sure that the information he receives from Y has not been modified by anyone during transmission. In addition, he must be sure that the information really does originate from Y and not someone impersonating Y. Cryptography is used to achieve the following goals [67]:

- **Confidentiality.** Confidentiality used to ensure data privacy and is usually achieved using encryption. Symmetric encryption algorithms use the same key for encryption and decryption, while asymmetric algorithms use a public/private key pair.
- **Data Integrity.** Integrity is usually provided by message authentication codes or hashes. Hash values are used to verify the integrity of data sent through insecure channels. The hash value of received data is compared to the hash value of the data as it was sent to determine whether the data is altered or not.
- **Authentication.** To assure that data originates from a particular party. Digital certificates are used to provide authentication. Digital signatures are usually applied to hash values as these are significantly smaller than the source data that they represent.

There are two main types of cryptography, which are:

1. Secret or Symmetric Key Cryptography
2. Public or Asymmetric Key Cryptography

3.2.1 Secret or Symmetric Key Cryptography

In secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 3.1, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is

used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

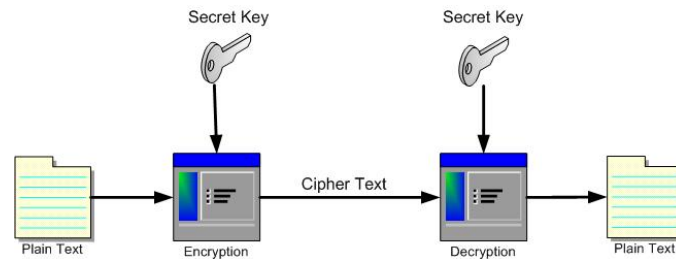


Figure 3.1: Secret or Symmetric Key Cryptography

3.2.2 Public or Asymmetric Key Cryptography

Public or asymmetric key cryptography involves the use of key pairs which includes private key and public key. Both keys are required to encrypt and decrypt a message. The private key means secret key only known by the owner, not to be confused with the key used in private key cryptography. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised.

On the other hand, the public key is public and known by everyone in the network. Public key cryptography intends for public keys to be accessible to all users and its owner's responsibility to distribute its correct public key among the users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement. Figure 3.2 describes the Public Key Cryptography.

As shown in Figure 3.2, sender encrypts the message with the public key of receiver and then forwards that encrypted message to the receiver over the network. Now on receiving that encrypted data, only receiver can decrypt it with the help of its corresponding secret key. No other user can decrypt that message, until, unless, has the knowledge about the secret key receiver.

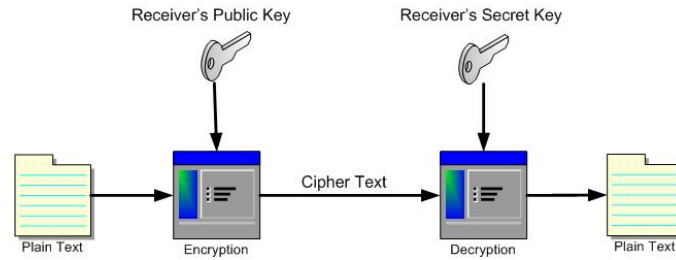


Figure 3.2: Public or Asymmetric Key Cryptography

3.3 Diffie-Hellman Key Exchange Protocol

Prevention of data from the unauthorised extraction during the communication process over an insecure channel is known as data privacy [28]. In order to ensure data privacy, cryptography is used. However, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as a private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

The other way is to exchange secret keys over the public network in a secure manner without compromising the security of the system. Diffie along with Hellman is one of the discoverers of the public-key encryption system which provided a mechanism to exchange secret keys over the insecure network [28, 27]. In public key cryptosystem enciphering and deciphering are governed by distinct keys, E and D , such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key can thus be publicly disclosed without compromising the deciphering key D . Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver is able to decipher it. As such, a public key cryptosystem is multiple access cipher. A private conversation can therefore be held between any two individuals regardless of whether they have ever communicated before. Each one sends messages to the other enciphered in the receiver public enciphering key and deciphers the messages

he receives using his own secret deciphering key.

Diffie-Hellman algorithm is used to enable two users to exchange a shared key securely over the network, which can be further use for encryption/decryption of messages between them. This algorithm is limited to the secure exchange of secret keys.

3.3.1 Algorithm

The effectiveness of Diffie-Hellman algorithm depends upon the difficulty of computing discrete logarithms [70]. Diffie-Hellman algorithm is shown in detail in table 3.1.

Global Public Elements	
q	prime number
α	$\alpha < q$ and α is a primitive root of q
User A Key Generation	
Select X_A	$X_A < q$
Calculate Y_A	$Y_A = \alpha^{X_A} \pmod{q}$
User B Key Generation	
Select X_B	$X_B < q$
Calculate Y_B	$Y_B = \alpha^{X_B} \pmod{q}$
Calculation of Secret Key by User A	
$K = (Y_B)^{X_A} \pmod{q}$	
Calculation of Secret Key by User B	
$K = (Y_A)^{X_B} \pmod{q}$	

Table 3.1: Diffie-Hellman Key Exchange Algorithm

In this algorithm, there are two global elements: a prime number q and an integer α that is a primitive root of q . Now suppose two users A and B wish to exchange a shared secret key over the network. User A first selects $X_A < q$ and computes $Y_A = \alpha^{X_A} \pmod{q}$. X_A and Y_A are private and public keys of user A. In similar way, user B independently selects a random number $X_B < q$ and computes $Y_B = \alpha^{X_B} \pmod{q}$. Now X_B and Y_B are private and public keys of user B.

Each user keeps the private key (X) private from other users and makes the public key (Y) public to other users. User A computes the shared secret key as $K = (Y_B)^{X_A} \pmod{q}$, whereas, user B computes the shared secret key as $K = (Y_A)^{X_B} \pmod{q}$. These two calculations produce identical results:

$$\begin{aligned}
K &= (Y_B)^{X_A} \pmod{q} \\
K &= (\alpha^{X_B} \pmod{q})^{X_A} \pmod{q} \\
K &= (\alpha^{X_B})^{X_A} \pmod{q} \\
&\text{by the rules of modular arithmetic} \\
K &= \alpha^{X_B X_A} \pmod{q} \\
K &= (\alpha^{X_A})^{X_B} \pmod{q} \\
K &= (\alpha^{X_A} \pmod{q})^{X_B} \pmod{q} \\
K &= (Y_A)^{X_B} \pmod{q}
\end{aligned}$$

In the result of this protocol, two users have exchanged a secret shared key over the network securely. Moreover, X_A and X_B are private to corresponding users. An adversary has no information about these private keys of users, whereas, adversary can has only knowledge of q , α , Y_A and Y_B . Thus, the adversary is forced to take a discrete logarithm to determine the key.

3.4 Digital Signatures

Authentication of a documents or data messages shared between users over the network is very important because of security risks. Authentication is also required in handwritten documents and signatures are being used for that purpose. A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The digital signature guarantees the source and integrity of the message over the network [70].

3.4.1 General Scheme

Assume that there are two users: Alice (A) and Bob (B). Each of them holds a public and secret key pair. (PK_A, SK_A) and (PK_B, SK_B) are the public and secret keys of Alice and Bob respectively. To sign a message m , Alice launches the signing algorithm Sign along with her secret key SK_A to generate a signature S over the message. Alice then publishes the signature as well as her public key PK_A . When Bob receives the signature and Alice's public key, he will be able to verify if the signature is generated by Alice using the verification algorithm Verify. If the

signature is authentic, Alice's public key will make the verification equation hold. Figure 3.3 shows the detailed procedure of digital signature.

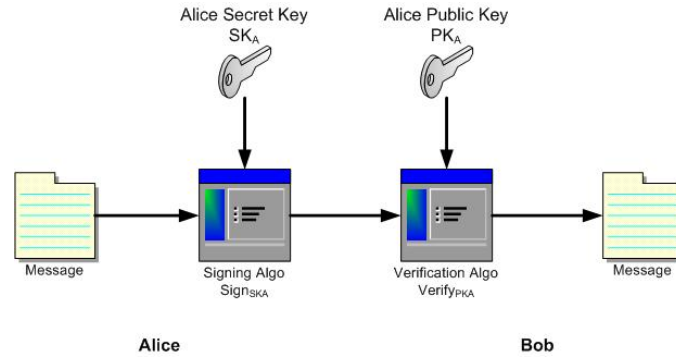


Figure 3.3: General Digital Signature Scheme

In 1988, digital signature scheme was presented in [34] and components of digital signature scheme are defined as:

- A security parameter K , which is chosen by the user when he creates his public and secret keys. This parameter determines a number of quantities, such as the length of signatures, length of signable messages, running time of the signing algorithm, overall security, etc.
- A message space M which is the set of messages to which the signature algorithm may be applied. The messages can be regarded as binary strings, i.e. $M \subseteq 0,1^+$. The length of messages to be signed is bounded by k^c for some constant $c > 0$.
- A signature bound B which is an integer bounding the total number of signatures that can be produced with an instance of the signature scheme. This value is typically bounded above by a low-degree polynomial in k , but may be infinite.
- A key generation algorithm G which on input 1^k (i.e. k in unary) by any user A , generates a pair (PK_A, SK_A) of matching public and secret keys in polynomial time.
- A signature algorithm σ which produces a signature $\sigma(M, S_A)$ for a message M using the secret key S_A .

- A verification algorithm V which tests whether S is a valid signature for message M using the public key P_A .

In a nutshell, we can say that key generation and signing algorithms are probabilistic, whereas verification algorithm is deterministic in case of digital signatures.

3.4.2 Security Requirements for Digital Signature Schemes

According to [34], the concept of security for a digital signature scheme is called existential unforgeability under a chosen message attack (EF-CMA). Assume the existence of a polynomial time adversary A and a challenger, who cooperate to perform the following game:

1. The challenger runs the key generation algorithm to generate the public-private key pair (PK, SK) . It sends PK to the adversary and keeps SK as secret.
2. The adversary A produces a message m under PK and submits it to the challenger. The challenger responds the query with a signature $\sigma = \text{Sign}(m, SK)$. A can request at most q_S messages of his choice under PK , where $m_1, \dots, m_{q_S} \in 0, 1^*$.
3. Eventually, A produces a pair (m^*, σ^*) . The adversary wins if σ^* is a valid signature of m^* according to the verification algorithm, and m^* is not queried during the signature query phase.

