*2007*年 *8*月

博士學位論文

# *Provisioning Robustness and Security in Ubiquitous Wireless Access Networks*

朝 鮮 大 學 校 大 學 院

情 報 通 信 工 學 科

*VAIDYA BINOD*

# *Provisioning Robustness and Security in Ubiquitous Wireless Access Networks*

*2007*年 *8*月 日

**朝鮮大學校 大學院**

**情報通信工學科**

*VAIDYA BINOD*

# *Provisioning Robustness and Security in Ubiquitous Wireless Access Networks*

**指 導 敎 授　韓　承　朝**

이 **論文**을 **工學博士學位申請 論文**으로 **提出**함.

*2007* **年**　*8* **月**　　**日**


**朝 鮮 大 學 校　大 學 院**

**情 報 通 信 工 學 科**

*VAIDYA BINOD*

*VAIDYA BINOD*의 **博士學位 論文**을
**認准**함

위원장　조선대학교　교수　박　종　안　**印**

위　원　조선대학교　교수　박　세　승　**印**

위　원　조선이공대　교수　김　정　호　**印**

위　원　호남대학교　교수　김　형　종　**印**

위　원　조선대학교　교수　한　승　조　**印**

*2007* **年**　*8* **月**　　**日**

# 朝鮮大學校　大學院

# *C O N T E N T S*

Abstract ····· iv
Acknowledgements ····· vii
List of Figures ····· viii
List of Tables ····· xii

I. Introduction ····· 1
1. Overviews ····· 1
2. Research Motivation ····· 3
3. Thesis Overviews ····· 5
3.1. Major Contributions ····· 5
3.2. Thesis Outline ····· 5

II. Background ····· 7
1. Single-hop Wireless Network ····· 7
1.1. Wireless LANs ····· 7
1.2. Mobile IP ····· 8
1.3. Security Issues in Single-hop Wireless Network ····· 10
2. Multihop Wireless Network ····· 14
2.1. Wireless Ad hoc Network ····· 14
2.2. Routing in Ad hoc Networks ····· 15
2.3. Multipath Ad Hoc Routing ····· 21
2.4. Multimedia Streaming over MANET ····· 26
2.5. Security Issues in Ad hoc routing ····· 32

3. Hybrid Ad Hoc Network ····· 37
3.1. Hybrid MANET ····· 37
3.2. Internet Gateway in Hybrid MANET ····· 38
3.3. Security Issues in Hybrid MANET ····· 44
3.4. Distributed Media Delivery ····· 46

III. Proposed Approaches ····· 49
1. Authentication scheme for Wireless mobile network ····· 49
1.1. Previous Works ····· 49
1.2. OTP-based Authentication Scheme ····· 50
2. Multipath Multihop Wireless Network ····· 54
2.1. Existing Approaches for Multipath Ad hoc Network ····· 55
2.2. Related Works ····· 59
2.3. AODV-MAP Routing Scheme ····· 60
2.4. Traffic allocation approach using AODV-MAP ····· 70
2.5. Secure AODV-MAP Scheme ····· 74
3. Hybrid Ad hoc Network ····· 81
3.1. Existing approaches for Hybrid MANET ····· 81
3.2. Related Works ····· 83
3.3. Approach for Internet connectivity in AODV-MAP based Hybrid MANET ····· 85
3.4. Secure Framework for Internet connectivity in AODV-MAP based Hybrid MANET ····· 94
3.5. AODV-MAP based Distributed multimedia delivery network ····· 102

IV. Evaluation ····· 106
1. Network Simulation Tool ····· 106
2. OTP-based Authentication Scheme for Wireless mobile network ····· 107
2.1. Analysis of OTP-based Authentication Scheme ····· 107
3. AODV-MAP based Framework for Multihop Wireless Network ····· 110
3.1. Evaluation of AODV-MAP routing scheme ····· 111
3.2. Evaluation of audio streaming over AODV-MAP based MANET ····· 124
3.3. Analysis of Secure AODV-MAP Scheme ····· 130
4. Approach for Internet connectivity in AODV-MAP based Hybrid MANET ····· 139
4.1. Evaluation of AODV-MAP based Hybrid MANET ····· 139
4.2. Analysis of Secure AODV-MAP based Hybrid MANET ···· 144
4.3. Evaluation of audio streaming over AODV-MAP based Hybrid MANET ····· 150

V. Conclusions & Future Works ····· 153
1. Conclusions ····· 153
2. Future Works ····· 156

Bibliography ····· 158

# *ABSTRACT*

## *PROVISIONING ROBUSTNESS AND SECURITY IN UBIQUITOUS WIRELESS ACCESS NETWORK*

Vaidya, Binod
Advisor : Prof. Han, Seung-Jo, Ph.D.
Department of Information & Communications,
Graduate School of Chosun University

The growth of the Internet use and wireless network has accelerated the rapid implementation of ubiquitous services. Internet connectivity to wireless access networks based IEEE 802.11 Wireless local area network (WLAN) have gained popularity due to fact that they minimize the need for expensive wired infrastructure and are relatively easy to deploy and maintain. Furthermore, Mobile Ad Hoc Networks (MANETs), which are systems of mobile nodes that dynamically self-organize in arbitrary network topologies allowing nodes to communicate each other without any pre-existing communication infrastructure, have tremendous potential to be the technology of choice for providing ubiquitous Internet connectivity. Even though multihop wireless networks enable truly pervasive, mobile access, they significantly exacerbate several wireless networking challenges that must be addressed before these networks can become practical and useful.

Future applications of wireless networks such as MANETs are expected to be based on all-IP architecture and be capable of carrying multitude real-time multimedia applications such as voice and video as well as data. It is necessary for MANETs to have an efficient reliable and secure routing to support diverse applications.

In this dissertation, we focus on some challenges that are particularly aggravated in multihop scenarios, and that we believe are among the most significant hurdles obstructing the widespread use of these networks.

We have depicted authentication scheme based on hash chain for wireless mobile network.

In this thesis, we deal with isolated as well as hybrid multihop wireless network. In this regard, we have proposed a multipath ad hoc routing scheme called "Ad hoc On-demand Distance Vector Routing - Multiple Alternative Paths (AODV-MAP)", which is robust and efficient scheme for the ad hoc network where frequent communication failure occurs. Multipath routing allows the establishment of multiple paths between a source and destination node. It is beneficial not only to frequent link breaks in communication because of mobility of nodes but also to avoid traffic congestion. The features of AODV-MAP scheme are path accumulation technique, selective route request forwarding scheme, path selection strategy, and path label setting strategy.

We have devised traffic allocation strategy in AODV-MAP scheme using scalable audio coding and hence evaluated the effectiveness of such a technique for multimedia delivery over multipath MANET.

Although AODV-MAP provides robust and efficient multipath routing in MANETs, it is vulnerable to various attacks. To provide security, we have developed Secure AODV-MAP, which is robust not only to topological changes but also malicious activities.

Moreover, we have illustrated an approach for global connectivity in hybrid multipath ad hoc network. This approach is suitable for the integrated Internet with MANET with multiple gateways. In this approach, we have put forward a robust gateway selection scheme to select optimum gateway as well as extended version of AODV-MAP to adopt well in hybrid environment.

We have also provided security extension to this approach considering vulnerability of Internet connectivity as well as ad hoc routing. Finally,

we have analyzed a reliable distributed multimedia delivery network over hybrid multipath MANET using unequal error protection (UEP).

# *Acknowledgements*

First and foremost, I would like to express my sincere gratitude my advisor, Prof. Seung-Jo Han. I thank him for leading me into this exciting research area and giving me help whenever I need. I am grateful for his constant encouragement, support, supervision and guidance during my Ph.D at Chosun University, Korea. I also thank him for being understanding and supportive to me and my family during our stay in Korea.

I thank all my past and present colleagues at the CNIS Lab for being such enthusiastic researchers and great friends and giving me help and valuable suggestions and comments over the years. In particular, I thank Sang-Duck Lee for his contribution towards my dissertation.

I thank the faculty of the Information and Communication Engineering Department, Chosun University for their teaching and support. I would also like to thank administrative staff and many others for their supports during my studies.

I would like to thank the Dean of Institute of Engineering, Tribhuvan University, Nepal for providing me this opportunity to pursue doctorate degree. I also thank Prof. Jagan Nath Shrestha from the Tribhuvan University, Nepal for his guidance and support during my studies.

On the more personal side, I thank my father for his love, encouragement, and support all through my life. I would like to thank my brothers, and parent-in-laws for their supports.

Finally, I would like to express my deepest gratitude to my wife who has generously and consistently provided me with endless support and love. I am very thankful to my daughter who always has a cheerful smile which is a source of energy.

# *List of Figures*

Figure 1.1. Types of Wireless Networks
Figure 1.2. Overviews of Ubiquitous Wireless access system
Figure 2.1. Mobile IPv4 Architecture
Figure 2.2. Overviews of EAP-TLS procedure
Figure 2.3. Overviews of Ad hoc Network
Figure 2.4. Route Discovery in DSR
Figure 2.5. Route Discovery in AODV
Figure 2.6. Types of multiple alternative paths
Figure 2.7. Overviews of SRTP packet
Figure 2.8. Typical Diagram of Scalable audio coding system
Figure 2.9. MPEG-4 CELP bit rate (SNR) scalable coder
Figure 2.10. Scalable coding with selective encryption
Figure 2.11. Invisible node attack
Figure 2.12. Worm hole attack
Figure 3.1. Conversation phases of OTP Authentication scheme
Figure 3.2. Path accumulation during route discovery
Figure 3.3. Partial flowchart for setting path label
Figure 3.4. Modules for determining alternative paths
Figure 3.5. Discovering multiple paths during route discovery
Figure 3.6. Selective RREQ forwarding process
Figure 3.7. Multiple alternative paths available for data forwarding
Figure 3.8. Flowchart for multimedia packet forwarding
Figure 3.9. Initial traffic distribution in AODV-MAP

Figure 3.10. Base layer forwarding in AODV-MAP
Figure 3.11. Enhancement layer forwarding in AODV-MAP
Figure 3.12. Route discovery process in ad hoc routing
Figure 3.13. Network Architecture for Sun's Approach
Figure 3.14. Network Architecture for AODV-MAP H-MANET
Figure 3.15. Network architecture for secure AODV-MAP H-MANET
Figure 3.16. MS Registration Process in AODV-MAP H-MANET
Figure 3.17. Fast Re-authentication process in AODV-MAP H-MANET
Figure 3.18. Network architecture for Distributed multimedia delivery network
Figure 4.1. Hierarchical Model of OPNET
Figure 4.2. System architectural Model for Wireless mobile network
Figure 4.3. Mean response time for different authentication schemes
Figure 4.4. Authentication delay for different authentication schemes
Figure 4.5. Network Model for ad hoc network
Figure 4.6. Node model for MANET node
Figure 4.7. FSM for Application manger
Figure 4.8. FSM for Routing protocol
Figure 4.9. FSM for mobility
Figure 4.10. Route discovery frequency in ad hoc routings

Figure 4.11. Average end-to-end delay in ad hoc routings
Figure 4.12. Packet delivery ratio in ad hoc routings
Figure 4.13. Normalized routing load in ad hoc routings
Figure 4.14. Packet loss rate for various scalable codings
Figure 4.15. End-to-end delay for various scalable codings
Figure 4.16. Simulation model for audio streaming over multipath MANET
Figure 4.17. Packet loss rate for different ad hoc routing schemes
Figure 4.18. End-to-end delay for different ad hoc routing schemes
Figure 4.19. Packet delivery ratio for AODV-MAP & SAODV-MAP
Figure 4.20. End-to-end delay for AODV-MAP & SAODV-MAP
Figure 4.21. Average Routing load for byte for AODV-MAP & SAODV-MAP
Figure 4.22. Packet delivery ratio for SRP and SAODV-MAP
Figure 4.23. Simulation Model for H-MANET
Figure 4.24. Packet delivery ratio for various H-MANETs
Figure 4.25. End-to-end delay for various H-MANETs
Figure 4.26. Packet loss rate for various H-MANETs
Figure 4.27. Packet delivery ratio for H-MANET with various number of gateways
Figure 4.28. Packet delivery ratio for H-MANETs in terms of security
Figure 4.29. Average latency for H-MANETs in terms of

security
Figure 4.30. NMR for Distributed media delivery networks
Figure 4.31. Average delay for Distributed media delivery networks

# *List of Tables*

Table 2.1. CODEC parameters

Table 3.1. Multiple Alternative paths for data transfer

Table 3.2. Security requirements for AODV-MAP routing

Table 3.3. Notations used for SAODV-MAP scheme

# I. Introduction

## 1. Overviews

With the recent advent in wireless technologies and mobile devices, wireless networks have become a ubiquitous communication infrastructure. Wireless communication systems [1] enable tetherless communication between a variety of nodes ranging from humans to computers. They may roughly be classified by their geographical coverage area. Cellular systems provide global coverage, and unconstrained mobility. Wireless access networks in contrast support locally constrained tetherless connectivity and mobile access to a backbone network (typically the Internet). Additionally, network service providers benefit from the relative ease and speed of deployment and the reduced costs of wiring and maintenance, which are significant advantages over traditional wireline networks. Fig 1.1 shows the types of wireless networks.

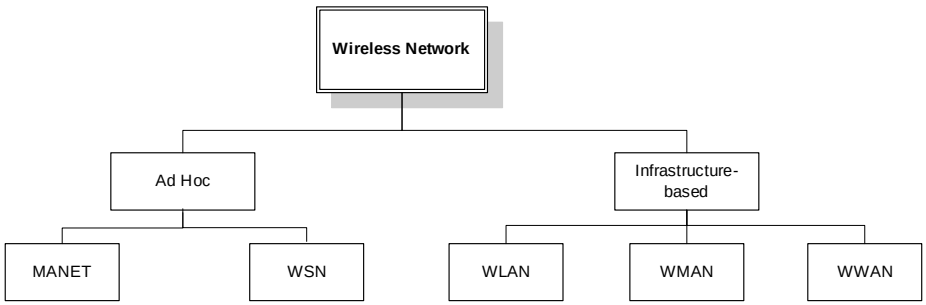



*Fig 1.1. Types of Wireless Networks*

Existing wireless access technologies range from Wireless Local area networks (WLANs), Ad hoc networks including Mobile Ad hoc networks (MANETs), and sensor network to Wireless Wide area networks

(WWAN)/ Wireless Metropolitan area networks (WMAN), which provide fixed broadband wireless access to the internet.

Among the emerging wireless technologies, IEEE 802.11 WLAN [2] have gained much popularity in various applications since its inception and is now well-positioned to complement much more complex and costly technologies such as the Third Generation (3G). A MANET [3] is a collection of mobile nodes that can communicate with each other using multihop wireless links without utilizing any fixed infrastructure and centralized management.

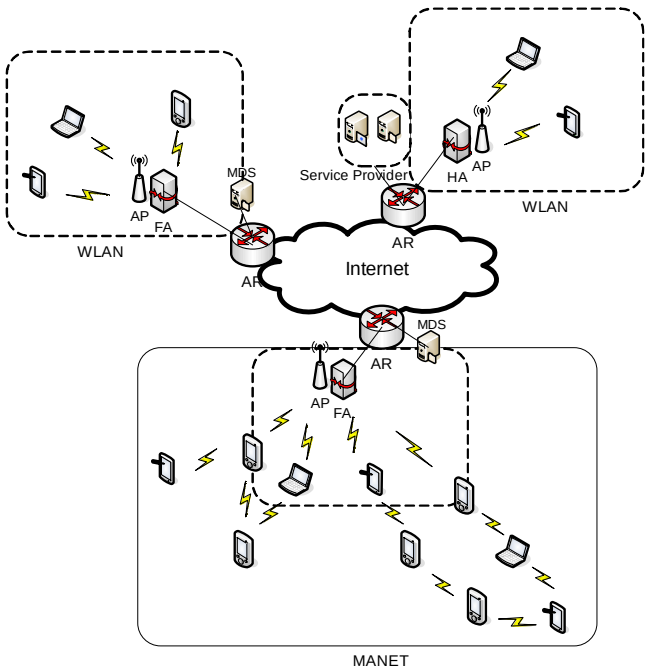



*Fig 1.2. Overviews of Ubiquitous Wireless access system*

A manifoldness of fascinating new applications are enabled if we succeed in providing mobile wireless connectivity for heterogeneous nodes. We refer to this breed of systems as ubiquitous wireless access systems, which is shown in Fig 1.2. From instance, ubiquitous network of sensors

and communication nodes in automobiles helps to substantially reduce traffic congestion and pollution by pollution aware traffic routing. This will have tremendous impact on our lifestyle and is inconceivable without ubiquitous wireless access networks. In the future, ubiquitous wireless access systems rather than human initiated communication will generate the bulk of traffic in the Internet.

## *2. Research Motivation*

Ubiquitous wireless access networks provide tetherless wireless connectivity for a variety of heterogeneous nodes. Access to the Internet is provided by specially, deployed devices called access points. The coverage of access point based wireless network is limited by the radio communication range of the deployed access points.

As wireless technology becomes more robust and sophisticated, multihop wireless networks are rapidly gaining attention. Due to the users' interests in accessing the Internet, it is an important requirement to consider the integration of multihop wireless network with the Internet. Thus, to put the multihop wireless access technology into the context of real life, we consider an Internet-based MANET, which is an evolving communication infrastructure that combines the wired Internet and wireless mobile ad hoc networks. These networks are also referred to as hybrid ad hoc networks. Multihop wireless networks thus have tremendous potential to be the technology of choice for providing ubiquitous Internet access and are applied to realistic Internet applications because of its flexible accessibility and information availability.

Even though multihop wireless networks can be deployed quickly and have the ability to self-configure and adapt to topology changes, they also present a new set of challenges. Robustness, reliability and security issues

are important factors that significantly affect the overall performance of the ubiquitous service delivery in wireless environment especially when it is connected to Internet. These issues are of particular concern given the increasing popularity of multimedia applications, such as Voice-over-IP (VoIP), audio streaming, video streaming, online gaming, and video conferencing.

In single path MANETs, previously created multi-hop route could frequently break because of node mobility and interference. New route discovery would initiate for each failure, in turn, inducing routing overheads and latency. Thus a multipath ad hoc network is a promising technique to cope with the frequent topological changes and consequently unreliable communication services. Moreover, multipath routing is effective means to achieve fault-tolerance, load balancing and reduce end-to-end delay.

Moreover, security provision for wireless system is an open and challenging research problem due to user mobility, limited resources in wireless devices and expensive radio bandwidth. Thus the increasing demand for ubiquitous Internet services imposes more security threats to communications. Some security mechanisms have implemented and some have been proposed to protect communications over ubiquitous wireless access networks.

Thus, we believe that robustness and security issues are two important challenges obstructing the widespread deployment and use of multihop wireless networks to enable ubiquitous Internet access. In order to provide ubiquitous services in wireless networks, it is essential to address the robustness and security issues in these networks.

The overall goal of this thesis is to provision robustness and security in integrated wireless multihop network with Internet for multimedia delivery.

In this research, we investigate an efficient and robust routing scheme

for isolated ad hoc network as well as an approach for global connectivity in hybrid ad hoc network. Furthermore, we present secure schemes for single hop wireless network as well as for multihop wireless network. We have considered OPNET Modeler [4] simulation tool for our research.

# 3. Thesis Overviews

## 3.1. Major Contributions

In this thesis, we address on robustness, reliability, and security issues in multihop wireless network connected to Internet which is used for efficient multimedia delivery. Thus our major contributions are as follows:

- OTP-based Authentication Framework for wireless mobile network
- Multipath ad hoc routing scheme named AODV-MAP
- Approach for traffic allocation using AODV-MAP
- Secure scheme for AODV-MAP
- Approach for Internet connectivity in AODV-MAP based Hybrid ad hoc network
- Secure framework for Internet connectivity in AODV-MAP Hybrid ad hoc network

## 3.2. Thesis Outline

The rest of this thesis is organized as follows. In Chapter 2, we describe basic background of single-hop wireless network and multihop wireless network including hybrid ad hoc network. In Chapter 3, we deal with proposed approaches for ubiquitous wireless access systems. In case of single-hop wireless network based on 802.11 WLAN, we present a secure authentication framework for mobile wireless network. In case of

multihop wireless network, we propose a multipath ad hoc routing protocol called AODV-MAP for multihop wireless network that utilizes multiple alternative paths to reduce route discovery frequency. We formulate traffic distribution strategy using AODV-MAP scheme as well as devise a secure scheme for AODV-MAP routing protocol. In this chapter, we present an approach for global connectivity in hybrid multipath ad hoc network. We also build secure framework for global connectivity in hybrid multipath ad hoc network. And we put forward AODV-MAP based distributed media delivery network.

In Chapter 4, we present analysis and evaluation of the proposed approaches. We evaluate the performance of OTP based authentication scheme for wireless mobile network. We also conduct performance evaluation of proposed multipath routing protocol (AODV-MAP) with and without security. And we analyze the use of AODV-MAP in efficient audio streaming over multipath MANET. In this chapter, we evaluate proposed approach for global connectivity in hybrid multipath ad hoc network and analyze AODV-MAP based framework for reliable distributed multimedia delivery. Finally, in Chapter 5, we conclude and mentions the future works.

# II. Background

## 1. Single-hop Wireless Network

### 1.1. Wireless LANs

Wireless local area networks (WLANs) are quickly becoming ubiquitous in our every day life. With the availability of cheap wireless solutions, they are seeing exponential growth which is expected to continue in future.

The IEEE 802.11 standard [5], which is popularly known as Wireless Fidelity "Wi Fi", specifies the Media Access Control (MAC) and physical (PHY) characteristics for devices capable of operation in the unlicensed radio frequency band of operation. The unlicensed radio frequency is divided into 2.4GHz and 5GHz. The IEEE has released a series of 802.11 WLAN standards. The term IEEE 802.11 is also used to refer to the original 802.11, which is now sometimes called "802.11 legacy". The IEEE 802.11a is an extension of the 802.11 standard that operates in the 5GHz band and uses OFDM (orthogonal frequency division multiplexing) with maximum data rate of 54Mbps. 802.11b standard uses the 2.4GHz band and has a maximum data rate of 11 Mb/s. 802.11g standard works in the 2.4 GHz band (like 802.11b) but operates at a maximum data rate of 54 Mb/s. [6] The 802.11 Task Group has been formed to develop 802.11n standard for WLAN. Its theoretical data throughput will be about 270 Mbit/s and should be up to 20 times faster than 802.11b, and up to 3 times faster than 802.11a.

IEEE 802.11 defines two types of wireless LAN configuration, which are Infrastructure (Basic Service Set) Wireless LAN and ad hoc (Independent Basic Service Set) Wireless LAN [6]. An infrastructure wireless LAN is

also a cell-based wireless LANs. In this kind of infrastructure, there will be a special node, called access point (AP), to connect one or more wireless LANs to the present wired network distributed system. Each cell is composed of an access point and several mobile nodes. The AP provides some clients in the wireless LAN to communicate to the client in another remote wireless LAN.

## *1.2. Mobile IP*

When a MN wants to roam between different WLANs, the MN needs a fixed network to access and the traffic should be redirected while the user moves to different places, so that the traffic will be redirected to the new location when the MN moves. IETF developed a standard, Mobile IP [17] to provide the described mobility. Mobile IP architecture is mainly composed of the components described as follows:

- Mobile Node (MN): A host that capable of applying while changing location. It is capable of changing its location without changing its IP address and using IP addresses to communicate with other node at any location continually.
- Correspondent Node (CN): A node that mobile node communicates with.
- Home Agent (HA): The agent on the home network of MN. When mobile node is away from home, HA will tunnels datagram and deliver packet to it, meanwhile record current location information of mobile node.
- Foreign Agent (FA): The agent on MN's visited network that de-tunnels and delivers datagram while mobile node registered. In principle, MN's registration message will send to the HA pass through the FA. FA served as a default router for registered MNs.
- Care-of-Address (CoA): The address that HA forwards the mobile IP packet. When a mobile node employs FA, the foreign agent will provide

a Care-of-Address for multiple nodes, if a mobile node does not use an FA, the Care-of-Address will be the address of the MN. In this case, it is so called a Co-located Care-of-Address (Co-CoA).

Under most circumstances, IP address indicates the location of a device. Users need to change IP to move to a new network while applying mobile devices and it became a challenge to current packet delivery. Mobile IP records the two IP addresses related to the mobile device to offer transparent mobility: the home address located in the home network and the changeable CoA located in the network user presently connected. Many applications need a fixed IP address first so all data traffic could be sent to the home network where a HA located. The HA compresses the incoming packets and forwards them to the CoA. After the FA receives the packet, it will compress and deliver the packets to the foreign network to reach the MN. Since receivers usually do not verify the sender, the traffic could be sent from the user directly to the host without passing the HA. Fig. 2.1 shows the architecture and working principle of Mobile IPv4.

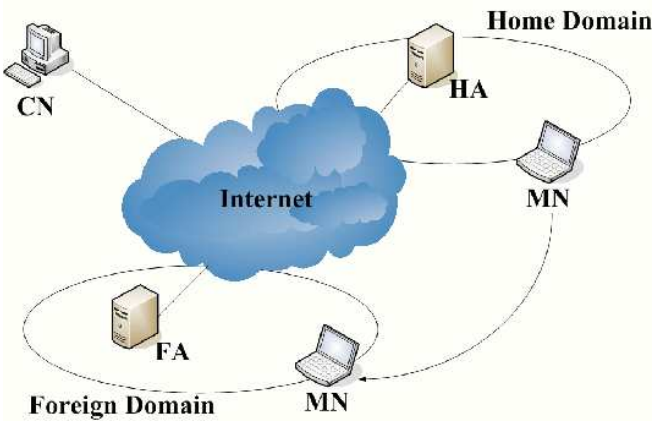



*Fig 2.1. Mobile IPv4 Architecture*

Although Mobile IPv4 provided the ability of IP mobility, its still has some shortcomings such as limited address space, triangle routing, and handoff packet lose, signaling cost and signaling delay. In order to improve the shortcomings of Mobile IPv4, Mobile IPv6 protocol [18] has been proposed.

## *1.3. Security Issues in Single-hop Wireless Network*

### *a. Security in Wireless LAN*

With the advent of wireless LANs, arises the issue of security in a wireless environment. As regards the security of WLAN, The IEEE 802.11 standards specify the Wired Equivalent Privacy (WEP) for link layer security. [7] However, due to the publication of the standard, WEP have been addressed of having many existing weaknesses. Therefore, WEP is not considered useful today. As WEP is known to be vulnerable, [8] other security protocols such as WPA and IEEE 802.11i are being developed to offer the higher level of privacy. [9] The 802.11i specification [10] includes both RC4-based encryption Temporal Key Integrity Protocol (TKIP) and AES (Advanced Encryption Standard) based algorithm [11] called the Counter Mode CBC-MAC Protocol (CCMP) for encryption and integrity protection, and 802.1x [12] for authentication and key distribution. The TKIP is an interim solution to fix the known problem with WEP, which is compatible with 802.11 products. Although TKIP is much securer than WEP, it is not considered as secure as the AES solution.[13]

The 802.1x [12] is a port-based network access control mechanism, which uses the Extensible Authentication Protocol (EAP) [14] for end-to-end mutual authentication between a Mobile Station and an Authentication Server. IEEE 802.1x defined a special frame format called

EAP over LAN (EAPOL) to allow EAP message to be sent over the LAN before higher layer protocol. By using EAPOL, an unauthenticated user can deliver authentication packet to the AP for further authentication procedure. The EAP authentication takes place between MN (mobile node) and AS (Authentication Server) and is transparent to the AP. After the AP received EAP message, the AP will encapsulates the EAP message in an AAA protocol, e.g. in RADIUS or DIAMETER and forward to the AS. Once the authentication is successful, the AS will send a RADIUS/DIAMETER-Access Accept message to the AP. AP will know that the user has been authenticated by the AS and then send EAP-Success message to the MN. As a result, the AP starts forwarding data to/from the MN.

EAP is a point-to-point protocol, and it is mainly used to provide extra authentication mechanism for remote login. The advantage of using EAP is that it allows many different methods of authentication to be used. Based on different security requirement and user consideration, EAP provides different authentication mechanism to be transported. The following is the examples of EAP mechanisms: [15]

- EAP-MD5: base on MD5-Challenge handshake authentication.
- EAP-TLS: Base on SSL v3.0, for certificate-based authentication
- EAP-SIM: for GSM SIM-based authentication.
- EAP-AKA : for UMTS USIM-based authentication

EAP-Transport Layer Security (EAP-TLS) defined in IETF RFC 2716 [16] is a Point-to-Point Protocol (PPP) extension supporting additional authentication methods within PPP. EAP-TLS is based on a certificate approach, and requires trusted Certificate Authorities (CAs). The security of EAP-TLS thus depends on the security of Transport Layer Security (TLS), well-know, well tested and widely used cryptographic protocol,

which is a standardized version of Secure Socket Layer (SSL) protocol. EAP-TLS supports mutual authentication between the client and the AS if the client also has a certificate signed by a CA that the AS trusts.

In wireless mobile networks, the challenges of authentication lie in obtaining the credentials, such as keys, for MN authentication when MNs are roaming among wireless networks. To provide efficient and secure authentication in wireless IP networks, authentication architecture and authentication scheme are two main issues. The objective of authentication architectures is to provide secure interconnection between wireless networks. The authentication scheme is designed to verify the user and generate credentials with mutual trust. Since the mutual trust is to protect the communication between networks and MNs, authentication process is necessary to provide security.

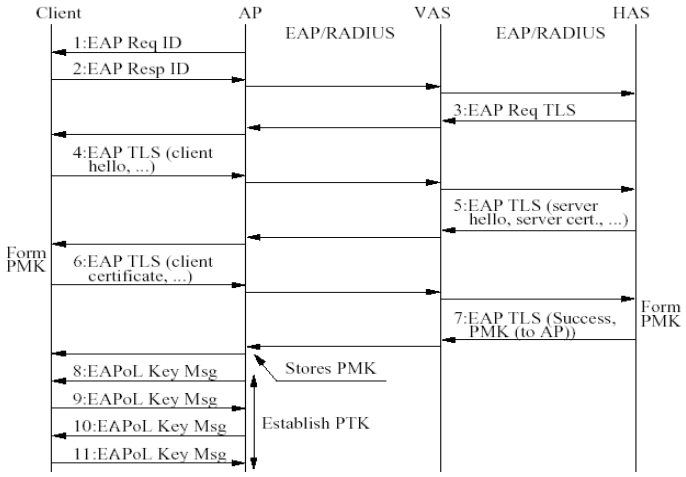



*Fig 2.2. Overviews of EAP-TLS procedure*

EAP-TLS also derives a per-session key between the AP and the client after successful TLS authentication. Authentication overview of EAP-TLS procedure is shown in Fig. 2.2.

### *b. Related Security Theory*

We address some related cryptographic theories involved in our study. While the need for encryption is typically fulfilled by employing appropriate cryptographic mechanisms, e.g. shared secret keys, authentication functions and protocols are implemented at different layers of TCP/IP protocol stack. [19]

- Authentication Functions: There are two main classes of authentication functions, which produce an authenticator, a value that is used to verify the identity of an entity such as a device or user. It is assumed that the key, used in the following techniques, is known only to the claimant (entity being authenticated) and the verifier.
- Message Encryption: The ciphertext of the message is used as the authenticator since only authorized entities would have possession of the encryption key. Either symmetric or asymmetric (public key) encryption can be used. While symmetric encryption provides confidentiality and authentication, asymmetric encryption, which employs a public-private key pair, provides support for non-repudiation as well. This security service is realized by having the initiator create a digital signature by encrypting the MAC of a message with his/her private key.
- Keyed-Hash Message Authentication Code (HMAC): Providing a way to check the integrity of information transmitted over in an insecure network environment is a very important issue. The "Message authentication codes" (MAC) mechanism is used to provide such integrity check based on a secret key. In general, message authentication codes are used between two parties that share a secret key in order to validate information transmitted between these parties. A MAC mechanism based on cryptographic hash functions is called HMAC which is described in RFC 2104 [20]. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in

combination with a secret shared key. In other words, the two parties that share a secret key can use HMAC to achieve the message integrity checks. The most common form of HMAC is as follows: *Hash (key, Hash (key, message)) or* $MAC_K(M)$

- Digital Signature: The digital signature presents a digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message is exactly who he or she claims to be. Digital signature is especially vital for electronic commerce and is a key component of most authentication schemes. To be effective, digital signatures must be unforgettable.
- Hash Chaining: Lamport [21] proposed one-time password/ hash chaining technique. Let's assume $h(s)$ be a one-way function and compute $h^m(s) = h(h.(h(s)..))$. Next, generate a digital signature of $h^m(s)$ and send to authenticator. When the claimant logins the system, it sends the *ith* password which equals $h^{m-i}(s)$ to some fixed message $s$. Then the authenticator will authenticate it by computing $h(h^{m-i}(s))$ and subsequently memorizing the last password sent by the claimant. Only the claimant knows the seed $s$, so the claimant can prove itself to authenticator for $m$ times and generate one-time password in each authentication; moreover, each hash chaining value can be taken as the non-repudiation evidence.

# 2. Multihop Wireless Network

## 2.1. Wireless Ad hoc Network

Wireless ad hoc network, both mobile ad hoc network and sensor network, is emerging as an important area for new developments in the ubiquitous network. A mobile ad hoc network (MANET) [26] is a system

of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies allowing people and devices to internetwork without any preexisting communication infrastructure as shown in Fig 2.3. For the nodes that are not within the direct communication range, other nodes in the network work collectively to relay packets for them.

