2013

Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secure routing protocol

Soke Mathew Onyemelukwe
University of Windsor

EVALUATION OF ON-DEMAND ROUTING IN MOBILE AD HOC NETWORKS AND PROPOSAL FOR A SECURE ROUTING PROTOCOL

By

Soke Mathew Onyemelukwe

A Thesis
Submitted to the Faculty of Graduate Studies
through **the Department of Electrical and Computer Engineering**
in Partial Fulfillment of the Requirements for
the Degree of **Master of Applied Science**
at the University of Windsor

Windsor, Ontario, Canada

2012

Library and Archives Canada

Published Heritage Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et Archives Canada

Direction du Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-84926-2

Our file Notre référence
ISBN: 978-0-494-84926-2

EVALUATION OF ON-DEMAND ROUTING IN MOBILE AD HOC NETWORKS AND PROPOSAL FOR A SECURE ROUTING PROTOCOL

by

Soke Mathew Onyemelukwe

APPROVED BY:

_____

Dr. A Edrisy,
Department of Mechanical Engineering

_____

Dr. H. Wu,
Department of Electrical and Computer Engineering

_____

Dr. S. Erfani, Advisor
Department of Electrical and Computer Engineering

_____

Dr. K. Tepe, Chair of Defense
Faculty of Engineering

(11th January 2013)

DECLARATION OF ORIGINALITY

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis and have included copies of such copyright clearances to my appendix.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

Secure routing Mobile Ad hoc Networks (MANETs) has emerged as an important MANET research area. Initial work in MANET focused mainly on the problem of providing efficient mechanisms for finding paths in very dynamic networks, without considering the security of the routing process. Because of this, a number of attacks exploit these routing vulnerabilities to manipulate MANETs. In this thesis, we performed an in-depth evaluation and performance analysis of existing MANET Routing protocols, identifying Dynamic Source Routing (DSR) as the most robust (based on throughput, latency and routing overhead) which can be secured with negligible routing efficiency trade-off. We describe security threats, specifically showing their effects on DSR. We proposed a new routing protocol, named Authenticated Source Routing for Ad hoc Networks (ASRAN) which is an out-of-band certification-based, authenticated source routing protocol with modifications to the route acquisition process of DSR to defeat all identified attacks. Simulation studies confirm that ASRAN has a good trade-off balance in reference to the addition of security and routing efficiency.

DEDICATION

To my beautiful and loving wife – Tochi; my brother – Fred; and my beloved family, for their love and support.

ACKNOWLEDGEMENTS

I would like to immensely thank my advisor, Dr. Shervin Erfani, for his guidance and support for this research work. I also appreciate his care and imparting of knowledge in other spheres of life.

I would also like to extend my gratitude and appreciation to Dr. A. Edrisy and Dr. H. Wu for their support, flexibility and valuable feedback.

I am grateful to Ms. Andria Ballo for her support and direction which made my stay at the Department awesome.

I would also like to take this opportunity to thank my brother – Fred Onuobia, all my friends, my sisters and parents.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS/SYMBOLS

MANET → Mobile Ad hoc Networks

AODV → Ad hoc On-Demand Distance Vector

DSR → Dynamic Source Routing

ARAN → Authenticated Routing for Ad hoc Network

ASRAN → Authenticated Source Routing for Ad hoc Networks

NS-2 → Network Simulator 2

CHAPTER ONE

INTRODUCTION

Networks are found almost everywhere and in most things in today's world. Here we define networks simply as a collection and interconnection of hardware components by communication channels that allow sharing of resources and information. Networks can be categorized based on a variety of characteristics such as the medium used to transport the data, topology layout and organizational scope etc.

Based on medium used for communication and transportation of data, there are mainly two types (I) Wire-line Networks (II) Wireless Networks

Wire-line Networks are networks of devices in which interconnection are achieved using physical channels (i.e IEEE 802.3, CAT5 cables, optical fiber etc), while Wireless Networks make use of radio waves and signals as the medium of propagation and interconnection.