Definition: An adversary $A(t, q_S, \epsilon)$ breaks a signature scheme, if A runs in time at most t , makes at most q_S signature queries, and the advantage that A wins the game is at least ϵ . A digital signature scheme is $A(t, q_S, \epsilon)$ -existentially unforgeable under a chosen message attack if no adversary $A(t, q_S, \epsilon)$ breaks it.

$$\text{AdvSig}_A^{\text{EF-CMA}} = \Pr \left[\text{Verify}(pk, m, \sigma) = \text{accept} \mid \begin{array}{l} (PK, SK) \leftarrow G(1^k); \\ \text{for } i = 1, 2, \dots, q_S; \\ m_i \leftarrow A(pk, m_i); \\ \sigma_i \leftarrow \text{Sign}(sk, m_i); \\ (m, \sigma) \leftarrow A(pk, m_i, \sigma_i); \\ m \neq m_1, \dots, m_{q_S}; \end{array} \right] \leq \epsilon$$

Figure 3.4: Verification of Digital Signature

3.5 Nyberg-Rueppel Signature Scheme

In 1993, Nyberg and Rueppel proposed a digital signature scheme in [55] and system parameters involved in this scheme are the same as in some other schemes. The system parameters consist of:

- a prime p
- a prime factor q of $p - 1$
- an element $g \in Z_p^*$ of order q
- Signer's private key is a random element $x \in Z_q$
- Signer's public key is $y = g^x \pmod{p}$

To sign a message $m \in Z_p$, the signer selects $k \in Z_q$ at random and computes r and s as follows:

- $r = mg^k \pmod{p}$
- $s = xr + k \pmod{q}$

The pair (r, s) is the signature of the message m . To verify the validity of a signature, one checks that the following equality holds:

- $m = g^{-s}y^r \pmod{p}$

As this scheme provides message recovery, the signature need not to be accompanied by the message m .

3.6 Blind Signatures

A blind signature scheme is a protocol which allows a user to obtain a valid signature for a message 'm' from a signer without knowing the contents of message or its signature. Later on, if signer checks message m and its signature, can verify that the signature is genuine, but signer is unable to link the message-signature pair to the particular instance of the signing protocol which has led to this pair [17].

The concept of a blind signature was introduced by David Chaum in [20]. Blind signature scheme is considered to provide secure electronic payment systems along

with customers' privacy (e.g. [14, 21, 30, 57]) as well as for protecting users' anonymity in different protocol scenarios (e.g. secure voting protocols [68]).

The basic concept behind the blind signature is to hide the identity of user in such a way that signature and message can be verified but user identity should remain anonymous. According to [17], the the blindness for a signature scheme is defined as: Let V denote user's complete view of an execution of the protocol, i.e. his random coin tosses and all exchanged values; and let $(m, \text{sig}(m))$ denote the message-signature pair generated in that particular execution.

Definition: A signature scheme is called blind if user's view V and the message-signature pair $(m, \text{sig}(m))$ are statistically independent.

3.6.1 Functions

Blind signature systems combines the features of true two key digital signature systems with commutative style public key systems in a special way. The main three functions [21] used in building the blind signature cryptosystem are as under:

- A signing function s' known only to the signer and the corresponding publically known inverse s , such that $s(s'(x)) = x$ and s provide no clue about s' .
- A commuting function c and its inverse c' , both known only to the provider, such that $c'(s'(c(x))) = s'(x)$ where, $c(x)$ and s' provide no clue about x .
- A redundancy checking predicate r , that checks for sufficient redundancy to make search for valid signatures impractical.

3.6.2 Protocol

In blind signature protocol, two main parties are involved, one is the "signer" and other is "receiver or user". The user only needs to know the public key, while the signer needs to know both the public and private keys. Steps involved in generation of blind signatures are as under:

1. Firstly user needs to choose x at random such that $r(x)$, then user forms $c(x)$ and sends $c(x)$ to signer.
2. Signer signs received $c(x)$ by applying s' and returns back signed data $s'(c(x))$ to user.

3. After receiving signed data $s'(c(x))$ from signer, user strips it by application c' , yielding $c'(s'(c(x))) = s'(x)$. Now $s'(x)$ is the blind signature for the user.
4. Any other user, who has knowledge about the public key of signer can check and verify the signature $s'(x)$ by applying $r(s(s'(x)))$.

3.6.3 Properties

Following security properties are provided by the blind signature system comprising the functions and protocols discussed in above sections:

1. **Signature verification.** Any user who has knowledge about public key of signer can check and verify that the signature $s'(x)$ was formed using signer's private key and are valid.
2. **Blindness of signature.** It is clearly shown above that signer does not know anything about the correspondence between the elements of the set of stripped signed data $s'(x_i)$ and the elements of the set of unstripped signed data $s'(c(x_i))$.
3. **Conversion of signatures.** User can create at most one stripped signature from signed data for each message signed by signer. (i.e. even with $s'(c(x_1))$... $s'(c(x_n))$ and choice of c , c' and x_i , it is impractical to produce $s'(y)$, such that $r(y)$ and $y \neq x_i$).

3.7 Blinding the Nyberg-Rueppel Digital Signature

In 1994, Camenisch, Piveteau and Stadler proposed blind Nyberg-Rueppel digital signature scheme in [17] and to obtain a blind Nyberg-Rueppel digital signature on a message m from the signer, the verifier needs to get a pair (r, s) in the form:

- $r = mg^k \pmod{p}$
- $s = xr + k \pmod{q}$

But the important thing is that signer does not learn anything about either r or s . To achieve this, following process can be used:

1. The signer selects $\tilde{k} \in Z_q$, computes $\tilde{r} = g^{\tilde{k}} \pmod{p}$, and sends \tilde{r} to the verifier.
2. The verifier selects $\alpha, \beta \in Z_q$, computes $r = mg^{\alpha\tilde{r}\beta} \pmod{p}$, $\tilde{m} = r\beta^{-1}$ and sends \tilde{m} to the signer.
3. Then signer computes $\tilde{s} = \tilde{m}x + \tilde{k}$ and forwards \tilde{s} to the verifier.
4. The verifier computes $s = \tilde{s}\beta + \alpha \pmod{q}$.

The pair (r, s) is then a blind signature of the signer on message m . The validity of the signature (r, s) for message m is done by verifying

$$g^{-s}y^r r = mg^{-\tilde{s}\beta + xr + \tilde{k}\beta + \alpha} = mg^{-\tilde{m}x\beta - \tilde{k}\beta + xr + \tilde{k}\beta} = m \pmod{p}$$

Furthermore, as α and β are randomly chosen, the signer does not learn anything about (r, s) . For a given signature (r, s) , there exists an unique pair of α and β . Thus for each signature from the signer, the verifier can generate only one blind signature.

3.8 Summary

Cryptography plays very important role in today's world of networking either its wired or wireless. Security is the main concern in today's networking especially in wireless because of open wireless medium and dynamic nature of network. Cryptography is being used to provide security features in the field of networking.

In this thesis, we have discussed cryptography in detail including public, secret keys cryptography, different types of digital signature schemes. Encryption and decryption are used to provide data confidentiality/privacy and data integrity, whereas digital signatures are used to provide authentication, anonymity in terms of users and data as well.

Different type of digital signature provide different levels of security as discussed in literature and it also depends upon the key length used to generate signatures. But in the case of wireless networks, larger key sizes are not recommended because of memory, computation cost and power limitations. Therefore, key size and cryptography algorithms selection should be done very intelligently so that network performance can be enhanced along with providing sufficient security.

We have used cryptography to provide security in our proposed protocols. We used PKI and shared secret keys to implement data confidentiality, whereas, used digital signature and certificates to provide authentication over the network. To implement user anonymity in WMNs, we have used blind signature scheme along with Nyberg-Rueppel digital signature.

Chapter 4

Ticket based Ad-Hoc On Demand Distance Vector Protocol

4.1 Introduction

In this chapter, we address security issues related to data exchange, routing and MAC layer (ARP in LAN based WMNs). We propose a cross-layer secure protocol that cover secure routing, authentication, integrity, exchange of public keys and ARP in one single step. This would facilitate the users to exchange parameters during the routing session and these parameters would subsequently be used to ensure confidentiality and integrity of data exchange. With the help of our proposed protocol, network traffic can be reduced because there is no need to broadcast ARP request for finding the MAC address of destination, since the MAC address is already part of ticket which is received by source during the routing discovery process and this ticket is also trusted because it is signed by AS.

All the routing algorithms available for WMNs work on the basis of IP addresses and routing tables contain IP addresses of hosts [65]. For instance in Layer 3, for obtaining the address of the destination, the node first looks up the routing table for the destination and next hop IP addresses. Then, the node sends an ARP ([45], [72]) request to get the MAC address for the destination and then once it has the MAC address it sends the frame to the next hop which follows the same procedure again. Therefore, in general, ARP is employed to achieve the corresponding MAC address of the target IP address. If the destination's IP address belongs to the same subnet of a source node, an ARP request initiated by the source node will be disseminated within the entire subnet. After receiving the request, the destination sends back an ARP reply to the source node with its own MAC address, and hence the source can know the destination's MAC address. The IEEE 802.11s [18] group's current proposal does not mention anything about the ARP mechanism. This is because

ARP runs in the upper layer of the 802 standard and hence they have not covered it in their draft [45].

However, it is important to note that, in the IEEE 802.11s [18] based mesh networks, ARP requests will be broadcasted within the entire WDS (Wireless Distribution System) according to the basic ARP mechanism similar to other wired LAN networks, resulting in the well-known broadcast storm problem [54]. In wireless networks, the broadcast storm caused by flooding consumes a lot of network bandwidth and significantly degrades the network performance. We believe that ARP requests will be repeatedly issued unless the destination MAC address is known, thus it might occur the broadcast storm and reduce the network performance. Moreover, in such a WLAN based mesh networks, ARP reply packets against the ARP request need to be delivered to the source in a multi-hop fashion. If a path to the source is unknown, this will require the destination node to issue an on-demand route request packet (RREQ) that would be flooded again to the whole network in the worst case. We have also rectified this problem in our solution, which is discussed in proposed solution section.

4.2 Protocol Design

Our proposed ticket-based security protocol for WMNs that is based upon the AODV [59] protocol. Our proposed protocol Ticket based AODV (TADOV) [63] is a cross layer protocol which works at network layer but it also provides security for data exchange and avoid transfer of ARP messages for finding MAC addresses of source and destination. Our proposed protocol can be used for different WMNs applications which require secure communication as discussed in Chapter 2.

In our protocol, there are four main participating entities i) Certification Authority, ii) Authentication Server, iii) Mesh Routers and iv) Mesh Client. Each entity is responsible for different functions which are as under:

- **Certification Authority (CA):** Certification authority is responsible for issuing of certificates to interested clients/users after getting required information which includes user details, MAC Address of client (MAP/MC), Public key of client (MAP/MC). These certificates are digitally signed by CA and used by clients/users to get ticket from AS. All the entities have trust on CA and can validate CA's signature. All this process is an offline process and CA is not

actively participating in the network.

- **Authentication Server (AS):** Authentication Server is responsible for assigning IP addresses to clients, issuing tickets to clients. Issuance of tickets by AS depends upon the successful verification of certificate provided by mesh client.
- **Mesh Routers/Mesh Access Point (MAP):** MRs/MAPs are under administrative control of AS and responsible to provide network service to specific area. An AS which has multiple domains has multiple MAP, one per domain. A MAP that provides Internet connectivity to mesh clients is called mesh gateway router. These MRs/MAPs are responsible to provide communication throughout the network.
- **Mesh Client (MC):** MCs are the main users of the network. They want to participate in the routing or want to have wireless Internet connectivity through MAP.