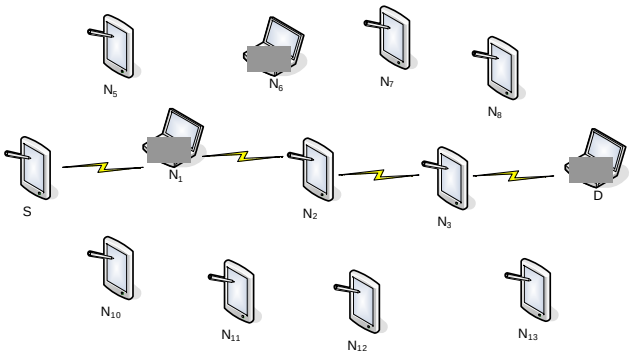



*Fig 2.3. Overviews of Ad hoc Network*

A MANET is characterized by its dynamic topological changes, limited communication bandwidth, and limited battery power of nodes. MANETs have received tremendous attention in the past few years.

## 2.2. Routing in Ad hoc Networks

Routing in ad hoc networks is clearly different from routing found in traditional infrastructure networks. Routing in ad hoc networks needs to take into account many factors including topology, selection of routing path and routing overhead, and it must find a path quickly and efficiently. Ad hoc networks generally have lower available resources compared with infrastructure networks and hence there is a need for optimal routing.

In wireless ad hoc networks, the communication range of a node is often limited and not all nodes can directly communicate with one another. Nodes are required to relay packets on behalf of other nodes to allow communication across the network. Since there is no pre-determined

topology or configuration of fixed routes, an ad hoc routing protocol is used to dynamically discover and maintain up-to-date routes between communicating nodes.

Designing a routing protocol for ad hoc networks is challenging because of the need to take into account two contradictory factors: a node needs to know at least "reachability" information to its neighbors for determining a packet route; and the network topology can change quite often.

According to their routing strategy, existing ad hoc routing protocols can be generally categorized into three classes: table-driven (or proactive), on-demand (or reactive), and hybrid.[27]

Proactive protocols require that nodes in a wireless ad hoc network should keep track of routes to all possible destinations so that when a packet needs to be forwarded, the route is already known and can be used immediately. Any changes in topology are propagated through the network, so that all nodes know of those changes in topology. Examples include Destination Sequenced Distance vector (DSDV) routing [28], Wireless Routing Protocol (WRP) [29], and Optimized Link State Routing protocol (OLSR) [30].

On-demand protocols only attempt to build routes when desired by the source node so that the network topology is detected as needed (on-demand). When a node wants to send packets to some destination but has no routes to the destination, it initiates a route discovery process within the network. Once a route is established, it is maintained by a route maintenance procedure until the destination becomes inaccessible. Examples include Ad hoc On-demand Distance Vector routing (AODV) [31], and Dynamic source routing (DSR) [32].

Proactive protocols have the advantage that new communications with arbitrary destinations experience minimal delay, but suffer the

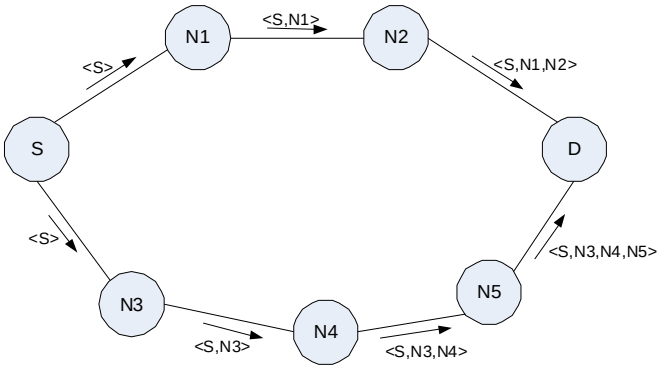
disadvantage of the additional control overhead to update routing information at all nodes. To cope with this shortcoming, reactive protocols adopt the inverse approach by finding a route to a destination only when needed. On-demand routing protocols adapt well with dynamic topology of wireless ad hoc networks, due to their lower control overhead and quick response to route break. Reactive protocols often consume much less bandwidth than proactive protocols, but they will typically experience a long delay for discovering a route to a destination prior to the actual communication. However, because reactive routing protocols need to broadcast route requests, they may also generate excessive traffic if route discovery is required frequently.

### *a. Dynamic source routing*

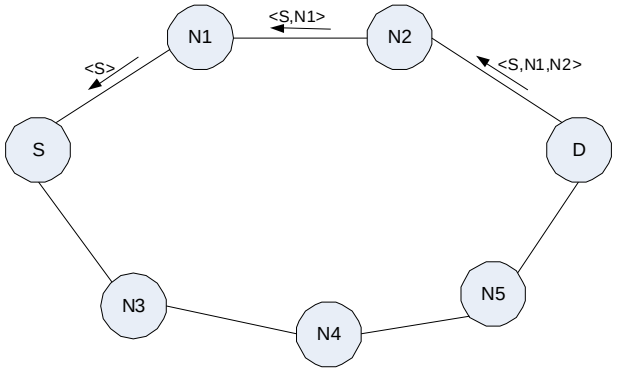
Dynamic source routing (DSR) [32] is an on-demand routing protocol for wireless ad hoc networks. DSR is based on the concept of source routing, in which a source node indicates the sequence of intermediate routes in the header of a data packet. The operation of DSR can be divided into two procedures: route discovery and route maintenance.

Each node in the network keeps a cache of the source routes that it has learned. When a node needs to send a packet to some destination, it first checks its route cache to determine whether it already has an up to date route to the destination. If no route is found, the node initiates the route discovery procedure by broadcasting a route request (RREQ) message to neighboring nodes. The RREQ contains the address of the source and destination nodes, a unique identification number generated by the source node, and a route record to keep track of the sequence of hops taken by the RREQ as it is propagated through the network. When an intermediate node receives a route discovery request, it checks whether its own address is already listed in the route record of the RREQ. If not, it

appends its address to the route record and forwards the RREQ to its neighbors. Fig 2.4a illustrates the formation of the route record as the RREQ propagates through the network.




*a. RREQ propogation*




*b. RREP propogation*

*Fig 2.4. Route Discovery in DSR*

When the destination node receives the RREQ, it appends its address to the route record and returns it to the source node within a new route reply (RREP) message. If the destination already has a route to the source, it can use that route to send the reply; otherwise, it can use the route in the RREQ to send the reply. The first case is for situations where a network might be using unidirectional links and so it might not

be possible to send the reply using the same route taken by the route request message. Fig. 2.4b shows the transmission of route record back to the source node.

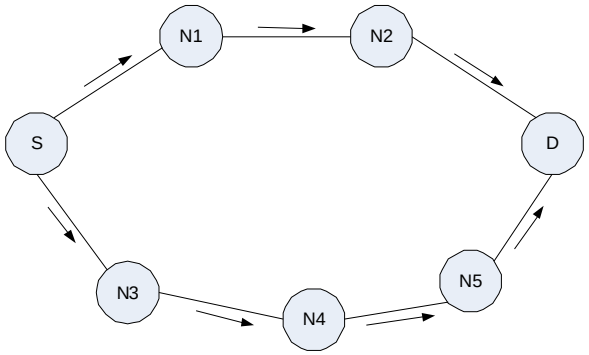
Route maintenance uses route error (RERR) messages and acknowledgement messages. If a node detects a link failure when forwarding data packets, it creates a RERR and sends it to the source of data packets. When the source node receives the RERR, it removes all routes from its route cache that have the address of the node in error. It may initiate a route discovery for a new route if needed. In addition to RERR message, acknowledgements are used to verify the correct operation of links.

### *b. Ad Hoc On-demand Distance Vector Routing*

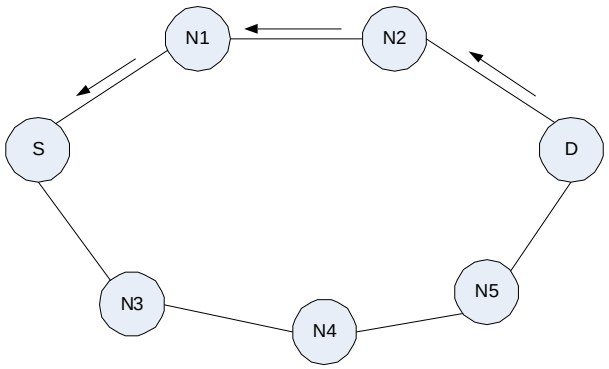
Ad hoc on-demand distance vector (AODV) routing [31] adopts both a modified on-demand broadcast route discovery approach used in DSR and the concept of destination sequence number adopted from DSDV.

When a source node wants to send a packet to some destination and does not have a valid route to that destination, it initiates a path discovery process and broadcasts a route request (RREQ) message to its neighbors. The neighbors in turn forward the request to their neighbors until the RREQ message reaches the destination or an intermediate node that has an up-to-date route to the destination. Fig 2.5a illustrates the propagation of the broadcast RREQs in an ad hoc network.

In AODV, each node maintains its own sequence number and a broadcast ID. Each RREQ contains the sequence numbers of the source and destination nodes and is uniquely identified by the source node's address and a broadcast ID. AODV utilizes destination sequence numbers to ensure loop-free routing and use of up-to-date route information.




*a. RREQ propogation*




*b. RREP propagation*

*Fig 2.5. Route Discovery in AODV*

Intermediate nodes can reply to the RREQ only if they have a route to the destination whose destination sequence number is greater or equal to that contained in the RREQ. So that a reverse path can be set up, each intermediate node records the address of the neighbor from which it received the first copy of the RREQ, and additional copies of the same RREQ are discarded. Once the RREQ reaches the destination (or an intermediate node with a fresh route) the destination (or the intermediate node) responds by sending a route reply (RREP) packet back to the neighbor from which it first received the RREQ. As the RREP is routed

back along the reverse path, nodes along this path set up forward path entries in their routing tables (Fig 2.5b).

When a node detects a link failure or a change in neighborhood, a route maintenance procedure is invoked:

- If a source node moves, it can restart the route discovery procedure to find a new route to the destination.
- If a node along the route moves so that it is no longer connectable, its upstream neighbor sends a link failure notification message to each of its active upstream neighbors. These nodes in turn forward the link failure notification to their upstream neighbors until the link failure notification reaches the source node.

## *2.3. Multipath Ad Hoc Routing*

Multipath ad hoc routing enables to find multiple paths between a source and a destination in a single route discovery. [33] Multipath ad hoc routing has drawn extensive attention in MANETs recently.

### *a. Need of Multipath ad hoc routing*

The network topology of a MANET can change frequently and dramatically. One reason is that nodes in a MANET are capable of moving collectively or randomly. When one node moves out of/in to the transmission range of another node, the link between the two becomes down/up. Another reason that causes the topological changes is the unstable wireless links, which might become up and down due to the signal fading (obstacles between the two end nodes), interference from other signals, or the changing of transmission power levels. Most of the mobile nodes are battery powered, when the nodes run out of the battery power, the node failure will also cause the topological changes.

The dense deployment of nodes in MANETs makes the multipath

routing a nature and promising technique to cope with the frequent topological changes and consequently unreliable communication services.

The authors [34] proved that the use of multiple paths in DSR can keep correct end-to-end connection for a longer time than a single path. Therefore, by keeping multiple paths to a destination, frequency of costly route discovery is much lower. Moreover, in a single path routing case, when a node fails to transmit a packet to its next hop, a route error message will be sent back to the source indicating breakage of the path. With multiple paths available, nodes can actively salvage the packet by sending it to an alternate path, a route error will occur only when all the available paths fail. Although the search for multiple paths may need more route request messages and route reply messages in a single route discovery process, number of overall routing messages is actually reduced.

Two primary technical focuses in this area are, (a) multipath routing protocols that are able to find multiple paths with desired properties, and (b) policies on usage of multiple paths and traffic distribution among multiple paths. In order to achieve fault-tolerance and robustness of data delivery, to improve reliability, to balance traffic load, to reduce the end-to-end delay and frequency of route discoveries, and to improve the network security, multipath routing protocols are required.

Multipath routing in MANET was originally developed as a means to provide route failure protection. For example, DSR protocol is capable of caching multiple routes to a certain destination. When the primary path fails, an alternate one will be used to salvage the packet. Temporally Ordered Routing Algorithm (TORA) [35] also provides multiple paths by maintaining destination-oriented directed acyclic graph (DAG) from the source node. Multipath extensions of single path routing protocols have also be proposed, such as Alternative Path Routing (APR) [36], Split Multipath Routing (SMR) [37], and AODV-BR [38].

### *b. Benefits of Multipath Routing*

We outline some of the applications of multipath routing that improve the performance of ad hoc networks. In order to achieve performance benefits from multipath routing algorithm, it depends not only on the availability of the desired multiple paths but also on the capability of the multipath finding technique.

Multipath routing protocols can provide fault tolerance by having redundant information routed to the destination via alternative paths. This reduces the probability that communication is disrupted in case of link failure. More sophisticated algorithms employ source coding to reduce the traffic overhead caused by too much redundancy, while maintaining the same degree of reliability. This increase in route resiliency is largely depended on metrics such as diversity, or disjointness, of available paths.

Another way of using multiple paths is to have the traffic flow through multiple paths simultaneously. By splitting data to the same destination into multiple streams, each routed through a different path, the effective bandwidth can be aggregated. This strategy is particular beneficial when a node has multiple low bandwidth links but requires a bandwidth greater than an individual link can provide. End-to-end delay may also be reduced as a direct result of larger bandwidth.

Another benefit of multipath routing is reduction of routing overhead. An important objective of multipath routing is to provide quality of service, more specifically, to reduce the end-to-end delay, to avoid or alleviate the congestion, and to improve the end-to-end throughput, etc. It has been shown that multipath routing helps significantly in providing QoS by reducing the end-to-end delay for packet delivery. [39] There are two types of latency caused particularly by ad hoc on-demand routing protocols. One is the latency the protocol takes to discover a route to a

destination when there is no known route to that destination. Multipath routing effectively reduces frequency of route discovery therefore the latency caused by this reason is reduced. The other one is the latency for a sender to recover when a route being used breaks. The latency caused by route errors is a significant component in the overall packet latency. Multipath routing reduces the occurrence of route errors therefore the packet latency is further reduced.

Some efforts have been made to improve the network security by using multipath routing.

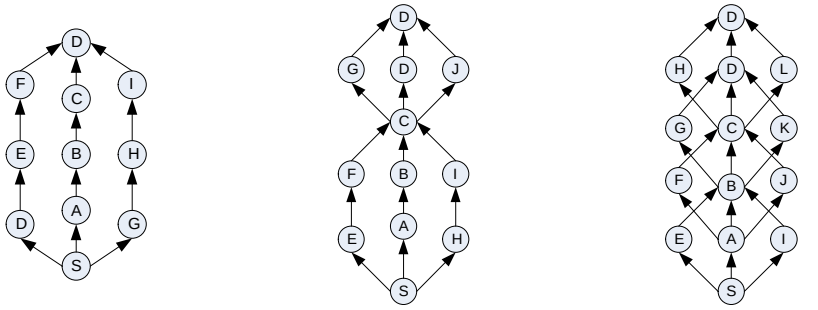
### *c. Multiple path Selection Criteria*

The multipath routing protocol is a promising technique to overcome problems of frequent topological changes and link instability since the use of multiple paths could diminish the effect of possible node and link failures. There are various criteria a protocol can use when selecting multiple paths such as disjointness, path selection, handling duplicate route request. However, creating multiple paths in the wireless ad hoc network efficiently with desired property still remains a key challenge in research.

Disjoint

Different multipath routing protocols have different approaches to create multiple paths. Depending on how much the created paths are disjointed from each other, we can classify the paths in three categories: [33] a. Non-disjoint path; b. Node-disjoint path c. Partially disjoint path. (Fig 2.6)

In creating non-disjoint paths, we do not care of joint points of the path. Instead, the algorithm focuses on finding the paths as more as possible. Node-disjoint paths do not have any nodes in common, except the source and destination.




a. Node-disjoint path b. Link-disjoint path c. Fail-safe path

*Fig 2.6. Types of multiple alternative paths*

In case of partially disjoint path, it depends on certain factors. One type of partially disjoint paths is link-disjoint path, which does not have common links, but may have nodes in common. Another partially disjoint path is a fail-safe alternate path [40]. It is a path between source and destination if it bypasses at least one intermediate node on the primary path. Fail-safe multiple paths are different from node-disjoint and link-disjoint multiple paths, in the sense that fail-safe route paths can have both nodes and links in common.

The higher degree of disjunction, the probability of simultaneous failure of all paths decreases. It is due to rare chance of locating of two disjoint paths near same source of noise or error. In contrast, probability of an internal competition for acquiring the shared channel becomes more when the routes have more joint points. Furthermore, two joint factors define to measure joint degree of routes: [41] correlation (the number of links connecting disjoint paths) and coupling (average number of blocked nodes by other ongoing transmissions).

Given the trade-offs between using node-disjoint and non-disjoint routing paths, partially disjoint path may offer a better compromise between two extremes.

Path selection

In the case of single path routing, the destination is responsible for path selection. For multipath routing, one approach is that after receiving all RREQ packets, the destination chooses the desired routes and sends them towards source node by means of RREP packet [42] [43] [44]. Another approach is that the intermediate nodes can participate in the process of selecting the paths in a distribute manner [45] [46] [47] [48].

Handling duplicate RREQ

One of important issues in multipath routing is to handle a duplicate RREQ by the intermediate node. A duplicate RREQ has probably passed more hops to reach destination than previous RREQ. In consequence, it has traveled longer distance and can be a good candidate for rejection. On the other hand, re-broadcasting of it could provide us by more alternate route paths. However, re-broadcasting may cause increase in RREQ transmission, in turn, broadcast storm. Hence, the intermediate nodes should handle duplicate RREQ packets more carefully.

## *2.4. Multimedia Streaming over MANET*

### *a. Real-time Transport Protocol*

Real-time transport protocol (RTP) [54] is IP-based protocol providing support for the transport of real-time data such as video and audio. Thus RTP provides end-to-end delivery services for data with real-time characteristics. The services provided by RTP include time reconstruction, loss detection, security and content identification. But RTP itself does not provide any mechanism to ensure timely delivery. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. RTP applications usually run it on top of a transport

protocol such as UDP (User Datagram Protocol). [55]

RTP is designed to work in conjunction with the auxiliary control protocol, Real-Time Control Protocol (RTCP), to get feedback on quality of data transmission and information about participants in the on going and to provide minimal control over the delivery of the data. RTCP provides support for real-time conferencing of groups of any size.

### *b. Secure Real-time Transport Protocol*

The Secure Real-time Transport Protocol (SRTP) [56] was designed to create an efficient security solution for the RTP, which would work in constrained environments. So SRTP offers confidentiality, authenticity, integrity and replay protection for RTP and RTCP packets, providing all the important elements to secure a media stream. Fig 2.7 shows overview of the SRTP packet.

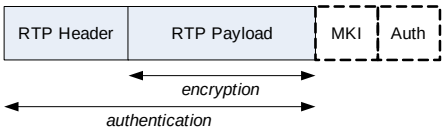



*Fig 2.7. Overviews of SRTP packet*

Confidentiality protection is achieved by encrypting RTP payload and integrity protection is achieved by applying a message authentication code (MAC) on the RTP packet. To make it easier to synchronize switching of keys for SRTP, especially when multiple streams share the same keys, an optional Master Key Identifier (MKI) can be used, with variable size. And for efficiency reasons and to avoid error-propagation the encryption algorithm currently defined is AES, but in a stream cipher mode. HMAC/SHA-1 is used for message authentication. To preserve bandwidth, the output message authentication tag is by default truncated to 4 bytes.

### *c. Challenges and Issues in media streaming over MANET*

For media streaming over MANET, the transmission delay budget is tight due to multihop routing and high bit error rates. Also the packet loss rate can be very high under adverse conditions, such as high channel noise or heavy traffic with multiple concurrent communication sessions causing a high collision rate. Generally, re-transmission of packets is not desirable for voice over MANETs since it adds extra delay and wastes bandwidth. Furthermore, communication might be lost if the packet loss rate is too high or a communication link is considered broken.

To meet these challenges, effective network protocols and audio processing techniques are needed. Following network measurements are commonly used to objectively evaluate performance:

- Packet loss rate is the fraction of transmitted packets from the source that are not received at the destination.
- Jitter is the random variation of the packet inter-arrival time at the destination. Jitter can be many tens of milliseconds in 802.11. A jitter buffer at the receiving end can control trade-off between speech quality and delay.
- End-to-end packet delay is difference between packet transmission time at the source and its reception time at the destination.

### *d. Voice CODEC Standards*

While a Voice-over-IP (VoIP) device can accept a digital call directly, a coder-decoder (CODEC) must convert analog calls before they can be transported over a packet-switched network. To transmit voice data over data network, the voice data must first be digitized and then compressed into small units known as packets. The compression algorithm determines the size and the transmission interval of these packets.

In order to transport these voice packets over the network, they are

encapsulated as RTP packets using UDP as the transport protocol. These protocols incur an overhead of 40 bytes for each packet sent.

The most popular coding standards for telephony and voice packet are: G.711, G.723.1 and G.729. [22] Table 2.1 summarizes their characteristics.

| CODEC | Bit rate (kbps) | Framing size (ms) | Compression delay (ms) | Data size (bytes) | IP packet size (bytes) | Packet interval (ms) |
|---|---|---|---|---|---|---|
| G.711 | 64 | 0.125 | 5 | 240 | 280 | 30 |
| G.723.1 | 5.3/6.3 | 10 | 30 | 24 | 64 | 30 |
| G.729 | 8 | 10 | 15 | 20 | 60 | 20 |

*Table 2.1 - CODEC parameters*

### *e. Scalable audio coding*

Scalable audio coding [57] consists of a minimum rate bit stream that provides acceptable coded speech quality, along with one or more enhancement bit streams, which when combined with a lower rate coded bit stream, provide improved speech quality. Fig. 2.8 shows the typical diagram of a scalable speech coding system. Basically, there are four scalable mechanisms: data partitioning, temporal scalability, SNR scalability, and spatial scalability.

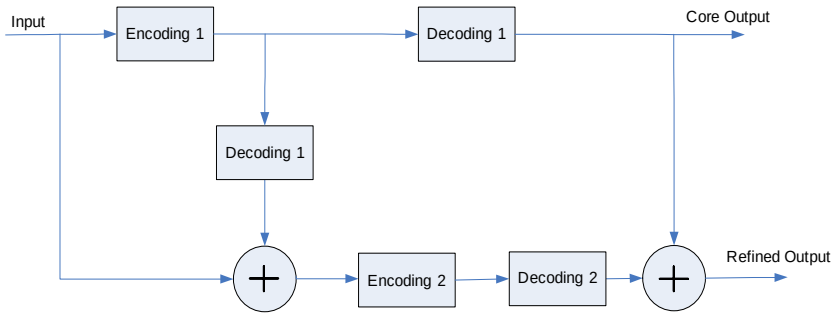



*Fig 2.8. Typical Diagram of Scalable audio coding system*

The standards for scalable speech coding are G.727 [58], and the

MPEG-4 speech coding tools [59]. The G.727 speech coding standard [58] is based upon adaptive differential pulse code modulation (ADPCM) and operates at data rates of 16, 24, 32, and 40 kbps. The core bit rate is 16kbps, and up to three 8 kbps enhancement layers can be included.

MPEG-4 Natural Speech Coding Tool Set [59] provides a generic coding framework for wide range of applications with speech signals. Its bitrate coverage spans from as low as 2 kbit/s to 23.4 kbit/s. Two different bandwidths of input speech signal are covered, namely, 4 kHz and 7 kHz.

MPEG-4 coding contains two algorithms: HVXC (Harmonic vector excitation coding) and CELP (Code excited linear predictive coding). HVXC is used at a low bitrate of 2 or 4 kbit/s. Higher bitrates than 4 kbit/s in addition to 3.85 kbit/s are covered by CELP. The algorithmic delay by either of these algorithms is comparable to that of other standards for two-way communications; therefore, MPEG-4 Natural Speech Coding Tool Set is also applicable to such applications. The bit rate scalability of any of these core layer bit rates is possible in increments of 2 kbps, with up to three enhancement layers.

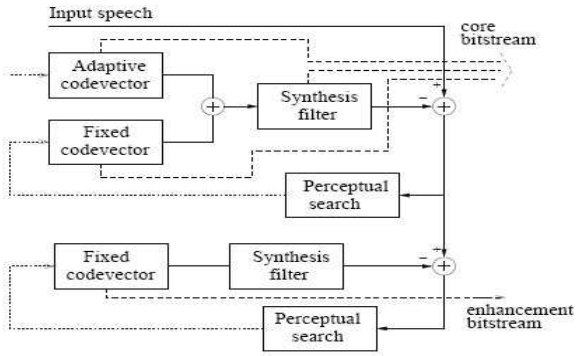



*Fig 2.9. MPEG-4 CELP bit rate (SNR) scalable coder*

The block schema of MPEG-4 CELP bit rate (SNR) scalable coder is shown in Fig. 2.9.

### *f. Selective Encryption*

Selective encryption is a technique wherein only a selected subset of the transmitted data is protected and the remainder of the data stream is sent in the clear. By not encrypting the entire data stream, valuable node resources can be conserved.

Basic requirement in selective encryption is to encrypt some media packets and not encrypt some other. This requires that every packet shall carry an indicator which indicates whether packet is encrypted or not. This does not interfere with other security requirements, like message integrity or authentication of source etc. The scalable coding scheme with selective encryption is depicted in Fig. 2.10.

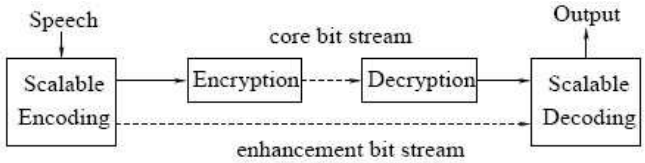



*Fig 2.10. Scalable coding with selective encryption*

The authors [60] have suggested some enhancements to SRTP protocol in order to enable SRTP to support selective encryption. SRTP uses a optional parameter called MKI (Master Key Index) in every SRTP packet. Current definition of SRTP protocol defines security context at both the ends of communication which is established using other mechanisms and also creates master key. Master key is used to create session keys for encryption and integrity. SRTP allows multiple master keys to be used to provide enhanced security features where master key can be changed during media communication over SRTP by indicating different MKI value in SRTP stream. However, it does not include encryption (cipher) algorithm to be part of MKI, so basically while establishing security

context at both ends of the communication, cipher algorithm is negotiated and multiple master keys are established and all the keys uses same cipher suite. SRTP also allows NULL encryption to be supported as valid cipher algorithm.

If SRTP definition is changed by linking encryption algorithm to the master key and each master key can hold its own cipher algorithms, SRTP can support selective encryption without changing protocol syntax.

In order to support selective encryption between two endpoints, security context establishment shall establish at least two master keys (two MKI values) and one of the master key carries a cipher algorithm and other one uses NULL Cipher. During RTP packet processing by SRTP stack, if encryption for that packet is needed, MKI value will be set to the one that has cipher algorithm attached and if encryption is not needed, MKI value will be set to one that has NULL Cipher.

## *2.5. Security Issues on Ad hoc routing*

Routing security is a challenging task in mobile ad hoc networks since the lack of fixed infrastructure makes routing an obvious target for adversaries.

### *a. Security Attributes*

To classify different security needs for applications of ad hoc networks, the following attributes are considered,

- Authentication: not only it matters to keep the information safe from eavesdroppers or otherwise unauthorized users. The need for knowing that the sender is actually who claims to be is important security issue for ad hoc networks.
- Integrity: when the information is sent through a wireless link, risk is that malicious attackers could change some important data and re-sends.

The integrity is ability of the network to guarantee that received message has not been forged or modified.

- Non-Repudiation: It is the ability not to be able to deny sending a message. This may be of great importance in some situations.

### *b. Threats and attacks on ad hoc routing protocols*

Some attacks on ad hoc routing protocols are as followings.[67] [68]

#### *Attacks using modification*

One of the simplest ways for a malicious node to disturb good operation of ad hoc networks is to announce better routes than the other nodes. This kind of attack is based on modification of metric value for a route or by altering control message fields.

- Redirection by changing route sequence number: In ad hoc networks, like in wired networks, better path to reach a destination node is determined by a specific value, which is the metric. Smaller this value is, better is the route. That's why a simple way to attack a network is to change this value with a smaller number than the last "better" value.
- Redirection with modified hop count: When a node cannot decide what the best route is regarding to different metrics, it can use number of hops to decide which path is the best route to reach a specific node. In AODV protocol, it uses hop count value to determine the best route. A malicious node can disturb the network by announcing the smallest hop count value to reach the node. In general, hackers use value zero to be sure to have the smallest hop count value.
- DoS attacks with modified source routes: In DSR, it utilizes source routes, thereby explicitly stating routes in data packets. These routes lack any integrity checks and a simple DoS attack can be launched by altering the source routes.

- Tunneling: Ad hoc networks have implicit assumption that any node can be located adjacent to any other node. This leads to a type of attack, called tunneling, where two or more nodes may collaborate to falsely represent the length of available paths by encapsulating and tunneling between them legitimate routing messages generated by other nodes. In this case, tunneling prevents honest intermediate nodes from correctly incrementing metric used to measure path lengths.

*Attacks using impersonation*

These attacks are called spoofing since the malicious node hide its real IP address or MAC address and uses another one. As ad hoc routing protocols like AODV and DSR do not authenticate IP address, a malicious node can launch many attacks by using spoofing.

*Attacks using fabrication*

- Falsifying route error messages: This attack is quite common in AODV and DSR because these protocols use route maintenance to recover good path when nodes move away. When a node moves, the closest node sends an "error" message to others to inform that the route is no more available. If a malicious node usurps the identity of another node by using spoofing and send error messages to others, these nodes will update their routing tables with this information.
- Route cache poisoning: This is a passive attack that can occur in DSR especially because of promiscuous mode of . In addition to learning routes from headers of packets, routes in DSR may also be learned from promiscuously received packets. A node overhearing any packet may update its routing table, even if that node is not on the path from source to destination. Vulnerability is that an attacker could easily exploit this method of learning routes and poison route caches.

*Attacks by dropping packets*

- Black hole and Grey hole attack: In black hole attack, the attacker sends out forged routing packets. It can setup a route to some destination via itself and when the actual data packets get in they are simply dropped, forming a black hole where data enters but never leaves. Another possibility is for the attacker to forge routes pointing into an area where the destination node is not located. Everything will be routed into this area but nothing will leave, thus creating a black hole. A special case of black hole attack is a grey hole. In this attack, the adversary selectively drops some kinds of packets but not other. For example, the attacker might forward routing packets but not data packets.

### *c. Vulnerabilities of multipath routing protocols*

Several vulnerabilities or security attacks may affect route discovery of multipath routing protocols, allowing a small set, or even a single malicious node, to control the routing paths of critical nodes.[69]

*Racing phenomenon*

With several multipath routing protocols, each intermediate node processes each RREQ only the first time it receives. Then, it drops any succeeding duplicates RREQ. This happens despite the fact that a succeeding instance of already processed RREQ may have propagated through a different path. Whether such protocols discover the complete set of node-disjoint paths, depends on the racing conditions of RREQ propagation through different paths. If an intermediate node happens to receive first RREQ that prevents discovery of another path that belongs to set of node-disjoint paths, then RREQ will end up without discovering all existing disjoint paths. Note that a node that experiences the racing

phenomenon will behave as if it was under Rushing attack [70], even though no malicious acts take place.

*Impersonation and lack of authentication*

If a protocol requires only end-to-end authentication and intermediate nodes participating in a routing path are not authenticated, then the protocol is subject to impersonation sybil attacks [71], under which a malicious node may present multiple identities. In this way, a malicious node may participate in more than one, seemingly node-disjoint, routing paths, by presenting different identity in each path. The adversary may then compromise a small fraction of nodes in selected areas of the network to control routing paths. The effects of this attack can be maximized if it is combined with "black-hole" attack, where the attacker responds to all route requests, with non-existent short path links. Then, adversary may manipulate communication by dropping all routing paths.

*Invisible node attack*

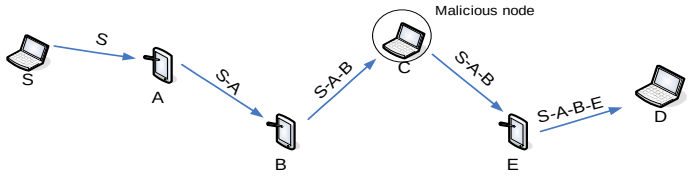



*Fig 2.11. Invisible node attack*

The broadcast nature of ad hoc network makes multipath routing protocols subject to a special case of Man-In-the-Middle attack, the invisible node attack [72]. In this situation, a malicious node does not reveal its presence in the routing path. Instead, the invisible node silently repeats communication between two-hop away nodes, which assume that

they communicate directly as one-hop neighbors. Indeed, a node may legitimately participate in one routing path and may also participate "invisibly" in other routing paths as shown in Fig 2.11.

***Wormhole attack***

In the wormhole attack [73] an attacker uses a pair of nodes connected in some way. It can be a special private connection or the packets are tunneled over the ad hoc network, which is shown in Fig. 2.12. Every packet that one of the nodes sees is forwarded to the other node which in turn broadcast them out. This might create short circuits for the actual routing in the ad hoc network and thereby create some routing problems. Tunneling attacks are a security threat to *multipath* routing protocols, which look for maximally disjoint paths [37]. It is difficult to guarantee integrity of path lengths with metrics like hop count.