Wireless communication between mobile users is getting more popular and prevalent in all areas of life. Recent technological advances in Very-Large Scale Integration (VLSI), transmitters, mobile computers and communication devices such as wireless modems, switches and routers has aided in the proliferation of wireless communication technology. Two distinct approaches for enabling wireless communication between two hosts exist. The first approach is the use of existing network infrastructure to carry data and possibly voice as well. The major problems in this approach are that of handoff and fading. Also these networks are limited to places with existing network infrastructure. The second approach is networks that do not require a pre-existing infrastructure.

Hence wireless networks can be classified into two categories by architectures: infrastructure based and infrastructure less Networks.

1.1 WIRELESS AD-HOC NETWORKS

An Ad hoc network is a collection of mobile nodes which forms a temporary network without the aid of centralized administration or standard support devices regularly available in conventional networks [66]. Hence an Ad hoc network can be said to be a collection of wireless mobile nodes forming a temporary network without the use of any existing network infrastructure. This allows them to be deployed easily as scalable topologies. Mobile Ad-hoc Networks (MANETs) are self-configuring networks of mobile nodes/routers connected by wireless links. A mobile node in a MANET has two functions: 1) as a host and 2) a router. Each MANET node functions as its own router and forwards packets to other peer nodes [53]. When a node wants to communicate with another that is out of transmission range, intermediate nodes are used to relay messages. This new type of self-deploying network may combine wireless communication with high degree node mobility. Due to its self-configuration and self-maintenance capabilities, MANETs have been receiving a lot of research attention lately. This flexibility makes them attractive for many applications for a situation where either supporting structure is unavailable or deployment is unfeasible [60]. The vision of mobile Ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes.

Nodes should be able to enter or leave the network as they wish. With the network nodes mobile, an Ad-hoc network will typically have a dynamic topology which will have profound effects on network characteristics. Every node wishing to be a part and participate in an ad-hoc network must be willing to forward packets for other nodes. These nodes generally do have a limited transmission range, hence seeks the assistance of its neighboring nodes in forwarding packets and therefore every node in an ad-hoc network can act both as a host and as a router, forwarding packets between other nodes as well as running user applications. A router is a device which routes and forwards packets using a routing protocol. A mobile host is simply an IP-addressable entity or device which might run user applications or offer some other services.

Ad-hoc networks have several advantages compared to traditional cellular systems. These advantages include: (a) On Demand setup (b) Fault tolerance, and (c) Unconstrained

connectivity. Ad-hoc networks are also capable of handling topology changes and malfunctions in nodes. It is fixed through network reconfiguration. This is for instance, when a node exits the network and causes link breakages, affected nodes can easily request new routes and use them to reach the destination. Mobile Ad-hoc networks often have inadequate security mechanism in place within the network layer or MAC layer.

1.1.1 Characteristics of Ad Hoc Networks

A mobile Ad hoc network is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways and an interface with a fixed network. MANET nodes are equipped with wireless transmitters and receivers employing antennas which may be omni-directional (broadcast), highly directional (point-to-point), or some combination of both. MANETs are characterized by:

1) *Dynamic Topologies*: This is due to the fact that nodes are free to move arbitrarily and change their physical location by moving around.
2) *Limited Resources*: Nodes in Ad hoc have the characteristics of limited CPU capability, memory, and bandwidth hence often referred to as "thin client". Also an effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception i.e. aggregate application demand will likely approach or exceed network capacity frequently.
3) *Energy-constrained operation*: Most or all of the nodes in a MANET may rely on batteries or other exhaustible means for power hence system design factoring optimization of energy conservation is highly important. Therefore due to power usage has to be limited, thus leads to having a limited transmitter range.
4) *Limited Security*: They are generally more prone to physical security threats. This includes but is not limited to possibility of eavesdropping, spoofing, and denial-of-service attacks. The decentralized nature of network control in MANETs, provides additional robustness against the single points of failure of more centralized approaches as well as throw up challenges as a result too.