Figure 4.1 below depicts the scenario considered for our protocol, where MCs, MAPs and AS are available.

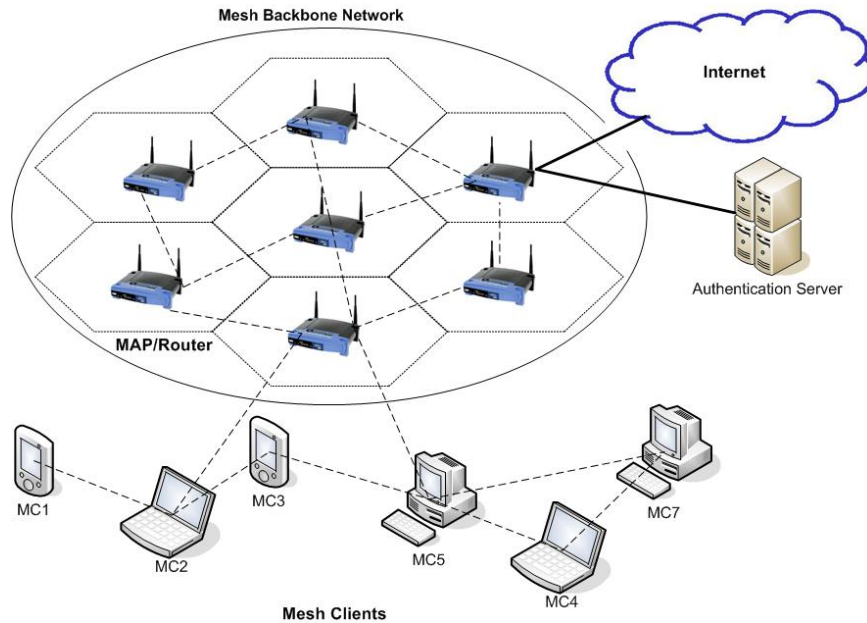


Figure 4.1: Wireless Mesh Network with Authentication Server

4.2.1 Notations

Notations used in our protocol are as under:

- AS : Authentication Server
- CA : Certification Authority
- MAP : Mesh Access Point
- MC : Mesh Client
- K_{ASM} : Shared secret key between AS and MAP
- K_{ASMC} : Shared secret key between AS and MC
- K_{MM} : Shared secret key between MAP and MAP
- K_{MMC} : Shared secret key between MAP and Mesh Client
- Cert : MAP/Client Certificate
- $Ticket_M$: MAP's Ticket
- $Ticket_{MC}$: MC's Ticket
- $PK_{M/C}$: Public Key of MAP/Client
- PK_{AS} : Public Key of AS
- SK_{MC} : Secret/Private Key of MC
- $()SK_{MC}$: Message digitally signed by MC
- $[Data]K_{MCMC}$: Encrypted data with shared key between two MCs

4.2.2 Setup

We assume that there is a trusted CA which is responsible for issuing certificates to new users (Mesh Access Points/Mesh Clients). Steps involved in issuance of certificate to new clients from CA are as under:

1. $NewMC \rightarrow CA : RequestMessage$
2. $CA \rightarrow NewMC : PK_{AS}, instructions$

3. $NewMC \rightarrow CA : PK_{MC}, UserInformation$

4. $CA \rightarrow NewMC : Cert_{MC}$

In step 1, New MAP/Client sends request message for joining the WMN.

In reply, CA sends public key of AS and necessary instructions including information about cryptography group, how to generate public/private keys and shared key generation mechanism, as shown in step 2 above.

After generation of public/private keys, new MC forwards its public key (PK_{MC}) and other information including user name/ID, its MAC address to CA, as shown in step 3.

After getting information from new MC, CA generates a certificate including all the required information and digitally sign it with its private key. Then forwards that certificate to new MAP/client.

It is assumed that a trust relationship exists between CA and AS (Authentication Server) available in the WMN. All this process is offline processes to be happened before joining the actual network. The structure of the certificate issued by CA is as under:

Type (0 for Client / 1 for MAP)
MAC Address
PK_{AS}
$PK_{M/C}$
Issue Time
Expiration Time
Signature (CA)

Table 4.1: Certificate

4.2.3 Proposed Run

In our protocol, AS is very important entity because it is responsible for initial authentication on the basis of certificate provided by new client (MC/MAP). After successful verification, AS creates ticket for new client and also assigns IP address to new client. Then AS forwards that ticket to new client wishes to join WMN.

According to the entities involved in the network, two different scenarios need to be considered:

1. When new MAP joins network
2. When new MC joins network

We have discussed each of the above scenario in detail in later sections because there are different requirements in both the scenarios.

4.2.4 In Case of New MAP

In this section, we have discussed the mechanism of new MAP. Whenever a new MAP wants to join an existing WMN, it needs to send its certificate issued by CA to AS. After getting the certificate of a new MAP, AS first needs to verify it with the help of public key of CA and after successful verification of certificate, AS issues a ticket to it. Steps involved in this process are as under:

1. $NewMAP \rightarrow AS : Cert_M$

Where $Cert_M = (Type, MAC, PK_{AS}, PK_M, IssueTime, ExpirationTime)SK_{CA}$

2. $AS \rightarrow NewMAP : [Ticket_M] K_{ASM}$

In step 1, new MAP forwards its certificate issued and signed by CA to AS.

After successful verification of certificate, AS generates shared secret key for new MAP and AS (K_{ASM}) on the basis of public key of MAP and its secret key by using Fixed Diffie-Hellman key exchange protocol. Then, AS assigns IP address to new MAP and generates a ticket for new MAP with required info (MAP ID, IP and MAC address, PK, issue time, expiration time etc.) and signs it with its private key. Then, after signing, AS encrypts that ticket with the shared secret key and then forwards this encrypted ticket to new MAP as shown in step 2.

MAP ID
MAC Address
IP Address
PK
Issue Time
Expiration Time
Signature (AS)

Table 4.2: Ticket

After receiving an encrypted ticket, new MAP first generates a shared secret key on the basis of AS's public key and its secret key (as AS generated) and then decrypts the ticket. For future communication (route discovery request/reply) MAP uses this ticket.

4.2.5 In Case of New MC

Whenever a new MC wants to join existing WMN, it just needs to send its certificate to nearby MAP. Then, that MAP forwards that certificate along with its ticket to AS. After receiving data from MAP, AS first verifies the certificate with the public key of CA.

On successful verification, AS generates a shared secret key for new MC and AS on the basis of public key of MC and its secret key by using Fixed Diffie-Hellman key exchange protocol. AS also assigns IP address to new MC and generates ticket for it. AS then sends back this ticket after encrypting it with shared key between AS and new MC through corresponding MAP. Steps involved in this process are as under:

1. $NewMC \rightarrow MAP : Cert_C$

Where $Cert_C = (Type, MAC, PK_{AS}, PK_{MC}, IssueTime, ExpirationTime)SK_{CA}$

2. $MAP \rightarrow AS : [Cert_C] K_{ASM}, Ticket_M$

3. $AS \rightarrow MAP : [Ticket_{MC}] K_{ASMC}$

where $Ticket_{MC} : (ID, MAC, IP, PK_{MC}, IssueTime, ExpirationTime)SK_{AS}$

4. $MAP \rightarrow NewMC : [Ticket_{MC}] K_{ASMC}, Ticket_M$

As shown above in step 1, new MC forwards its certificate to nearby MAP.

Then, MAP forwards client's certificate for verification to AS after encrypting it with the shared secret key between MAP and AS (K_{ASM}) along with its ticket as shown in step 2.

AS first verifies the MAP's ticket and then decrypts the data with the shared secret key between AS and MAP (K_{ASM}). Then AS verifies the certificate of MC and on successful verification, AS generates a shared secret key for new MC (on the basis of new MC's public key and its secret key by using Fixed Diffie-Hellman key exchange protocol) and ticket for new MC.

DHCP [29] is also running on AS, therefore AS also assigns IP address to new MC and then forwards to sender (MAP) after encryption using shared secret key between AS and new MC as mentioned in step 3.

In step 4, MAP then forwards this encrypted ticket to new MC along with its ticket for authentication. After receiving encrypted ticket, client first verifies the ticket of MAP with the help of public key of AS. On successful verification, client first generates a shared secret key (as AS generated) using its secret and public key of AS. Then decrypts its ticket which is used by MC for future communication (route request/reply).

The first phase of our protocol is completed by getting ticket and establishment of shared secret keys between AS and MC. The second phase is the secure communication including routing and data transfer between different clients with the help of MAPs, which is discussed in detail in next section.

4.2.6 Communication Between Different MCs

Communication among different clients is dependent on the routing, means selection of the best path for transfer of data from one client to other client over the network. Routing information is stored in routing tables and is routing protocols are used to establish/find new routes between the clients. If a MC (source) wants to send data to any other MC (destination) in the network and source doesn't has route entry in its routing table for destination, so in that case source needs to first find route between them.

We use the AODV protocol for route discovery with slight changes like the first thing is RREQ message is digitally signed (same like ARAN [26] and SAODV [74]) by the source and only destination can send back reply message after verification of signature whereas the intermediate nodes only verify signature. On successful verification, intermediate nodes create or update reverse route to the source and then forward that request to next node after attaching their tickets.

For the verification process, intermediate nodes and the destination can get public key of source from its ticket attached with that RREQ message. Secondly, with every RREQ and RREP messages, ticket of source (in case of RREQ) and ticket of destination (in case of RREP) must be attached.

To discuss the working of our ticket based protocol, we assumed that MC_1 is

source and MC_5 is destination as shown in Figure 4.2. MC_2 and MC_3 are intermediate nodes.

T_1 is ticket belongs to MC_1 , T_2 belongs to MC_2 and so on.