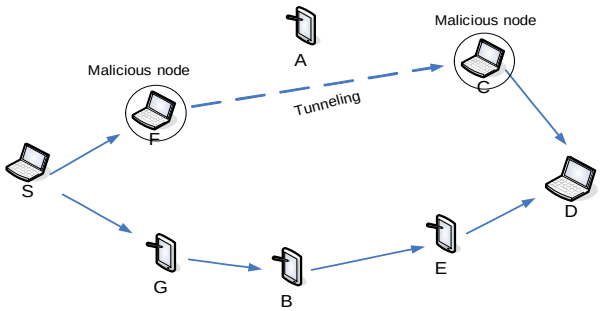



*Fig 2.12. Worm hole attack*

# 3. Hybrid Ad Hoc Network

## 3.1. Hybrid MANET

An isolated MANET is a network that is autonomously set-up among wireless mobile nodes localized in the same geographical area. In this type

of MANET, there is no connection to an external network: all traffic is generated by MANET nodes and destined to MANET nodes. However, in hybrid MANET (H-MANET), a node is connected to an external network (e.g Internet) by means of one or more gateways. A MANET node can exchange data traffic with every other node through multihop paths and communicate with hosts located in the external network, routing its upward traffic towards a gateway. Such gateway, in turn, will receive return traffic from the external host(s) and will route it to the source node. It is also called connected MANET. Although isolated MANET is useful in many applications, connected or hybrid MANET is much more desirable in many applications.

## *3.2. Internet Gateway in Hybrid MANET*

Because ad hoc routing protocols were designed for communication within isolated MANET, it has the limited communication range. To increase communication range and enhance the usability of MANET, Internet Gateway (IGW) is used for the connection of a MANET node to the global Internet. The Internet connectivity can be achieved via user nodes with access subscription to other (infrastructure-based) networks, such as WLAN, WMAN or WWAN. [85] The infrastructure-based network (WLAN) and ad hoc network (MANET) can be integrated to more flexible and wider connectivity. WLANs offer mobile nodes to access the services of Internet. If a mobile node moves into an area where the radio signal off an access point, it may reconfigure itself into ad hoc mode and use multihop mechanism to connect the Internet by MANET's gateway. The integration of the Internet and ad hoc mobile hosts can be used to eliminate dead zones in wireless network.

However, ad hoc routing protocols only maintain routes within the ad hoc network, and do not provide a way to utilize an access point to the

wired network when one is available. So ad hoc routing protocols need to be modified in order to achieve routing between a mobile node in MANET domain and a fixed device in a wired network (e.g. Internet). To achieve this network interconnection, gateways that understand protocols of both MANET protocol stack and TCP/IP suite are needed.

### *a. Internet Gateway Discovery*

When an ad hoc network is connected to the Internet, it is important for mobile nodes to detect available Internet gateways providing access to the Internet. Mobile IP agent discovery methods are discussed in [86-88]. There are two major approaches - reactive and proactive:

- Proactive Discovery: The FA periodically broadcasts Agent Advertisement that can be re-broadcast by ad hoc nodes to flood the entire ad hoc network. All mobile nodes can register with the FA once they have received the rebroadcasting message, and periodically refresh the registration information.
- Reactive Discovery: The FA does not broadcast advertisements periodically, but instead mobile nodes broadcast solicitation messages in search of an agent. The FA unicasts its advertisement to the mobile node via the multi hop route once it receives the solicitation. In this method, mobile nodes may elect to seek a Foreign Agent and register only when they have data to transmit across the gateway to the wired network.

In a Hybrid approach, the gateway sends proactive HELLO messages to a limited group (e.g. the number of hops from the gateway) and let the nodes further away reactively find the gateway. For a minimal overhead, an optimal size of the group must be found. As shown in [34] optimal size of group varies depending on scenario and network condition so some

sort of estimation must be made by the gateway on these parameters.

In the proactive approach, flooding gateway advertisements will enable MANET nodes to select a closer gateway. This will reduce number of packet transmissions required to transfer user data between gateways and MANET nodes. Depending on user activity, this reduction can be larger than the overhead of flooding control packets. Thus proactive approach leads to lower delays and better throughput performance. With the increasing size of ad hoc network, the performance of proactive agent discovery generally decreases.

### *b. Issues and Challenges in Internet Gateways*

In a simpler case where there is only one gateway, the issue is quite simple how to discover the gateway and configure a globally valid address to the mobile node for incoming and outgoing traffic. In a more complicated case where several gateways co-exist, the availability of multiple gateways provides the network with higher robustness and more flexibility for global Internet connectivity. Therefore, it is important, especially for such a network, to discover and select a gateway that is the 'optimal' one among all available gateways, according to certain criteria.

Whenever a mobile node roams to a new wireless access network, it must discover a mobile agent/internet gateway and register with it. In case of single gateway scenario, the traffic between MANET node and the Internet must travel through the same internet gateway. Simultaneous use of internet gateway by several MANET nodes results in heavy traffic congestion around the gateway node. Also, use of single gateway has the drawback of single point of failure. In order to solve these problems, multiple gateways can be used for a particular MANET domain. The multiple internet gateway scenarios may have multiple of FAs at the

border.

Another challenging case is when the Internet connectivity is provided to ad hoc network nodes by those nodes that happen to also have 3G or LAN connectivity, such scenario with multiple gateways is very likely. Under such scenario, we expect that ad hoc network nodes will be able to select the most appropriate gateway. This, and the fact that gateways to the same ad hoc network may generally be connected to different IP subnetworks, leads to challenges such as Mobile IP handovers between gateways, discovery and selection of gateways, allocation of ad hoc nodes to gateways, and many others.

With multiple IGWs, if any one of the IGWs fails, another IGW can take over the failed one. To increase the overall throughput of the MANET to the global Internet, balancing the load on IGWs is required. The network performance can be improved if the load is balanced well among the gateways.

### *c. Handover Strategy*

To extend the coverage or performance of integrated Internet with MANET, usually multiple gateways are used. In general, a handover between gateways is initiated because of mobility, packet loss or to reach a better path. After the handover is done, all packets must be sent through the new gateway. Conventional wireless networks perform handovers depending on the link quality. However, in multihop topologies, usually just a few nodes have a direct connection with the gateway and most of mobile nodes access the wired network through multiple nodes.

Handover is also useful to load balance between different gateways, avoiding packet drops because of buffer overflow or network congestion. Two different kinds of handover can occur: Forced and optimizing handovers.

Forced handover is involuntary. In some situations, communication is not possible with the gateway due to broken route or just that a mobile node has been disconnected. Then a new gateway discovery has to be started, just like the first time that the node appears in the network. Forced handover is possible in all gateway discovery approaches, proactive, reactive and hybrid.

Optimizing handover is voluntary and finds a better gateway in terms of number of hops, as well as other parameters that may be influent to the delivery of packets. Not all gateway discovery approaches can implement this handover because advertisements from the gateways are required, as in proactive and hybrid. From this information, mobile nodes can decide if another gateway is better than the current one. If Mobile IP is used, to maintain transmissions while changing IP address, the mobile node will start a registration with the new access router before it breaks the link with the old one.

It is important to determine precisely when an optimizing handover really is beneficial, instead of waiting for a forced handover. This is because each optimizing handover introduces a delay and a break in the flow of packets transmitted.

### *d. Addressing in MANET*

MANET nodes desiring to communicate with the global Internet should have a set of global IPv4 address(es) to allow the packets to be originated from an Internet node, that is, it must have a globally routable IP address. When a node has IP address that is valid on its home network, normal Mobile IP operation applies; the node must obtain a CoA on the visited network to obtain Internet connectivity. The node may obtain such an address in one of three ways:

(i) It may wait for reception of Agent Advertisement message, initiated by

FA.

(ii) It may request address by issuing Agent Solicitation message for FA.

(iii) It may acquire a co-located CoA through some external means.

Foreign agents periodically broadcast Agent Advertisement messages on their wireless channels. These messages contain IP address of the FA and optionally one or more advertised CoAs. When a mobile node receives such an advertisement, it selects one of the advertised COAs to be its new CoA.

Alternatively, according to (ii) above, a node may solicit a CoA from a FA by issuing Agent Solicitation. A mobile node that does not know IP address of any FAs must discover a route to its closest FA. It is possible for a mobile node to not have received Agent Advertisement if the node has just joined the network and is in the interval between Agent Advertisements, or if network collisions prevented the broadcast Agent Advertisement from reaching the mobile. Finally, a node may obtain a co-located CoA through some external means, such as a DHCP server.

In order to access the Internet, MANETs need to one or more gateways, which enable each node's interface to have auto-configured global address(es). For the purpose of announcing the gateway prefix information, route advertisement and route solicitation messages should be processed in multihop fashion at each gateway and node. Along with the prefix information, the stateless mechanisms for IP address auto-configuration and duplicate address detection for valid global IP addresses should be executed. In the case of multiple gateways, each node's interface can be assigned multiple global IP addresses due to the presence of multiple gateways. However, since most ad hoc routing protocols did not consider multiple addresses of one network interface,

they should be modified to support not only MANET local address but also multiple global addresses.

## 3.3. Security Issues in Hybrid MANET

The security in IEEE 802.11 WLAN connected to the Internet is well studied. However interconnection between Internet and MANET is still challenging task. To support global connectivity in MANET, infrastructure-based network (WLAN) route to corresponding node is required by following the Mobile IP. There are two critical issues for providing a secure multihop route discovery: Internet connectivity and ad hoc routing protocol.

To obtain Internet connectivity, each MS has to register with the visiting FA and creates a mobility binding at its HA. If the MS is misled by a forged FA or a malicious intermediate MS, it cannot get a correct Internet connection with services as the registration messages may be modified by a malicious intermediate MS and may not allow MSs to register with its HA correctly. The existing ad hoc routing security approaches cannot provide a secure FA discovery. The existing Mobile IP protocol cannot provide the security protection for a multihop registration. Thus, for providing global connectivity to connected MANET, two major schemes are required: a secure FA discovery and a secure Mobile IP registration for MS.

### *a. Vulnerability in hybrid MANET*

Vulnerability in the connected MANET can be categorized into two: vulnerability in ad hoc network and vulnerability in Internet connectivity.

Ad hoc routing protocols are vulnerable to different types of attacks that have been extensively studied in chapter 2 section 2.5.

*Attacks on the Internet Connectivity*

Malicious nodes can modify, drop, forge or generate Mobile IP messages (e.g., advertisement, registration request, or registration reply) and disrupt mobile IP support for MANET. Three main types of attacks in Internet connectivity are bogus registration, replay attack, and forged FA.[96]

- Bogus registration: In the integrated MANET, bogus registration occurs when a malicious node makes a fake registration by masquerading itself as someone else (a genuine one). For instance, $MN_1$ may attack the Internet connectivity by bogus registration in the disguise of $MN_2$, and thereafter the packets of $MN_2$ will be forwarded to the malicious $MN_1$. The malicious $MN_1$ could send bulk packets on behalf of $MN_2$ to take up the bandwidth of Internet gateway and may disallow the Internet connectivity to other MNs, causing DoS.
- Replay attack: The replay attack occurs when an attacker obtains a copy of legitimate packet (e.g., a registration message) sent by a MN and then replays the packet later. For example, $MN_1$ stores some mobile IP messages which were sent by other MNs. Then, $MN_1$ resends these messages to the FA to impersonate as the senders. If the FA is tricked into believing that the genuine messages, the attacker could perform valid but unwanted operations afterwards by sending old messages.
- Forged FA: Forged FA attack can be implemented by using fraudulent beacons or recorded beacons. By advertising fraudulent beacons, an attacker might be able to entice MSs in a MANET to register with the attacker as if the MN has reached the Internet. This type of attack is difficult for an attacker to implement because the attacker must have the detailed information about the FA. While broadcasting the recorded beacons, the attacker entices other MNs to register with the forged FA. When MN hears the fraudulent or recorded beacons from the forged FA, MN assumes that it is a genuine FA, and then initiates a

registration procedure. A registration request is issued from the MN to the forged FA. Furthermore, after receiving the registration result, the MN assumes that it has obtained the Internet connection through the forged FA and disconnects its communication from the genuine FA.

## *3.4. Distributed Media Delivery*

Initially Content Delivery Network (CDN) [98] was developed to overcome performance problems, such as network congestion and server overload in the network topology, which arise when many users access popular contents. CDNs have been widely used to provide low latency, scalability, fault tolerance, and load balancing for the delivery of web content and more recently streaming media. CDNs improve end-user performance by caching popular content on edge servers located closer to users. Delivering content from a nearby edge server reduces response time, probability of packet loss, and total network resource usage. [99]

With the emerging wireless technology, streaming high-fidelity audio over wireless channels is in demand. Meanwhile, IP-based architecture for wireless systems promises to provide next-generation wireless services such as voice, high-speed data, Internet access, audio and video streaming on an all IP network. It is known that real-time audio streaming can only tolerate very few errors. Moreover, bandwidth fluctuates in wireless channels present new challenges to audio streaming. Thus, it is important that audio streaming scheme has the ability to adapt audio bit rate according to network conditions. With scalable audio compression [100], [101], a single compressed bit stream can be generated with different subsets of it corresponding to the compressed version of the same audio clip at various rates. This is very beneficial for audio delivery over time-varying networks with bandwidth fluctuation.

Like in other wireless multimedia applications, efficient compression

techniques must be employed to meet bandwidth limitations in audio streaming. Source compression is achieved at the cost of sensitivity to transmission errors, which have severe adverse effects on decompressing the received bit stream and sometimes completely crash the decoder.

Two techniques have been proposed in the literature to deal with transmission errors: error resilience and error protection [102].

*Error Robustness*

Error robustness means that the encoded audio data can be transported over error prone channels without unacceptable loss in signal quality.

MPEG-4 ver. 2 has included two kinds of techniques - "Error Resilience" and "Error Protection". MPEG-4 Audio ver. 2 coding algorithms have ability to generate such error resilient bit streams that can be decoded with minimal degradation even if they are partially corrupted, if the corrupted part is distinguished.

MPEG-4 ver. 2 contains Error Protection (EP) Tool which can be used by all MPEG-4 audio coding algorithms and is able to adapt to a wide range of channel error conditions. MPEG-4 algorithms provide a classification of each bit stream field according to its error sensitivity. Based on this, the bit stream is divided into several classes, which can be separately protected by the EP tool, such that more error sensitive parts are protected more strongly. This technique is known as Unequal Error Protection (UEP). Main features of the EP tool are

- providing a set of error correcting/detecting codes with wide and small-step scalability, in performance and in redundancy
- providing UEP configuration control with low overhead

*Forward Error Correction*

Forward Error Correction (FEC) [103] is used mainly for real-time communications where an effective way to deal with channel unreliability is needed. The idea is to add a level of redundancy as a function of the

network state. Then this level of redundancy should be decreased when the network is well-behaved and increased when it is not. Suppose a block of K encoded at the sender using FEC K+R so a total of N=K+R packets are sent per block. The Redundancy packets are calculated using block codes that are a class of codes with memory. Normally Reed-Solomon codes are used.

To serve as an error resilient tool, scalable coding must be paired with UEP in the transport system, so that the base layer is protected more strongly, e.g., by assigning a more reliable sub-channel, using stronger FEC codes [104], or allowing more re-transmissions.

# III. Proposed Approaches

## 1. Authentication scheme for Wireless mobile network

Many authentication protocols for the wireless mobile networks have been proposed. Further, there is a desire to increase the security and performance of authentication mechanisms in wireless network due to strong user authentication, protection of user credentials, mutual authentication and generation of session keys. As demand for strong user authentication grows, one-time password (OTP)-based authentications tend to become more common.

### 1.1. Previous Works

Lamport [21] proposed a one-time password/ hash chaining technique, which has been used in many applications. S/KEY [23] is an authentication system that uses OTP. The S/KEY system [24] is designed to provide users with OTPs which can be used to control user access to remote hosts.

The IETF RFC 3748 [14] has defined that with Extensible Authentication Protocol (EAP), OTP method can be used. Further the Internet draft [25] defines OTP method, which provide one way authentication but not key generation. As a result, the OTP method is only appropriate for use on networks where physical security can be assumed. This method is not suitable for using in wireless IP networks, or over the Internet, unless EAP conversation is protected.

## 1.2. OTP-based Authentication Scheme

### a. Overviews

We put forward a scheme for implementing authentication mechanism based on the hash function. The authentication protocol is proposed to solve the weak authentication and security flaw problem of WEP in 802.11 WLAN.

We devise concept of authentication scheme using one-time password for IEEE 802.11 network. In this scheme, the AP receives the password which is processed from the client and the server's original password exclusive-OR (XOR) the stream bits, in order to defend malice attack. The client needs remote authentication, so the AP not only receive the password from the client but fetch client's basic data from Home Network Server (HNS) by roaming, then the AP computes and compares the hash value to accomplish mutual authentication. The key exchange between the client and the AP generates a session key and responses new stream bits to HNS to update client's database. Finally, the client sends OTP to the AP, and the client refreshes secret key of WEP in IEEE 802.11, to defend replay attack.

In order to prevent client and AP in this protocol from several attack methods. The techniques include per-packet authentication and encryption, etc are adopted.

### b. Working Principle

There are four phases in this authentication scheme, which are:

- Phase 0: Discovery phase;
- Phase 1: OTP Authentication phase;
- Phase 2: Secure key exchange phase;
- Phase 3: Refreshing OTP phase.

The conversation phases and relationship between the parties in OTP based Authentication scheme is shown in Fig 3.1.

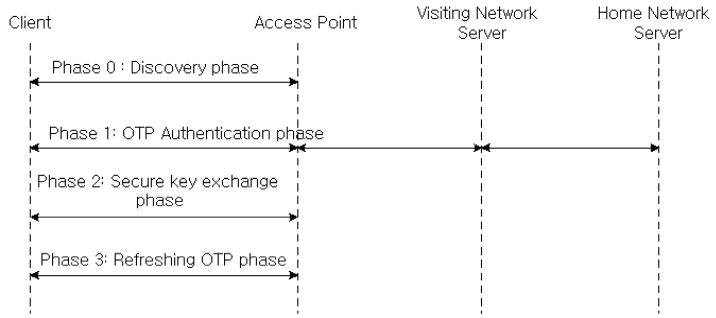



*Fig 3.1. Conversation phases of OTP Authentication scheme*

***Phase 0: Discovery phase***

In the discovery phase (phase 0), the client or the station (STA) and Access Point (AP) locate each other and discover each other's capabilities. IEEE 802.11 provides integrated discovery support utilizing beacon frames, allowing the STA to determine the MAC address and capabilities of AP. When the client receives beacon frame, it knows itself is in Visiting Network, and requires authentication from Home Network.

***Phase 1: OTP authentication phase***

The authentication phase (phase 1) begins once the client and AP discover each other. This phase always includes OTP authentication. In this phase, the client authenticates itself as a legal member for a particular AP and needs remote authentication. The steps are shown as the follows:

Step 1:

The AP send Request message.

Step 2:

The client will send $\{ID_C || ID_{HNS} || Y_C || H(ID_C, A)\}$. Where $ID_C$ is client's identity; $ID_{HNS}$ is Identity of Home Network Server (HNS); $Y_C$ =

$d^{R_C}$ mod $q$; $R_C$ is random number produced by a client; $H()$ is one way hash function; $A = PW_C \oplus SB$; $PW_C$ is client's password; and $SB$ is stream bits generated by the server to share with the client.

Step 3:

After receiving $\{ID_C || ID_{HNS} || Y_C || H(ID_C, A)\}$ from the client, the AP sends $\{ID_{HNS} || ID_C || ID_{AP}\}$ to the Visiting Network Server (VNS) Where $ID_{AP}$ is AP's Identity.

Step 4:

After receiving $ID_{HNS}$ from the client, the VNS will encrypt $ID_C$ and $ID_{AP}$ with $K_{VH}$ which is a secret shared key between VNS and HNS. Then it sends $\{ID_{HNS} || E_{VH}(ID_C || ID_{AP})\}$ to the HNS.

Step 5:

Depending on $ID_C$, the HNS examines $PW_C$, SB, and client's privacy key ($K_C$) from user's database, and generates a new stream bits ($SB_N$) and $A$. The $ID_C$ and $SB_N$ are encrypted with private key $K_C$ producing $E_{KC}(ID_C || SB_N)$. Then $E_{K_C}(ID_C || SB_N)$, $ID_C$, $ID_{AP}$ and $A$ are encrypted by HNS with symmetric cryptosystem to get $E_{VH}(ID_C || ID_{AP} || A || E_{K_C}(ID_C || SB_N))$. Then HNS will send $\{ID_{VNS} || E_{VH}(ID_C || ID_{AP} || A || E_{K_C}(ID_C || SB_N))\}$ to the VNS.

Step 6:

Upon receiving $\{ID_{VNS} || E_{VH}(ID_C || ID_{AP} || A || E_{K_C}(ID_C || SB_N))\}$ VNS will decrypt it using $K_{VH}$, then $E_{K_C}(ID_C || SB_N)$, $ID_C$ and $A$ are encrypted by VNS with symmetric cryptosystem using $K_{AS}$, which is shared key between AP and VHS. Then, it sends $\{ID_A || E_{AS}(ID_C || A || E_{K_C}(ID_C || SB_N))\}$ to AP.

Step 7:

Upon receiving $\{ID_A || E_{AS}(ID_C || A || E_{K_C}(ID_C || SB_N))\}$ from the VNS, then the AP computes and verifies $H(ID_C, A)$ between the client and the server. If true, it will send authentication success frame $\{ID_C ||$

$Y_A$ || $E_{K_C}(ID_C$ || $SB_N)\}$ to the client. Where $Y_A = d^{R_A} \bmod q$; $R_A$ is random number produced by AP. $Y_A$ will be used for key exchange in later steps.

Step 8:

The client accomplishes authentication procedure, then it sends $\{ID_C$ || $IPA_{HNS}$ || $H(SB_N)\}$ to AP. Where $IPA_{HNS}$ is IP address of HNS.

Step 9:

AP will send $\{ID_C$ || $H(SB_N)\}$ to the HNS to update client's database in the HNS.

Step 10:

The client and the AP apply $Y_A$ or $Y_C$ to generate a session key ($K$), then the client sends $\{ID_C$ || $E_K(otp$ || $ctr$ || $ID_C)\}$ to the AP. Where *otp* is the client's one-time password shared with the AP; and *ctr* is the counter of *otp*.

Step 11:

The AP responds with $\{ID_C$ || $H(otp, ctr)\}$ to the client.

It should be noted the counter is a positive integer and will decrease by one once the *otp* is changed.

***Phase 2: Secure key exchange phase***

The Secure key exchange phase (phase 2), begins after the completion of OTP authentication. In practice, the phase 2 is used to negotiate a new secret key between the client and the AP. Similar to the authentication phase, a MAC is added to each packet and then is encrypted together, and the receiver should check the MAC. The steps of the protocol are as shown in the following:

Step 1:

The client sends $\{ID_C$ || $E_K(otp_{I+1}$ || $H(otp_I, ctr, ID_C))\}$ to AP. It should be noted that $H(opt_{I+1})$ is equal to $otp_I$ and $K$ is session key by phase 1.

Step 2:

The AP checks MAC and $ID_C$ by checking if $H(otp_{I+1})$ is equal to $otp_I$. If this is true, the client is a legal member. It will replace $otp_I$ by $otp_{I+1}$ and decrease the counter by 1. And AP transmits $H(otp_I, ctr)$ to client.

Step3:

The client checks Hash value and decreases the counter by 1.

By these three steps, the client and the AP can achieve the goal of mutual authentication. In this phase, both the client and the AP have the same new secret key of WEP just for this session.

***Phase 3: Refreshing OTP phase***

When the counter decreases to zero, the client should change its OTP, otherwise the AP has right to prohibit the client from using its services. The steps of the protocol are shown in the following:

Step 1:

The client sends its $\{ID_C, || E_K(otp_{I+1} || otp_N || ctr_N H(otp_{I+1}, otp_N, ctr_N, ID_C))\}$ to AP, where $H(otp_{I+1})$ is equal to $otp_I$ ,$otp_N$ is its new OTP, $ctr_N$ is a new counter and $K$ is session key by authentication phase.

Step 2:

The AP verifies MAC and $otp_{I+1}$ (check $H(otp_{I+1})$ is equal to $otp_I$). If this is true, the client is legal member, and AP replaces $otp_I$ by $otp_N$ and resets $ctr$ to $ctr_N$. Then the AP sends $\{ID_C || H(otp_I, ctr)\}$ to the client.

Step3:

The client checks his ID and the hash value.

## 2. Multipath Multihop Wireless Network

For ubiquitous services, the robustness and security issues in multipath multihop wireless network have to be considered.

## 2.1. Existing Approaches for Multipath Ad hoc Network

### a. Existing Multipath Ad Hoc Routing Protocols

Some of well-known multipath protocols based on reactive routing are Ad hoc on-demand multipath distance vector (AOMDV) [46], Ad hoc on-demand distance vector multipath (AODVM) [47], and SMR [37].

#### *Ad hoc On-demand Multipath Distance Vector*

AOMDV [46] is an extension to AODV protocol for computing multiple loop-free and link-disjoint paths. Loop-freedom is guaranteed by using a notion of "advertised hop count". Link-disjointness of multiple paths is achieved by using a particular property of flooding.

To find disjoint routes, each node does not immediately reject duplicate RREQs. Each RREQ carries an additional field called first hop to indicate the first hop neighbor of the source taken by it. Also, each node maintains a first hop list for each RREQ to keep track of the list of neighbours of the source through which a copy of the RREQ has been received. In an attempt to get multiple link-disjoint routes, the destination replies to duplicate RREQs regardless of their first hop. To ensure link-disjointness in the first hop of the RREP, the destination only replies to RREQs arriving via unique neighbors. Trajectories of each RREP may intersect at an intermediate node, but each takes a different reverse path to the source to ensure link-disjointness.

#### *Ad hoc On-demand Distance Vector Multipath Routing*

AODVM [47] is an extension to AODV for finding multiple node-disjoint paths. Instead of discarding duplicate RREQ packets,

intermediate nodes are required to store them. For each received copy of RREQ, the intermediate node records the source that generated the RREQ, the destination for which the RREQ is intended, the neighbor that transmitted the RREQ, and some additional information in RREQ table. Furthermore, intermediate relay nodes are precluded from sending RREP directly to the source.

*Split Multipath Routing*

SMR [37] is an on-demand multipath source routing protocol that builds multiple routes using a request/reply cycle. SMR can find an alternative route that is maximally disjoint from the source to the destination. When the source needs route to the destination but no route information is known, it floods RREQs to the entire network in order to find maximally disjoint paths, so this approach has disadvantage of transmitting more RREQ packets. Because this packet is flooded, several duplicates that traversed through different routes reach the destination. The destination node selects multiple maximally disjoint routes and sends RREP packets back to the source via the chosen routes. In order to choose proper maximally disjoint route paths, the destination must know the entire path of all available routes. Therefore, SMR uses the source routing approach where information of the nodes that comprise the route is included in RREQ.

Unlike DSR, intermediate nodes do not keep a route cache, and therefore, do not reply to RREQs. This is to allow the destination to receive all the routes so that it can select maximally disjoint paths. Maximally disjoint paths have as few links or nodes in common as possible. The algorithm only selects two routes. In the algorithm, the destination sends a RREP for first RREQ it receives, which represents the shortest delay path. The

destination then waits to receive more RREQs. From the received RREQs, the maximally disjoint path from the first RREQ is selected. The destination then sends RREP for the selected RREQ.

### *b. Ad hoc security scheme*

In many applications, secure routing of packets is critically essential for the wireless ad hoc network. There are many algorithms [74] that provide security on top of routing protocols such as AODV and DSR. Some of the well-known ad hoc security protocols are SRP[75], ARAN[68], ARIADNE[76], SEAD[77] and SAODV[78]. Almost all of them are designed for single path ad hoc routing.

With the growing popularity of multipath routing, several studies have been conducted on providing protection on data transmission by using multiple paths between source and destination [79]. Some examples of secure data transmission using multipath routings are Secure Message Transmission (SMT) protocol [80] and Secure Protocol for Reliable Data Delivery (SPREAD) [81].

In multipath ad hoc networks, secure routing schemes designed for single path ad hoc routing may not be suitable. Thus security issues in multipath ad hoc routing are still open challenge.

#### *Secure Routing Protocol*

Secure Routing Protocol (SRP) [75] proposed by Haas and Papadimitratos, is based on DSR, and could be applied to existing *reactive* routing protocols. The SRP routing protocol guarantees the acquisition of correct topological information and could cope with malicious attacks such as disrupting discovery process, modifying, replaying and fabricating routing messages.

Main SRP's assumption is the existence of an underlying *security association* (SA) between the source node and the destination node. Because only the end nodes need to perform previous cryptographic operation, this could be done efficiently by using *message authentication code* (MAC).

RREQ include the source and destination addresses, query sequence number and query identifier. The source node generates MAC by keyed hash algorithm. The destination node verifies received RREQ. If the RREQ is valid then the destination generates RREP message back to the source, else the request message is discarded.

SRP suffers from route cache poisoning attack because malicious node can fabricate the routing information that gather routing information and operate in promiscuous mode.

SRP suffers also from lack of validation of route errors packets. However, the source node could verify that the provided route error feedback refers to the actual route and is not generated by a node that is not part of the route. A malicious node can harm only the route it belongs.

SRP is vulnerable to the wormhole attack, as two colluding malicious nodes can misroute the routing packets on a private network connection and alter the network topology vision a benign node can collect.

SRP has no defense against the "invisible node" attack that simply puts itself somewhere along the message path without adding itself to the path, thereby causing potentially big problems as far as routing goes. A malicious node could in SRP insert itself in the network and do damage by delaying or dropping packets. This decreases the networks performance and affects the shortest path requirement as well as exposing the network topology to adversaries.

## 2.2. Related Works

We briefly present the related works to multipath routing. Some multipath routing protocols have been proposed for wireless ad hoc networks [42] [47] [49]. Multipath routing protocols based on the source routing protocol DSR are found such as Multipath source routing (MSR) [49] and SMR [37].

Multipath protocols based on distance vector routing scheme have also been proposed for wireless ad hoc networks. AOMDV [46], AODVM [47], AODV-BR [38], and Caching and multipath routing protocol (CHAMP) [50] are some of well-known protocols of this kind. Li and Cuthbert [43] proposed a stable Node-disjoint multipath routing (NDMR), which applies path accumulation feature of DSR to AODV and achieves multiple node-disjoint paths with low routing overheads. And Scalable multipath on-demand routing (SMORT) [40] uses the idea of fail-safe alternate path, which bypasses at least one intermediate node on the primary path, to determine multiple paths.

We also address the techniques for streaming through multiple paths. Basically we can stream the whole flow through a single path as in RMPSR [45] or divide the content into multiple minor flows and stream them through the available paths as in MDSR [61].

The authors [62] have developed models for multiple description (MD) streaming over multiple paths and based on these models we propose a multipath selection method.

Several studies of selective encryption for video and image compression have been performed [63] [64], and some on selective encryption of coded speech have been presented [65].

Futhermore, we discuss on secure routing schemes for multipath ad hoc routing. Some of the proposed secure multipath routing schemes are SRP[75], SecMR[82] and Burmester's approach [83].

SRP [75] is a multipath routing protocol which uses end-to-end symmetric cryptography to protect integrity of the route discovery. It is efficient but still vulnerable to some attacks of malicious nodes.

Burmester [83] proposed a secure multipath routing protocol based on Ford-Fulkerson MaxFlow algorithm. This protocol satisfies completeness, i.e., it discovers all existing paths bounded by a TTL field. However, the propagation of RREQ is not efficient, in context of computation and space costs. Furthermore, the use of digital signatures by intermediate nodes of each RREQ message costs both in delay and processing power.

R. Mavropodi [82] proposed a complete on-demand multipath routing protocol, Secure Multipath Routing (SecMR) protocol, which provides protection against DoS attacks from a bounded number of collaborating malicious nodes. SecMR discovers complete set of existing non-cyclic, node-disjoint paths between source and target node, for given maximum hop distance.

## *2.3. AODV-MAP Routing Scheme*

In this section, we propose a multipath routing scheme for diminishing the effect of frequent communication failures. Our main intentions are to lower frequencies of costly route discoveries; to keep end-to-end connection for longer time; and to provide labeled multiple alternative paths for efficient traffic distribution among these paths.

### *a. Overviews*

The proposed multipath routing protocol for mobile ad hoc network is a modification of single path AODV protocol. It is basically intended for highly dynamic ad hoc networks in which communication failures occur frequently and designed to compute not only node-disjoint paths but also

fail-safe paths. So the combination of these paths allows the computation of more alternative paths than in node-disjoint or link-disjoint multipath routings. Thus the proposed scheme is named as AODV with Multiple Alternative Paths (AODV-MAP).

In AODV-MAP scheme, each node in MANET keeps and maintains tables - routing table, and neighbor node table. Neighbor node table is used to record neighborhood information, which is periodically updated.

The structure of routing table entry is as follows:

<dest_ipaddr, dest_seqno, hop_cnt, nxt_hop, route_flag, path_label, innode_full, fsnode, route_path>

Where

dest_ipaddr - Destination IP Address;

dest_seqno - Destination Sequence Number;

hop_cnt - Number of hops needed to reach destination;

nxt_hop - Next Hop;

route_flag - Routing table entry flags (eg valid, invalid, repair)

path_label - Path type;

innode_full - Number of intermediate nodes in the route path which are not protected;

fsnode - Number of intermediate nodes in the route path which are protected

route_path - Whole routing path list

As in AODV, it has control messages - Route Request (RREQ), Route Reply (RREP) and Route Error (RERR).