1.1.2 Advantages of Mobile Ad Hoc Networks

The high interest in Mobile Ad hoc networks stems from its viability and benefits as enumerated below:

(a) *Low Cost of Deployment:* Ad hoc networks do not require infrastructure deployment as they are infrastructure-less. Hence it negates the cost and administrative time required in the deployment and maintenance of wireless infrastructure such as routers, switches, base transmitters etc.

(b) *Fast deployment:* Compared to other wireless networks such as WLAN, Ad hoc networks are very convenient and easy to deploy requiring less manual input and can be set up immediately on the fly when needed.

(c) *Dynamic Configuration:* Ad hoc network configuration and topology is very flexible and can change dynamically with time. This is a useful feature for easier administration.

1.2 WIRE-LINE AND WIRELESS ROUTING PROTOCOLS

Rules and conventions for communication between network devices or nodes are defined by network protocol. Routing protocols are special purpose network algorithms designed specifically for use by routers.

Both wireless and wire-line networks use the conventional layer three routing protocols and algorithms.

1.3 STATEMENT OF PROBLEM

Network nodes will often be battery powered which limits the capacity of CPU, Memory and bandwidth. Hence network functions have to be resource effective. Also Mobile Ad hoc Networks comes with negligible or no security mechanisms built into its network and

routing functions. Hence, MANET Network functions such as routing, and security services such as confidentiality, integrity, authentication and authorization has to be incorporated and designed to cope with a dynamic and volatile network topology. Securing MANET protocol is of the utmost importance and this thesis proposes solutions to that effect.

In this work, we evaluated the existing routing protocols in MANET to obtain the best performing. Among the metrics used, least routing overhead in a protocol was the most desired. This is as a result of the additional load or bits of information needed to incorporate our security improvements on the prototype protocol. We then proposed a security enhancement (ASRAN), which is the addition of confidentiality, authentication, and integrity security services and mechanisms.

CHAPTER TWO

ROUTING IN MANET

In a data communication network, if two or more nodes are not connected directly by a communication link, for them to receive or send messages to each other, it needs to be forwarded by intermediate nodes. Finding a path between two nodes on which to send messages in data communication networks is called route acquisition process of routing. Nodes dedicated to the routing task in a traditional network are called routers. Router functions in a network include Packet switching; Packet filtering; Internetwork communication; and Path selection. The routing protocol has two main functions, selection of routes for various source-destination pairs and the delivery of messages to their correct destination. There are three classes of routing protocols:

Link State: Link state protocols are based on Dijkstra Algorithm. It enables each node to maintain a complete view or knowledge of the network topology having cost or metrics for each link and route. This detailed overview of the entire routing domain enables each node to calculate and make a decision on the best route from this first-hand information, rather than listen to what its neighbor believes is the best route. Each node periodically updates its view of the network topology by means of flooding of link costs by other nodes. On initially discovering their neighbors, they synchronize their known topology routes, after which they send only periodic hello messages to let their neighboring nodes know they are still functioning and online. Link state routing protocols apply shortest path algorithm in choosing the next-hop for each destination. It has fast convergence, uses less bandwidth for updates and better scalability while conversely it takes up more CPU power and requires more memory.

Distance Vector: Distance vector protocols are based on Bellman-Ford algorithm. They concern themselves with the direction (vector) in which a destination lies and some means of measurement (metric) it takes to reach that destination. Hence in distance vector, each node only monitors the cost of its outgoing links and periodically informs its directly connected nodes, an estimate of the shortest distance of all the connected and

learned network routes it knows. For this reason, they are referred to as "routing by rumor". It has the benefit of been more computation efficient, easier to implement and requires less CPU resources and memory. However, it has the issues of slow convergence as a result of the "counting-to-infinity" problem, not been bandwidth efficient and the formation of both short-lived and long-lived routing loops to contend with.