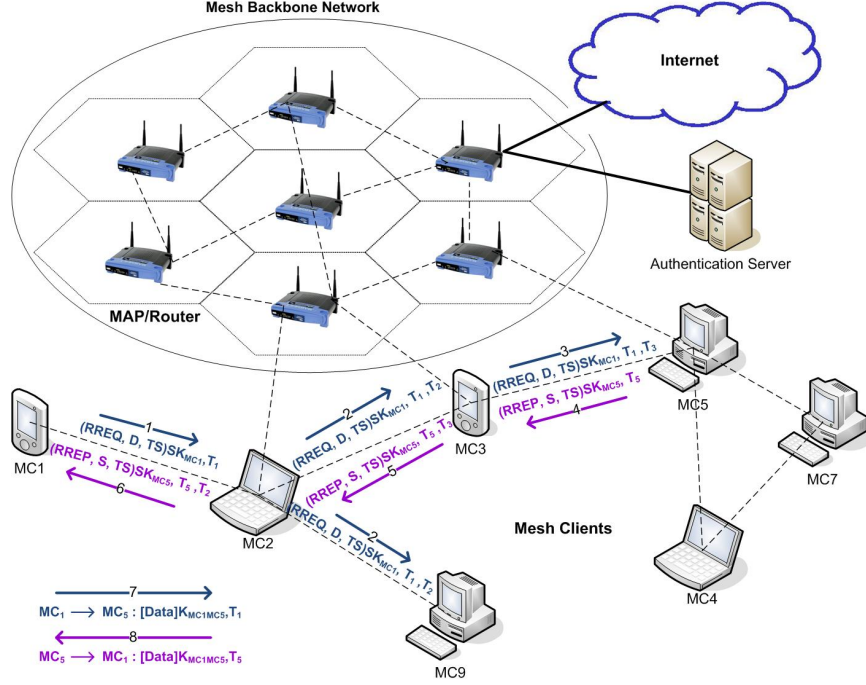


Figure 4.2: Communication Process in Wireless Mesh Network

1. $MC_1 \rightarrow * : (RREQ, D, TS)SK_{MC1}, T_1$
2. $MC_2 \rightarrow * : (RREQ, D, TS)SK_{MC1}, T_1, T_2$
3. $MC_3 \rightarrow * : (RREQ, D, TS)SK_{MC1}, T_1, T_3$
4. $MC_5 \rightarrow MC_3 : (RREP, S, TS)SK_{MC5}, T_5$
5. $MC_3 \rightarrow MC_2 : (RREP, S, TS)SK_{MC5}, T_5, T_3$
6. $MC_2 \rightarrow MC_1 : (RREP, S, TS)SK_{MC5}, T_5, T_2$
7. $MC_1 \rightarrow MC_5 : [Data] K_{MC1MC5}, T_1$
8. $MC_5 \rightarrow MC_1 : [Data] K_{MC1MC5}, T_5$

Therefore, source (MC_1) generates signed RREQ message that includes destination (MC_5) IP address and timestamp (TS) for freshness of message, attaches its ticket and broadcast it for route discovery as shown in step 1.

Intermediate node (MC_2) first verify the ticket attached with RREQ and then verify the actual signed RREQ message with the help of public key of sender from its ticket. On successful verification, it creates or update reverse route to source and then attach its ticket with it and rebroadcast the RREQ packet as shown in step 2, until it reaches the destination.

Another intermediate node (MC_3) receives this request and first verifies the ticket of intermediate node (in this case MC_2) and on successful verification remove ticket of intermediate node and then creates or update reverse route to last node and attaches its ticket with it and rebroadcast the RREQ packet as shown in step 3, until it reaches the destination.

On receipt of RREQ, destination will first verify ticket of last node and then verify the signed RREQ message. After successful verification, destination (MC_5) will get public key of source for generation of a shared secret key for future secure data exchange. Then, destination will forward digitally signed RREP message which includes IP address of source (MC_1) and time stamp (TS) along with its ticket back to last node.

In steps 5 and 6, intermediate nodes (MC_3 and MC_2), after verification of RREP message, they will update their routing table accordingly and then forward that message to source.

Upon receipt of signed RREP message and ticket (T_5) from destination (MC_5), source (MC_1) will get public key of destination and routing information as well. Now, the source will generate shared secret key by using its secret key and public key of destination. Then, the source will decrypt data with that shared secret key to be sent to destination. On receipt of encrypted data, the destination will also generate the shared secret key using its secret key and public key of source and will decrypt the data. Now both source and destination have the shared secret key and for future secure communication, they will use this key (as shown in step 7 and 8 above).

With the help of these tickets used with RREQ and RREP messages, we have secure routing and also in one single step public keys of source and destination have also been exchanged and we also achieved authentication and integrity of routing messages. If a MC (source) wants to send data to any other MC (destination) in

the network and source knows the routing information (route between them) which means that they already have exchanged their tickets and now they can generate shared secret key and can have secure communication.

In this protocol, source and destination need to generate shared secret key for the first time only and as they are using symmetric keys for encryption and decryption so they require less computation as compared to in case of asymmetric keys. In our protocol, if the ticket of source is not verified at any point, then intermediate nodes involved in multi-hop routing just discard that message and will not forward that message to destination. By doing this, network traffic can be reduced by discarding unauthorized messages or clients.

4.2.7 Address Resolution Protocol Security

In our protocol, tickets comprised IP and MAC addresses of a node along with other values. So there is no need to broadcast $ARP_{Request}$ message to find out the MAC address of destination because during route finding process source already got the ticket of destination which includes its MAC address as well. And one thing more, MAC address included in ticket is trustworthy because ticket is signed by AS. So with the implementation of proposed protocol, users will be able to overcome ARP security problems like ARP Poisoning, ARP Spoofing and Man-In-The-Middle attacks, as discussed earlier, because there is no need to broadcast ARP messages for address resolution from IP to MAC address mapping.

4.3 Security Analysis

Our proposed protocol TAODV is a cross-layer protocol, therefore it provides different security measures at different layers at the same time. Our protocol provides following security features in WMNs:

- *Confidentiality/Privacy/Authorization.* With the help of symmetric cryptography based upon shared secret key generated on the basis of PK and SK of sender and receiver, which provides message confidentiality/privacy because only sender and receiver know the shared secret key between them and for every different pair they have different shared secret key.
- *Authentication.* with the help of tickets, sender and receiver can authenticate

each other and also other nodes in the network because tickets are digitally signed by the AS, so no other MC can generate its new ticket for any purposes.

- *Reduced Network Traffic.* Generally, in WMNs, there are different type of broadcast messages involved in communication between users. First broadcast message is to get routing information between source and destination which is generated by source. Exchange of public keys between users in secure WMNs is also network load and require communication between users. Another important broadcast message is the mapping of IP address with concern MAC address. Normally all these messages generate a lot of network traffic which consumes network bandwidth as well as overload network traffic. But proposed protocol (TAODV) reduces network traffic by combining all these broadcast messages in one single message. There is no need of broadcasting separate ARP messages (request/reply) for mapping of IP address to MAC address for actual transfer of data from source to destination because during the route discovery process the source already received destination's ticket which includes its MAC address as well. Therefore, this proposed protocol reduces network traffic.
- *Security against ARP attacks.* As all these tickets are digitally signed by AS and already authenticated so MAC address received from ticket is also authenticated. Therefore, at the end, our WMN will be secured from the broadcast storm problem [6], ARP attacks like MITM, ARP poisoning and spoofing attacks [11].
- *Low Computation Cost.* According to this approach, there is no need to generate shared secret keys in the start or during initialization process. If two nodes want to communicate with each other, then they need to generate shared secret key (for the first time only) after that both can use the same key for the rest of communication. If they do not need to communicate during their entire life time, then they do not need to generate keys. Data encryption is based upon symmetric-key methods, so there is less computation required in case of encryption and decryption. Note that AS does not know the secret keys of any nodes available in WMN, whereas only node itself knows its secret key. For an authentication point of view, nodes only need to verify the signatures of AS and comparison of ticket with sender's MAC/IP address and if they are valid,

then they will accept data or can forward it to some other node otherwise they will just simply discard that messages.

- *Routing Security.* Malicious nodes cannot initiate DoS attacks due to the neighbor node authentication through tickets. Spoofing attacks on routing are also prevented in proposed protocol through node level attachment of ticket and encryption. Due to the strong cryptographic features of proposed protocol (TAODV), malicious nodes cannot participate in any type of attack patterns. Only compromised nodes can participate in any attack pattern.

As discussed in chapter 2, ARAN and SAODV are also implemented on AODV protocol same like in proposed protocol. But in proposed protocol (TAODV) only source needs to sign the RREQ message and attach its ticket and all intermediate nodes need to verify it and after verification they only need to attach its ticket rather than signing it again, which is different from ARAN.

In TAODV, malicious nodes cannot initiate DoS attacks due to the neighbor node authentication with the help of tickets. Spoofing attacks on routing are also prevented in proposed protocol through node level attachment of ticket and encryption. Due to the strong cryptographic features of proposed protocol (TAODV), malicious nodes cannot participate in any type of attack patterns. Only compromised nodes can participate in any attack pattern.

Another important feature is that proposed protocol is a cross-layer security protocol which is concentrating in addressing security concerns related to data exchange, routing and MAC layer (Address Resolution Protocol in LAN based WMNs) at the same time and it accumulate the routing, authentication, integrity, exchange of public keys and ARP in a single step. Therefore, this solution provides facility to the nodes to exchange parameters (public keys, MAC addresses) during the routing session and these parameters would subsequently be used to ensure confidentiality and integrity of data exchange.

4.4 Summary

The security deployment of WMN routing operations has been extensively discussed in the literature. Different secure routing protocols have been proposed on the basis of existing routing protocols like AODV and DSR. But, as mentioned earlier, due to dynamic nature and open wireless medium, a cross-layer protocol is better suitable

for providing secure routing and data transfer. The main reason to support cross-layer protocol is its working nature, because cross-layer protocol carry out different layers' tasks in a single step, as covered in proposed protocol (TAODV). This results in reducing the network traffic and rising the performance of network. Therefore, the existing secure routing protocols are not working properly in the sense of achieving security and efficiency.

In this chapter, we presented a cross-layer protocol which performs different steps at a same time in a single step to reduce network traffic. Our protocol also provides secure routing, data confidentiality/privacy, user authentication, authorization and security against ARP attacks. Steps involved in our protocol are as under:

1. Getting certificate from CA
2. Getting ticket from SA
3. Route definition including generation of shared secret key and exchange of MAC addresses in one single step
4. Secure communication with other users

Our proposed protocol has an advantage over the other protocols because of cross-layer nature by performing route definition process, generation of shared secret keys and exchange of IP/MAC addresses in one single step.

Chapter 5

Achieving User Anonymity in WMNs

5.1 Introduction

Wireless mesh networking is much better and efficient solution to provide wireless Internet connectivity in a sizable geographical area [46], as compared to other solutions. The major problem in using WMNs is to provide security to users. Because of open wireless medium, mesh networks are vulnerable to anonymity, privacy and other security attacks which we discussed in earlier Chapters. In this Chapter, first, we will discuss anonymity and its importance in WMN and then we will propose a protocol to achieve user anonymity in WMNs.

5.1.1 Anonymity and Its Importance

User authentication is very important for the security of communication systems either wired or wireless but at the same time, user anonymity is also important and needs to be implemented. In wired networks, anonymity is not much important as compared to wireless networks because in wired networks, most of the time number of users are fixed and normally network can be monitored easily, whereas, in case of wireless networks, users are not fixed and they are dynamic in nature (users come and join network for some time and leave afterward like in case of WMN providing Internet service). Therefore, providing anonymity in wireless networks is important as users may wish to hide the fact that “who is accessing what” on the Internet from other users and also from gateway routers [69].