Route Request (RREQ) Message Structure

- src_ipaddr - IP Address of the originator
- src_seqno - The sequence number of the originator
- dest_ipaddr - IP Address of the destination

- dest_seqno - The sequence number of the destination.
- bcast_ID (RREQ_ID) - A sequence number
- hop_cnt - Number of hops from the source to the current node handling the request.
- route_path - path accumulation list of the route path.

Route Reply (RREP) Message Structure

- dest_ipaddr - IP Address of the destination
- dest_seqno - The sequence number of the destination.
- src_ipaddr - IP Address of the originator
- hop_cnt - Number of hops from the source to the destination.
- route_path - path accumulation list of the route path.
- path_label - type of path to determine primary, node-disjoint or fail-safe.

Route Error (RERR) Message Structure

- dest_cnt - Number of unreachable destinations included in the message.
- unreach_destipadd - IP address of the destination that has become unreachable due to a link break.
- unreach_destseqno - Sequence number in the route table entry for the destination listed in the previous Unreachable Destination IP Address field.

### *b. Operations*

As in AODV, AODV-MAP has two phases:

- Route Discovery
- Route maintenance.

***Route Discovery***

RREQ Generation

A source node S initiates route discovery process, when it wants to communicate to a destination D, for which it does not have a valid route. Valid route is a route to the destination, whose lifetime has not expired. The source node S inserts last known destination sequence number (DSN), address of the destination, RREQ ID, its own address and sequence number into a route request packet and broadcasts it. The source node appends own address to the route path in RREQ message.

The RREQ ID is incremented every time when the source node initiates a RREQ. In this way, broadcast ID and the address of the source node form a unique identifier for the RREQ.

RREQ processing and forwarding at Intermediate nodes

When a node receives a RREQ, it checks to determine whether it has received a RREQ with the same source and RREQ ID. If a node receives a RREQ for the first time, it searches for a reverse route to the source. If no reverse route, then create one. Intermediate nodes are not allowed to send RREPs back to the source even when they have route information to the destination. This is essential to find desired multiple paths at the destination.

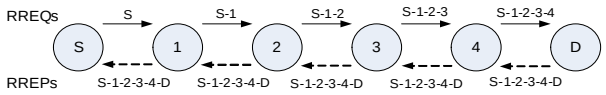



*Fig 3.2. Path accumulation during route discovery*

Further, when RREQ is forward by intermediate nodes in the network, each node appends its address to it. Path accumulation during route discovery is shown in Fig. 3.2 and the path information ensures to send

RREP to the source as well as enables to set path label at the destination.

AODV-MAP allows intermediate nodes to forward duplicate RREQ packets that come from different neighbors than previous RREQ and whose hop count is not larger than that of previous RREQ. This ensures to discover desired alternative paths.

RREQ processing and RREP generation at Destination

In this scheme, the destination is responsible for not only selecting primary path, node disjoint and fail-safe paths from all the received routes but also defining the path with specific path label.

When receiving the first RREQ, the destination records the route path of RREQ and sets it with path label 1. Then after copying route path of RREQ to a RREP packet, the destination node sends RREP to S using path information in it. Hence the intermediate nodes can forward this packet using path information in RREP.

When the destination receives a duplicate RREQ, it will compare route path of RREQ to that of the routing table. If only source and destination nodes are same, a path is said to be a node-disjoint path and the destination determines it as path label 3. If at least one of intermediate nodes in the route path in the routing table is different from nodes in the route path of the RREQ, a route is said to be a fail-safe path and destination determines it as path label 2. After setting appropriate path label in RREP, the destination sends it to the source along the path information in it. Partial flowchart for setting path label at the destination is shown in Fig. 3.3.

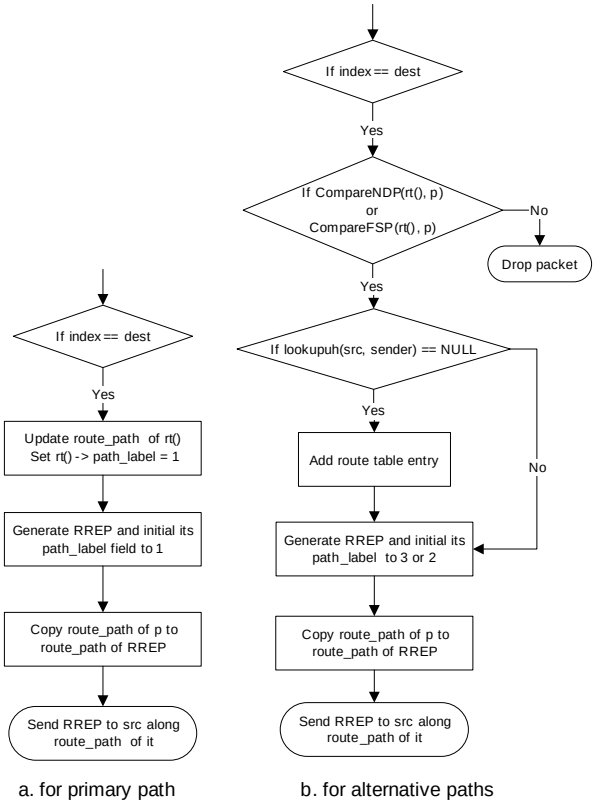



*Fig. 3.3. Partial flow chart for setting path label*

When destination receives a duplicate RREQ, the destination uses the modules shown in Fig 3.4 a and b to decide whether the route path of the packet is a node-disjoint path or fail-safe path.

RREP forwarding at Intermediate nodes

RREPs follow the reverse paths to reach the source node. After storing the routing information, intermediate nodes relay RREP packet to the next hop according to route path field toward the source.

```
Module CompareNDP(entry, packet)
Begin
   For each intermediate node in the route_path of entry
        For each intermediate node in the route_path of packet
             If the node in route_path of entry == the node in route_path of packet
                  Return TRUE
             End If
        End For
   End For
   Return FALSE
End
```

*a. For determining node-disjoint path*

```
Module CompareFSP(entry, packet)
Begin
   If entry -> innode_full > 0
        For each intermediate node in the route_path of entry
             If the node in the route_path of entry is not protected
                  For each intermediate node in the route_path of packet
                       If the node in the route_path of entry != the node in route_path of packet
                       Else
                        Break
                  End For
                  If all intermediate nodes in route_path of packet are different from node in route_path of  entry
                       Set the node in the route_path of entry is protected
                       entry-> innode_full --
                       Return TRUE
                  End If
             End If
        End For
   Else
        Return FALSE
End
```

*b. For determining fail-safe path*

*Fig 3.4. Modules for determining alternative paths*

RREQ Forwarding Approach

We formulate two approaches for RREQ forwarding by the intermediate nodes. Initially, we put forward first RREQ forwarding approach in which an intermediate node would forward duplicate RREQs from two neighbor nodes only. As this scheme is not scalable, we replace it by second approach.

In order to meet need of robustness and scalability in our multipath routing scheme, we have used second approach – selective RREQ forwarding scheme, in which RREQ shall be forwarded by intermediate node if only satisfies following criteria:

$$hop\_cnt_{RREQi} \leq hop\_cnt_{prevRREQ}$$

$$nn_{RREQi} \neq nn_{prevRREQ}$$

where $nn$ is neighbor node

Selective RREQ forwarding scheme is preferred in order to discover desired multiple alternative paths. Fig. 3.5 presents the intial process of discovering multiple paths during route discovery.

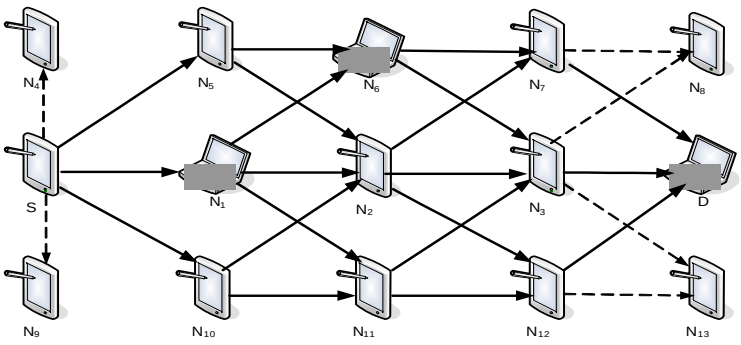



*Fig. 3.5. Discovering multiple paths during route discovery*

Fig. 3.6 shows the process of RREQ forwarding process in intermediate nodes. Suppose an intermediate node $N_2$ receives RREQ from three different neighbors ie $N_1$, $N_6$ and $N_{10}$. Since $N_2$ has not seen RREQ from these neighbors, it will forward all the received RREQs. In case of an intermediate node $N_3$, it also receives RREQs from three different neighbor nodes $N_5$, $N_2$, and $N_{11}$. Only first RREQ from each neighbor will be

forwarded by $N_3$ while other RREQs taking different paths will be discarded.

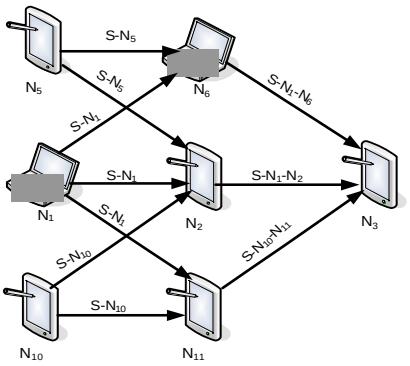



*Fig 3.6. Selective RREQ forwarding process*

Finally D can receive all the RREQ packets from its neighbor nodes - $N_7$, $N_3$ and $N_{12}$. Fig 3.7 shows the multiples alternative paths available for data forwarding.

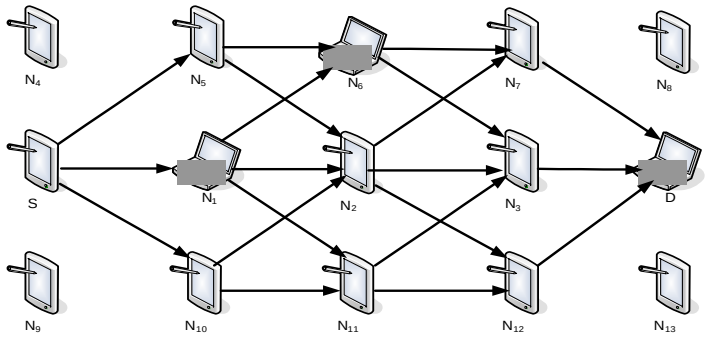



*Fig. 3.7. Multiple alternative paths available for data forwarding*

After route discovery process, there will be a primary path and a number of multiple paths which are shown in Table 3.1.

| | |
|---|---|
| Primary path | S-$N_1$-$N_2$-$N_3$-D |
| Node-disjoint paths | S-$N_5$-$N_6$-$N_7$-D<br>S-$N_{10}$-$N_{11}$-$N_{12}$-D |
| Fail-safe paths | S-$N_5$-$N_2$-$N_7$-D<br>S-$N_1$-$N_6$-$N_3$-D<br>S-$N_1$-$N_2$-$N_{12}$-D<br>S-$N_{10}$-$N_{11}$-$N_3$-D |

*Table 3.1 Multiple Alternative paths for data transfer*

***Route maintenance***

Normally route links in wireless ad hoc networks are broken frequently due to the mobility of nodes, congestion and packet collisions. The proposed scheme is capable of recovering broken routes immediately. When a node fails to deliver the data packets to the next hop of the route by receiving a link layer feedback from link layer or receives RERR packet, it removes entries in its route table that uses the broken link and looks up its routing table if there is another entry for the destination.

If it has another entry for the destination, data packets therefore can be delivered through the alternate route. If it has no another entry for the destination, it sends a RERR packet to the upstream node. When the source has no entry for the destination and the session is still active, it would initiate a new route discovery.

A node initiates processing for a RERR message in three situations:

- If it detects a link break for the next hop of an active route in its routing table and it has no other entry to the same destination while transmitting data.
- If it gets a data packet destined to a node for which it does not have an active route.
- It receives a RERR from a neighbor for one or more active routes but it cannot protect all of unreachable destinations.

## 2.4. Traffic allocation approach using AODV-MAP

We devise a traffic allocation approach using AODV-MAP scheme and scalable audio coding for media streaming. At the initial, the source node begins to send core bitstream or base layer (BL) on the primary path and enhancement bitstream or layer (EL) on the node-disjoint path. Since the primary path and the node-disjoint path are not correlated, source node uses the node-disjoint path to provide load balancing.

Generally, a multihop path is up or down for random periods of time, leading to bursty packet losses. According our approach, when forwarding paths break, nodes receiving base layer or enhancement layer may use different paths in the routing table to forward packets. The traffic distribution is as follows: in case of BL, the proposed approach first finds alternate fail-safe path for each node on the primary path as it has higher packet delivery rate. If no fail-safe paths are available then only it uses node-disjoint paths. In case of EL, the proposed approach first finds an alternate fail-safe path. If no fail-safe paths are available then only it uses primary path. The flowchart for multimedia packet forwarding is shown in Fig, 3.8.

Example of traffic allocation using AODV-MAP is shown in Fig 3.9 - 3.11. In Fig. 3.9, it can be seen that initially BL is forwarded through the primary path ("S-$N_1$-$N_2$-$N_3$-D") whereas EL is passed through the node-disjoint path ("S-$N_5$-$N_6$-$N_7$-D").

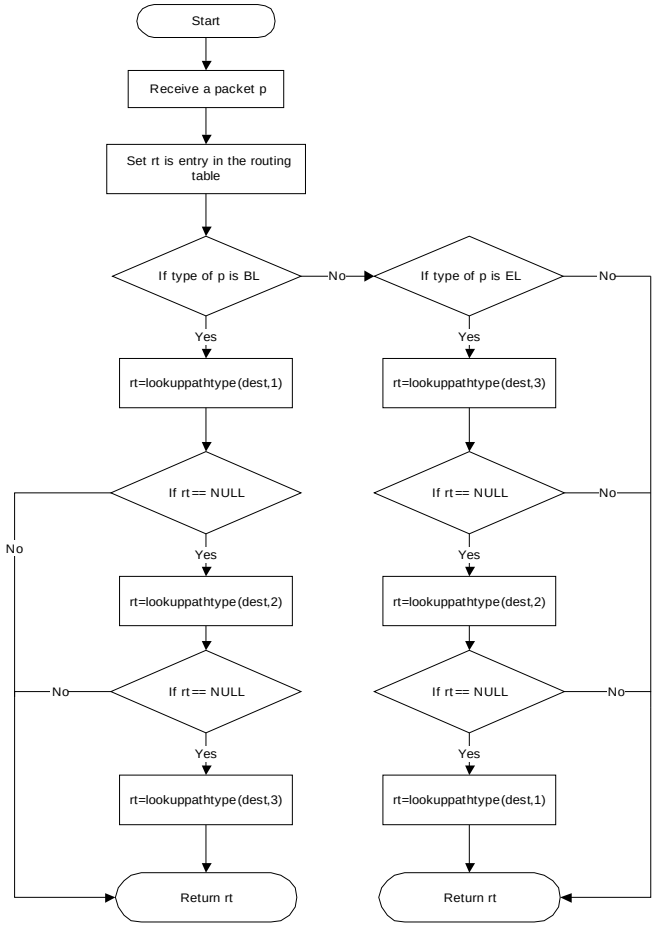



*Fig. 3.8. Flow chart for multimedia packet forwarding*

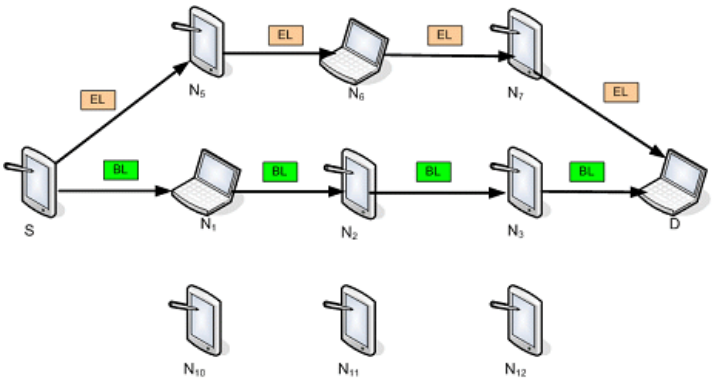
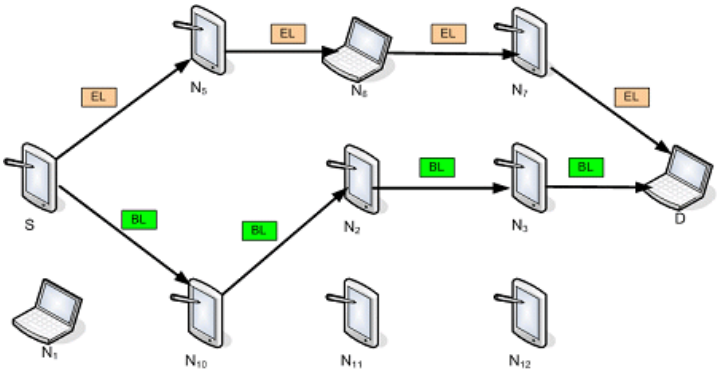
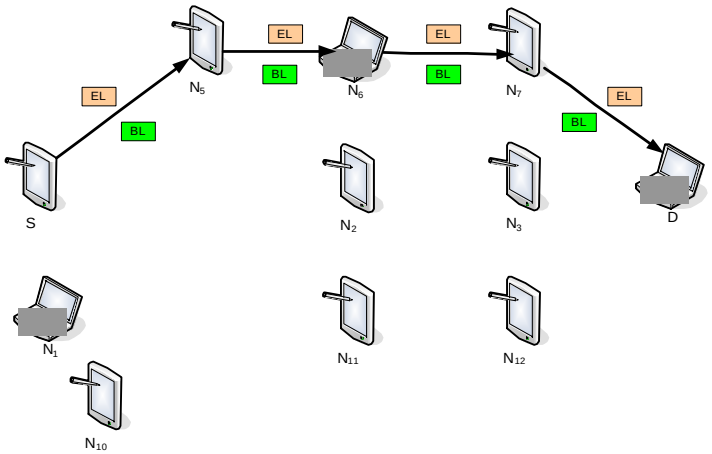



*Fig. 3.9. Initial traffic distribution in AODV-MAP*




*a. using fail-safe path*



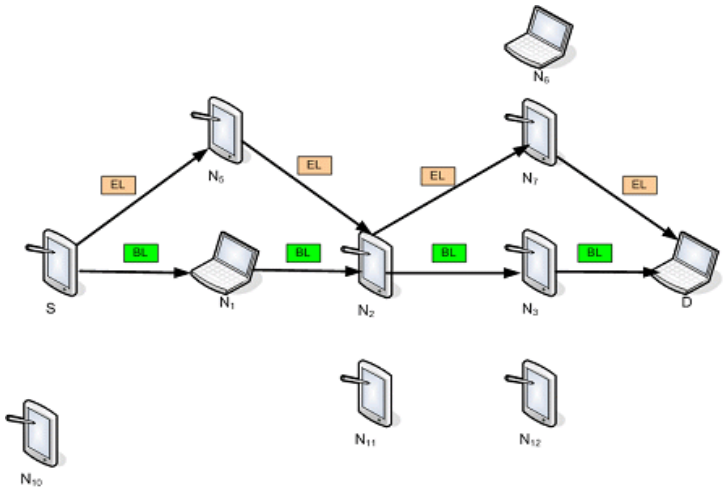

*b. using node-disjoint path*

*Fig 3.10. Base layer forwarding in AODV-MAP*

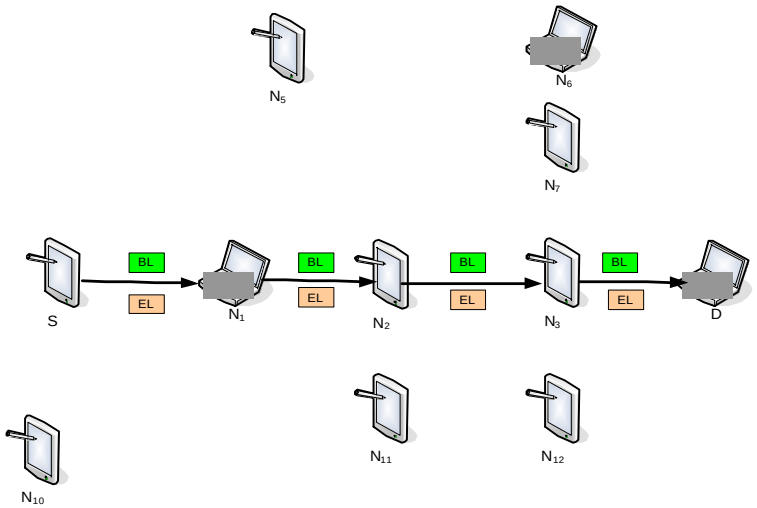
As in Fig. 3.10a, assume node $N_1$ moves away, then the primary path breaks. In this case, the source will look up path in the routing table and can use one of fail-safe paths ("S-$N_{10}$-$N_2$-$N_3$-D") to forward BL to the intended destination. As in Fig. 3.10b, if node $N_{10}$ moves away, then the fail-safe path also breaks. If there are still fail-safe paths available, the source will use them. If not, then it uses node-disjoint path

("S-$N_5$-$N_6$-$N_7$-D") to forward BL to the intended destination.

In case of enhancement layer forwarding, the source choose fail-safe paths first then only primary path.




*a. using fail-safe path*




*b. using primary path*

*Fig 3.11. Enhancement layer forwarding in AODV-MAP*

As in Fig. 3.11a, assume node $N_6$ moves away, then the node-disjoint

path breaks. As along as there is another node-disjoint path, the source will use that one. But there is no node-disjoint paths, then the source uses fail-safe path ("S-$N_5$-$N_2$-$N_7$-D") to forward EL to the intended destination. As in Fig. 3.11b, if node $N_5$ moves away, then the fail-safe path also breaks. If there are still fail-safe paths available, the source can use them. If not, then it will use primary path ("S-$N_1$-$N_2$-$N_3$-D") to forward EL to the intended destination.

## 2.5. Secure AODV-MAP Scheme

Normally according to security needs, ad hoc networks can be classified into three environments: open, managed-open and managed-hostile. [84] Among them, the managed-open environment is probably the one where most research is being done today and needs to satisfy security requirements [84] listed in Table 3.2.

| Security Requirement | Details |
|---|---|
| SR1 | Fabricate routing messages cannot be injected into the network by malicious node |
| SR2 | Routing loops cannot be formed through malicious nodes |
| SR3 | Routes cannot be redirected from the shortest path by malicious nodes |
| SR4 | Routing messages cannot be altered in transit by malicious nodes |
| SR5 | Routing signaling cannot be spoofed |
| SR6 | Unauthorized nodes should be excluded from route computation and discovery |

*Table 3.2 Security requirements for AODV-MAP routing*

Multipath routing protocols should be robust against not only dynamic

topological changes but also malicious attacks. Since AODV-MAP does not have any security mechanism, it is vulnerable to specific types of attack. SAODV-MAP is a security extension to AODV-MAP routing protocol. It targets an environment similar to managed-open environment. In addition, multipath ad hoc routing protocol should have lightweight computation, that means, need for lengthy and demanding computations should be avoided when possible. If not, computations should be affecting as few nodes as possible.

The main objective of SAODV-MAP is to secure multipath ad hoc routing and detect node misbehavior while reducing load of cryptographic processing. SAODV-MAP has acquired similar approach as in Secure Routing Protocol (SRP) [75]. SAODV-MAP implements HMAC shared key and requires security association (SA) between two communicating nodes. Further, SAODV-MAP also implements public key cryptography, certificate to ensure secure routing thus it also requires a trusted certificate server.

In SAODV-MAP, a node only accepts routing messages from verified one hop neighbors before including them in the routing process. Hence SAODV-MAP maintains neighbor node table, and src-rreqid table.

### *a. Operations*

SAODV-MAP has two phases. The first phase is the secure neighbor discovery phase, which involves the mutual authentication of neighbor nodes. The second phase of SAODV-MAP is the route discovery and maintenance phase, which involves the establishment and maintenance of multiple paths between the source and destination nodes securely. Notations used for the proposed security scheme is shown in Table 3.3.

| | |
|---|---|
| $K_{A+}$ | Public key of node A |
| $K_{A-}$ | Private key of node A |
| $MAC_K(M)$ | MAC value of message M under key K |
| $Sign_{K_{A-}}$(M) | Message M digitally signed by node A |
| $E_{K_{A+}}$(M) | Encryption of message M with $K_{A+}$ |
| $cert_A$ | Certificate belonging to node A |
| $t$ | Timestamp |
| $t_e$ | Certificate expiration time |
| $IP_A$ | IP address of node A |
| $MAC_A$ | MAC address of node A |

*Table 3.3. Notations used for SAODV-MAP scheme*

*Secure Neighbor Discovery Phase*

It is required that each node have access to a trusted certificate server prior to participate in the network. Thus before joining to the network, each node will obtain a certificate consisting of node address, its public key, timestamp t, and time $t_e$ at which the certificate expires.

T → A : $cert_A = Sign_{K_{T-}}(IP_A, MAC_A, K_{A+}, t, t_e)$

It requires every node to use certificates that bind their IP and MAC addresses with their public key. Each node will posses T's public key so it can decrypt certificates of other nodes. It's not possible for any node to change contents of the certificate being encrypted in T's private key $K_{T-}$.

Every node must authenticate itself with its one hop neighbor(s) to gain access to the network. Neighbors mutually authenticate each other when a node enters a neighborhood. Thereafter, nodes observe each other to ensure that nodes continue to use the same IP and MAC as provided during the authentication process.

Assume a node A is joined MANET domain. Then it broadcasts a *Hello* packet to one-hop neighbors in order to gain access to the network. The

*Hello* packet generated by A contains its IP address, MAC address, the certificate from a trusted third party (T).

A → * : *[Hello, $IP_A$, $MAC_A$, $cert_A$]*

Neighbor node (say node B) verifies the certificate signed by T using T's public key $K_{T+}$. If the certificate is expired, neighbor nodes discard the *Hello* packet and node A cannot gain access through its neighbors.

The neighbor node verifies if node A is using the same IP and MAC as in the certificate. If either of these changes, neighbor nodes can identify this spoofing after comparing IP and MAC of the *Hello* packet to the certificate IP and MAC. Thus a misbehaving node is denied any network access – since neighbor nodes cannot authenticate such a node.

If the $cert_A$ is valid, then neighbor node B creates an entry for A in the neighbor node table where A's public key will be stored.

In response to such *Hello* packet, neighbor node unicasts *Hello_rep* packet to the node A. After receiving *Hello*_rep packet, the node A also authenticates its neighbors.

B → A: *[Hello_rep, $IP_B$, $MAC_B$, $cert_B$]*

At the end of the neighbor discovery process, each node has a list of its one-hop neighbors with their IP addresses, MAC addresses, and public keys in neighbor node table. This data structure is used in local monitoring to detect malicious nodes.

Binding the MAC strengthens robustness of the protocol by disallowing nodes from appearing as multiple ones at the data link layer and by assisting against DoS attack.

In single-hop neighbor authentication process, *Hello* packet is repeated periodically to ensure that only nodes currently in the neighborhood have access and no malicious node(s) gain access through stale authentication.

*Route Discovery*

The route discovery process is similar to AODV-MAP scheme, with addition of keyed-hash message authentication codes to RREQ and RREP packets for end-to-end security. The part of route discovery process is shown in Fig. 3.12.

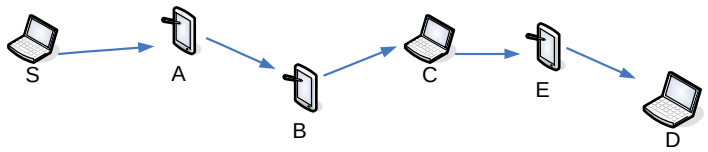



*Fig. 3.12. Route discovery process in ad hoc routing*

RREQ Generating and Processing at Source Node

A source S initiates a route discovery for a destination node D if no route discovery is under way for the same node D. S generates RREQ with the most recent Destination Sequence Number it has received from the desired destination.

The source also computes and appends HMAC to RREQ that covers RREQ ID, Src IP, Dest IP, and Sequence Numbers. The key $K_{SD}$ used in this HMAC is the one shared by this source and destination.

$$AUTH = MAC_{K_{SD}}(RREQ\_ID,\ IP_S,\ IP_D,\ seq\_no)$$

After appending its address in route_path, it will broadcast RREQ to neighbors.

$$S \rightarrow * : [RREQ\_ID,\ IP_S,\ IP_D,\ seq\_no,\ route\_path,\ AUTH]$$

RREQ_ID, $IP_S$ being unique, S maintains src-rreqid table that has RREQ_ID, src ipaddr and forwarded_node_list. S adds each neighbor to

forwarded_node_list if it overhears relaying RREQ with route_path{S, A}.

To update, the entry of scr-rreqid table, information of src-rreqid is piggybacked with neighbor discovery updates:

B → A: $E_{K_{A+}}(Hello\_rep,\ IP_B,\ MAC_B,\ cert_B,\ Sign_{K_B}(RREQ\_ID,\ IP_S,\ forwarded\_node\_list))$

The information is essential to ensure the neighbor nodes are correctly forwarding given RREQ.

RREQ Processing and Forwarding at Intermediate Nodes

Intermediate nodes cannot verify the HMAC in RREQ packets, but forward the duplicate RREQ as per the selective RREQ forwarding scheme specified in AODV-MAP scheme.

Intermediate node extracts last entry of route_path and verifies if this address is in neighbor node table. If not, RREQ is discarded; Intermediate node checks the route_path for duplicate entries; if a loop is detected, RREQ is discarded. Then intermediate node appends it's address to RREQ and broadcast.

Intermediate node maintains src-rreqid table, so it appends each neighbor to forwarded_node_list if it overhears relaying RREQ with route_path{S,B,C,E}

RREQ Processing and RREP Generation at Destination

The destination checks the Destination Sequence Number in incoming RREQ packets and discards stale requests. The HMAC from the source is checked, and illegitimate requests are discarded.

The recipient recomputes the authentication tag on the received message using the shared key. The integrity of the message is deemed valid only if the two authentication tags match.

Further, the destination is responsible for discovering multiple alternative paths - node-disjoint and fail-safe paths as specified in AODV-MAP scheme.

D generates a route reply (RREP), which comprises: RREQ_ID, $IP_S$, $IP_D$, seq nos, route_path. RREP packet contains the discovered paths and also serves as the information necessary to be forwarded across the network towards S.

To determine route_path, D extracts the identifiers of the intermediate nodes previously accumulated route_path in the RREQ, D stores them in reverse order in the RREP. And, it computes authenticator

$$AUTH_1 = MAC_{K_{SD}}(IP_S, IP_D, seqno, route\_path)$$

The destination unicasts RREP along the path information in it ie, transmits the RREP to the first entry of the route_path.

Route Reply Processing at Intermediate nodes:

Each intermediate node verifies that its successor is indeed the node that now forwards the RREP. If not, it discards RREP. Otherwise, intermediate node verifies that RREP sending node is in forwarded_node_list. If not, it discards RREP. Otherwise, intermediate node checks if there is any duplicate entry in Route; if yes, it discards RREP. Otherwise, intermediate node relays the reply to its predecessor, i.e., the next entry in the route_path until RREP reaches the source S.

Route Reply Processing at Source:

Once source S receives RREP, it verifies that its successor is indeed

the node that now forwards the RREP. If not, it discards RREP. Otherwise, S calculates and compares $AUTH_{1'}$ to $AUTH_1$. If there is not a match, S rejects the reply. Otherwise, S accepts the reply, and extracts the route entries.

***Route Maintenance***

Nodes continually monitor connectivity to their neighbors by exchanging *HELLO* messages. In response to an outage on an active link, nodes generate RERR message to inform the source and destination nodes of all active routes using this link of the link break. Any node that participates in the broken route marks the particular route as invalid and re-broadcasts the message until source and destination are informed about the path breakage.

SAODV-MAP uses a timestamp, along with digital signature that covers the RERR fields, to authenticate the packet and ensure freshness. If the error messages are not signed, malicious nodes might flood the network with fake error messages even for routes that they do not participate in, and in this way disable communication.

According to the operation mode, an end node may restart the route request either when a threshold number of paths or all existing paths from source to destination are broken.

# 3. Hybrid Ad Hoc Network

## 3.1. Existing Approaches for Hybrid MANET

***Mobile IP for Mobile Ad Hoc Networks***

Jonsson et al [86] proposed MIPMANET (Mobile IP for Mobile Ad Hoc Networks) enabling visiting nodes to get wireless Internet access.

MIPMANET uses Mobile IP with foreign agent care-of-address and reverse tunneling, and exploits the mobility services of Mobile IP. MIPMANET combines Mobile IP protocol, which guarantees location independent routing, and AODV routing protocol, which is reactive in nature. When visiting node wishes to communicate with a correspondent node on the Internet, it should tunnel its packet to the Mobile IP foreign agent it is currently registered with, which will de-tunnel it and forward it to the Internet. It is clear that Mobile IP foreign agents act as default routers for the visiting node. The use of tunneling helps implement the notion of default router within a MANET. Mobile IP foreign agents advertise their presence by broadcasting their agent advertisements. A visiting node will be able to select a foreign agent based on the hop count metric. According to MIPMANET cell switching (MMCS) algorithm, a registered visiting node should switch to a new foreign agent if for two consecutive agent advertisements, it is at least two hops closer to this foreign agent than to its current one. Any message sent by a correspondent node to a visiting node will be received by the Mobile IP foreign agent currently serving the visiting node. The foreign agent will forward the message to the visiting node.