Source Routing: This is a type of routing whereby a packet to be forwarded has to have the complete path information to its intended destination. Hence the routing decision is made at the source which is advantageous in avoiding routing loops. The key advantage of a source routing design is that intermediate nodes do not need to maintain up-to-date routing information in order to route the packets that they forward since the packets themselves already contain all the routing decisions. It has a cost of requiring slightly more overhead in acquiring and maintaining the path information used.

A number of ways exist to classify routing algorithms [39]. Routing protocols can be classified into different categories depending on these properties

- Centralized versus Distributed
- Static versus Adaptive
- Reactive versus Proactive

- *Centralized vs. Distributed:* For centralized routing, all route choices are made at a central node, which means the presence of dedicated infrastructure (i.e. a router) for the computation of valid and best routes. In distributed protocols, the computation of routes and decision making is shared among the network nodes with information exchanged between them as necessary. The distributed protocol approach applies aptly to Ad hoc networks where every node acts as both a host and router.

- *Static vs. Adaptive:* This refers to route response to topology changes and traffic input patterns. In static routing, the route path used by source-destination pairs is fixed regardless of change in topology or traffic conditions. It is adversely affected by link or node failure and is not flexible in response. High throughput is not

guaranteed using static routing algorithm. It is recommended for either simple network or networks where efficiency is not essential.

Adaptive routing is more of an interactive type where a change in traffic input patterns and or network topology elicits a response in route computation to offset or match the change. It is also referred to as Dynamic Routing. The routing protocol in this case tries to change its routes and guide traffic using other route paths to mitigate congestion and ensure high throughput. This applies to mobile Ad hoc networks because it is adapted and suited for high mobility nodes and changing network topology.

- *Reactive vs. Proactive:* This classification highly relates to ad-hoc networks. Proactive routing protocols maintain routing information that is immediately available by continuously evaluating the routes within the networks. This is so that when a packet needs to be forwarded, the route is already known and can be immediately used. On the contrary, reactive protocols must first determine the route hence can be said to invoke a route determination procedure on demand basis only.

2.1 DESIRABLE QUALITATIVE PROPERTIES OF MANET ROUTING PROTOCOLS

These are properties desirable in Ad hoc routing protocols [8]:

- *Distributed Operation:* As Ad hoc network is basically a distributed collection of nodes, its routing protocol is also expected to be distributed. Therefore, MANET routing protocols should be distributed, independent without relying on a central controlling node. This applies even in the case of a stationary network as in an Ad hoc network, mobility should always be factored in, as nodes can enter or leave the network easily.
- *Unidirectional Link Support:* In conventional design of routing algorithms, bidirectional links are typically assumed as many protocols are incapable of functioning properly over unidirectional links. However, unidirectional links can

and do often occur in Ad hoc wireless networks hence is a property expected of MANET routing protocols.

- *Loop-freedom:* It is generally desirable to avoid route loops in any network protocol. This guarantees improved overall performance by avoiding wastage of bandwidth and CPU consumption.
- *Demand-based operation:* It is more efficient if the routing protocol adapts to traffic patterns on a demand or need basis instead of assuming uniform traffic distribution within the network hence maintaining routing between all nodes at all times. The protocol should be reactive and if designed intelligently, can utilize node's power and network bandwidth resources more efficiently at the cost of increased route discovery delay.
- *Energy conservation:* As the nodes in Ad hoc networks are usually devices or thin clients which are mainly battery powered and therefore needs to conserve power when inactive using standby modes. It is therefore important, a routing protocol should be able to accommodate and support such sleep modes without overly adverse consequence. This property may require link layer protocol support through a standardized interface.
- *Multiple routes:* Multipath routing should be supported. In the case of topological changes and or congestion, the reaction or response will be more efficient if multiple routes are used. This saves the routing protocol from initiating another route discovery procedure and reduces latency and network resources usage [59].
- *Quality of Service Support (QoS):* This is a set of service requirements that needs to be met by the network while transporting a packet stream from a source to its destination. Its needs are normally set according to the service requirements of end user or host applications, of which it is expected to guarantee a set of measurable pre-specified service attributes to the users in terms of end-to-end performance, such as delay, bandwidth, packet loss probability, delay variance (jitter) etc. Power consumption is a QoS attribute also more specific to MANETs.
- *Security:* MANET routing protocol is vulnerable to many forms of attack without some form of network level or link-layer security. As it is harder to maintain "physical" security of the radio transmission media which make MANETs open to