In a nutshell, important security requirements for a wireless network are confidentiality over the wireless medium, anonymity of the user and, most importantly, authentication of the user in order to prevent unfair use of the system [76]. In different type of WMNs, security requirements are different, for example, if we are using

WMN to extend Internet service to users in a remote area, security requirements are different as compared to the WMN which is used as extension of enterprise network.

5.1.2 Application Scenario

As we discussed earlier in Chapter 2, WMNs can be used in different application scenarios like extension of Internet services to users in remote areas, enterprise networking, disaster recovery network, network for military operations, etc. Security requirements for these application scenarios may vary from each other. Like as shown in Figure 5.1, an ISP providing Internet services to users in remote areas with the help of WMN.

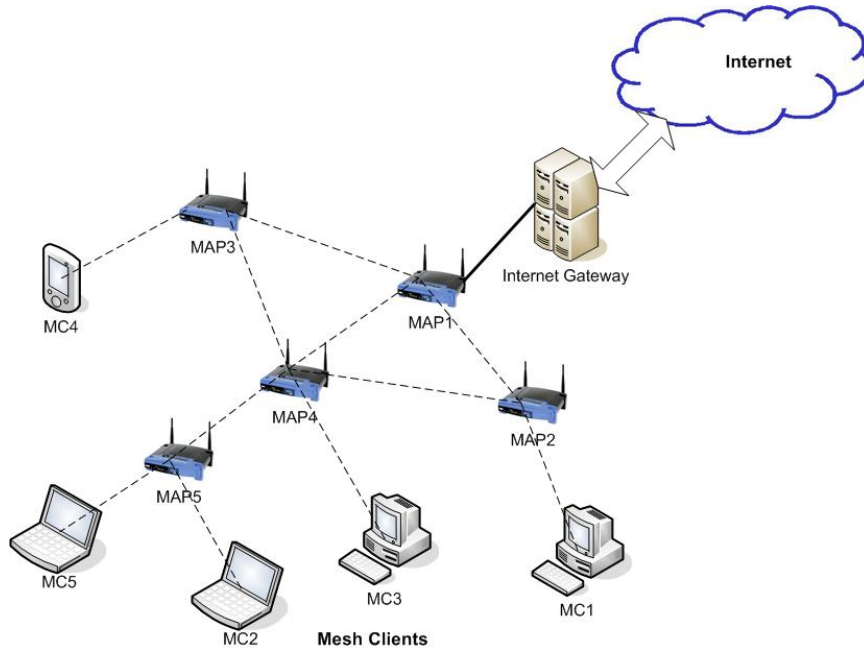


Figure 5.1: ISP using WMN for extension of Internet to users in remote area

Consider the above application scenario, in which an ISP is extending its services to users in remote area, also needs to implement different security parameters. From an ISP point of view, billing or accounting and provision of service to authentic users are the most important factors which can be achieved by user authentication process. In this case, only authentic user can be facilitated by the Internet service and ISP also needs to track the users' usage but on the other hand, IGW should be able to authenticate users either they are valid or not, regardless of their actual identities.

This means only valid users can access Internet but their identity must be remain anonymous for IGW.

Another application scenario can be WMN for military/defence operations in remote areas. In this network also, users may not want to share their identities to gateway routers/servers because of shared wireless medium but its gateway routers'/servers' responsibility to forward only traffic from the authentic users to their base networks. Server at the base headquarter would be able to check the identity of users (who is sender) and also issue new valid identities to new users as per requirements. In Figure 5.2 below, an overview of WMN used for communication in military/defence operations with their base headquarters.

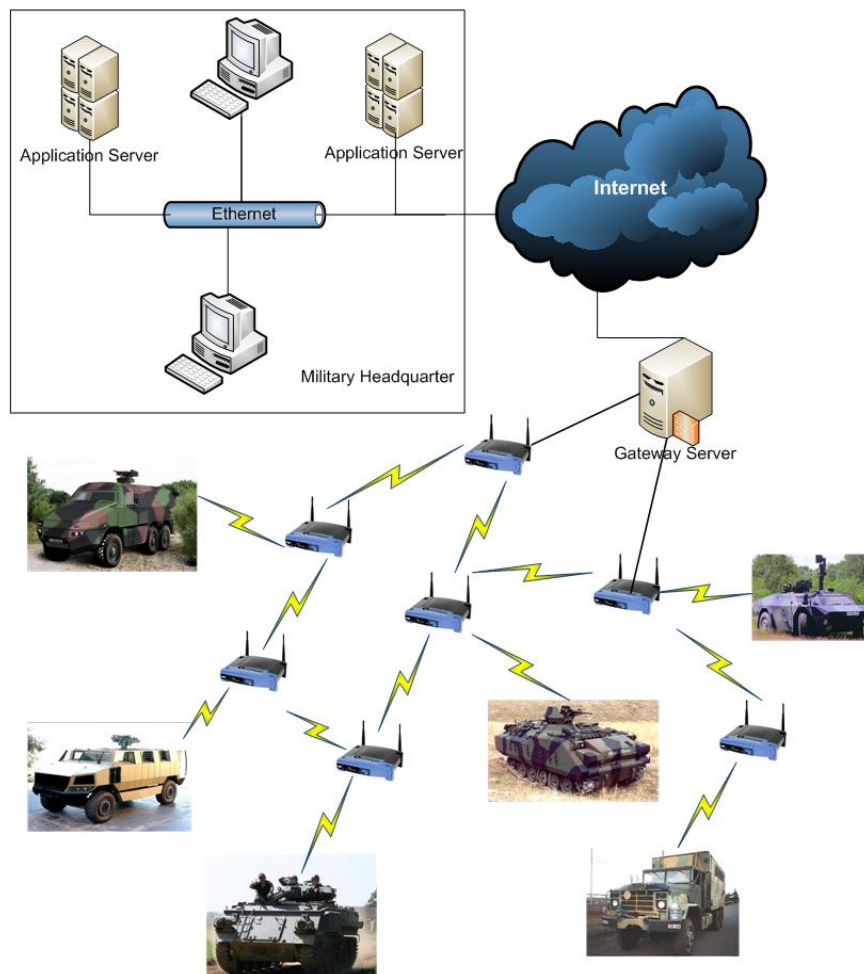


Figure 5.2: Military Operation using WMN for communication

Some other WMN applications discussed in chapter 2 also require implementation of user anonymity, authentication and data confidentiality. In this Chapter, we present a protocol to achieve user anonymity, user authentication, data confidentiality and privacy. In [51], authors presented a fair anonymous electronic cash scheme that meets all the basic security requirements for fair electronic cash including fairness, anonymity, confidentiality, authenticity etc. Our protocol also used the same mechanism to achieve user anonymity in WMN. Detailed design and functioning of protocol is discussed in later sections.

5.2 Protocol Design

In this section, we present our proposed protocol to achieve user anonymity, data confidentiality and user authentication in WMNs. In this protocol, tickets are issued by Network Operator (NO) to all valid users. These tickets are used by users for authentication purposes while requesting for Internet or other services. The important point in this protocol is about the usage of ticket, this ticket can be used by a user only once to maintain anonymity among its neighbors including MCs, MRs and IGW. If any user tries to use the same ticket twice then identity of that user can be compromised, which is discussed in detail in later section.

This protocol is actually based on blind Nyberg-Rueppel [55] digital signature scheme and anonymous digital cash scheme proposed in [53]. In our proposed protocol, ticket is issued to every valid user by the NO which can be used only once, and IGW can only verify the ticket either it is valid or not but cannot able to check the identity of user. Secondly, only NO can be able to trace the identity of user with the help of ticket but if any client uses the same ticket twice then identity of that client can be compromised. There are four main entities in our protocol to be dealt with them:

- Network Operator (NO): NO is the main controller of the WMN. NO is responsible for registration of users, issuance of tickets after initial verification and tracing of users, if required.
- Internet Gateway (IGW): IGW is responsible for providing Internet services to all valid clients available in the WMN based upon their tickets

- Mesh Routers/Mesh Access Point (MAP): MAPs are responsible for transferring data/message from one point to other point.
- Mesh Client (MC): MCs are the actual users of the network, want to have wireless Internet connectivity through IGW.

5.2.1 Notations

Notations used in our protocol are as under:

- NO : Network Operator
- IGW : Internet Gateway
- MAP : Mesh Access Point
- MC : Mesh Client
- T_{MC} : MC's Ticket
- PK_{MC} : Public Key of Mesh Client
- PK_{IGW} : Public Key of Internet Gateway
- $[Data]PK_{IGW}$: Encrypted data with public key of IGW

5.2.2 Registration of New Mesh Client

Registration of a new MC is very important process in our protocol because during this process, new MC sends joining request to NO and after getting necessary information, NO issues a ticket to new MC. Later on, this ticket is used by MC for authentication and to access Internet through IGW. Steps involved in registration of new MC and issuance of ticket are as under:

1. $NewMC \rightarrow NO : RequestMessage$
2. $NO \rightarrow NewMC : PK_{IGW}, PK_{NO}, instructions, challenge$
3. $NewMC \rightarrow NO : (PK_{MC}, UserInformation, response)$
4. $NO \rightarrow NewMC : T_{MC}$

In step 1, new MC sends request message (I want to join your network) for joining WMN to network operator NO whereas, in reply NO sends instructions about cryptography group information and public/private key generation mechanism, public keys of IGW, NO and challenge (which is discussed in later section). In response, new MC sends its public key and other user information (discussed in later section) including response of challenge in 3 step. In step 4, new MC gets new ticket from NO which is identity of MC can be used later on for accessing Internet services.

5.2.3 Ticket Generation Process

In this section, we will discuss ticket generation process in detail, which is based upon blind Nyberg-Rueppel digital signature scheme and was proposed in [53].

First NO runs a key generation algorithm generating the following:

- a large prime p and a large number q such that $q|(p-1)$
- three generators g, g_1 and g_2 of the unique subgroup G_q of the multiplicative group Z_p^*
- a randomly chosen collision-intractable hash function $H()$ of polynomial size in k that maps its inputs to Z_q
- a random number $x \in Z_q$
- three numbers h, h_1 and h_2 computed as $h = g^x$, $h_1 = g_1^x$ and $h_2 = g_2^x$ (all are computed under Z_p)

Therefore, NO's secret key and public keys are (x) and $(p, q, g, g_1, g_2, h, h_1, h_2, H())$ respectively.

Now when new MC wants to join WMN, new client communicates with NO over an authenticated channel and NO is responsible to provide its public key, public key of IGW and instructions to setup account. New MC needs to generate its public and private keys as per instructions received from NO, then new MC sends all the details to NO. After getting all the details from client, NO issues a new ticket which can be used to access the internet with the help of IGW. Steps involved in this process are as under:

For getting ticket from NO, first new MC needs to generate a pair of secret and public keys (u, I) . MC chooses a random $u \neq 0 \in G_q$, which is its secret key and

then forms $I = g_1^u \pmod{p}$. NO regards $I \neq 1$ and register it as identity of MC. NO computes $z = (Ig_2)^x \pmod{p}$, signs it with its secret key $Sign_{NO}(z)$ and then sends to new MC as the certificate of its identity. Note that I is the unique link to the new MC's real ID, while u is unknown to the NO, u can be computed by the NO only when the MC uses same ticket twice.