*Sun's Approach*

Sun et al [87] proposed an approach using AODV routing protocol and Mobile IP to provide MANET nodes with Internet connectivity (see Fig. 3.13). Furthermore, they suggested a simple scheme allowing mobile nodes to obtain co-located CoA when CoAs are not available. Co-located CoA assignment requires at least one gateway be located between a MANET and the Internet to advertise routable network prefixes on the underlying network. Mobile nodes should also run a duplication address detection to guarantee uniqueness of their selected IP addresses. When foreign agents

exist, Mobile IP protocol is used to provide mobile nodes with care of addresses, while AODV is exploited for route discovery and maintenance within MANET. Mobile IP foreign agents advertise their presence via periodical agent advertisement, which are broadcast within a MANET. The interested mobile nodes unicast their request registration to the selected foreign agent using available fresh routes. Then, mobile nodes can start their Internet access session and communicate with the wired Internet through their selected Mobile IP foreign agents. Alternatively, a mobile node can discover existing foreign agents by proactively sending a route request targeting all mobility agents multicast group address 224.0.0.11. In order to find whether a particular destination is within a MANET or on the Internet, a mobile node broadcasts a route request within a MANET. If the source node receives a route reply from a mobile node, it concludes that the destination is located within a MANET. Otherwise, the destination is on the Internet if the source node receives a special route reply from a foreign agent.

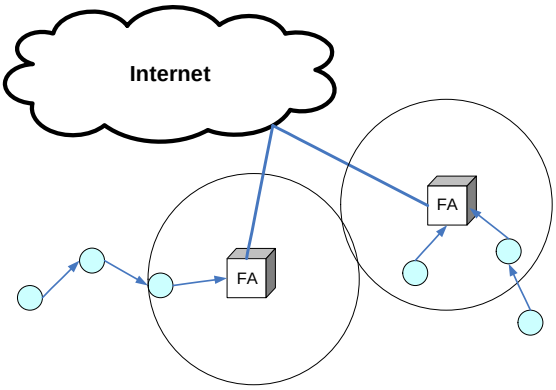



*Fig. 3.13. Network Architecture for Sun's Approach*

## 3.2. Related Works

Lots of research works have focused on the integration of MANETs and the Internet [89]. The idea of integrating the Internet and MANETs

was originally introduced by Lei and Perkins [90].

Ergen and Puri proposed two protocol architectures - MEWLANA-TD and MEALANA-RD [91]. Broch et al. [92] proposed a solution to the integration of MANET with Mobile IP while Jonsson et al. [86] proposed MIPMANET. Sun et al. [87] proposed an approach, where AODV routing protocol and Mobile IP cooperate to provide MANET nodes with Internet connectivity.

Ratanchandani and Kravets [93] proposed a hybrid scheme - reactive and proactive approaches using Mobile IP to provide global Internet connectivity to MANET nodes. Ahlund and Zaslavsky [94] proposed a multihomed Mobile IP-based solution. Xi and Bettstetter [95] proposed a solution for Interworking between wireless ad hoc networks and the internet. Ryuji Wakikawa et al. [88] specifies a method for global connectivity for IPv6 MANET networks.

Furthermore, the authors [94] have proposed the concept of dynamic gateway, which acts as an interface between MANET and the Internet, the load-balancing problem is considered on the dynamic gateway for ad hoc Internet connectivity, and secDSDV protocol is proposed to enhance security performance for the network.

Bin Xie and et [96] proposed the infrastructure-supported distributed authentication protocol to enhance trust relationships amongst ad hoc hosts. In addition, an effective secure routing protocol is discussed to protect the multihop route for internet and ad hoc communication. In the integrated ad hoc networks with Internet accessibility, the ad hoc routing security deployed with the help of infrastructure, has a fundamental impact on ad hoc hosts in term of internet access, integrity, and authentication.

And several error protection schemes had been studied for audio streaming over the Internet and wireless channels. Error control scheme based on FEC is proposed in [105] for audio streaming over the Internet.

Yung et al. described a fixed UEP scheme for MPEG audio over wireless channels [106]. In [107], the authors introduce error resilience in conjunction with error protection for scalable audio streaming over wireless networks.

## 3.3. Approach for Internet connectivity in AODV-MAP based Hybrid MANET

We put forward an approach for IP routing in ad hoc network based on Mobile IP. Network Architecture of MANET integrated with the Internet is shown in Fig. 3.14.

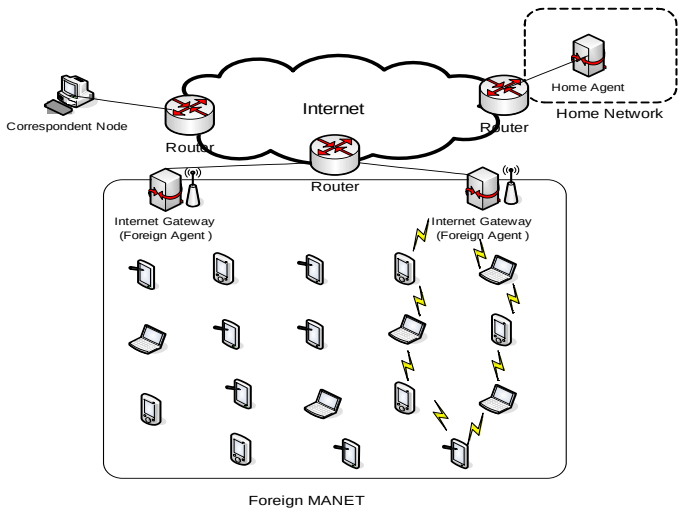



*Fig. 3.14. Network Architecture for AODV-MAP H-MANET*

We assume the network under consideration comprises the following elements:

- MANET consisting of mobile nodes with wireless interfaces and routing capabilities to perform multihop communications.
- Correspondent nodes are nodes connected to the Internet, (i.e. Internet node), and connectivity is possible with all other nodes, including

MANET nodes.

- Internet Gateways can connected the ad hoc network via, wireless LAN interface and access to the Internet via other interfaces. In this architecture, multiple fixed Internet gateways are considered.

The challenge with integrating MANET with the Internet is to ensure the MANET nodes and Internet nodes can communicate seamlessly. Hence, we need to utilize Mobile IP, combined with enhancements to cope with the additional complexities introduced by the wireless ad hoc network.

According to Mobile IP principles, when a node roams to a new foreign domain, it can receive a CoA from the FA, and all packets addressed to this node's home address will be tunneled to the CoA. In the case of a connected MANET, the mobile ad hoc network becomes the foreign domain for the roaming node, and the gateway node becomes its serving FA. The home IP address of the roaming node will therefore have to be the IP address identifying the node globally, and it also has to be retained as the roaming node's identifier within the foreign MANET domain.

The mobile ad hoc network is visible from the Internet side via the IP address of the gateway. This gateway also happens to be a FA for the nodes currently in the mobile ad hoc network. However, MANET nodes will have their home addresses featuring a network prefix different from that of the gateway, and therefore will have to register with the gateway as their FA.

This section presents an architecture framework suitable for integration of ad hoc networks with the Internet via multiple gateways. We discuss gateway discovery and selection scheme suitable for the Mobile IP based routing of IP packets across the multiple gateways.

Specifically, this approach integrates Mobile IP and AODV-MAP protocols (refer to chapter 3 section 2.3), such that mobile nodes may

obtain a CoA and access the global Internet, even when they are multiple hops away from the access point. The proposed approach utilizes AODV-MAP routing for discovery and maintenance of routes within the MANET, whereas Mobile IP protocol is utilized such that mobile nodes may obtain CoAs, and hence Internet connectivity, through multihop paths to FA. However, since the scope of AODV-MAP scheme is limited to the interior of the MANET, we have modified AODV-MAP scheme to support Internet connectivity via gateway. In this architecture, we assume that fixed multiple IGWs connect the MANET to the Internet and broadcast their own global prefix information to the MANET.

### *a. Operations*

In the proposed approach, there are following operations:

- FA discovery
- Multiple gateway Selection
- MN registration
- Route Discovery

#### *Foreign Agent Discovery*

Foreign agent discovery procedure is operated as follows. When a mobile node wishes to reactively discover a foreign agent, it may do so by issuing RREQ. This RREQ is same as in AODV-MAP that has the destination IP address set to 224.0.0.11, the “All Mobility Agents” multicast group address. The mobile cannot put the IP address of the FA into the RREQ because it may not know FA's address. The mobile node then broadcasts this RREQ to its neighbors.

When a neighbor node receives this RREQ, it first checks its Foreign Agent List to determine whether it is currently registered with a FA. If the node is not running Mobile IP, then it does not have a Foreign Agent

List, and so it simply re-broadcasts the request. Also, if the mobile node is not registered with any FAs, then it likewise re-broadcasts the request. If, on the other hand, the mobile node is currently registered with a FA, then the mobile checks whether it has a current route to that FA. It is possible for the node to be registered with a FA while its route to that agent has expired or been invalidated. If the mobile node does not have a current route to the FA, then it re-broadcasts the request. Otherwise, if it does have a current route to the FA, it creates a route reply with the IP address of the FA. The agent's IP address is placed in the Foreign Agent IP Address field of the RREP extension. The foreign agent group IP address (224.0.0.11) is placed in the Destination IP Address field of the RREP. The RREP is then unicast back to the source node. In case of AODV-MAP, several RREPs with same FA's address or with different FA's address will be received by the source node. If it receives RREP for same FA's address, it will discard other than the first one.

When the source node receives a route reply for a FA, it can then use that route to unicast Agent Solicitation message to the FA. The TTL of the Agent Solicitation should be set appropriately, so that the FA is ensured of receiving the Solicitation. Upon receiving the Agent Solicitation message, the FA unicasts an Agent Advertisement back to the mobile node.

After receiving the Agent Advertisement messages from different FAs, the mobile node proceeds by selecting the optimum gateway and then selects one of the advertised CoAs to be its own CoA.

### *Agent Advertisements*

The gateway between the ad hoc network and Internet is configured as a Mobile IP Agent. On the wireless interface, it has to advertise its existence by broadcasting Agent Advertisement, an ICMP Router

Discovery Protocol (IRDP) packet. The ICMP packet is generated in order to broadcast the address of a router. The Agent Advertisement has an IP header with local broadcast as a destination address, and an ICMP header. The Registration Request and Registration Reply packets in standard Mobile IP [17] are application layer packets using UDP as the transport protocol. The standard Agent Advertisement message is a direct (local) broadcast packet which will not be propagated further than one-hop away. Hence in the ad hoc network where majority of mobile nodes are located multiple hops away from the gateway, the approach to propagating the ICMP and registration packets multiple hops away from the source is the key for mobile nodes to receive the appropriate agent discovery information.

***Multiple Gateway Selection***

The different methods for multiple gateway selection can be used to forward packets between the Internet and ad hoc network. The challenge stems from the need to inform ad hoc nodes about available gateways and their associated capabilities in an infrastructure-less and extremely dynamic environment.

A straightforward solution for gateway selection is to select the gateway that has the shortest number of hops to the mobile node as the 'working' gateway. This means that when a mobile node is closer to a new gateway than the previous one, the mobile node will usually switch to the second gateway for the global connectivity. Generally speaking, selecting a gateway based on only the shortest number of hops does not appear to be good enough.

However, in a case of multiple gateways, the availability of multiple gateways provides the ad hoc network with higher robustness and more flexibility for global Internet connectivity. Therefore, network with multiple

gateways, it is important to discover and select a gateway that is the 'optimal' one among all available gateways, according to certain criteria.

The existing IGW selection mechanisms for MANET with multiple IGWs take the hop count between MANET node and IGW, the load of IGW or the receiving interval of IGW advertisement (IGWADV) messages as the metric.

In this approach, we have considered two metrics – distance-based hop count (shortest path to IGW) and offered load by IGW. Based on these metrics, we propose robust IGW selection scheme. In this scheme, a MN first computes the optimum IGW and chooses a default IGW among the IGWs. Total offered load that is the sum of all loads on any IGW;

$$\mu = \sum_{i=1}^{n} \lambda_i \kappa_i$$

where $\lambda$ is the average traffic arrival rate per second, $\kappa$ is the average packet length per second, $n$ is the number of nodes connected to an IGW.

The selection formula is calculated as follows:

$IGW = a \times sp + \beta \times \mu$ ; $a + \beta = 1$

$IGW_{opt}$ = min $\{IGW_1, \ldots IGW_n\}$ = $\min\{IGW_i\}_{i=1}^{n}$

where

$sp$ – distance by hop count

$\mu$ – offered load

$a$, $\beta$ – weighting factors

***MS Registration with Foreign Agent***

When a mobile node receives an Agent Advertisement with 'R' bit set, the mobile node must register with the foreign agent, as specified in [17]. If the mobile node receives an Agent Advertisement without 'R' bit set, then it MUST register with the foreign agent if it requires Internet

connectivity. To register with the foreign agent after receiving an Agent Advertisement, the node creates a Registration Request and fills in the fields of the Registration Request as indicated in [17]. The node then unicasts the Registration Request message to the foreign agent. The node should have a valid path to the foreign agent because it has just received an Agent Advertisement from the agent. In the event that the mobile node's route to the foreign agent has become invalid, the node can initiate a route discovery procedure to find a new route to the foreign agent. It can then use that route for the transmission of the Registration Request.

The foreign agent processes the Registration Request as specified in [17], with the exception that, when it receives the Registration Reply from the home agent, it unicasts this Reply along the (possibly) multihop path back to the mobile node. Upon reception of the Registration Reply, if the foreign agent's route to the mobile node has timed out or been invalidated, the foreign agent must discover a route to the mobile node. For instance, it may use the route discovery procedure described in AODV-MAP scheme.

***Route Discovery***

In an isolated MANET, the route discovery is based upon a query-reply cycle, with flooding of queries towards a target of an unknown address. In Hybrid Ad hoc network, if the target node is located outside the ad hoc network, the source node will not receive a reply from the target directly, but via other nodes acting as proxies for the target.

A mobile node that needs a route to a destination does not initially know whether the destination node is within the ad hoc network, or whether it is reachable through the wired interface of the FA. It therefore must first search the ad hoc network for the destination. If a route to the destination is not discovered within the mobile ad hoc network, the mobile

can conclude that the destination is not in the ad hoc network, and hence it can use the foreign agent as a default router and send the data packets for the destination directly to the FA.

The gateway shall be able to respond promptly if it can maintain more routing information in its IP routing table. Since the gateway is a FA, it should have information about all ad hoc nodes registered with it. On the other hand, the gateway may gather external routing information in a way typical of an edge router. The gateway can use the information about the exterior and about the registered ad hoc nodes to form responses to route request queries.

If MANET nodes have IP addresses (e.g. home addresses) with a range of network prefixes, the initiator will not know whether the target is within the ad hoc network or not. To begin the search for the destination, the source node creates a route request for the destination, as specified in AODV-MAP scheme. It will broadcast a RREQ to enquire about a route to the target. At the intermediate nodes, the route request is processed as specified in AODV-MAP routing as well. The RREQ packet floods the ad hoc network and eventually will also be received by the gateway.

For a gateway to know which hosts are in the ad hoc network, the AODV-MAP protocol requires information from the visitor list in the FA. All hosts homed in the ad hoc network have to have the same network number as the gateway interface connecting to the ad hoc network (the visitor list is a part of the MIP information distributed into AODV-MAP). When a route is requested for a destination with a network number different from the ad hoc network, the visitor list is searched by the AODV-MAP process to see if the destination is available in the ad hoc network.

To manage multiple FAs covering mobile ad hoc network, visitor information need to be synchronized between the FAs. Without

synchronization, a gateway may conclude that a destination is within the wired IP network and send a proxy RREP to the source, while the destination is in fact within the ad hoc network but registered with another FA.

The FAs update their visitor lists using the wired IP network to relieve the ad hoc network. The information is synchronized when an entry is added or deleted from the visitor list in a gateway. All gateways will thus be able to see if a visiting host is within the mobile ad hoc network even if it is not registered with the gateway receiving the RREQ. The gateway looks up its IP routing table and visitor list to find a matching network prefix for the target address.

When a FA receives a RREQ, it checks its route table to determine whether it has an explicit route entry for the destination node. The FA may have such an entry if the destination is a registered mobile node within the ad hoc network. If the destination is known to be within the mobile ad hoc network, the gateway will function as an ad hoc host forwarding the RREQ and the destination will respond with a RREP.

If the target address is confirmed to be outside the MANET domain, the gateway will create a proxy RREP containing the route from the target to the initiator. The initiator can use the proxy RREP to update the route to the target. If the initiator of the RREQ does not receive any RREP within the request expiry time, it will conclude that the target is an unknown address on the Internet and send packets to the gateway.

### *Extended AODV-MAP Routing*

Since AODV-MAP routing protocol has features such as discovering multiple alternative paths, path accumulation approach and setting path labels, problems arise when external routes are incorporated into isolated ad hoc routes.

Every data packet exchanged between hosts on the ad hoc network will have AODV-MAP header with path accumulation listing all intermediate addresses of nodes along the path to the destination.

Nodes from outside the ad hoc network are excluded from AODV-MAP route discovery procedures, hence packets to and from external nodes cannot normally be routed by means of AODV-MAP protocol. Therefore, it is essential to develop extensions to ad hoc routing to facilitate routing of packets across a gateway.

In the case when the gateway receives first RREQ from the source, it appends itself as the last-hop-external node and also sets path type to 1 to indicate that this path is primary path. Then it sends proxy RREP back to the initiator of the RREQ. For the duplicate RREQs from same source and same RREQ ID, it will follow same procedure as in discovering multiple alternative paths for AODV-MAP scheme.

When an IP packet arrives at the gateway from the Internet, the gateway inserts the AODV-MAP header, including route_path, and marks the AODV-MAP packet as first-hop-external node. The packet indicates the source is the Internet correspondent node, and route_path contains the gateway node as the first intermediate node, followed by the rest of the route to the destination ad hoc network node. The destination MANET is responsible to discover multiple alternative paths to the first-hop-external node, that is, the gateway.

## *3.4. Secure Framework for Internet connectivity in AODV-MAP based Hybrid MANET*

We propose a secure framework for global IP connectivity in MANET connected to Internet. Network architecture for hybrid MANET is shown in Fig 3.15.

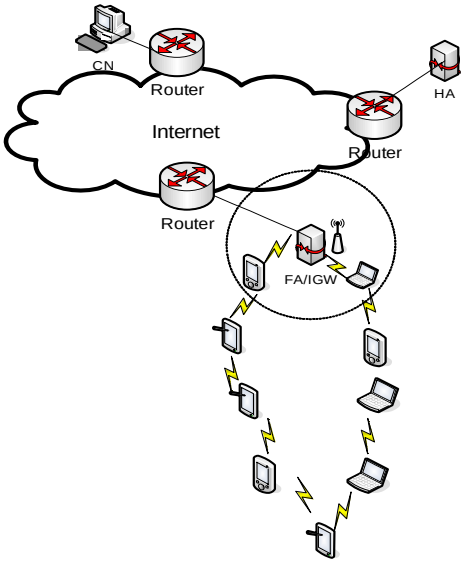



*Fig 3.15. Network architecture for secure AODV-MAP H-MANET*

### *a. Operations*

Our proposed approach accounts both the Mobile IP security and ad hoc routing security. Thus the approach for secure connected MANET includes two portions: Mobile IP security and ad hoc security. In order to communicate with the MNs within MANET domain or outside, a MN performs the following four operations:

- Neighbor Discovery
- FA discovery
- MN registration
- Route Discovery

In the proposed approach, when a mobile node is added to Mobile IP system, HA will allocate new mobile node permanent address ($MN_{HM}$), secret key ($S_{MN-HA}$) and *nonce*. This data is consigned to MN on a secret channel. After the user registration step, MN stores records of a mobile node permanent address ($MN_{HM}$), secret key ($S_{MN-HA}$) and *nonce*. HA also

stores same records in the local table.

A secret key $S_{MN-HA}$ is used not only for calculation and validation of MAC (Message Authentication Code) but also for data encryption. Certification Authority, HA, and FA have a pair of public and private keys separately for their mutual authentication.

***Neighbor Discovery***

MN uses a key generation function to calculate a pair of private and public keys. Prior to the joining in the network, each node gets cert from Trusted CA which is located at home network. Neighbor Discovery process is same as in secure AODV-MAP scheme (refer to chapter 3 section 2.5).

***Secure FA Discovery***

A FA periodically broadcasts this *advertisement* to MNs.

$FA \rightarrow MN$ : $M_1$, $\mathrm{Sign}_{K_{FA}}(M_1)$ , $Cert_{FA}$

where $M_1$ is A*dvertisement, SeqNo,* $FA_{id}$ , $N_{FA}$ and $MN_{CoA.}$

The sequence number is incremented every time when a new advertisement is issued by the FA. While receiving an advertisement from the FA, the MN decrypts the advertisement by using FA's public key, and compares the FA's address, nonce, and the sequence number with those of previously received advertisement in its table. MN discards the duplicate advertisements. If it is a fresh advertisement, MN records the FA's certificate, IP address, a nonce and sequence number. A MN may rebroadcast this *advertisement* on its interface to send advertisement to these MNs who might have recently moved into its domain.

In this case, a mobile node is not allowed to discover reactively the gateway and depends upon the proactive discovery. When a mobile node

receives Agent advertisements from multiple FAs/gateways, it will first select optimum gateway.

***MN Registration with FA and HA***

Each MN must register with the FA before ad hoc route discovery. There are two features for MS registration: 1) mutual authentication between MS and visiting network (FA) and 2) mobility binding for MS as per Mobile IP protocol. Full-fledge registration and authentication with FA and HA is shown in Fig 3.16.

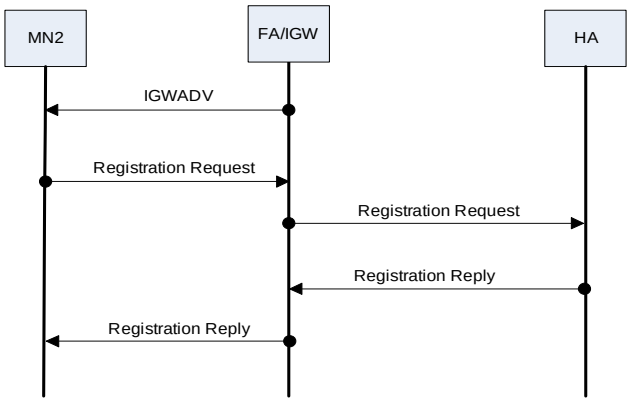



*Fig. 3.16. MS Registration Process in AODV-MAP H-MANET*

Step 1

$MN \rightarrow FA$: $M_2$, $MAC_{S_{MN-HA}}(M_2)$

where $M_2$ = *Registration Request*, $FA_{id}$, $HA_{id}$, $MN_{HM}$, $MN_{COA}$, $N_{HA}$, $N_{MN}$, $h^n(s)$, $N_{FA}$

Compute hash chain with random seed s: $h^n(s) = h(h.(h(s)..))$

When the MN receives the agent advertisement, the MN will issue a registration request along with the actual address $MN_{HM}$, HA address $HA_{id}$, HA's nonce $N_{HA}$, FA address $FA_{id}$, mobile user's care of address

$MN_{COA}$, FA's nonce $N_{FA}$ and random nonce $N_{MN}$ and $h^n(s)$. It uses the secret key $S_{MN-HA}$ to create MAC for registration request in order to protect the integrity of message. Then it will send it to FA.

Step 2

$FA \rightarrow HA$: $E_{K_{HA}}(M_3 , Sign_{K_{FA}} (M_3) ), HA_{id} , Cert_{FA}$

where $M_3 = MAC_{S_{MN-HA}}( M_2 ) , MN_{HM}$

When FA receives the message, it will validate $N_{FA}$. If the nonce is lawful, the FA will use HA's public key to encrypt the message after digital signature of message $MAC_{S_{MN-HA}}(M_2)$ and $MN_{HM}$ generated using FA's private key.

Finally, the message is sent to HA with $HA_{id}$ and FA's certificate $Cert_{FA}$. If the nonce isn't lawful, FA will ignore the registration message and return an error message to the MN.

Step 3

HA

HA checks if the $Cert_{FA}$ is lawful, and uses its private key and FA's public key to decrypt and verify the message integrity and validity. If the message integrity and validity are lawful, it will proof the message contents, otherwise it will abort the registration request and return an error message to FA.

The HA use the $MN_{HM}$ find the common secure key to decrypt message $M_2$. Then the $N_{MN}$ is validated in the database with the received message and the $MN_{COA}$ corresponding to the MN is saved after the message is effective.

If HA verify the message have any error, HA will return an error message to the FA and abort the registration procedure.

Step 4

$HA \rightarrow FA$: $M_4$

where $M_4$ = $E_{K_{FA}}(Sign_{K_{HA}}(M_5, S_{sk}, N_{FA}, h^n(s), MN_{COA}), M_5, S_{sk}, N_{FA}, h^n(s), MN_{COA}), FA_{id}$ , $Cert_{HA}$

and $M_5$ = $E_{S_{sk}}(Registration\ Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA},)$, $E_{S_{MN-HA}}(S_{sk}, N_{MN})$

If the authentication messages are lawful, the HA produces a new random nonce $N'_{HA}$, session key $S_{sk}$ and save in database.

HA response ($Registration\ Reply, Result, FA_{id}$ , $HA_{id}, MN_{HM}, N'_{HA}$ ) use the session key encryption and response $S_{sk}$, $N_{MN}$ use secret key $S_{MN-HA}$ encryption. The HA sends message $M_5$, $S_{sk}$, $h^n(s)$, $N_{FA}$ and $MN_{COA}$ and use the HA private key to generate the message's digital signature and use FA's public key encryption to send to FA with $FA_{id}$ and $Cert_{HA}$.

Step 5

$FA \rightarrow MN$: $M_5$

where $M_5$ = $E_{S_{sk}}(Registration\ Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA},)$, $E_{S_{MN-HA}}(S_{sk}, N_{MN})$

When FA receives the message, it uses it's private key to decrypt the message. It then uses HA's public key to decrypt and verify the message's integrity and validity with $Cert_{HA}$. Then FA will check if received $N_{FA}$ is equal to the previously sent nonce. If the nonce is lawful, FA uses the $S_{sk}$ to the decrypt message and check the registration result. FA will keep $S_{sk}$ for future communication. If the register result is successful; the FA will send $M_5$ to the corresponding MN. After the test and verification, the FA will deliver the message with mobile node's encrypted message using the session key $S_{sk}$.

Step 6

*MN*

When the MN receives the message, it uses the $S_{MN-HA}$ decrypt the $S_{sk}$ with the $N_{MN}$. If the received $N_{MN}$ is equal to the previously sent nonce, the MN uses the $S_{sk}$ to decrypt the registration result. If the authentication succeeds, the MN saves the new nonce $N'_{HA}$ and $S_{sk}$. The MN will use the $S_{sk}$ to communicate with the FA whereas the $N'_{HA}$ for next full authentication.

## *Fast Authentication Process*

In Mobile IP protocol, a MN must perform the home registration to register with HA frequently. If the FA is far from the home network, full authentication processes need more computation cost and the authentication time delay will be long. To reduce the time delay of authentication at home registration every time, efficient local authentication can be used to achieve efficiency and robustness. Thus when the MN roams into the same MANET foreign network, the fast re-authentication protocol is used.

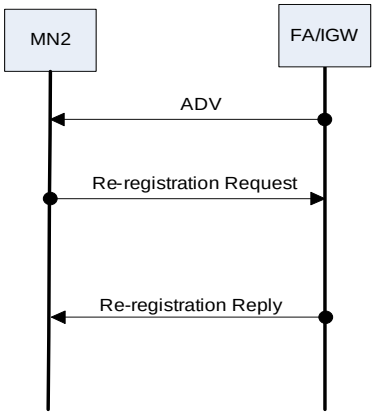



*Fig. 3.17. Fast Re-authentication process in AODV-MAP H-MANET*

The detailed authentication message exchange of the fast

re-authentication protocol is shown in Fig 3.17. The authentication method is based on the hash chaining technique.

Step 1

FA → MN

Adv: $N'_{FA}$

FA will send Adv with nonce $N'_{FA}$.

Step 2

MN → FA: $M_1$

$M_1 = Auth_1, MN_{HN}, h^{n-i}(s), t$

Where $Auth_1 = MAC_{S_{sk}}(MN_{HN}, N'_{FA}, h^{n-i}(s))$

MN computes $h^{n-i}(s)$ and then $Auth_1$ by using session key. MN sends $M_1$ to FA. (the MN will compute $h^{n-1}(s)$, $h^{n-2}(s)$, $h^{n-3}(s)$ for each re-authentication procedure, so it can prove itself by $n$ times), the AAA server verify the $h(h^{n-1}(s)) =? h^n(s)$.

Step 3

FA

Validate $N'_{FA}$

Verify $h(h^{n-i}(s)) =? h^{n-i+1}(s)$

$Auth_2 = MAC_{S_{sk}}(h^{n-i}(s))$

$S'_{sk} = prf_{S_{sk}}(Auth_2)$

where $prf_{S_{sk}}$ is pseudo-random function with key $S_{sk}$

When FA receives the message, it will validate $N_{FA}$. Then FA verifies hash chain (one-time password) by $h(h^{n-i}(s)) =? h^{n-i+1}(s)$. If passed, the foreign AAA server has authenticated the MN. The $h^{n-1}(s)$ is stored for next re-authentication process. FA computes as $Auth_2 = MAC_{S_{sk}}(h^{n-i}(s))$

and computes session key $S'_{sk} = prf_{S_{sk}}(Auth_2)$.

Step 4

FA → MN

$Auth_2$, $S'_{sk}$

FA responses a challenge by sending $Auth_2$, $S'_{sk}$

Step 5

MN

Verify $Auth_2$

$S'_{sk} = prf_{S_{sk}}(Auth_2)$

MN first verifies the $Auth_2$ by the $S_{sk}$. MN derives the $S'_{sk}$ by $S'_{sk} = prf_{S_{sk}}(Auth_2)$

If $Auth_2$ is lawful, it means the reply is trustworthy. Otherwise, the MN will ignore this message. Our scheme provides the mutual authentication for MN and IGW/FA. And localized authentication is efficient to decrease the authentication time delay.

*Route Discovery*

MN must have SA with FA in order to precede route discovery process. Secure route discovery is same as specified in Secure AODV-MAP (Refer to chapter 3 section 2.5).

## 3.5. AODV-MAP based Distributed multimedia delivery network

### a. Overviews

In this section, we present a framework for media delivery over AODV-MAP based hybrid ad hoc network. We not only focus on the use

of an approach for global connectivity as specified in chapter 3 section 3.3 but also use of robust scalable audio streaming over multipath MANET.

With the comprehensive consideration of concepts of CDN and scalable audio coding, a framework for distributed multimedia delivery network is put forward in order to provide audio streaming services in hybrid ad hoc network. The network architecture for Distributed multimedia delivery network based on AODV-MAP hybrid MANET is illustrated in Fig. 3.18.

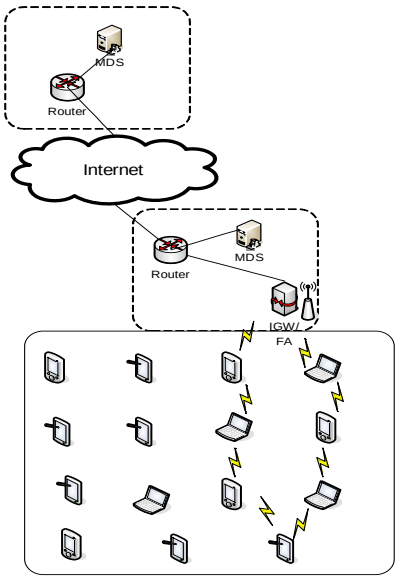



*Fig. 3.18. Network architecture for Distributed multimedia delivery network*

Distributed multimedia delivery network is an approach for the delivery of streaming media over multipath hybrid MANET. The audio streaming services are pushed to the edge server so that the delivery time for services is significantly reduced by the media delivery network. The scalable speech coding is deployed for audio streaming purpose. The scalable audio coding alone may not be a good match to the unreliable

network, the ability to perform prioritized re-transmission or unequal error protection at the end hosts can provide a virtual end-to-end channel that can better exploit the scalable coding properties. Thus we have used basic coding technique of MPEG-4 audio coding, which is capable of provisioning UEP for scalable audio coding.

The media streaming services are pushed to the edge of delivery network so that the delivery time for services is significantly reduced by the media delivery network. In each media delivery network, a set of distributed *Media Distribution Servers* (MDSs) interact and collaborate with each access network for media delivery to mobile nodes in the wireless access network, ie MANET. Each MDS stores the audio contents that were originally downloaded from the service provider during the streaming service publication.

The distributed multimedia delivery network helps to deal with the following problems:

- Network congestion and server overload problems in the star-type network topology.
- The streaming media is delivered from the closest edge server and not from the origin server, the streaming media is sent over a shorter network path, thus reducing the media service delivery time (end-to-end delay), the probability of packet loss, and the total network resource occupation.
- The high requirement of storage, reliability and load balancing among the distributed media edge servers and thus high cost of network components in the conventional CDN.