all forms of security threats and attacks, preventive security measures are highly needed. Authentication and encryption will aid the mitigation most threats but the problem here lies in the distributed nature of the Ad hoc network. Securing MANET protocol is of the utmost importance and this thesis proposes solutions to that effect.

2.2 MOBILE AD HOC NETWORKS AND PROTOCOLS

There are different criteria for designing and classifying routing protocols for wireless Ad hoc networks. MANET routing protocols can be divided into the following categories:

- *Flat Routing Protocols*
    - Proactive Routing (Table-Driven)
    - Reactive Routing (On-Demand)
    - Hybrid Routing (blend of reactive and proactive)
- *Hierarchical (Zone/Cluster-Based) Routing Protocols*
- *Geographic Position Assisted Routing Protocols*
- *Power-Aware Routing Protocols*
- *Security-Aware Routing Protocols*
- *Routing Protocols with efficient flooding mechanisms*
- *Multicasting Routing Protocols*
    - Geographical Multicast (Geocasting)
    - Tree-Based
    - Mesh-Based
    - Zone Routing
    - Associativity-Based
    - Differential-Destination
    - Weight-Based
    - Preferred Link-based

All these categories of routing protocols are primarily based on flavors of distance-vector or link-state routing or a combination of both in addition to extra functionalities to aid and adapt the routing operations in particular ways.

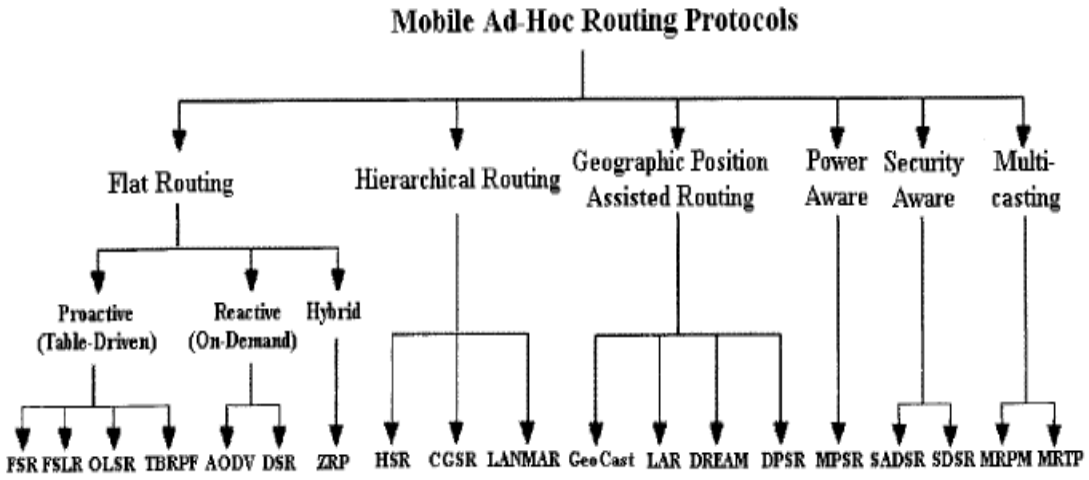


Figure 2.1 Broad Categories of Mobile Ad hoc Routing Protocols

The goals of these protocols could be summarized as [41]:

- Minimal Control Overhead
- Minimal Processing Overhead
- Multi-hop Routing Capability
- Dynamic Topology Maintenance
- Loop Prevention

Though Ad hoc routing protocols can be loosely classified using various criteria's as enumerated above but we will be using a broad classification based on network structure and topology as shown in figure 2.2 below.