As mentioned in previous section, in step 1, new MC sends joining request to NO. Whereas in step 2, along with other details, NO sends challenge a to new MC.

Where **Challenge** = **a**

$$w \in_R Z_q$$

$$a \leftarrow (Ig_2)^w$$

In step 3, new MC sends response back to NO which is calculated by new MC as under:

Response = m'

$$t, x_1, x_2 \in_R Z_q^*$$

$$a' \leftarrow (Ig_2)^t$$

$$z' \leftarrow z^t$$

$$A \leftarrow g_1^{x_1} g_2^{x_2}$$

$$Z \leftarrow h_1^{x_1} h_2^{x_2}$$

$$m \leftarrow H(A, Z, a', z')$$

$$\alpha, \beta \in_R Z_q^*$$

$$r' \leftarrow ma'^\alpha a^{t\beta}$$

$$m' \leftarrow r'/\beta \pmod{q}$$

Ticket

At the end, New MC should receive the ticket signed by NO,

$$Sign(A, Z) = (A, Z, z', a', r', s', I)$$

Where

$$s \leftarrow m'x + w \pmod{q}$$

$$s' \leftarrow s\beta + \alpha \pmod{q}$$

1. NO chooses a random number $w \in_R Z_q$, and computes $a = (Ig_2)^w$ and forwards a to MC.
2. MC generates three random numbers (t, x_1, x_2) , and computes a', A, Z, z' , as shown above.
3. MC forms the message $m = H(A, Z, a', z')$, generates a random number α and a Nyberg-Rueppel blind factor β , then calculates r' and m' as shown above. After this MC sends m' to NO.
4. NO computes its Nyberg-Rueppel signature on the blind message m' by forming $s' = m'x + w \pmod{q}$ and sends it to MC.
5. MC removes the blind factor β and obtains $s' = s\beta + \alpha \pmod{q}$.

At the end of this protocol, $(A, Z, z', a', r', s', I)$ represents a valid ticket. Now this ticket can be used for further communication between IGW and MC. After successful verification of ticket, IGW will provide Internet services to MC. Verification process of ticket is discussed in detail in later section.

5.2.4 Proposed Run

Now new MC (MC_5) has ticket and also has knowledge about public key of IGW, therefore that client can now participate in the network to access Internet. MC_5 needs to send a message to its neighboring MAP (MAP_5), which then forwards that message to next hop (MAP_4), then to next hop (MAP_1) and then till IGW, as shown in Figure 5.3.

IGW broadcasts a beacon messages $c \leftarrow H(IGW || Date || Time)$ over the network after a specific time period. Now if MC_5 wants to send an Internet request (user wants to access a ftp/email server or wants to access any web site), MC_5 needs to get beacon message from its neighboring MAP first which is:

1. $IGW \longrightarrow * : c$
2. $MAP_1 \longrightarrow * : c$

After getting beacon message c , MC needs to calculate two variables r_1 and r_2 and then forwards its request, ticket along with r_1 and r_2 , after encrypting with PK_{IGW} to neighboring MAP.

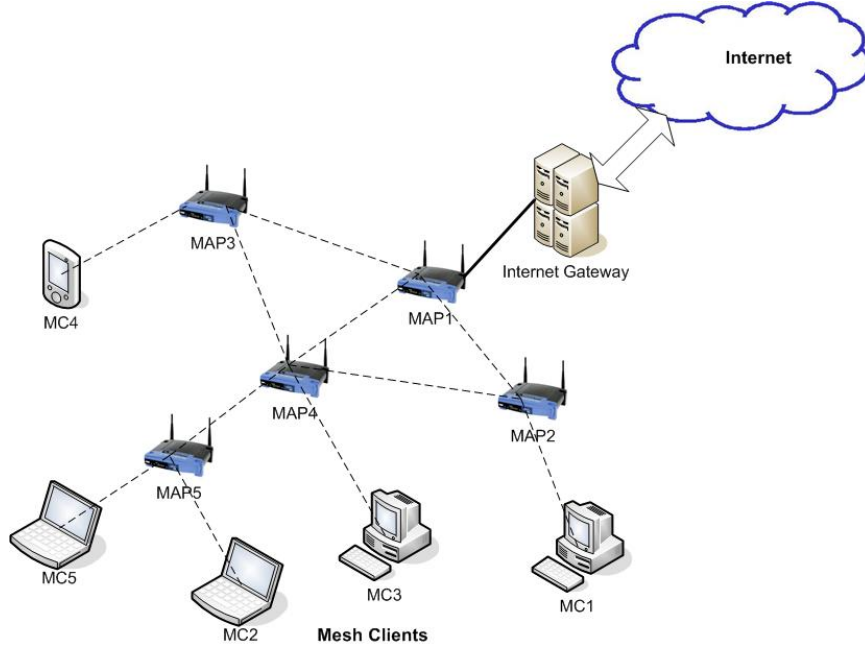


Figure 5.3: Internet extension using WMN

1. $MC_5 \longrightarrow MAP_5 : E_{PK_{IGW}}(Request)$
 where $Request : (message, r_1, r_2, T_5)$
2. $MAP_5 \longrightarrow MAP_4 : E_{PK_{MAP_4}}(MAP_4, MAP_1, E_{PK_{IGW}}(Request))$
3. $MAP_4 \longrightarrow MAP_1 : E_{PK_{MAP_1}}(MAP_1, IGW, E_{PK_{IGW}}(Request))$
4. $MAP_1 \longrightarrow IGW : E_{PK_{IGW}}(Request)$

As mentioned above, in step 1, MC_5 forward encrypted request to MAP_5 . After receiving this request message, MAP_5 prepares request message for further communication. MAP_5 includes next hops IDs (MAP_4 and MAP_1) involved in the route to forward that message to IGW and then encrypts request message with the public key of next hop (MAP_4) as shown in step 2. After encryption, MAP_5 forwards message to MAP_4 .

In step 3, MAP_4 first decrypts received message from MAP_5 and then encrypts the message with the public key of next hop involved in routing (MAP_1). After encryption, MAP_4 forwards this encrypted message to MAP_1 .

In step 4, MAP_1 first decrypts received message from MAP_4 and then check for next hop (if there is any). But in this case, MAP_1 is within direct range of IGW,

so forwards request message generated by MC to IGW. This message is already encrypted with the public key of IGW.

Now IGW first decrypts the request message received with its private key and then verifies the ticket attached with the message (verification process is explained in later section). After successful verification of ticket, IGW prepares the response or forward its request to Internet. After getting response, IGW will first decrypt it with public key of MC and then prepare the reply packet according to MAPs involved in reverse route, which is as under:

1. $IGW \longrightarrow MAP_1 :$
 $E_{PK_{MAP_1}}(MAP_4, E_{PK_{MAP_4}}(MAP_5, E_{PK_{MAP_5}}(MC_5, E_{PK_{MC_5}}(Response))))$
2. $MAP_1 \longrightarrow MAP_4 : E_{PK_{MAP_4}}(MAP_5, E_{PK_{MAP_5}}(MC_5, E_{PK_{MC_5}}(Response)))$
3. $MAP_4 \longrightarrow MAP_5 : E_{PK_{MAP_5}}(MC_5, E_{PK_{MC_5}}(Response))$
4. $MAP_5 \longrightarrow MC_5 : E_{PK_{MC_5}}(Response)$

Now IGW prepares the response for MC in such an order that first it decrypts response with public key of MC and then with the public key of neighboring MAP (in this case its MAP_5) and then with public key of next MAP (MAP_4) and so on. IGW then forwards this encrypted response next hop (MAP_1) using reverse routing information, as shown in step 1.

After receiving this response, MAP_1 first decrypts it with private key and then forwards it to next hop (MAP_4) as shown in step 2.

In step 3, MAP_4 first decrypts response message with its private key and then forwards it to next hop (MAP_5).

After receiving response message from MAP_4 , MAP_5 decrypts it with its private key and then forwards it to MC_5 , as shown in step 4. After this step, MC_5 gets response from IGW in encrypted format and which is secured from intruders.

In this way, MC_5 will be able to receive response from IGW securely and MAPs involved in routing would not be able to know anything about the destination, only neighboring MAP knows about final destination. One another important thing is that data/response of Internet request is also encrypted with public key of concerned MC, therefore, no other MC/MAP can view that response, unless they know the secret/private key of that MC.

The most important thing in this protocol is that IGW would not be able to know about the user because user only sending its ticket which is digitally signed by NO and IGW can only verify that ticket whether its valid or not. And if user/MC uses the same ticket more than once then IGW would be able to know the details about the user/MC, hence anonymity of user/MC would be compromised in that case. And if IGW wants to check the identity of MC in case of any misbehavior, IGW needs to request NO to check the real identity of MC.

5.2.5 Ticket Verification Process

Ticket verification is the responsibility of IGW, and if ticket received is valid then MC's request will be processed, otherwise request will be discarded by IGW. After getting "Request" packet from MC, IGW first decrypts it with its private key and then check the validity of request packet which contains message, r_1 , r_2 and ticket of MC. Details are as under:

$$Request = (message, r_1, r_2, T_5)$$

Where

$$r_1 \leftarrow c(ut) + x_1 \pmod{q}$$

$$r_2 \leftarrow ct + x_2 \pmod{q}$$

$$T_5 : (A, Z, z', a', r', s', I)$$

After receiving this Request message from MC, IGW verifies it by performing following steps:

$$H(A, Z, a', z') \stackrel{?}{=} a'^{-s'} z'^{r'} r'$$

$$g_1^{r_1} g_2^{r_2} \stackrel{?}{=} a'^c A$$

$$h_1^{r_1} h_2^{r_2} \stackrel{?}{=} z'^c Z$$

As for the proof of equality of discrete logarithms, for a random challenge c if

$$g_1^{r_1} g_2^{r_2} \stackrel{?}{=} a'^c A$$

$$h_1^{r_1} h_2^{r_2} \stackrel{?}{=} z'^c Z,$$

we must have $\log_{a'} z' = \log_{g_1} h_1$. This shows that the NO's secret key $x = \log_{g_1} h_1$ was used in the generation of Ticket.

5.2.6 Ticket Uniqueness Checking

There are two possible anonymity controls in this scheme. One is to identify the user in communication and the other is to identify the history, i.e., the life cycle of a ticket. The former is referred as user tracing and the latter is referred as ticket tracing.

Identifying a ticket history can be done by checking the ticket submitted by user for communication.