In MANET domain, we have implemented AODV-MAP scheme as a routing protocol which is described in chapter 3 section 2.3. As per our

study, when we use scalable audio coding, the different layers of media traffic can be forwarded in different paths as specified in chapter 3 section 2.4.

In this framework, the audio traffic coming from Internet enters the integrated MANET through the gateway, so when either core bit stream or enhancement bit stream of MPEG-4 audio traffic reaches the gateway, the gateway will deliver BL or EL on the appropriate path. This scheme can provide better traffic allocation and easily provide load-balancing.

# IV. Evaluation

## 1. Network Simulation Tool

There are several different simulation programs that can be used for the simulation such as ns2, OPNET, QualNet, Glomosim etc.

OPNET is a simulation tool that is developed by OPNET Technologies Inc. OPNET can be used in different areas like, performance troubleshooting; deployment planning; auditing; network capacity and resiliency planning; and network technology research and development.

OPNET is graphic user interface (GUI) and user friendly. OPNET is based on hierarchical modeling – Process, Node and Network, which is shown in Fig. 4.1. For our research work, we have considered OPNET Modeler.[4]

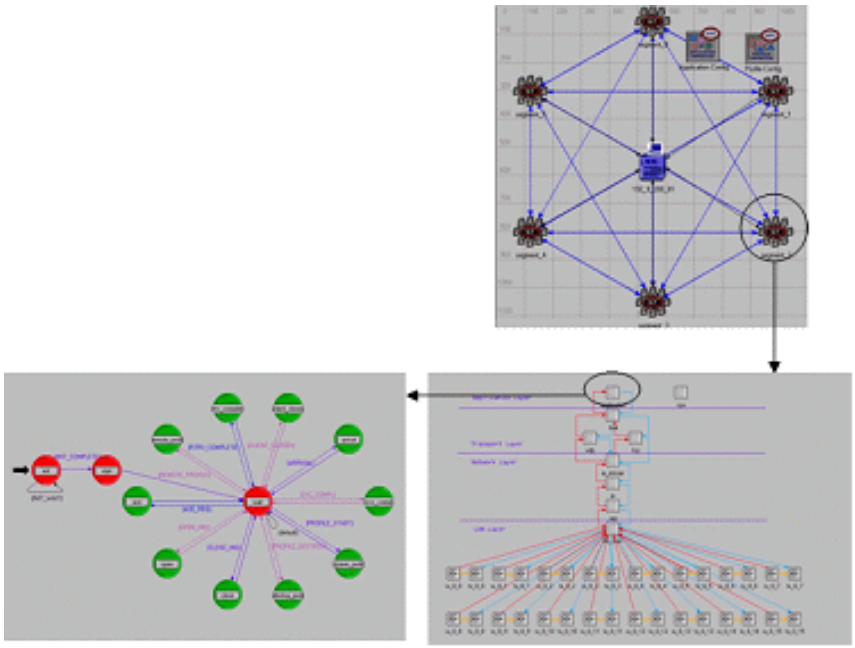


*Fig 4.1. Hierarchical Model of OPNET*

## 2. OTP-based Authentication Scheme for Wireless mobile network

OTP-based Authentication Scheme for wireless mobile network is proposed in chapter 3 section 1.2.

### 2.1. Analysis of OTP-based Authentication Scheme

#### A. Security Analysis

The OTP-based authentication mechanism is analyzed:

- Malice attack Protection - In this scheme, the AP receives the password which is processed from the client and the server's original password XORing with stream bits and verify it in order to defend malice attack.
- Mutual Authentication - This scheme provides mutual authentication. Strong mutual authentication can prevent user from being impersonated.
- Replay Protection - This scheme is inherently designed to avoid replay attacks by choosing one-time password is that it refreshes secret key of WEP in IEEE 802.11 anytime. Because of refresh OTP, the lifetime of the share key can be extended.
- Confidentiality Each the element of the key exchange is protected by a shared secret that provides high confidentiality.

#### B. Performance Evaluation

It has been conceived a system architectural model in order to analyze the authentication mechanisms in wireless network. In order to evaluate

the performance of the above authentication scheme in Wireless IP network, we have designed experimental model and simulated using OPNET Modeler [4].

We have considered EAP-TLS and proposed authentication scheme based on OTP protocol as authentication schemes. The roaming user can be authenticated in the Visiting Network by Home Network Server (HNS). Thus for the experimental purpose, two scenarios have been designed. First one with the implementation of OTP-based authentication scheme whereas second with implementation of EAP-TLS in wireless network. The system architectural model is shown in Fig. 4.2.

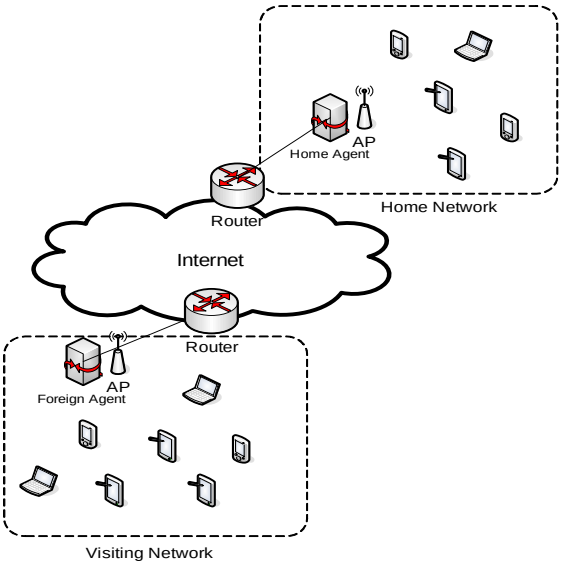



*Fig. 4.2. System architectural Model for Wireless mobile network*

### *a. Simulation Environment*

For the experimental evaluation, we have assumed the various performance metrics in order to analyze the effect of proposed authentication scheme and the EAP-TLS. We have considered following performance metrics:

- Authentication Delay – the time involved in an authentication phase of a given protocol.
- Response Time – the total time required for traffic to travel between two points. It includes connection establishment, security negotiation time as well as the actual data transfer time.

We have implemented the OTP-based authentication mechanism and the EAP-TLS in our experiment. For VoIP services, a base voice codec scheme is considered to be G.729.

For the wireless users, we have considered IEEE 802.11b as our WLAN protocol. And the transmission speed is 11 Mbps between the AP and the clients. We have considered the scenario that a mobile client is roaming into visiting network domains.

### *b. Results and Analysis*

In order to investigate the performance of OTP-based authentication scheme and EAP-TLS authentication scheme in wireless 802.11 network, we have analyzed different aspects of experimental results obtained. Particularly we have investigated the impact of proposed authentication scheme and EAP-TLS in Wireless IP network on the response time and authentication delay with number of concurrent VoIP calls.

Fig 4.3 illustrates the mean response time for different number of concurrent VoIP calls with implementation of OTP-based and EAP-TLS authentication schemes. The result shows that with increase in no of concurrent VoIP calls, the mean response time increases. It can be seen that the response time in second scenarios has slightly higher than that of first one.

The Authentication delays for different numbers of concurrent VoIP calls with implementation of OTP-based and EAP-TLS authentication schemes is depicted in Fig. 4.4. On analyzing two scenarios of the experiment, it can be seen that the Authentication delay for OTP-based is reduced than that for EAP-TLS.

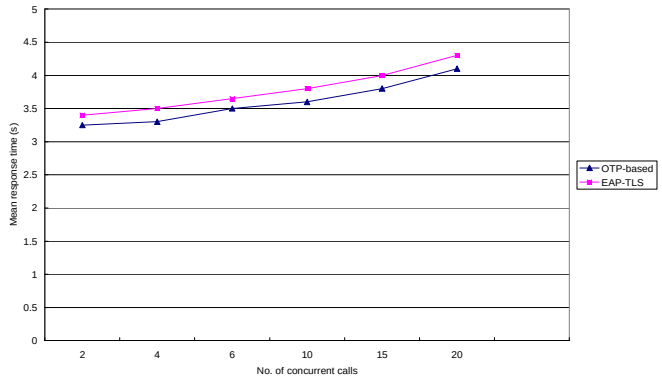



*Fig. 4.3. Mean response time for different authentication schemes*

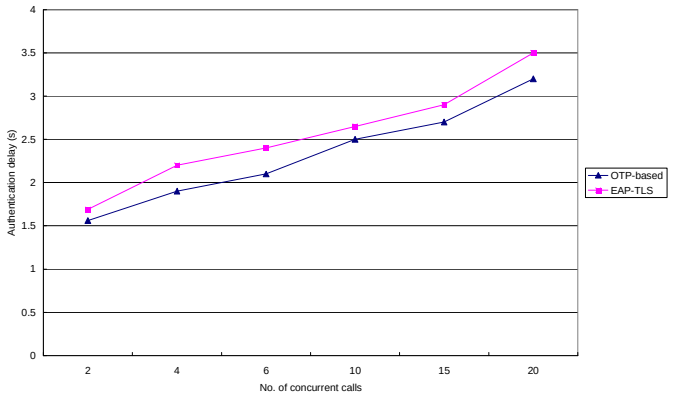



*Fig. 4.4. Authentication delay for different authentication schemes*

# 3. AODV-MAP based Framework for Multihop Wireless Network

In Chapter 3 section 2, we have proposed not only novel AODV-MAP ad hoc routing protocol but also its application for traffic distribution. We have also considered secure scheme for AODV-MAP routing.

## 3.1. Evaluation of AODV-MAP routing scheme

In order to evaluate performance of the proposed protocol and compare with node-disjoint multipath routing and AODV, we have simulated using OPNET Modeler. [4]

### a. Implementation of AODV-MAP

We present implementation details of AODV-MAP routing scheme in OPNET Modeler simulation tool.[4] The implementation details include network model, node model and several process models.

Network Model

The network model is shown in Fig. 4.5. The number of mobile nodes can move around a specified area. Nodes communicate over wireless links with a transmission range of 250m.

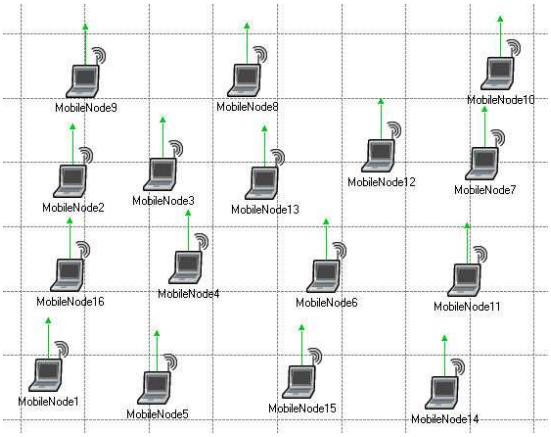



*Fig. 4.5. Network Model for ad hoc network*

Node Model

As shown in Fig. 4.6, the node model has a protocol stack. Each node within the network is uniquely identified by its IP address.

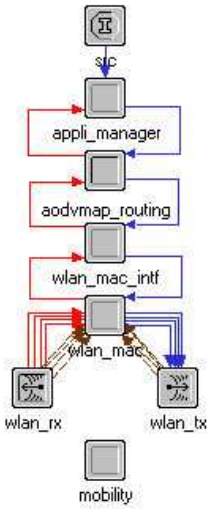



*Fig 4.6. Node model for MANET node*

- *src* module: This is the packet source module. It generates packets according to specific packet size and inter-arrival distributions. Once generated, packets are sent to the immediate lower layer.
- *appli_manager* module: This module sets a random destination address to the incoming packet from *src* module. The *src* and *appli_manager* modules form application layer.
- *aodvmap_routing* module: This module is deployed to discover and maintain routing information of mobile ad hoc network. Receiving a data packet from the application layer, the module firstly checks its route table. The module implements AODV-MAP routing to discover multiple route paths to a destination node.
- *wlan_mac_intf* and *wlan_mac* modules: These modules represent data link layer, which are meant for interfacing and implementation of the IEEE 802.11 standard [5] *medium access control* (MAC) protocol.
- *wlan_tx and wlan_rx* modules: The *wlan_tx* module transmits packets from *wlan_mac* module and sends these packets on the radio channel

while the *wlan_rx* module receives packets from the radio channel and forwards packets to wlan_mac module. These modules are implemented to satisfy specifications of the IEEE 802.11 standard physical layer.

- *mobility* module: Each mobile node has a position and velocity and moves around on a wide area. This module performs the movement of the current node by changing its position according to the actual movement scheme.

Process Model

Process module represents behavior of a module. OPNET uses Finite state machine (FSM), which is defined by states and transitions between those states. Two states are possible: blocking and non-blocking states.

Application manager Process Model

The main function of the application manager process (Fig. 4.7) is to allocate a destination IP address for each incoming packet from *src* module.

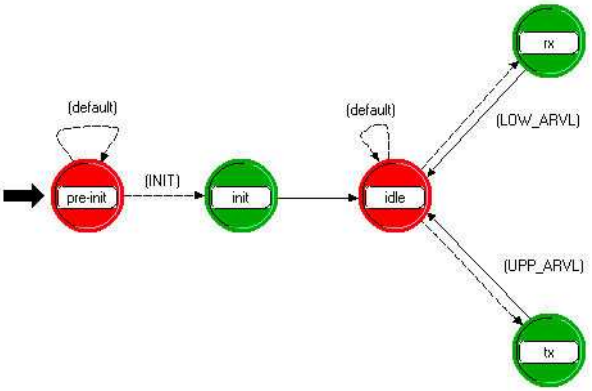



*Fig 4.7. FSM for Application manger*

Each node, at the *pre-init* state, randomly picks a waiting period before transiting to the *init* state. The idea is to introduce some sort of

differentiation between the existing nodes. Thus, as nodes consecutively transit into the *init* state, remaining flows are progressively granted to arriving nodes until no more flows are available. Depending upon communicator attributes, the node will be allowed to communicate with any node randomly or with specific node or none. When a node is in the *idle* state, it can transit either to the *rx* state (upon packet arrival from route layer) or *tx* state (upon packet arrival from the source layer).

Routing Process Model

The *aodvmap_routing* process implements AODV-MAP routing as specified earlier, which is shown in Fig. 4.8.

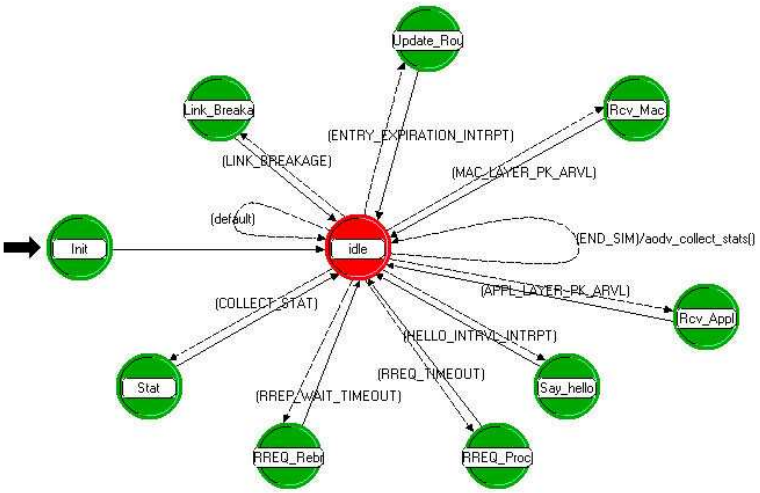



*Fig. 4.8. FSM for Routing protocol*

- *Init* state: This state consists of initialization of the process model. User defined attributes are loaded and routing information tables are initialized. A self-interrupt is scheduled to initiate the first Hello Interval. Once the initialization step is accomplished, the process transits to the idle state.
- *Rcv_App* state: The *routing* process transits to this state when a

service request is received from the application layer to transmit a data packet to a given destination. The current state first extracts the destination IP address from the received packet, and then checks the route table. If a route path exists in its route table, the current state inserts the IP address of the next hop to the data packet and forwards it to next hop node. Otherwise, the current state saves the data packet to a waiting queue and initiates a route discovery process.

- *Rcv_Mac* state: This state receives the incoming packet stream from the MAC layer. It first checks type of the received packet and then calls appropriate function to proceed. If a packet has reached its final destination, the current state unencapsulates its payload and sends it to the application module.
- *RREQ_Rebroadcast* state: This occurs when RREP_WAIT_TIMEOUT timer expires for a given destination. This means that the current node still did not receive a route reply to its request. In this case, the current state checks whether a rebroadcast is possible or not. If maximum authorized number of retries is reached, discovery process for that destination is aborted. Consequently, any data packet waiting for this route is dropped from buffer. In other case, RREQ packet is rebroadcast.
- *RREQ_Process* state: This state is responsible to processing received RREQ packet. Basically it can discover multiple alternative paths and setting path type at the destination.
- *Update_Route_Table* state: This state occurs when the timer of an entry expires.
- *Say_hello* state: Node should broadcast hello message in order to advertise its presence to the neighborhood.
- *Link_Breakage* state: When a node detects that there is a link break to a neighbor node, it sends a RERR packet to its upstream node.

- *Stat* state: The current process periodically transits to this state in order to collect different global statistics. These statistics are written into a file which is created at the beginning of each simulation run.

Medium Access Control Model

OPNET supports models for simulating ad hoc wireless networks on physical layer model and medium access control (MAC) layer model. The IEEE 802.11 protocol with Distributed Coordination Function (DCF) [5] is deployed as the MAC layer in the simulation. DCF is the basic access method used by mobiles to share wireless channel and avoid hidden and exposed terminator problems. The access scheme is Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) with acknowledgements. The nodes can make use of Request-To-Send/Clear-To-Send (RTS/CTS) channel reservation control frames for unicast, virtual carrier sense, and fragmentation of packets larger than a given threshold. In the model, the RTS/CTS and virtual carrier sense are deployed to minimize the effect of collisions over the wireless medium.

Mobility Process Model

The mobility process model, shown in Fig. 4.9, implements a *random waypoint* mobility scheme [51] that is described below.

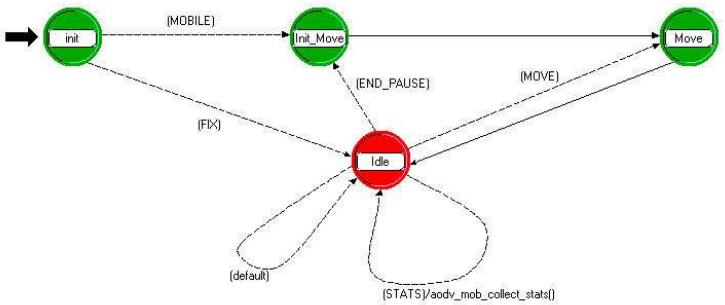



*Fig 4.9. FSM for mobility*

In the *init* state, each node picks a random position within the specified grid. After that, each node checks the *mobility* attribute in order to determine whether it should move or not: if the *mobility* attribute is set to Disabled, the current node transits immediately to the *idle* state and remains at the same position during the whole simulation time. In the other case, the *mobility* attribute is set to Enabled, the current node transits to the *init_move* state in order to initialize its next movement parameters.

### *b. Simulation Environment*

In the simulation, network coverage areas are 1000m x 1000m and 1500m x 1500m for 50 node network and 100 node network respectively. Nodes communicate via radio signals with 250m of propagation range and the channel capacity of 2 Mbps. The IEEE 802.11 DCF is used as the MAC layer protocol and DCF uses CSMA/CA technique.

The mobility and traffic models similar to the previous article [52] are used. The nodes are initially uniformly distributed throughout the network area and their movement is determined by the random waypoint mobility model. According to this model, a node randomly selects a location with in the network area and moves towards it with a speed uniformly chosen between a predefined minimum and maximum values. The node stays in that position for a period, ie pause time, and then again selects another random location to move. The pause time is constant at 30 sec.

Constant bit-rate (CBR) sessions between source and destination pair in the network were occurred with each CBR session generating 10 packets/ sec and the size of each data packet is 512 bytes. Each node buffers all data packets while waiting for a route. All packets (both data and routing) sent by the routing layer are queued at buffer until the MAC

layer can transmit them. Routing packets are given higher priority than data packets in buffer. Sources and destinations are chosen randomly with uniform probabilities. Each run executes 800 seconds of simulation time.

In order to evaluate performance of the AODV-MAP scheme and compare with other routing schemes such as AODV and node disjoint multipath routing in different network conditions, two parameters are varied in the simulation:

- Number of nodes (50 nodes and 100 nodes)
- Maximum velocity of the nodes

To evaluate performance of these protocols in mobility condition, 20 and 40 sources are modeled respectively to study the effect of varying mobility in networks of 50 and 100 nodes.

In our simulation, four following performance metrics are used: [53]

- Route discovery frequency which is total number of route discoveries initiated per second.
- Average end-to-end delay includes all possible delays from the moment the packet is generated to the moment it is received by the destination node.
- Packet delivery ratio: Ratio of data packets delivered to destinations to those generated by CBR sources.
- Normalized routing load: Number of routing control packets transmitted per data packet delivered at the destination.

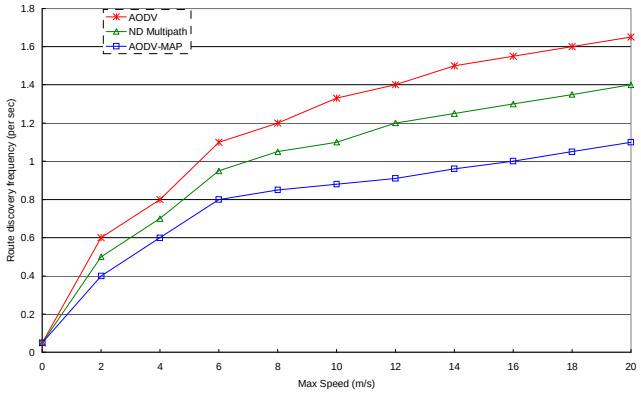
### *c. Simulation Results*

The series of experiments were conducted with maximum velocity for 20 sources of 50 nodes network and 40 sources of 100 nodes network. The mobility was varied in order to observe effects of route discovery frequency, average end-to-end delay, packet delivery ratio, and normalized

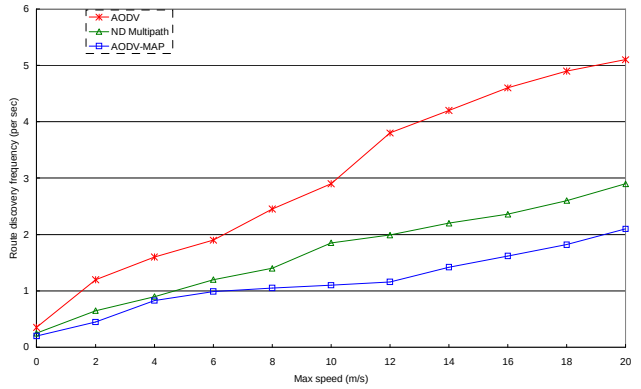
route load. A node can choose a speed between minimum (0 m/s) and maximum speed (20 m/s).

Route discovery frequency

Route discovery frequency (RDF) is a very important metric as smaller route discovery frequency of a given routing protocol implies that it can increase opportunities for setting up more alternative paths.




*a. for 50 nodes*




*b. for 100 nodes*

*Fig. 4.10. Route discovery frequency in ad hoc routings*

Fig. 4.10 a and b show the route discovery frequency with respect to the maximum speed for networks of 50 nodes and 100 nodes respectively. In both cases, AODV-MAP has smaller route discovery frequency than AODV and the node-disjoint multipath routing. It can be seen that in case of AODV-MAP scheme and node-disjoint multipath routing, a new route discovery is invoked only when all paths fail.

In Fig 4.10a, at the maximum speed of 10 m/s, route discovery frequency in AODV-MAP is lesser than AODV and node-disjoint multipath routing by about 34% and 20% respectively. Whereas in Fig 3.22b, at the maximum speed of 10 m/s, route discovery frequency in AODV-MAP is lesser than AODV and node-disjoint multipath routing by about 62% and 40% respectively. AODV-MAP scheme maintains a low route discovery frequency compared to node-disjoint multipath routing and single path AODV. This indicates that the robust nature of the scheme to mobility of nodes and topological changes.

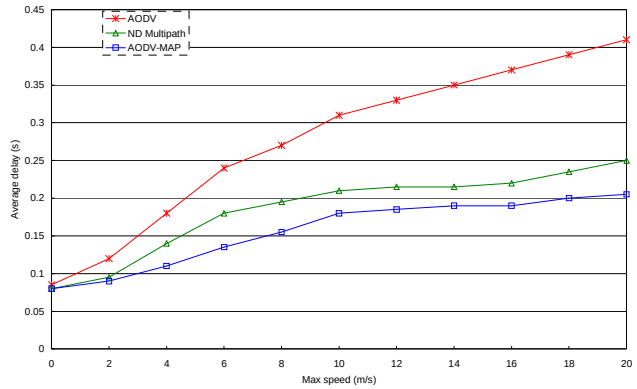
Average end-to-end delay

Average end-to-end delay of data packets which includes all possible delays caused by buffering during route discovery latency, queuing at interface queue, length of routing paths, re-transmission delays at MAC, propagation and transfer times.

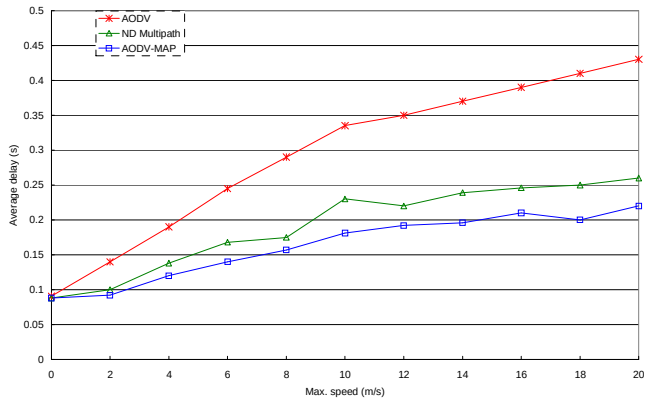
Fig. 4.11 a and b illustrate the change in the average end-to-end delay as a function of speed of nodes for networks with 50 nodes and 100 nodes respectively. It can be seen that general trend of all curves is an increase in delay with the increase of velocity of nodes. The reason is mainly that high mobility of nodes results in increased probability of link failure that causes an increase in number of routing rediscovery processes.

AODV-MAP exhibits the smallest end-to-end delay whereas AODV incurs the largest delay. Delays of AODV-MAP scheme and node-disjoint

multipath routing are gradually increased after node velocity of 10m/s, while delay in AODV increases quickly as velocity increases. This is because availability of alternate paths in AODV-MAP and node-disjoint multipath routing eliminate route discovery latency that contributes to delay when active route fails. This result shows that AODV-MAP scheme is effective especially in situations where nodes move frequently.




*a. for 50 nodes*

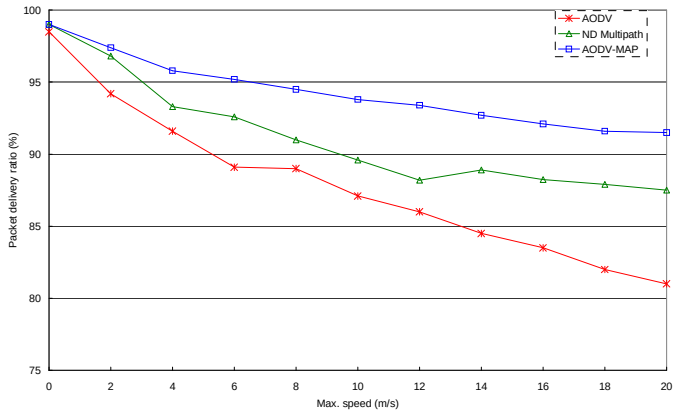



*b. for 100 nodes*

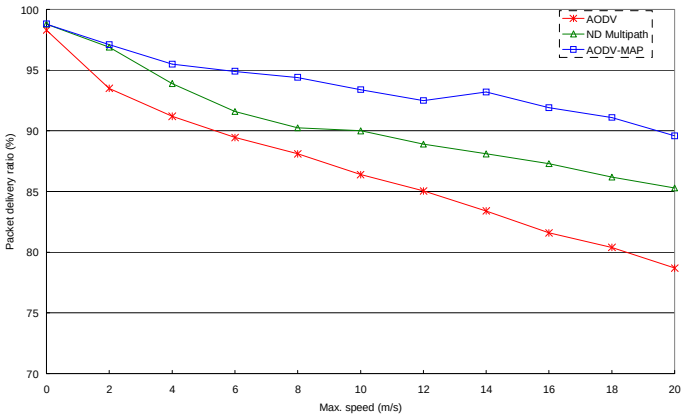
*Fig. 4.11. Average end-to-end delay in ad hoc routings*

Packet Delivery Ratio

Packet delivery ratio (PDR) is one of important metrics since it shows loss rate, which in turn affects maximum throughput of the network.




*a. for 50 node network*




*b. for 100 node network*

*Fig. 4.12. Packet delivery ratio in ad hoc routings*

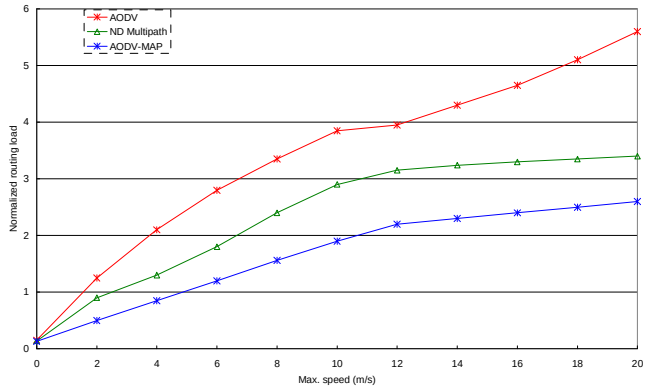
The packet delivery ratios of three protocols are shown in Fig. 4.12 a and b. The figures describe the variation of the packet delivery ratio as a

function of the node speed. The probability of link failure increases with increase in the node speed, and hence the number of packet drops also increases. AODV-MAP scheme and node-disjoint multipath routing produce high packet delivery ratio due to presence of multiple paths. So when an active routing path is broken due to mobility of nodes, these protocols still can manage the communication between source and destination without pause or interrupt. Since AODV-MAP has both node-disjoint and fail-safe alternative paths, it can survive longer. Thus AODV-MAP scheme has much higher packet delivery ratio than both node-disjoint multipath routing and AODV. This mechanism of AODV-MAP assures high packet delivery ratio.

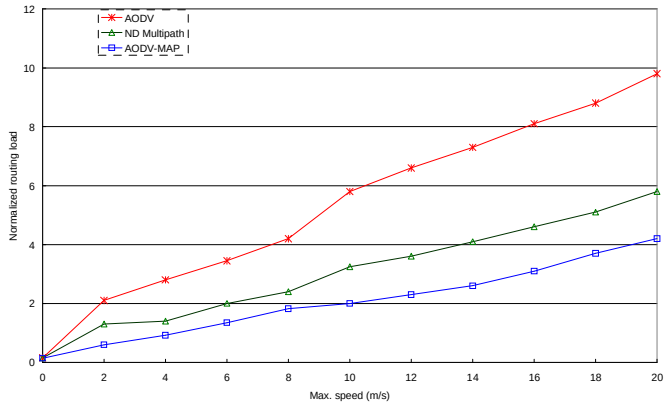
Normalized routing load

Normalized routing load is an important metric to compare the performance of different protocols since it can give a measure of the efficiency of protocols, especially in a low bandwidth and congested wireless environment. Fig 4.13 a and b show the routing load for networks of 50 nodes and 100 nodes respectively.

It can be observed that the normalized routing load in AODV-MAP is slightly better than that of node-disjoint multipath routing whereas much better than that of AODV. The normalized routing load in AODV increases more quickly than that in both AODV-MAP and node-disjoint multipath with the increase of velocity. This is due to fact that both AODV-MAP and node-disjoint multipath can find multiple alternative route paths in a route discovery process, so the protocol decreases tremendously the number of route rediscovery process. Whereas, since AODV encounters more link failures with the increase in mobility, they have to trigger more new route discovery processes which cause more routing control packets to be sent to the whole networks.




*a. for 50 node network*




*b. for 100 node network*

*Fig. 4.13. Normalized routing load in ad hoc routings*

## *3.2. Evaluation of audio streaming over AODV-MAP based MANET*

In order to evaluate the performance of the proposed framework for audio streaming over AODV-MAP based MANET, we have conducted the performance evaluation of audio streaming over AODV-MAP MANET using scalable audio coding schemes and selective encryption technique.

## *A. Evaluation of scalable coding techniques for multipath MANET*

In order to evaluate the performance of the framework for audio streaming over AODV-MAP based MANET using scalable audio coding techniques, we have designed experimental model and simulated using OPNET Modeler [4].

### *a. Simulation Environment*

In the simulation, MANET consists of sixteen mobile nodes are located inside a 600m x 600m region. Each node is randomly placed in the region initially. We consider the continuous mobility case only. A mobile node moves around continuously with using random waypoint mobility model with pause time of 0s and a maximum speed of 5 m/s. We use the IEEE 802.11 protocol in the MAC layer working in the DCF mode. The channel has a bandwidth of 1Mb/s. The transmission range is 250 m. UDP is used as transport protocol.

Among these nodes, one is randomly chosen as the streaming source with different scalable speech coding techniques and another node is chosen as the destination. Five UDP traffic flows are introduced as background traffics. Each of these flows has the traffic rate of four packets per second. The size of data payload was 512 bytes. The source, destination and duration of these background flows are set random. Each of nodes has a queue size of 10 packets.