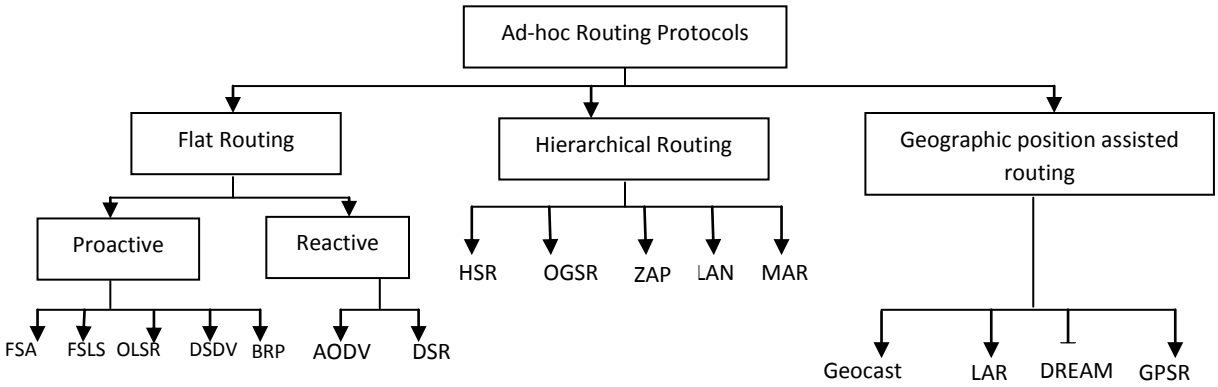


Figure 2.2 Classification of MANET Routing Protocol based on Network Structure & Topology

As shown in Figure 2.2, Ad hoc routing protocols can be grouped and fall into three major vertical and two horizontal categories. The vertical categories are: *Flat, Hierarchical, and Geographic Position Assisted Routing.* Horizontal categories are: *Reactive (On-Demand)* and *Proactive (Table-Driven).*

- *Geographic Position Assisted Routing:* This category uses geographical location as a basis. The main purpose is to integrate concept of physical location into the current design which relies on logical addressing. In Geographic Position Assisted Routing, a message is sent to a group of mobile nodes within a particular geographical region i.e. the geocast region. Hence this category uses the position of nodes i.e. Global Positioning System (GPS) for an efficient routing. Examples of related routing protocols are:
    - Location Aided Routing (LAR)
    - Geocast
    - DREAM
    - GPSR

- *Hierarchical Routing:* Here there is a grouping of individual nodes into clusters or grouping of clusters into bigger ones with a delegation of tasks or functions. This entails some nodes performing tasks while others wait until the task is handed over to the next level. The network is split logically into tiers, with probably a tier one node as the controlling node for a cluster. They are also referred to as cluster heads of which a cluster head is just a node in a cluster but also shares a boundary with another cluster and is assigned some control functions or tasks to be performed on behalf of its cluster.

  In hierarchical routing, the Ad hoc network is logically separated into subnets. A hierarchical addressing structure is needed for routing in the network [46]. Examples of protocols in this category are:

  - Host Specific Routing (HSR)
  - Cluster-head Gateway Switch Routing (CGSR)
  - Zone Routing Protocols (ZRP)
  - LANMAR

- *Flat Routing:* As the name infers, all Ad hoc elements and routing are of the same level. This means all nodes are on the same tier. Therefore there is no splitting or segregation of the network into tiers or levels. Neither is there typically a grouping of nodes into clusters. Flat routing protocols regard the Ad hoc network as a number of nodes without subnet partitioning, thus does not require a hierarchical addressing structure [46]. Flat routing protocols can be grouped further more into horizontal categories of:

  - Proactive (Table Driven) and
  - Reactive (On-Demand) routing protocols.