In this case, *IGW* sends to *NO* the user's ticket. Then *NO* computes the value $a'/g_3^\tau = ((Ig_2)^t)^\tau = g_1^{ut\tau} g_2^{t\tau} = h_{T_1}^{ut} h_{T_2}^t = e \pmod{p}$

The anonymity revocation is done by searching for the computed value e in the ticket reference database.

5.3 Security Analysis

In this section, we discuss about the security which is provided by our proposed protocol in terms of user anonymity, authentication, data confidentiality etc. Following security features are provided by our protocol:

- *Confidentiality/Data Privacy.* With the help of asymmetric cryptography based upon public and private keys of sender and receiver, which provides message confidentiality/data privacy because data is encrypted by public key of a user (either MC or IGW) and it can only be decrypted with the corresponding private key of same user. In this case, if data is encrypted with the public key of MC_5 then only MC_5 can decrypt it with the help of its private key, no other user can decrypt it, unless user has knowledge about private key of MC_5 .
- *Authentication.* With the help of tickets, users can be authenticated by IGW, when they send request for Internet because tickets are digitally signed by the NO, so no other MC can generate its new ticket for any purposes, unless they have knowledge about private key of NO and signing algorithm.
- *Authorization.* In our protocol, only authorized users can access the Internet or other services based upon the network requirements because IGW first verifies the ticket provided by the users and if this ticket is valid then IGW provide access to that user otherwise it just discard that request. Data is

also transferred in encrypted format, therefore, data is also secured against unauthorized access.

- *User Anonymity.* In our protocol, user anonymity is protected unconditionally. Each ticket is blindly signed by the NO. When the client submits its ticket to IGW, it is not feasible for the IGW and the NO to link the ticket and the user. IGW can only verify the ticket whether it is valid or not and it is only issued by the NO. During the communication between user and IGW, apart from the ticket, the user needs to show the response:

$$r_1 \leftarrow c(ut) + x_1 \pmod{q}$$

$$r_2 \leftarrow ct + x_2 \pmod{q}$$

With x_1 and x_2 secretly chosen by the user, it is impossible to compute u , v or w from the response. So user's anonymity is unconditionally protected.

- *Communication Untraceability.* Our protocol treats each ticket independently and there is no connection between any two tickets even issued to same user. Hence when two tickets are issued to one user and are used in two different communications, it is impossible for IGW to find any link between the two communications from these tickets. This leads to untraceability of communications between user and IGW at different time instances.
- *Ticket Forgery.* It is computationally impossible to forge tickets used in our protocol. To forge a ticket, the enemy needs to create a blind Nyberg-Rueppel signature on $m = H(\alpha, \beta, \lambda)$, which is not possible according to [17]. Combining several old tickets to get a new ticket is also infeasible, as each ticket contains $m = H(\alpha, \beta, \lambda)$ and H is a strong one-way hashing function.

Another important security feature which is implemented in our protocol is hiding the identity of MC (who has started this communication) from other MAPs involved in routing during communication from MC to IGW and back from IGW to MC. Only directly linked/neighbors MAP knows that which client send this request and the rest of MAPs do not know about client's ID. Because they receive data encrypted with public key of IGW and need to forward it to next MAP. Whereas on the way back from IGW to MC, first data is first encrypted with the public key of MC and then it is again encrypted with public key of MC's neighboring MAP and then with the public key of next MAP on the way and so on. This means that IGW performs this in reverse order, so that first MAP in the route decrypts message and

forward data packet to next hop (MAP) and that MAP receives it and decrypts it with its private key and forward to next hop until it reaches the destination.

In the nutshell, our proposed protocol provides user anonymity, authentication, authorization, data privacy/confidentiality, communication untraceability, detection of fake tickets etc for WMNs.

5.4 Summary

The importance of user anonymity in wireless networks including WMNs is discussed in literature in very detail since the evolution of wireless networks. Due to open wireless medium, importance of user anonymity has gained much more importance. Therefore, the requirement to design a secure routing protocol for WMNs which also maintains user anonymity along with providing authentication mechanism is a active research area.

In this chapter, we presented a protocol which provides user anonymity, user authentication and also data confidentiality/privacy throughout the WMN. Our protocol is based upon blind Nyberg-Rueppel digital signature scheme. In this protocol, NO issues tickets to valid users only and these users can then use these tickets to access Internet or other services provided by IGW. IGW can only verify these tickets whether tickets are valid or not but can not check who's ticket is this?. In this way user anonymity has been achieved along with user authentication and data privacy throughout WMN.

Chapter 6

Conclusions

In this thesis, our main emphasis was to design and deploy security features for wireless mesh networks. Our aim was to provide authentication, integrity, anonymity, confidentiality/privacy and non-repudiation from routing as well as user point of view in WMNs. Security issues related to routing and users of WMNs are covered in proposed protocols.

We conducted a thorough study about the WMNs to achieve a comprehensive understanding of the application domains available for WMNs. We also studied routing protocols (AODV and DSR) already available for WMNs including their routing operations and data structure, so that we could take some benefit from these protocol for our proposed protocols. In our first proposed protocol, we have used the AODV protocol as the base protocol for routing purposes and added new features to provide secure routing, user authentication and data confidently.

We reviewed the literature in detail and identified different types of attack which are generally regarded as the most serious attacks in disrupting routing and communication operations. By analysing their attacking approaches, existing counter-measures and different application scenarios, we were able to come up with the security requirements to be achieved in wireless mesh networks. We also studied some existing secure routing protocols for wireless mesh networks and justified their performance according to our security requirements. We noticed that the security of the existing proposals is not established from a realistic point of view because these protocols do not provide multi-layer/cross-layer protocol facilities means provision of different layers tasks in one single step, as we have proposed in TAODV. Three of the secure protocols which we discussed are ARAN, SADOV and SAR. All of these protocols are based on AODV protocol. We have discussed these protocols in chapter 2 and also provided comparison with proposed protocol TAODV in chapter 4. According to the comparison in chapter 4, it is clearly mentioned that proposed

protocol TAODV is much better than these protocols because it provides cross-layer solution to implement security against different layers security problems in a single step.

We also discussed the cryptographic primitives to be used in the design of new security protocols for WMNs. We discussed public/secret key and shared key cryptography. The digital signature which has long been used to provide authentication, integrity and non-repudiation is recognised as our primary goal. Then we also discussed Diffie-Hellman key exchange protocol, blind signature and Nyberg-Rueppel Digital Signature schemes. We have used these digital signature schemes in our proposed protocols because of infrastructure support available in WMNs as compared to MANETS and other wireless networks. With the help of infrastructure, authentication servers, certificate authority and network operators can easily provide support for generation and implementation of these signature schemes.

Firstly, we presented a new cross-layer protocol based upon the AODV protocol which provides data security, route discovery security and security against ARP security issues. Proposed cross-layer security protocol provides a secure WMN using ticket based approach, in which authentication is achieved with the help of tickets (issued and signed by AS) and asymmetric cryptography (using public and private keys of source and destination respectively) is used for generation of shared secret key. Data confidentiality and integrity can be achieved by data encryption using strong symmetric key algorithm. This proposed protocol also reduces network traffic by combining the different steps in one single step like transfer of public keys, exchange of MAC addresses and route discovery from source and destination is done in a single step during route discovery with the help of tickets. Hence, our protocol also provides security against ARP security problems like MITM, ARP poisoning and ARP spoofing attacks.

Secondly, we presented another security protocol based upon the Blind Nyberg-Rueppel Digital Signature scheme which provides client/user anonymity, user authentication and data confidentiality / privacy. Proposed security protocol provides a secure WMN using ticket based approach, in which authentication is achieved with the help of tickets (issued and signed by NO) and user identity remains anonymous throughout the network. Data confidentiality and integrity can be achieved by data encryption using asymmetric key algorithm.

In future work, we envisage to provide a solution for such WMNs where AS are

not available and also plan to provide a more efficient solution instead of incorporating symmetric or asymmetric key cryptography. We have planned to implement these protocols first in network simulator (ns-2) [3], to check and compare the efficiency of these protocols with the existing protocols.

Appendix A

Glossary

Ack	Acknowledgment
AODV	Ad Hoc On Demand Distance Vector
ARAN	Authenticated Routing for Ad hoc Networks
ARP	Address Resolution Protocol
AS	Authentication Server
CA	Certification Authority
CGSR	Clusterhead Gateway Switch Routing protocol
DBF	Distributed Bellman-Ford
DoS	Denial of Service
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
IGW	Internet Gateway
ISP	Internet Service Provider
LAN	Local Area Network
MAC Address	Media Access Control Address
MANET	Mobile Ad Hoc Network
MAP	Mesh Access Point
MC	Mesh Client
MITM	Man-In-The-Middle
MR	Mesh Router
NLOS	Non-Line-of-Sight
NO	Network Operator
OSPF	Open Shortest Path First
PDA	Personal Data Assistant
RDP	Route Discovery Packet
PK	Public Key
RERR	Route Error
RREP	Route Reply
RREQ	Route Request
SAODV	Secure Ad hoc On-Demand Distance Vector Routing
SEAD	Secure Efficient Distance Vector Routing
SK	Secret Key
TAODV	Ticket based Ad Hoc On Demand Distance Vector
TORA	Temporally Ordered Routing Algorithm
WDS	Wireless Distribution System
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WRP	Wireless Routing Protocol
ZRP	Zone Routing Protocol

Bibliography

- [1] [Online]. Available: www.linksys.com
- [2] [Online]. Available: www.arm.com
- [3] [Online]. Available: <http://www.isi.edu/nsnam/ns>
- [4] “Firetide networks, <http://www.firetide.com>.”
- [5] “Kiyon autonomous networks, <http://www.kiyon.com>.”
- [6] “Microsoft mesh networks, <http://research.microsoft.com/mesh/>.”
- [7] I. F. Akyildiz and I. H. Kasimoglu, “Wireless sensor and actor networks: research challenges,” *Ad Hoc Networks*, vol. 2, no. 4, pp. 351–367, 2004.
- [8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.
- [9] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless mesh networks: a survey,” *Computer Networks Journal (Elsevier)*, vol. 47, pp. 445–487, March 2005.
- [10] M. Al-Shurman, S.-M. Yoo, and S. Park, “Black hole attack in mobile ad hoc networks,” in *ACM-SE 42: Proceedings of the 42nd annual Southeast regional conference*. ACM, 2004, pp. 96–97.
- [11] M. Alicherry, R. Bhatia, and L. Li, “Joint channel assignment and routing for throughput optimization in multi-radio wireless mesh networks,” in *in Proc. ACM MobiCom05*, Cologne, Germany, August 2005, pp. 58–72.
- [12] N. Beijar, “Zone routing protocol (zrp),” Networking Laboratory, Helsinki University of Technology, Finland.