For the experimental purpose, two scenarios have been considered - a framework using G.727 coding technique for audio streaming in multipath

MANET whereas another using MPEG-4 speech coding technique for audio streaming in multipath MANET. In the simulation, to evaluate performance of the proposed framework following performance metrics were computed: Packet loss rate and end-to-end packet delay.

### *b. Simulation Results*

In order to analyze preliminary results for the framework for streaming audio over mobile ad hoc network using AODV-MAP scheme, we compare the performance of two scalable speech coding techniques - G.727 and MPEG-4 audio coding in terms of packet loss rate with respect to bit error rate (BER) and end-to-end delay (latency).

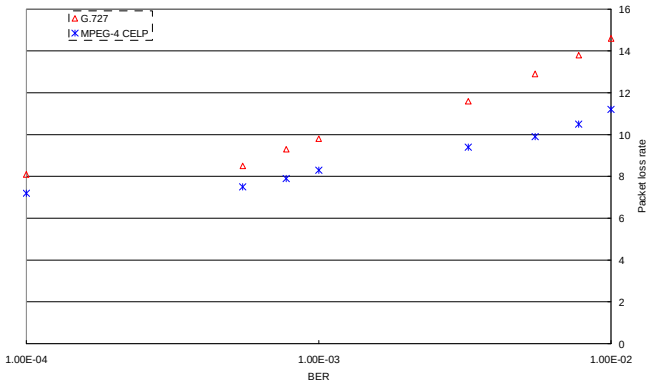



*Fig. 4.14. Packet loss rate for various scalable codings*

Fig. 4.14 shows packet loss rate for the both scenarios with respect to BER. It can be seen that the packet loss rate in G.727 coding scheme increases rapidly than in case of MPEG-4 CELP scheme. At BER of $10^{-3}$, packet loss rate for G.727 coding scheme is about 10% whereas for MPEG-4 CELP scheme it is about 8.1%.

Fig 4.15 illustrates the end-to-end delay for scalable speech coding techniques. It can be seen that end-to-end delay for G.727 coding scheme

has higher average end-to-end delay than that of MPEG-4 CELP scheme. It can be derived that for audio streaming over MANET, MPEG-4 CELP shows better performance than with G.727 coding scheme.

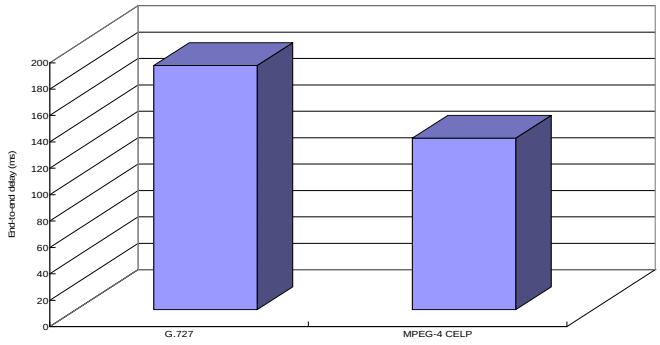



*Fig. 4.15. End-to-end delay for various scalable codings*

## *B. Evaluation of secure audio streaming over multipath MANET*

In order to evaluate the performance of the framework for secure media streaming over AODV-MAP based MANET, we have designed experimental model and simulated using OPNET Modeler.

### *a. Simulation Environment*

In the simulation, MANET consists of sixteen mobile nodes are located inside a 600m x 600m region. Each node is randomly placed in the region initially. We consider a popular random waypoint mobility model. We have used a pause time of 1.0s for all the experiments. The speed of nodes varies from 1m/s to 10m/s. We use IEEE 802.11 protocol, the MAC layer working in DCF mode. The channel has a bandwidth of 1Mb/s. The transmission range is 250 m. UDP is used as transport protocol.

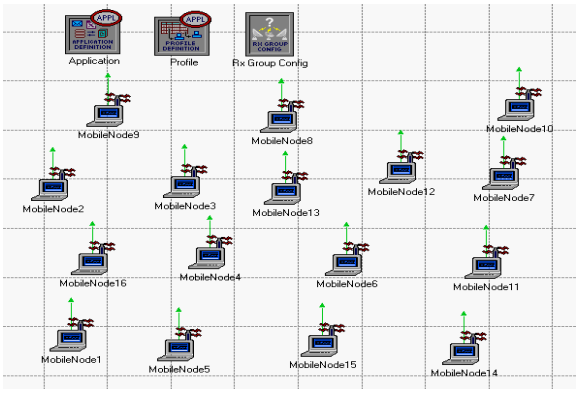



*Fig. 4.16. Simulation model for audio streaming over multipath MANET*

Fig. 4.16 shows the simulation model of the framework for secure audio streaming over multipath MANET. Among these nodes, one is randomly chosen as the streaming source with MPEG-4 speech codec and another node is chosen as the destination. Five UDP traffic flows are introduced as background traffics. Each of these flows has traffic rate of four packets per second. The size of data payload was 512 bytes. The source, destination and the duration of these background flows are set random. Each of nodes has a queue size of 10 packets.

For experimental purpose, two scenarios have been considered - a framework for secure audio streaming using single-path AODV routing whereas another for secure audio streaming using AODV-MAP scheme. In the simulation, we have used following performance metrics: packet loss rate and end-to-end packet delay.

### *b. Simulation Results*

In order to analyze preliminary results for the above frameworks, we compare performance of AODV-MAP scheme with node-disjoint multipath

routing scheme and AODV scheme in terms of packet loss rate and end-to-end delay with respect to max speed.

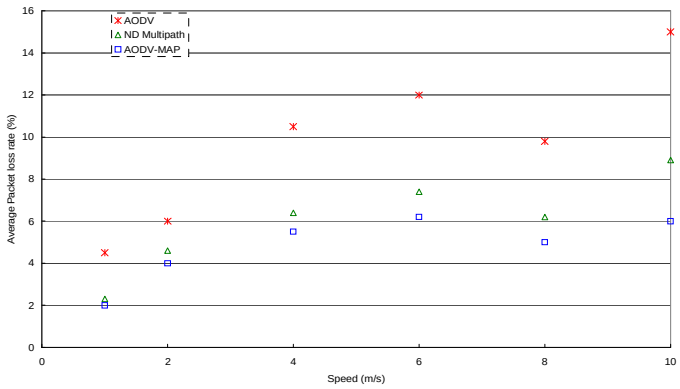



*Fig. 4.17. Packet loss rate for different ad hoc routing schemes*

Fig. 4.17 shows the average loss rate for three scenarios at different mobility, that is, rate of node movement. As the velocity of nodes increases, the probability of link failure increases and hence the number of packet drops also increases. It can be seen that the mean packet loss rate in both multipath routing schemes are reduced than in case of AODV. AODV-MAP scheme has slightly lower packet loss rate than node-disjoint multipath scheme whereas much lower loss rate than AODV scheme. With speed of 6m/s, average loss rates for AODV-MAP scheme and node-disjoint multipath scheme are about 6.1%, and 7.5% respectively while that of AODV is about 12%.

Fig 4.18 illustrates the average packet delay as a function of speed of nodes. For the all the scenarios, it can be seen that there is increase in average delay with the increase of velocity of nodes. Both multipath routing schemes provide smaller end-to-end packet delay than in case of AODV. This is because multipath routing protocols have alternate paths

and need smaller route discovery time.

However, when comparing two multipath routing schemes, it can be seen that average packet delay in AODV-MAP scheme is smaller than that of node-disjoint multipath scheme. This is due to fact that in AODV-MAP scheme, frequency of route discovery process is lesser than that of node-disjoint multipath routing. Delays of both multipath schemes are gradually increased after speed reaches 4m/s, while delay in AODV increases quickly as velocity increases. After the maximum velocity reaches 4m/s, the delays in both schemes are lower than that in AODV.

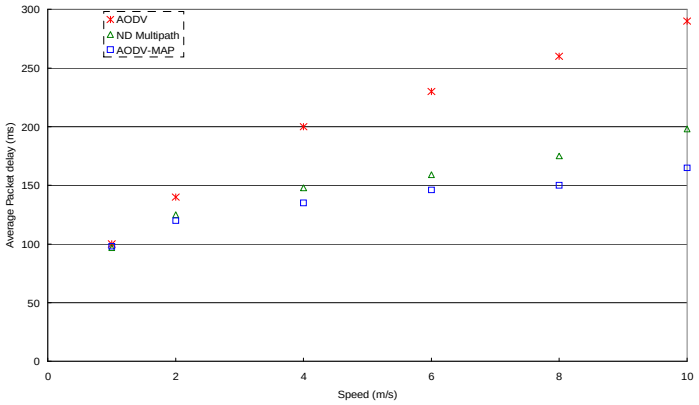



*Fig. 4.18. End-to-end delay for different ad hoc routing schemes*

## *3.3. Analysis of Secure AODV-MAP Scheme*

### *A. Security Analysis*

In this section, we provide security analysis of the secure AODV-MAP routing scheme (SAODV-MAP) by evaluating its robustness in the presence of the attacks described in security requirements in chapter 2 section 2.5.

*Unauthorized network access*

SAODV-MAP scheme allows network access only for nodes that have been authenticated using the certificate issued by the trusted authority, and only so long as they use the same IP and MAC addresses bound by that certificate. Packets are discarded for nodes that are not authenticated. Trusted authority is a single point of failure and attack, however, multiple redundant authorities may be used (e.g., as by Zhou and Haas [79]).

*Impersonation attacks*

Main idea of SAODV-MAP scheme is to prevent IP or MAC spoofing. During the neighbor discovery phase, a node entering a neighborhood must authenticate with its neighbors and store their public keys. And every node creates neighbor node table and maintains by frequent updates, so it can locally monitor neighbors. This procedure ensures that IP and/or MAC spoofing by any node can be easily detected. And during route discovery, since HMAC shared key is used, only the communicating nodes can verify the authenticity and nodes cannot spoof other nodes during route discovery. This prevents impersonation attacks where either the source or destination nodes is spoofed.

*Formation of routing loops*

Routing loops are formed because of the following misbehavior: IP/MAC spoofing, and stale routing information within the intermediate nodes. SAODV-MAP can detect any IP/MAC spoofing, thus a malicious node cannot spoof identity, without detection, and create routing loops. Also, the source and the destination maintain a destination sequence number that is used only by these end nodes. Moreover, modification of this sequence number can be easily detected.

*Modification of routing information*

Modification of routing information like hop-count and destination sequence number could be used in a DoS attack. It defeats modification attacks by employing two security mechanisms. One is the use of HMAC used by the source and destination nodes that can detect such a modification. And second, the intermediate nodes ensure the integrity of the message transmitted by the next hop node by the use of local monitoring mechanisms. The local monitor mechanism can detect some of misbehaving nodes during RREQ forwarding process.

*Fabrication of routing information*

- RERR Fabrication attack: It is trivial to disrupt an established route by generating fake RERR packets and forcing the intermediate nodes to relay them to the source of a route and may also initiate a new route discovery. SAODV-MAP defeats this fabrication attack because all RERR messages are authenticated link-by-link. RERR message is digitally signed by the sender in order to ensure authenticity and integrity of RERR messages.
- Black hole and Gray hole attacks: These attacks involve forging routing packets to cause all routes to go through a misbehaving node. The malicious node then drops all or some packets for the destination, thus carrying out the black hole or gray hole attack respectively. In SAODV-MAP, forged routing packets are detected and discarded.

*Replay attacks*

- Malicious Route Request floods: Malicious nodes may forge RREQ packets and flood the network. In SAODV-MAP, RREQ packets are

authenticated by the destination node only. However, intermediate nodes will be forced to process these RREQs thus carrying out a resource depletion attack, although less costly than in protocols such as SAODV which authenticate RREPs at each hop.

- Rushing attack: SAODV-MAP is secure against Rushing attack. As discussed above, rushing attack exploits duplicate RREQ suppression employed in all on-demand routing protocols. For example, a malicious node rushes RREQ by transmitting with excessive power, reaching nodes more than one-hop away (at normal power). However, SAODV-MAP scheme does not allow nodes to accept packets from nodes that have not been authenticated by neighbor discovery process. Because SAODV-MAP ensures that all the one-hop links are bidirectional, node cannot authenticate with nodes two hops away.

***Worm hole attack***

The worm hole attack is carried out by two malicious nodes that have an out of band link between them. These nodes use this special link to offer the quickest route between many source-destination pairs, forcing those sources to choose this route over the other slower but legitimate routes. This pair can then carry out a DoS attack. However, in case of the worm hole attack, the upstream malicious node can ignore the routing protocol maintenance procedure by not generating a RERR for any packets dropped by its collaborating downstream node.

SAODV-MAP scheme is vulnerable to this attack. End-to-end acknowledgments provide a reasonable solution, especially when collective ACKs can be sent via alternate routes (identified during route discovery and retained by the destination).

*Invisible node attack*

In SAODV-MAP, packets are only accepted between neighbor nodes one-hop away from each other and it maintains not only neighbor table but also src-rreqid table to monitor its neighborhood, this is to avoid the "invisible node attack".

## *B. Performance Evaluation*

In order to evaluate performance of the proposed security scheme in wireless multipath multihop network, we have designed experimental model and simulated using OPNET Modeler. [4]

### *a. Simulation Environment*

We compare through simulation performance of SAODV-MAP with AODV-MAP in as well as with the existing SRP routing protocol. [75]

In the simulation, the network coverage area is 1000m x 1000m square with 50 mobile nodes, each having radio power range of 250m. The channel capacity is 2 Mbps. The IEEE 802.11 DCF is used as the MAC layer protocol. We used CBR traffic over UDP.

The initial positions of nodes were uniformly distributed throughout the network. Node mobility was simulated according to the random waypoint mobility model, in which each node travels to a randomly selected location at a configured speed and then pauses for a configured pause time, before choosing another random location and repeating the same steps. Node transmission range was 250m. We ran simulations for constant node speeds from 0 to 20m/s, with pause time fixed at 30 seconds. We simulated 20 CBR sessions in each run, with random source and destination pairs. Each CBR session generates 10 packets per second with data packets of 512 bytes. Simulation time is 800 seconds.

For the simulation, two scenarios have been designed – first one is under benign setting, ie there is no misbehaving nodes, whereas second is under adverse environment, there may be some individual misbehaving nodes.

For the experiment with benign setting, we have considered the following performance metrics:

- Packet Delivery Ratio: This is the ratio of the data packets generated by CBR sources that are delivered to the destination. This evaluates the ability of the protocol to discover routes.
- Average Routing Load for byte: This is the ratio of overhead bytes to delivered data bytes. The transmission at each hop along the route was counted as one transmission in the calculation of this metric.
- Average End-to-End Delay of Data Packets: This is the average delay between the sending of the data packet by CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, re-transmission delays at the MAC layer, etc.

And for the experiment with adverse environment, we have evaluated packet delivery ratio only.

### *b. Results and Analysis*

In the simulation, we have examined the performance of the proposed security scheme under benign and adverse environments.

#### *Scenario 1: Under benign environment*

Under benign environment, AODV-MAP and SAODV-MAP are compared in order to verify cost of the proposed security scheme. Fig 4.19 shows the packet delivery ratio plotted against maximum speed for

AODV-MAP and SAODV-MAP. As shown in Fig 4.19, the packet delivery ratio obtained using SAODV-MAP is above 90% in all the node speed and almost alike to that obtained using AODV-MAP. This suggests that SAODV-MAP is effective in discovering and maintaining routes for delivery of data packets, even with high node mobility.

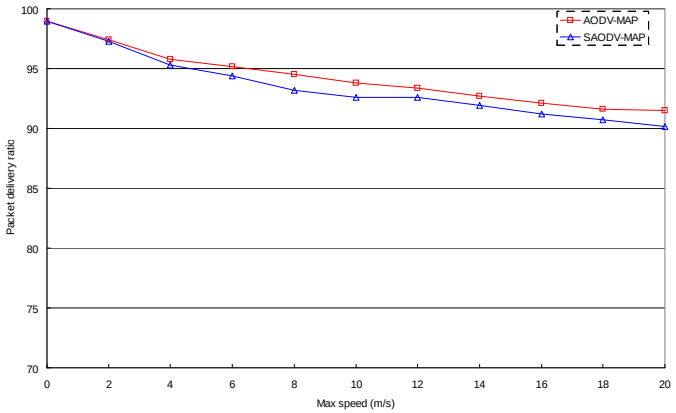



*Fig. 4.19. Packet delivery ratio for AODV-MAP & SAODV-MAP*

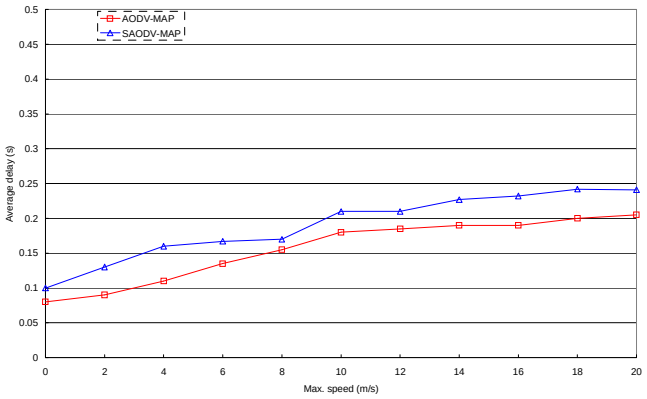



*Fig. 4.20. End-to-end delay for AODV-MAP & SAODV-MAP*

Fig 4.20 shows the average delay plotted against maximum speed for AODV-MAP and SAODV-MAP schemes. It can be seen that the average

packet delay of SAODV-MAP scheme is slightly higher than that of AODV-MAP scheme. This is due to security measures used in SAODV-MAP scheme.

Fig. 4.21 shows average byte routing load for AODV-MAP and SAODV-MAP schemes. It can be observed that average byte routing load in SAODV-MAP significantly increases than AODV-MAP scheme after maximum speed of 10m/s. At the node speed of 10 m/s, average byte routing load for SAODV-MAP is about 40% higher than that of AODV-MAP scheme.

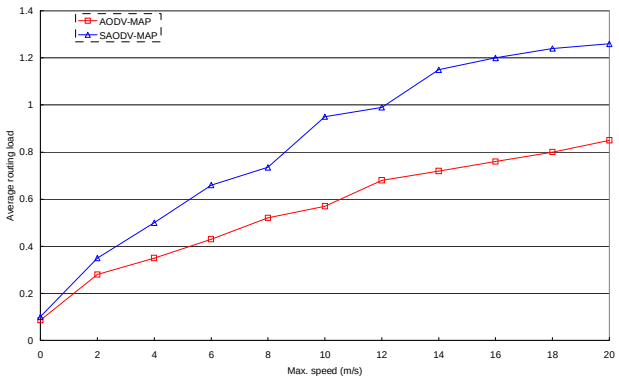


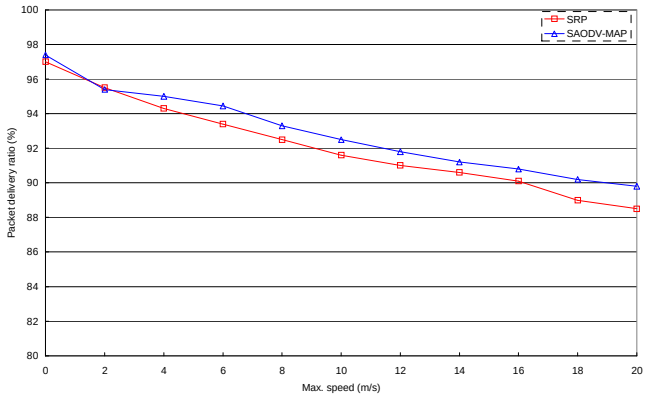

*Fig. 4.21. Average Routing load for byte for AODV-MAP & SAODV-MAP*

*Scenario 2: Under adverse environment*

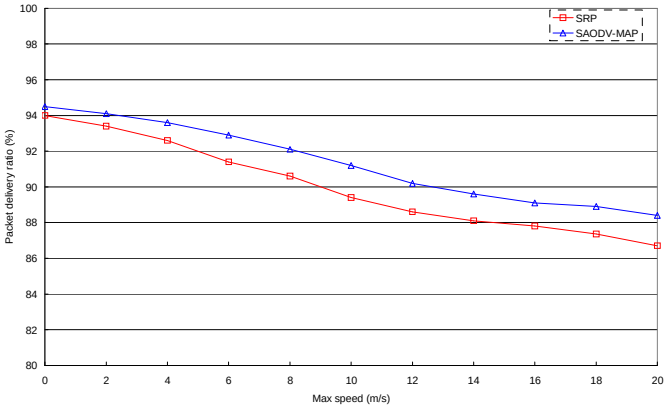
In this scenario, the proposed scheme is chosen to compare with SRP under adverse environment. We have considered the malicious nodes are existed in the network and they can corrupt the accumulated route in all the request packets and re-broadcast. We analyzed the effect of malicious nodes in SAODV-MAP with varying the number of malicious nodes and compared with SRP. We have used 10 CBR pairs.

Fig 4.22 a and b show packet delivery ratio plotted against node speed when percentage of malicious nodes are 10% and 20% respectively. It can

be seen that the packet delivery ratios in both SAODV-MAP scheme and SRP decreases as the maximum speed increases. When percentage of malicious nodes is 10%, packet delivery ratios are almost similar in SAODV-MAP and SRP scheme for all the node speed. However, when the percentage of malicious nodes is increased to 20%, then SADOV-MAP scheme has better performance in terms of packet delivery ratio than in case of SRP scheme for all the node speed.




*a. for 10% malicious node*




*b. for 20% malicious node*

*Fig. 4.22. Packet delivery ratio for SRP and SAODV-MAP*

# 4. Approach for Internet connectivity in AODV-MAP based Hybrid MANET

In chapter 3 section 3, we have proposed not only the robust approach for global connectivity in AODV-MAP based hybrid ad hoc network with multiple Internet gateways but also security framework for such an approach. And also we have shown distributed approach for audio streaming over multipath hybrid MANET.

## 4.1. Evaluation of AODV-MAP based Hybrid MANET

In this section, we have considered two approaches for our experiment - one is our proposed approach and another is an approach using AODV routing and Mobile IP with shortest path criterion. We analyzed and evaluate the proposed approach using OPNET Modeler and compare with above-stated AODV.

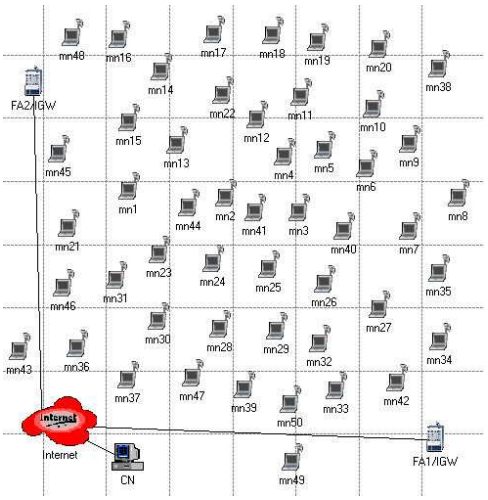



*Fig 4.23. Simulation Model for H-MANET*

Fig 4.23 shows basic model of the approach for connecting AODV-MAP based MANET with Internet using two Internet gateways.

### *a. Simulation Environment*

In the simulation, the network coverage area is a 800m x 800m square with 50 mobile nodes. Initially the internet is connected with two foreign agents/gateways, which are placed at opposite ends of the simulation area. The nodes are initially randomly distributed throughout the network area Nodes communicate via radio signals with 250m of propagation range and the channel capacity of 2 Mbps. In order to support wireless LAN in the simulator, DCF of the IEEE 802.11 is adopted as the MAC layer protocol. DCF uses CSMA/CA technique.

Source nodes communicate with corresponding nodes (CN) using CBR source traffic. Each CBR session generates 4 packets /sec and the size of each data packet is 512 bytes. CBR sources are randomly distributed in the network. As a mobility model, we use the random waypoint mobility model The pause time is constant at 30 sec. In order to evaluate capability of these approaches for different node mobility, we changed node mobility by varying the maximum speed. Each node moves at a speed that varies from 0 to 20 m/s. Each run executes 800 seconds of simulation time.

### *Simulation Results and Analysis*

In the simulation, we have compared the performance of our approach with the conventional approach, using following performance metrics:

- Packet delivery ratio is the ratio of the amount of data packets

delivered to the destination and total number of data packets sent by source.

- Average end-to-end delay is defined as all possible delays from the source node to the destination.
- Packet loss rate is the percent of transmitted packets that never reach the intended destination due to incorrect route information, mobility, collisions, and congestion.

Two scenarios were considered - one under various speeds and another under various loads. The first experiment was conducted with the maximum velocity for 10 sources of 50 nodes network. The mobility was varied in order to see the effects of average delay and packet delivery ratio. The packet sending rate is fixed at 4 packets / sec.

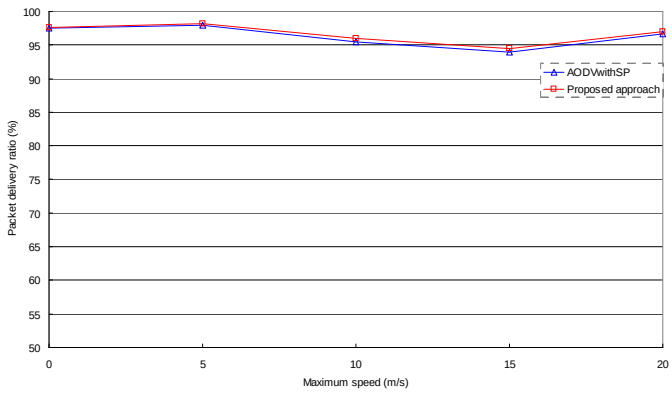



*Fig. 4.24. Packet delivery ratio for various H-MANETs*

Fig. 4.24 shows the packet delivery ratio for various maximum speeds for our approach and AODV with shortest path. In both techniques packet delivery ratios change in similar manner with the change in node speed. It

can be seen that packet delivery ratio in our approaches is slightly better than that of AODV with shortest path.

Fig. 4.25 shows the average end-to-end delay for various maximum speeds for our approach and AODV with shortest path. Our approach has significantly lower average end-to-end delay than AODV with shortest path. After the maximum speed of 10 m/s, average delay in our approach gradually rises than in AODV with shortest path.

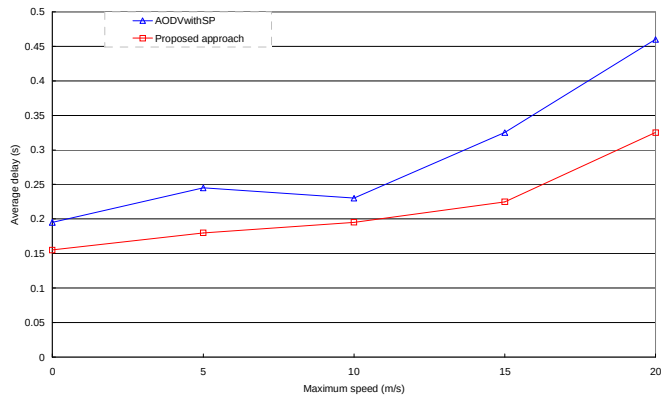



*Fig. 4.25. End-to-end delay for various hybrid MANETs*

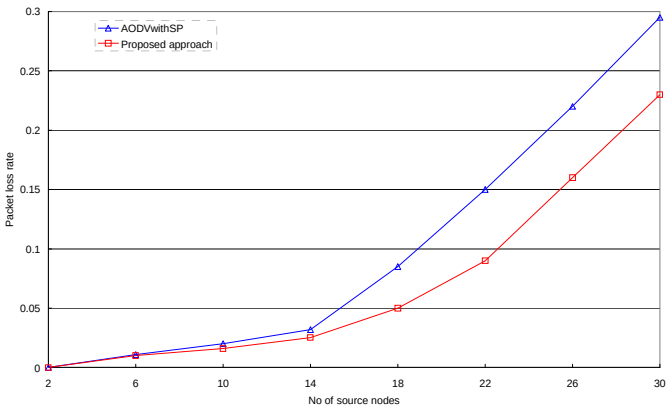
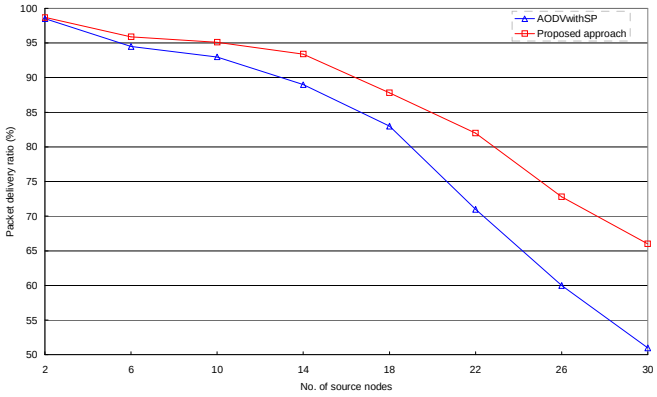
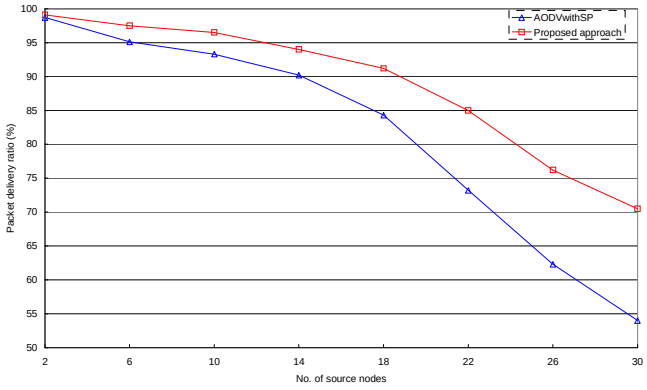



*Fig. 4.26. Packet loss rate for various H-MANETs*

The second experiment was conducted by varying traffic loads. Fig. 4.26 plots the packet loss rate versus traffic load at IGW. In both case packet loss rises when traffic load increases; the reasons for packet loss include incorrect information, mobility, collisions and congestions. The proposed approach exhibits lower packet loss than AODV with shortest path under heavy traffic load.




*a. for 2 Internet gateways*




*b. for 3 Internet gateways*

*Fig. 4.27. Packet delivery ratio for H-MANET with various number of gateways*

Fig. 4.27 a and b show the packet delivery ratio for various traffic loads. It can be seen that higher traffic load results in lower packet delivery ratio. The proposed approach exhibits better performance than AODV with shortest path under the heavy traffic load. Furthermore, when the number of gateway is increased, ie from 2 to 3 gateways, packet delivery ratio is also increase in both the cases. But in case of the proposed approach the increment in packet delivery ratio is significant than in case of AODV with shortest path; this is due to fact that our scheme uses not only hop count but also offered load as its gateway selection metrics.

## 4.2. Analysis of Secure AODV-MAP based Hybrid MANET

### A. Security Analysis

In this section, security analysis of AODV-MAP based hybrid MANET has been preformed. The security analysis illustrates security achievements on the Internet connectivity as well as the integrated MANET.

#### a. Security Analysis on Internet Connectivity

We assume that $S_{MN\text{-}HA}$ is kept secret meaning that a malicious node cannot obtain $S_{MN\text{-}HA}$. We also assume the security operations at the FA and the HA are strong enough from being compromised. In this secure protocol, the multihop route can only be established among the authenticated MNs. The proposed security scheme achieves the goals of preventing the attacks of bogus registration, reply attacks, unauthorized routing, and forged FA.

***Bogus Registration***

When a malicious MN makes a fake registration by masquerading itself as someone else in the integrated MANET, the malicious MN issues a forged registration with an invented or spoofed address. The forged registration will be stopped when validating $MAC_{S_{MN-HA}}(M_2)$ using $S_{MN-HA}$ at HA because the malicious node does not have the knowledge of secret key ($S_{MN-HA}$), which is associated between the invented or spoofed address and the related HA.

***Replay Attacks***

The nonce (e.g., $N_{MN}$, $N_{HA}$, and $N_{FA}$) and timestamp are used in all mobile IP and routing messages to ensure a registration or routing message contains a unique data to prevent replay attacks. Each registration or route request has a nonce, and a new nonce in the registration or route reply message indicates the next nonce for the next request.

***Forged FA***

When a node advertises itself as a fraudulent FA, there are two possibilities for MNs that are under the coverage of the forged FA

- MNs that have not yet registered with HA via a correct FA, and
- MNs that have successfully registered with FA and HA.

When $MN_1$ wants to register with FA, it starts FA discovery. Assume the forged FA replies the $MN_1$ directly because the $MN_1$ is under the coverage of the forged FA. Then $MN_1$ proceed with the registration with the forged FA. A registration message with a MAC association created by using $MN_1$'s secret key ($S_{MN-HA}$) is sent to the forged FA. However, the forged FA cannot verify the message with $S_{MN-HA}$. If the forged FA

sends the registration message to $MN_1$'s HA, the registration is declined while validating $Cert_{FA}$ and its digitally signed message. If the forged FA uses an earlier registration reply in attempt to cheat the $MN_1$, the $MN_1$ can detect forged FA during fast re authentication since MN use temporary session key $S_{sk}$ to compute MAC and also use $h^i(s)$ for re-authentication. Therefore the forged FA cannot cheat $MN_1$ and it's HA.

*Guessing attack*

In this scheme, the secret key $K_{MN-HA}$, shared between MN and home domain, is for authentication purpose. Therefore, it is not possible for an attacker to obtain the secret key $K_{MN-HA}$. During fast re-authentication process, the hash chaining $h^n(s)$ will be used as a one time password to get the access right hence it is useless to obtain the password. Since $S_{sk}$ is frequently changed so this will prevent guessing attack.