  This category of routing will be discussed in detail in this thesis. Also this is where the optimal routing protocol employed in the security solution and enhancement proposed in this work is chosen from.

2.3 PROACTIVE ROUTING PROTOCOLS

This kind of routing protocols record routes for all destinations in the network, which is based on traditional wire-line routing protocols. In proactive routing, routes to all destinations are computed prior with the protocol having a complete knowledge of the topology and link states are maintained in the nodes' routing tables in order to compute routes in advance. The routing information is disseminated among all nodes in the network throughout the operating time irrespective of the need for such a route [55]. Therefore, proactive routing is has most basic characteristics of "link state" routing protocol as each node maintains a view of the entire network topology with a cost for each link.

Proactive is also regarded as table-driven routing protocols. It can be subdivided depending on how the routing tables are constructed, maintained and updated [4]. Some of the existing proactive routing protocols are:
Fisheye State Routing (FSR); FSLS; Wireless Routing Protocol (WRP); Optimized Link-State Protocol (OLSR); Destination Sequenced Distance Vector (DSDV); Global State Routing (GSR); Source Tree Adaptive Routing (STAR); BRF.

2.3.1 Characteristics of Proactive Routing

- To keep up information up to date, routing tables or new routes are periodically broadcasted in the network between nodes.
- The updates are grouped into two according to the overhead packets generated. There are two types of packets called 'full dump' packets and 'incremental' packets.
- Initial convergence occurs by the exchange of the full routing table and routes (full dump packets) when establishing or during initial network setup. Subsequent network topology changes or mobility are periodically communicated by the use of incremental packets of the specific network changes.
- Each node periodically broadcasts the link costs of its outgoing links to all other nodes using flooding.

- The keep record in one or more routing tables and information of the routes in the topology is stored there.
- Each mobile node maintains a routing table that contains information about a route to every possible destination in the network and the number of hops of each route.
- Each route contains a sequence number assigned by the destination node. The sequence number allows a mobile node to distinguish between stale routes and new routes.

Route creation and maintenance are accomplished through some combination of periodic and event-triggered routing updates. Periodic updates consist of routing information exchanges between nodes at particular time intervals. This occurs regardless of the mobility and traffic characteristics of the network. However, event-triggered updates are transmitted whenever some event, such as a link addition or removal occurs.

2.3.2 Advantages of Proactive Routing

- ✓ There is reduced latency in proactive routing as the route is already available and can be immediately selected from the routing table when a source needs to send packets [66].
- ✓ Efficient forwarding of packets as the route is known at the time when the packet arrives at the node.
- ✓ Proactive protocols tend to perform well in networks where there are significant numbers of data sessions within the network as the overhead of maintaining each of the paths is justified as many of the paths are utilized.

2.3.3 Disadvantages of Proactive Routing

- × It has the disadvantage in that some routes may never be used and dissemination of routing information takes up a lot of the scarce network bandwidth as the states of the links and network topology change rapidly in large networks or high mobility ones.

- Also, proactive routing performs full lookup of the routing table for every packet, hence consumes more power as a result of higher CPU cycles needed for the task [47].
- Additional control traffic is needed to regularly update stale route entries of broken and re-established links as in Ad hoc mobile networks, there is bound to be a mobility of nodes [55].
- Also, purely proactive routing schemes use a large portion of bandwidth to keep routing information up-to-date and because of fast node mobility, route updates may be more frequent than the route requests.