- [13] T. Bradley, C. Brown, and A. Malis, "Inverse address resolution protocol, rfc 2390," Tech. Rep., September 1998.
- [14] S. Brands, "Electronic cash systems based on the representation problem in groups of prime order," in *Proceedings of CRYPTO'93*, 1993, pp. 26.1–26.15.
- [15] R. Bruno, M. Conti, and E. Gregori, "Mesh networks: commodity multihop ad hoc networks," *IEEE Communication Magazine*, pp. 123–131, March 2005.
- [16] A. Burg, "Ad hoc network specific attacks," in *In Seminar Ad Hoc networking: Concepts, Applications and Security*. Technische University Munchen, 2003.
- [17] J. L. Camenisch, J.-M. Piveteau, and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," in *Advances in Cryptology- EUROCRYPT'94*, A. De Santis, Ed. Berlin,: Springer, 1994, pp. 428–432.
- [18] J. Camp and E. Knightly, "The ieee 802.11s extended service set mesh networking standard," *Communications Magazine, IEEE*, vol. 46, no. 8, pp. 120–126, August 2008.
- [19] G. Celine, "Predeployment testing of wireless mesh networks," August 2006.
- [20] Chaum, "Blind signature systems," in *Advances in Cryptology*. Springer US, 1983, p. 153.
- [21] D. Chaum, "Blind signatures for untraceable payments," in *CRYPTO*, 1982, pp. 199–203.
- [22] I. Chlamtac, M. Conti, and J. J. Liu, "Mobile ad hoc networking: imperatives and challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13–64, July 2003.
- [23] J. Y. Choi, "Security problems for ad hoc routing protocols," Indiana University at Bloomington, Technical report, 2003.
- [24] CISCO, *Internetworking Technology Handbook*, 4th ed. CISCO Systems, 2003.
- [25] R. G. D Bertsekas, "Data networks," Prentice Hall Inc, 1992.
- [26] B. Dahill, K. Sanzgiri, B. N. Levine, E. M. Belding-Royer, and C. Shields, "A secure routing protocol for ad hoc networks," in *IEEE Journals on Selected Areas in Communications, Special issue on Wireless Ad hoc Networks*, Amherst, MA, USA, 2002.

-
- [27] W. Diffie and M. Hellman, "Multiuser cryptographic techniques," in *IEEE Transactions on Information Theory*, November 1976.
 - [28] W. Diffie and M. E. Hellman, "New directions in cryptography," in *Proceedings of the AFIPS National Computer Conference*, June 1976.
 - [29] R. Droms, "Dynamic host configuration protocol, rfc 2131," IETF, Tech. Rep., March 1997.
 - [30] N. Ferguson, "Single term off-line coins," in *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*. Springer-Verlag New York, Inc., 1994, pp. 318–328.
 - [31] R. Finlayson, T. Mann, J. Mogul, and M. Theimer, "A reverse address resolution protocol, rfc 903," Stanford University, Tech. Rep., June 1984.
 - [32] B. Fleck and J. Dimov, "Wireless access points and arp poisoning: Wireless vulnerabilities that expose the wired network," Cigital Inc., Tech. Rep., 2001.
 - [33] M. N. Forum, "Building the business case for implementation of wireless mesh networks," in *Mesh Networking Forum*. San Francisco: Mesh Networking Forum, October 2004.
 - [34] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, pp. 281–308, 1988.
 - [35] S. Gupte and M. Singhal, "Secure routing in mobile wireless ad hoc networks," in *Ad Hoc Networks*, vol. 1, no. 1. Elsevier, July 2003, pp. 151–174.
 - [36] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: secure efficient distance vector routing for mobile wireless ad hoc networks," in *WMCSA '02: Proceedings of the 4th annual international conference on Mobile computing systems and applications*. IEEE, 2002, pp. 3–13.
 - [37] Y.-C. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security and Privacy*, vol. 2, no. 3, pp. 28–39, 2004.
 - [38] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," in *MobiCom '02: Proceedings of the 8th annual*

- international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2002, pp. 12–23.
- [39] Y. C. Hu, A. Perrig, and D. B. Johnson, “Rushing attacks and defense in wireless ad hoc network routing protocols,” in *WiSe '03: Proceedings of the 2nd ACM workshop on Wireless security*. ACM, 2003, pp. 30–40.
- [40] *IEEE 802.16-2005-Standard for Local and metropolitan area networks; Part 16: Air Interface for Fixed Broadband Wireless Access Systems, Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands*, IEEE Std., 2005.
- [41] *IEEE std. 802.11-1997, IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Computer Society Std., 1997.
- [42] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, “The dynamic source routing protocol for mobile ad hoc networks (dsr),” IETF MANET Working Group, Tech. Rep., 2003.
- [43] J. Jun and M. L. Sichitiu, “The nominal capacity of wireless mesh networks,” *Wireless Communications, IEEE [see also IEEE Personal Communications]*, vol. 10, no. 5, pp. 8–14, 2003.
- [44] L. Krishnamurthy, S. Conner, M. Yarvis, J. Chhabra, C. Ellison, C. Brabenac, and E. Tsui, “Meeting the demands of the digital home with high-speed multi-hop wireless networks,” *Intel Technology Journal*, vol. 06, pp. 57–68, November 2002.
- [45] S.-H. Lee and Y.-B. Ko, “An efficient multi-hop arp scheme for wireless lan based mesh networks,” *1st Workshop on Operator-Assisted (Wireless Mesh) Community Networks*, pp. 1–6, September 2006.
- [46] G. Li, “An identity-based security architecture for wireless mesh networks,” in *NPC '07: Proceedings of the 2007 IFIP International Conference on Network and Parallel Computing Workshops*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 223–226.

-
- [47] W. Liu, C. Chiang, H. Wu, and C. Gerla, "Routing in clustered multihop mobile wireless networks with fading channel," in *Proc. IEEE SICON'97*, April 1997, pp. 197–211.
 - [48] Y. Lu, W. Wang, Y. Zhong, and B. Bhargava, "Study of distance vector routing protocols for mobile ad hoc networks," in *in Proceedings of the First IEEE International Conference on Pervasive Computing and Communications. IEEE Computer Society*, 2003, p. 187.
 - [49] P. Misra, "Routing protocols for ad hoc mobile wireless networks," The Ohio State University, Computer Science and Engineering, Tech. Rep., 1999.
 - [50] J. Moy, "Ospf version 2," IETF," RFC: 2178, 1997.
 - [51] Y. Mu, K. Q. Nguyen, and V. Varadharajan, "A fair electronic cash scheme," in *ISEC '01: Proceedings of the Second International Symposium on Topics in Electronic Commerce*. London, UK: Springer-Verlag, 2001, pp. 20–32.
 - [52] S. Murthy and J. J. G. luna aceves, "A routing protocol for packet radio networks," 1995, pp. 86–95.
 - [53] K. Q. Nguyen, Y. Mu, and V. Varadharajan, "A new digital cash scheme based on blind nyberg-rueppel digital signature," in *ISW '97: Proceedings of the First International Workshop on Information Security*. London, UK: Springer-Verlag, 1998, pp. 313–320.
 - [54] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*. New York, NY, USA: ACM, 1999, pp. 151–162.
 - [55] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the dsa giving message recovery," in *CCS '93: Proceedings of the 1st ACM conference on Computer and communications security*. New York, NY, USA: ACM, 1993, pp. 58–61.
 - [56] R. Ogier, F. Templin, and M. Lewis, "Topology dissemination based on reverse-path forwarding (tbrpf)," IETF, Tech. Rep., February 2004.

-
- [57] T. Okamoto and K. Ohta, "Universal electronic cash," in *CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*. Springer-Verlag, 1992, pp. 324–337.
- [58] V. D. Park, "Temporally-ordered routing algorithm (tora)," Naval Research Laboratory, Information Technology Division, Washington, DC 20375, 2001.
- [59] C. E. Perkins, E. B. Royer, and S. R. Das, "Ad hoc on demand distance vector (aodv) routing, rfc 3561," IETF, Tech. Rep., July 2003.
- [60] C. E. Perkins and P. Bhagwat., "Highly dynamic destination-sequenced distance-vector routing (dsv) for mobile computers." in *In Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications*, August 1994, pp. 234–244.
- [61] R. Poor, "Wireless mesh links everyday devices," *Electronic Engineering Times*, July 2004.
- [62] S. Y. Prasad, S. Yi, P. Naldurg, and R. Kravets, "A security-aware routing protocol for wireless ad hoc networks," in *in: Proceedings of ACM Symposium on Mobile Ad Hoc Networking & Computing (Mobihoc)*, 2002, pp. 286–292.
- [63] S. Qazi, Y. Mu, and W. Susilo, "Securing wireless mesh networks with ticket-based authentication," in *International Conference on Signal Processing and Communication Systems*, 2008.
- [64] A. Raniwala and C. Tzi-cker, "Architecture and algorithms for an ieee 802.11-based multi-channel wireless mesh network." in *in Proc. IEEE INFOCOM05*, March 2005, pp. 2223–2234.
- [65] E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," in *IEEE Personal Communications*, vol. 6. IEEE, April 1999, pp. 46–55.
- [66] X. E. S E D Lim, "Study of secure reactive routing protocols in. mobile adhoc networks," National University of Singapore," Technical report, 2003.
- [67] M. Z. H. Sarker and M. S. Parvez, "A cost effective symmetric key cryptographic algorithm for small amount of data," in *9th International Multitopic Conference, IEEE INMIC*, 2005.

-
- [68] B. Schneier, *Applied Cryptography*, 2nd ed. John Wiley & Sons, 1996.
- [69] S. Seys and B. Preneel, “Arm: Anonymous routing protocol for mobile ad hoc networks,” in *in Proceedings of the 20th IEEE International Conference on Advanced Information Networking and Applications (AINA 2006*, 2006, pp. 133–137.
- [70] W. Stallings, *Cryptography and Network Security*, 4th ed. Pearson Prentice Hall, 2006.
- [71] J. Walker, “Wi-fi mesh networks, the path to mobile ad hoc,” *Wi-Fi Technology Forum*, 2005. [Online]. Available: <http://www.wi-fitechnology.com/Papers+req-showcontent-id-8.html>
- [72] M. H. R. M.-E. Y. Amir, C. Danilov and N. Rivera, “Fast handoff for seamless wireless mesh networks,” *MobiSys '06: Proceedings of the 4th international conference on Mobile systems, applications and services*, pp. 83–95, 2006.
- [73] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang, “Security in mobile ad hoc networks: Challenges and solutions,” *IEEE Wireless Communication*, vol. 11(1), pp. 38–47, February 2004.
- [74] M. G. Zapata, “Secure ad hoc on demand distance vector (saodv) routing,” IETF, Tech. Rep., September 2006.
- [75] W. Zhang, Z. Wang, S. K. Das, and M. Hassan, *Wireless Mesh Networks*. Springer US, 2007, ch. Security Issues in Wireless Mesh Networks, pp. 309–330.
- [76] J. Zhu and J. Ma, “A new authentication scheme with anonymity for wireless environments,” *Consumer Electronics, IEEE Transactions on*, vol. 50, no. 1, pp. 231–235, Feb 2004.