*Data confidentiality*

The $S_{sk}$ that is distributed by the HA can be used to encrypt the communications data. Only the FA and MN can read the data in the wireless environment. This provides data confidentiality between the FA and MN over the air. The FA and HA communicate through the Internet environment. In the proposed method, the use of encryption technique provides data confidentiality.

### *b. Security Analysis on connected MANET*

In SAODV-MAP, a node only accepts messages from verified one-hop neighbors. The proposed secure framework for AODV-MAP based hybrid ad hoc network prevents attacks in terms of integrity, impersonation, confidentiality and non-cooperation.

***Integrity***

As agent advertisement is signed by using the private key of FA, the receiver verifies the certificate and signature of the FA. Thus the signature and verification prevent anti-integrity attacks. The attacks of modification and routing loop can be prevented by integrity protection.

***Impersonation attack***

In the connected ad hoc network, the proposed approach binds the MN's home IP address and MAC address with public key in the ad hoc network. The binding is unique due to uniqueness of MN's home address and its MAC address. Neighbor discovery process assures the communication between authenticated one-hop neighbors. The secret key encryption prevents impersonation on registration. Therefore, it becomes difficult for any MN to masquerade itself by spoofing or inventing an address either during registration or in route discovery. Fabrication can be avoided by protecting the identity of each MS.

The $h^n(s)$ is known to the FA during full authentication. So in fast re-authentication phase, the attacker cannot compute hash chaining to impersonate the MN because without the random seed $s$, one cannot compute backward value using the published one-way value.

***Non-cooperation***

In this scheme, neighbors with valid certificates can participate properly in ad hoc routing and communication protocol. On the hand, we can consider some MNs are selfish and are not willing to relay traffic for other MNs in order to save their own resources. Each neighbor is monitored so it can be easily discarded during the routing process.

## *B. Performance Evaluation*

In order to verify the proposed security extension in our framework for global connectivity in hybrid ad hoc network, experiments have been carried out using OPNET Modeler [4]. We have considered two scenarios for our experiment - one is under normal condition and another is under adverse environment. We evaluate the effect of the proposed security scheme in the approach for global IP connectivity in hybrid ad hoc network.

### *a. Simulation Environment*

In the simulation, the network coverage area is a 800m x 800m square with 50 mobile nodes, which can be connected to the Internet with two foreign agents/gateways. These gateways are placed at opposite ends of the simulation area. The nodes are initially randomly distributed throughout the network area. Nodes communicate via radio signals with 250m of propagation range and the channel capacity of 2 Mbps. In order to support wireless LAN in the simulator, DCF of the IEEE 802.11 is adopted as the MAC layer protocol. DCF uses CSMA/CA technique.

Source nodes communicate with corresponding nodes (CN) using CBR source traffic. Each CBR session generates 4 packets /sec and the size of each data packet is 512 bytes. As a mobility model, we use the random waypoint mobility model. The pause time is constant at 40 sec. Each run executes 300 seconds of simulation time.

### *b. Results and Analysis*

In order to evaluate and compare the performance of our approach for global IP connection in hybrid MANET with security and without security, we used following performance metrics:

- Packet delivery ratio is the ratio of the amount of data packets delivered to the destination and total number of data packets sent by CBR source.
- Average end-to-end latency is all possible delays from the source node to the destination.

In the simulation, we have considered a scenario under adverse environment. The malicious nodes selectively drop or modify packets they are asked to forward. In our experiment 10 CBR sources was selected randomly in 50 nodes network. The packet sending rate is fixed at 4 packets/ sec. A node speed is constant at 20 m/s. To analyze the effect of security scheme used in our approach, we vary the percentage of malicious nodes.

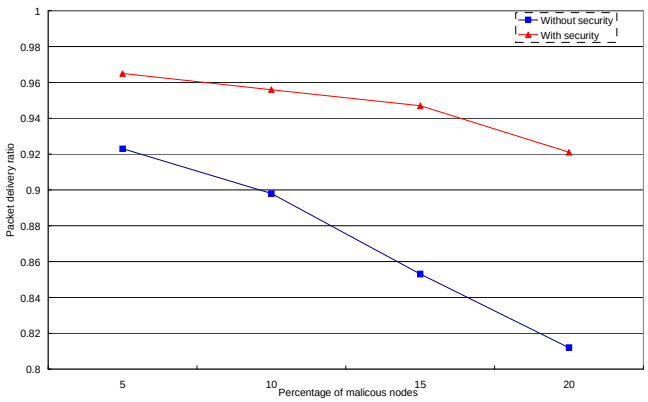



*Fig. 4.28. Packet delivery ratio for H-MANETs in terms of security*

Fig. 4.28 shows the packet delivery ratio for various percentages of malicious nodes. It can be seen that our approach with security was able to maintain delivery ratio of over 90% even when 30% percent of the nodes are malicious. With the increase in the percentage of malicious

nodes, the packet delivery ratio of our approach without security drastically drops. Thus the proposed secure approach is very effective in delivering packets even in the presence of large proportion of malicious entities.

Fig. 4.29 shows the average packet latency for various percentages of malicious nodes. In figure, the trend shows the rise in average latency for both with security and without security with the increase of percentage of malicious nodes. It can be seen that average latency in the approach with security is higher than that without security when the percentage of malicious nodes are high.

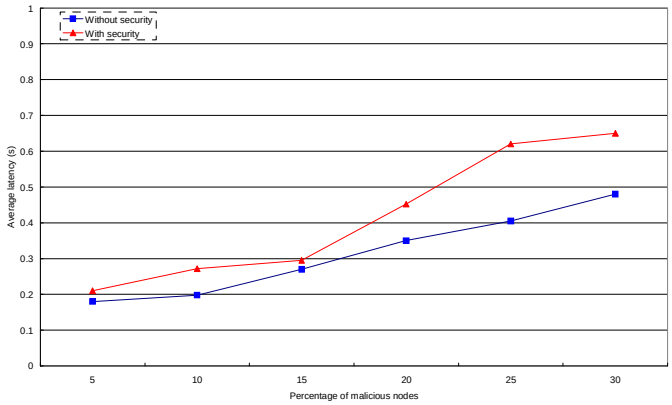



*Fig. 4.29. Average latency for H-MANETs in terms of security*

## *4.3. Evaluation of audio streaming over AODV-MAP based Hybrid MANET*

We have conducted simulation to show the effectiveness of our proposed approach for audio streaming over hybrid ad hoc network using OPNET Modeler [4]. We have considered a scenario in which hybrid MANET using AODV-MAP and Mobile IP for global connectivity. We have considered UEP in order to provide robustness and efficiency.

### *a. Simulation Environment*

In the simulation, the network coverage area is a 800m x 800m square with 50 mobile nodes. Internet is connected with one foreign agent/gateway. The nodes are initially randomly distributed throughout the network area. Nodes communicate via radio signals with 250m of propagation range and the channel capacity of 2 Mbps. DCF of the IEEE 802.11 is adopted as the MAC layer protocol.

As a mobility model, we use the random waypoint mobility model. The pause time is constant at 40 sec. In the experiment, we have considered MPEG-4 standard audio clip "horn23_2". And in addition, five UDP traffic flows are introduced as background traffics. Each of these flows has the traffic rate of four packets per second. The size of data payload was 512 bytes. The source, destination and the duration of these background flows are set random. Each of nodes has a queue size of 10 packets. Each run executes 300 seconds of simulation time.

### *b. Simulation Results*

In the simulation, we have compared the performance of framework using UEP in scalable coding with framework without using UEP in scalable coding. We have considered following performance metrics:

- Noise-mask-ratio (NMR):[108] The quality of decoded audio can be evaluated through the objective measurement of NMR. For a given band, NMR is the ratio of the noise energy to the masking threshold. It may equivalently be viewed as a weighted squared error measure. It can be seen that a lower value of NMR shows a better audio quality.
- Average end-to-end delay is delay from the source node to IGW.

In first experiment, we have demonstrated effectiveness of using UEP in scalable coding. Fig. 4.30 shows average NMR for various packet loss

ratios when BER is constant at $2.532\times10e^{-3}$. It can be seen that framework using UEP in scalable coding has much better quality of audio in compared to that of framework without using UEP in scalable coding. When packet loss rate is above 10%, average NMR in a framework using UEP is almost double in compared to a framework without using UEP.

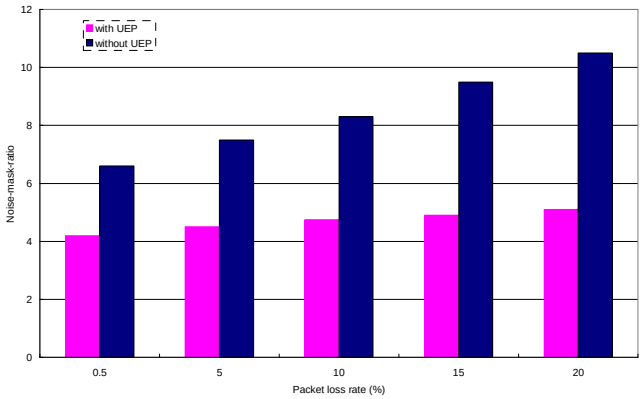



*Fig 4.30. NMR for Distributed media delivery networks*

In Fig. 4.31, average delay is plotted against BER. It can be seen that the average delay increases with BER. And average delay in framework using UEP is lesser than that of framework without using UEP.

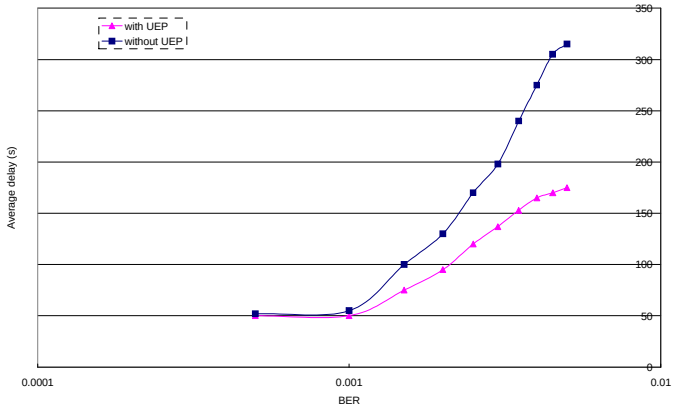



*Fig 4.31. Average delay for Distributed media delivery networks*

# V. Conclusions & Future Works

## 1. Conclusions

The growth of the Internet use and wireless network has accelerated the rapid implementation of ubiquitous services. The network of the future will be comprised of mostly wireless devices not only be capable of simple delay-tolerant packet delivery, but also real-time applications such as voice and video. In order to overcome the challenges and problems in existing wireless networks, we have developed some approaches in the areas of single hop wireless network, multihop wireless network, and interconnection of Internet and MANET.

Design of efficient, reliable and secure routing in multihop wireless network are challenging issues. In this thesis, robust, efficient and secure multipath routing scheme in multihop wireless network has been proposed. This scheme can be used in isolated ad hoc network as well as in hybrid ad hoc network.

In chapter 3, we have proposed several approaches such as secure authentication scheme for wireless mobile network; robust, efficient and secure multipath routing scheme for wireless ad hoc network; and robust and secure approach for global connectivity for connected MANET. In chapter 4, we have evaluated the proposed approaches.

In case of single hop wireless network, we put forward authentication scheme based on hash chain (one-time password) in wireless mobile network. Proposed authentication scheme has advantage that it makes the simpler computational complexity with sufficient security. The concept of refresh password is proposed to renew the secret key of the WEP in IEEE 802.11. Moreover, it will be convenient for a user to register once to a server for roaming every AP. We have simulated the experimental

scenarios with implementation of OTP-based scheme and EAP-TLS in Wireless IP network Both mean response time and authentication delay is reduced in case of OTP-based authentication scheme. However, this authentication scheme is not suitable for multihop wireless network.

In case of multihop wireless network, we have proposed the multipath ad hoc routing scheme called AODV-MAP, which is robust and efficient scheme for the ad hoc network where frequent communication failure occurs. A simulation showed that the performance of the proposed scheme is much better than AODV and node-disjoint multipath routing in terms of route discovery frequency, end-to-end delay, packet delivery ratio and normalized routing load.

Furthermore, we have depicted framework for media streaming using multipath routing in wireless ad hoc network. For this purpose, we devise traffic allocation scheme using AODV-MAP. To investigate the performance of scalable speech coding techniques - G.727 and MPEG-4 CELP, we have simulated. It can be seen that the performance of MPEG-4 CELP scheme is much better that G.727 in terms of packet loss rate and end-to-end delay. We have also depicted a framework for secure media streaming using multipath routing in wireless ad hoc network. We have simulated the experimental scenarios with implementation of the above framework using proposed scheme, node-disjoint multipath routing scheme and AODV in wireless ad hoc network. It can be seen that the performance of the proposed protocol is much slightly better than node-disjoint multipath routing scheme whereas much better than AODV in terms of packet loss rate and end-to-end delay.

In order to provide security in the proposed multipath routing scheme, we have provided security extension to AODV-MAP (SAODV-MAP). It SAODV-MAP is intended to have minimum load of cryptographic processing. The simulation results show that SAODV-MAP is as efficient

as AODV-MAP in discovering and maintaining routes. It can be observed that the performance of the proposed scheme is much better than SRP in terms of packet delivery ratio in presence of malicious nodes.

In case of hybrid ad hoc networks, we analyzed several issues arising when an ad hoc network is connected to the Internet via multiple gateways. We proposed an architecture framework for supporting IP mobility and communications across the boundary between ad hoc network and the Internet. This robust approach is suitable for the integrated Internet with MANET with multiple gateways. In this approach, we have put forward a robust gateway selection scheme in order to select optimum gateway. The simulation results show that the proposed approach with hybrid gateway selection has better performance than AODV with shortest path only. Moreover, it can be observed that increasing number of gateway in the connect MANET domain, the packet delivery ratio can be increased.

Moreover, we have also presented a secure framework for global IP connectivity for hybrid MANET. The proposed security scheme provides protection for interconnection of mobile nodes with the Internet as well as secure ad hoc routing. Security analysis shows that the proposed scheme is robust against various attacks in Internet connection and ad hoc routing. The simulation results shows comparison between the proposed global connectivity approach with and without security. It can be seen that even though there is higher average latency in the approach with security, the packet delivery ratio is much higher than that without security.

We have analyzed the reliable distributed multimedia delivery network over hybrid multipath MANET using robust technique such as UEP. We have put forwarded a concept of a distributed multimedia delivery network using scalable coding. It is primarily used to delivery audio streaming

over hybrid ad hoc network. It can be seen that when UEP is used with scalable audio coding, the performance of such a framework is relatively good.

## 2. Future Works

Our research work can be expanded in several directions. In order to model the ubiquitous wireless network more robust, and reliable, this research needs to be extended by including other aspects of wireless networks. Thus we have listed some future works, which are as follows:

- *Interconnection to other WMAN/WWAN*

  Currently we have focused only on 802.11 based WLAN and MANET and interconnection between infrastructure-based and ad hoc networks. In future we need to extend the heterogeneous network where different technologies can be integrated seamlessly.

- *Extend to use of Mobile IPv6*

  In this thesis, we have considered Mobile IPv4 which is quite popular nowadays. But for future network we need to migrate to Mobile IPv6. We can use Mobile IPv6 and Hierarchical Mobile IPv6 mobility management (HMIPv6) for more flexible and robust solutions.

- *Extend this novel routing to emerging wireless environment*

  Currently we have proposed a novel multipath ad hoc routing scheme which is designed for isolated MANET as well as hybrid MANET. In near future, we can adopt this novel scheme in emerging wireless environment such as Network Mobility (NEMO) technology.

- *Provisioning Quality of Service (QoS) with robust DiffServ technique*

  Currently we have used FEC to provide UEP in the distributed multimedia delivery network. However, we are planning to design more robust approach for providing UEP using DiffServ.

1 *Extend to video communication and use of Multiple Descriptions Coding*

  In this thesis, we have used scalable audio coding for multimedia delivery in the distributed environment. We can extend such a network to video communication such real time video conference and other services. Moreover, we can use Multiple Descriptions Coding (MDC) for flexible solutions.

# *Bibliography*


[1] P. Nicopolitidis, et al., Wireless Networks, John Wiley, 2003

[2] T. A. Wysocki, A. Dadej, B. J. Wysocki Ed., Advanced Wired and Wireless Networks, Springer 2005

[3] Basagni, Conti, Giordano, and Stojmenovic Ed., Mobile Ad Hoc Networking, IEEE Press, 2004

[4] OPNET Modeler Simulation Software, http://www.opnet.com

[5] IEEE Standard 802.11-2003, "Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2003

[6] M. Gast, 802.11 Wireless Networks- The Definitive Guide, O'Reilly, Dec. 2002

[7] B. Potter, and B. Fleck, 802.11 Security, O'Reilly, Dec. 2002

[8] W. A. Arbaugh, N. Shankar, and Y.C. Justin Wan., "Your 80211 wireless network has no clothes," IEEE Wireless Communications, vol. 9, Dec. 2002, pp 44 - 51

[9] K.H Baek, S. W. Smith, and D. Kotz, "A Survey of WPA and 802.11i RSN Authentication Protocols", Dartmouth College Computer Science, Technical Report TR2004-524, Nov 2004

[10] IEEE P802.11i/D10.0. Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 11: Wireless MAC and PHY Specs. Apr 2004.

[11] National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES)

[12] IEEE Standards for Local and Metropolitan Area Networks: Port

based Network Access Control, IEEE Std 802.1X-2004, Dec 2004

[13] J. Edney, and W. A. Arbaugh, "Real 802.11 Security - Wi-Fi Protected Access and 802.11i", Addison Wesley, Jul 2003

[14] B. Aboba, et al, "Extensible Authentication Protocol (EAP)" IETF RFC 3748, June 2004

[15] Interlink Networks, Inc. EAP Methods for Wireless Authentication Apr 2003

[16] B. Aboba, and D. Simon, "PPP EAP TLS Authentication Protocol", IETF RFC 2716, Oct 1999

[17] C. Perkins, Ed., "IP Mobility Support for IPv4", IETF RFC 3344, Aug 2002

[18] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", IETF RFC 3775, Aug 2002.

[19] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997

[20] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, Feb 1997.

[21] L. Lamport, "Password Authentication with insecure communication", Communications of the ACM, Vol. 24 No. 11, Nov. 1981, pp 770-722.

[22] W. Wang, S.C. Liew, V.O.K. Li, "Solutions to Performance Problems in VoIP Over a 802.11 Wireless LAN", IEEE Trans on Vehicular Technology, Vol. 54 (1), Jan 2005.

[23] N. Haller, "The S/KEY One-Time Password System", IETF RFC 1760, Feb. 1995.

[24] N. Haller, et al, "A One-Time Password System," IETF RFC 2289. Feb 1998.

[25] L. Blunk, J. Vollbrecht, B. Aboba. "The One Time Password (OTP) and Generic Token Card Authentication Protocols", Internet draft <draft-ietf-eap-otp-00.txt>.

[26] IETF Mobile Ad hoc Networks (MANETs) Working Group

Charter. <http://www.ietf.org/html.charters/manetcharter.html>

[27] E. M. Royer, C. K Toh, “A review of current routing protocols for ad hoc mobile wireless networks”, IEEE Personal Communications, 6(2): April 1999 pp. 46-55.

[28] C.E. Perkins, and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Proc. of ACM SIGCOMM, 1994 pp 234-244.

[29] S. Murthy and J.J. Garcia-Luna-Aceves, “An efficient routing protocol for wireless networks”, ACM Mobile Networks and Applications Journal, pp.183-197, 1996.

[30] T. Clausen, P. Jacquet Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October 2003.

[31] C.E. Perkins, E. Belding-Royer, and S.R. Das, "Ad hoc on-demand distance vector (AODV) routing", IETF RFC 3561, Jul 2003.

[32] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", IETF RFC 4728, Feb. 2007.

[33] S. Mueller, R. P. Tsang, and D. Ghosal, “Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges,” Springer Velag LNCS Vol. 2965, 2004, pp. 209-234.

[34] Nasipuri, R. Castaneda, S. R. Das, “Performance of multipath routing for on-demand protocols in mobile ad hoc networks”, Mobile Networks and Applications, 6(4): 2001, pp. 339-349.

[35] V. D. Park, M. S. Corson, “A highly adaptive distributed routing algorithm for mobile wireless networks”, IEEE INFOCOM’97, Kobe, Japan, April 1997, pp. 1405-1413.

[36] M.R. Pearlman, et al, “On the impact of alternate path routing for load balancing in mobile ad hoc networks”, Proc. of ACM

MobiHOC'00, Boston, MA, August 2000, pp. 3-10.

[37] S.J. Lee, M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks", Proc. of IEEE ICC'01, Helsinki, Finland, vol. 3, June 2001 pp. 867 - 871.

[38] S.J. Lee, M. Gerla, "AODV-BR: backup routing in ad hoc networks", IEEE WCNC'00, vol. 3, Sep 2000, pp. 1311 - 1316

[39] S.K. Das, et al, , "An adaptive framework for QoS routing through multiple paths in ad hoc wireless networks", J. Parallel Distributed Computing, 63, 2003, pp. 141-153

[40] L. R Reddy, and S.V Raghavan, "SMORT: Scalable multipath on-demand routing for mobile ad hoc networks", Elsevier Ad hoc Networks Journal, vol 5(2), 2007, pp. 162-188.

[41] K. Wu and J. Harms, "Performance Study of a Multipath Routing Method for Wireless Mobile Ad Hoc Networks," Proc. of Symposium on Modeling, Analysis and Simulation on Computer and Telecommunication Systems, 2001, pp. 99-107

[42] Nasipuri, S. R. Das, "On-Demand Multipath Routing for Mobile Ad Hoc Networks," Proc. of the 8th International Conference on Computer Communications and Networks, 1999

[43] X. Li and L. Cuthbert, "On-demand Node-Disjoint Multipath Routing in Wireless Ad hoc Networks", Proc. of IEEE LCN 2004, Nov. 2004, pp. 419-420.

[44] Y.S. Chen, et al, "On-Demand, Link-State, Multi-Path QoS Routing in a Wireless Mobile Ad-Hoc Network," Proc. of European Wireless, 2002

[45] W. Wei, and A. Zakhor. "Robust Multipath Source Routing Protocol (RMPSR) for Video Communication over Wireless Ad Hoc Networks," IEEE International Conference on multimedia and expo (ICME 2004), Taipei, Taiwan, June 2004.

[46] M.K Marina, and S.R Das, "Ad hoc on-demand multipath distance vector routing", Wiley Wireless Communications and Mobile Computing, vol. 6(7), 2006, pp. 969-988.

[47] Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A routing framework for providing robustness to node failures in mobile ad hoc networks," Elsevier Ad Hoc Networks Journal, vol 2(1) 2004 , pp. 87-107

[48] R. Leung, et al, "MP-DSR: A QoS-aware Multipath Dynamic Source Routing Protocol for Wireless Ad hoc Networks," Proc. of 26th IEEE Annual Conference on Local Computer Networks, 2001 pp. 132-141.

[49] L. Wang, et al, "Multipath source routing in wireless ad hoc networks", Proc. of Canadian Conference on Electrical and Computer Engineering, vol. 1, Mar 2000, pp. 479 - 483.

[50] A. Valera, W.K.G. Seah, S.V. Rao, "Cooperative packet caching and shortest multipath routing in mobile ad hoc networks", IEEE INFOCOM 2003 1 Apr 2003 pp. 260 - 269.

[51] J. Broch, et al, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols", Proc. of the 4th Annual ACM/IEEE Int. Conference on Mobile Computing and Networking (MobiCom'98), October 1998, Dallas, USA, pp 1 - 13

[52] C. E. Perkings, E. M.Royer and S. R.Das, "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks", IEEE Personal Communications, Feb 2001, pp16-28.

[53] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations," IETF RFC 2501, January 1999

[54] H. Schulzrinne, et al, "RTP: A Transport Protocol for Real-Time Applications", IETF RFC 3550, Jul 2003

[55] C. Perkins, RTP, Audio and Video for the Internet, Addison Wesley, 2003

[56] M. Baugher, et al, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, Mar 2004.

[57] H. Dong, J.D. Gibson, M.G. Kokes, "SNR and bandwidth scalable speech coding", IEEE International Symposium on Circuits and Systems, ISCAS 2002. vol.2, 859-862pp.

[58] ITU-T, 5-, 4-, 3- and 2-bit/sample embedded adaptive differential pulse code modulation (ADPCM), Dec. 1990.

[59] ISO/IEC JTC1 SC29/WG11, ISO/IEC FDIS 14496-3 Subparts 1, 2, 3, "Coding of Audio-Visual Objects Part 3: Audio", ISO/IEC JTC1 SC29/WG11 N2503, Oct. 1998.

[60] S. Pallapothu, S.Mahajan "Selective Encryption Support in SRTP", draft-smahajan-srtp-selective-encryption-01.txt, work in progress, Feb, 2007.

[61] S. Mao, et al, "Video transport over ad hoc networks: multistream coding with multipath transport," IEEE Journal on Selected Areas in Communications, Vol 21 (10) Dec. 2003, 1721-1737 pp

[62] A. C. Begena, et al, "Multi-path selection for multiple description video streaming over overlay networks", Signal Processing: Image Communication 20 (2005) pp 39 - 60

[63] A. M. Alattar, G. I. Al-Regib, "Evaluation of selective encryption techniques for secure transmission of MPEG-compressed bit-streams", IEEE International Symposium on Circuits and Systems, ISCAS 1999, pp. 340-343

[64] T. Lookabaugh, I. Vedula, D. C. Sicker, "Selective encryption and MPEG-2", ACM Multimedia, 2003

[65] J. D. Gibson, et al, "Selective Encryption and Scalable Speech Coding for Voice Communications over Multi-Hop Wireless Links", IEEE Military Communications Conference, 2004

[66] A. Mishra and K. M. Nadkarni, "Security in Wireless Ad Hoc Networks" The Handbook of Ad Hoc Wireless Networks: Ed. M.

Ilyas, CRC Press, 2002

[67] S. Gupte, and M. Singhal, "Secure routing in mobile wireless ad hoc networks", Elsevier Ad Hoc Networks 1 (2003) pp. 151 - 174

[68] K. Sanzgiri, et al, "A Secure Routing Protocol for Ad hoc Networks", Proc. of 2002 IEEE International Conference on Network Protocols (ICNP), Nov. 2002

[69] P. Kotzanikolaou, R. Mavropodi, C. Douligeris, "Secure multipath routing for mobile ad hoc networks", Proc. of 2nd Annual Conference on Wireless On-demand Network Systems and Services (WONS'2005), IEEE, Jan 2005, pp. 89 - 96

[70] Y.C. Hu, A. Perrig, and D.B. Johnson, "Rushing attacks and defense in wireless ad hoc routing protocols", Proc. of WiSe'03, 2003, pp. 30 - 40

[71] J.R. Douceur, "The sybil attack", Proc. of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), American Mathematical Society, March 2002

[72] J. Marshall, V. Thakur, and A. Yasinsac, "Identifying Flaws in the Secure Routing Protocol", Proc. of the 22nd International Performance, Computing, and Communications Conference, April 9-11, 2003, pp. 167-174

[73] Y.C. Hu, A. Perrig, D.B. Johnson, "Wormhole detection in wireless ad hoc networks", Technical Report TR01-384, Rice University

[74] Y. C. Hu, and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy 2004 pp. 28-39

[75] P. Papadimitratos, and Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, USA, Jan. 2002

[76] Y.C. Hu, A. Perrig and D. B. Johnson, "Ariadne A Secure On-Demand Routing Protocol for Ad Hoc Networks", Springer

Wireless Networks, Vol 11, Nos 1-2 / Jan. 2005, pp. 21-38

[77] Y.C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient distance vector routing for Mobile Ad hoc Networks", Proc. of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), Calicoon, NY, Jun. 2002, pp. 3-13

[78] M. G. Zapata, and N. Asokan, "Securing ad hoc routing protocols", Proc. of the 3rd ACM workshop on Wireless security WiSe'02, Atlanta, USA, Sep 2002

[79] L. Zhou, and Z. J. Haas, "Securing ad hoc networks", IEEE Network, Nov/Dec 1999, pp 24-30

[80] P. Papadimitratos and Z. J. Haas, "Secure message transmission in mobile ad hoc networks," Elsevier Ad Hoc Network Journal, vol. 1, no. 1, pp.193 - 209, Jul. 2003

[81] W. Lou, W. Liu and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks", Proc. of IEEE INFOCOM 2004, Vol 4, Hong Kong, China, Mar 2004, pp. 2404 - 2413

[82] R. Mavropodi et al, "SecMR - a secure multipath routing protocol for ad hoc networks", Elsevier Ad Hoc Networks 5, 2007, pp 87-99

[83] M. Burmester, T. van Le, "Secure multipath communication in mobile ad hoc networks", Proc. of ITCC'04, Las Vegas, USA, IEEE, April 2004

[84] B. Dahill, et al, "A Secure Routing Protocol for Ad Hoc Networks". University of Massachusetts Technical Report 01-37, 2001

[85] Y.C. Tseng, C.C. Shen, and W.T. Chen, "Integrating Mobile IP with Ad Hoc Networks", IEEE Computer, Vol. 36(5), May 2003, pp. 48-55

[86] U. Jonsson, et al., "MIPMANET: Mobile IP for mobile ad-hoc networks," in Proc. MobiHoc, (Boston, USA), 2000

[87] Y. Sun, E. M. Belding-Royer, and C. E. Perkins. "Internet Connectivity for Ad hoc Mobile Networks." Intl. J. Wireless Information Networks, 9(2), April 2002

[88] R. Wakikawa, et al., “Global Connectivity for IPv6 Mobile Ad Hoc Networks” (draft-wakikawa-manet-globalv6-04.txt), Internet Draft, work in process, Jul 2005

[89] H. M. Ammari, "A survey of current architectures for connecting wireless mobile ad hoc networks to the Internet", Wiley International Journal of Communication Systems, 2006

[90] H. Lei and C. E. Perkins, "Ad hoc Networking with Mobile IP", Second European Personal Mobile Communication Conference, 1997

[91] Ergen M, Puri A. "MEWLANA - mobile IP enriched wireless local area network architecture", Proc. of 56th IEEE Vehicular Technology Fall Conference (VTC 2002), Vancouver, Canada, Sep 2002

[92] Broch J, Maltz DA, Johnson DB, "Supporting hierarchy and heterogeneous interfaces in multi-hop wireless ad hoc networks", Proc. of Workshop on Mobile Computing, Perth, Australia, June 1999

[93] P. Ratanchandani and R. Kravets, "A hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks", Proc. of IEEE WCNC, 2003

[94] Ahlund C, Zaslavsky A, "Extending global IP connectivity for ad hoc networks", Telecommunication Systems, vol. 24(2-4). Kluwer Academic Publishers: Dordrecht, October 2003

[95] Xi J, Bettstetter C. "Wireless multihop internet access: gateway discovery, routing, and addressing", Proc. of Int. Conf. on third Generation Wireless and Beyond 2002, San Francisco, USA, May 2002

[96] B. Xie, and A. Kumar, “A Framework for Integrated Internet and Ad hoc Network Security”, IEEE Symposium on Computers and Communications (ISCC-2004), IEEE, June 2004

[97] J. Zhao, et al, "Secure Dynamic Gateway to Internet Connectivity for Ad-hoc Network", Int. Journal of Information Tech. Vol. 11(2) 2005

[98] J. Apostolopoulos, et al, “On Multiple Description Streaming with

Content Delivery Networks", Proc. of 21st Annual Joint Conf. of the IEEE Computer and Communications Societies, Vol. 3, 2002 pp. 1736 -1745

[99] J. G. Apostolopoulos and M. D. Trott, "Path Diversity for enhanced media streaming", IEEE Communications Magazine, Vol 42-8, Aug. 2004 pp 80-87

[100] T. Moriya, et al, "A design of lossy and lossless scalable audio coding," Proc. of ICASSP'00, vol. 2, 2000, pp. 889 - 892

[101] P. Kudumakis and M. Sandler, "Wavelet packet based scalable audio coding," Proc. of IEEE ISCAS'96, vol. 2, 1996, pp. 41 - 44

[102] "Report on the MPEG-4 Audio Version 2 Verification Test," MPEG w3075, 1999

[103] K. Park and W. Wang "AFEC: An Adaptive Forward Error Correction Protocol for End-to-End Transport of Real-Time Traffic" IEEE IC3N, October 1998 pp 196 - 205

[104] A. Ortego, K. Ramchandran, "Rate-distortion Methods for Image and Video Compression", IEEE Signal Processing Magazine, Vol. 15, No. 6, Nov. 1998, pp. 23-50

[105] J. Bolot, S. Fosse-Parisis, and D. Towsley, "Adaptive FEC-based error control for interactive audio in the internet," Proc. of IEEE INFOCOM' 99, New York, Mar. 1999

[106] C. Yung, et al, "Unequal error protection for wireless transmission of MPEG audio," Proc. of IEEE ISCAS '99, vol. 6, 1999

[107] Q. Zhang, et al, "Error Robust Scalable Audio Streaming Over Wireless IP Networks", IEEE Transactions on Multimedia, Vol. 6 (6), Dec 2004

[108] R. Beaton et al., "Objective perceptual measurement of audio quality," in Digital Audio Bit-Rate Reduction, N. Gilchrist and C. Grewin, Eds: Audio Engineering Society, 1996, pp. 126 - 152