2.4 REACTIVE ROUTING PROTOCOLS

These protocols are called reactive protocols as they initiate routing activities on an "*on-demand*" basis. This reactive nature of these protocols is a significant departure from more traditional proactive protocols that find routes between all source-destination pairs, regardless of the use or need of such routes. Reactive protocols do not maintain routing information or routing activity at the network nodes if there is no communication. A source node obtains a path to a specific destination only when it needs to send some data to it. In an Ad hoc network, link connectivity can change frequently and control overhead is costly hence reactive routing approaches take a departure from traditional internet routing approaches by not continuously maintaining a route between all pairs of network nodes. Instead, routes are only discovered when they are actually needed.

Reactive routing protocols are also called source initiated on-demand routing protocol. When a source wants to send a packet to another node, it checks to determine whether it has a route, if not, then this protocol searches for the route in an on-demand manner by it initiating a route discovery process in the network and establishes the connection in order to transmit and receive the packet. The route discovery process usually occurs by flooding route request packets throughout the network [49]. The discovered routes are maintained by a route maintenance procedure.

2.4.2 Characteristics of Reactive Routing

- Reactive routing does not have a complete knowledge of the network topology. That is, it does not maintain routes for all destination nodes in the network topology.
- Routes to active destinations already traversed and maintained at a node, will expire after some time of inactivity, during which the network is not being used.
- It can maintain traditional routing tables specifying the next hop to reach a destination or a route cache of routes already traversed.
- Routes are maintained only between nodes which need to communicate [10].

2.4.3 Advantages of Reactive Routing

- ✓ Control signaling overhead is likely to be reduced compared to proactive approaches, particularly in networks with low to moderate traffic loads.
- ✓ Uses far less bandwidth in maintaining routes at each node hence aids in conserving precious bandwidth of Ad hoc network.
- ✓ Key motivation behind the design of on-demand protocols is the reduction of the routing load. High routing load usually have a significant performance impact on low bandwidth wireless links [16].

2.4.4 Disadvantages of Reactive Routing

- × A drawback to reactive approaches is the introduction of latency due to its route acquisition processes. That is, when a route is needed by a source node, there is some finite latency while the route is discovered.
- × If the topology of networks changes rapidly, a lot of update packets will be generated and disseminated over the network consuming a lot of precious bandwidth.
- × Also, mobility when using reactive routing protocols may cause too much fluctuation of routes.
- × Pure reactive routing is less suitable for real-time traffic as a result of its increased latency or long setup delay.

Examples of the protocols in the Reactive routing protocol class are: Dynamic Source Routing Protocol (DSR), Ad hoc On-Demand Distance Vector Routing Protocol (AODV), and Temporally Ordered Routing Protocol (TORA). We are going to use Ad hoc On-Demand Distance Vector Routing Protocol (AODV) and Dynamic Source Routing (DSR) as our reference reactive protocols, discussing and comparing them to greater detail.

2.5 AODV – (Ad Hoc On-Demand Distance Vector)

The Ad hoc On-Demand Distance Vector (AODV) Routing Protocol enables multi-hop routing between participating mobile nodes in an Ad hoc network. As a reactive routing protocol, it minimizes the number of broadcasts by providing route discovery on-demand in mobile Ad hoc networks. That is, AODV only requests a route when needed and does not require nodes to maintain routes to destinations that are not recently or actively used in communication. It is based upon the distance vector algorithm. As with most reactive routing protocols, route finding is achieved by a route discovery cycle involving a broadcast network search and a uni-cast reply containing discovered paths. Similar to DSDV, AODV relies on sequence numbers for routing loop prevention and to identify most recent route path. For a network using AODV routing, nodes stores next-hop routing information for destination nodes, in a route table. Each routing table entry has an associated lifetime value. If a route is not utilized within the lifetime period, the route expires, becoming invalid with the entry then deleted from the routing table. However, each time the route entry is used, the lifetime period is updated so that route is not prematurely deleted.

2.5.1 Characteristics of AODV

- It enables multi-hop routing between mobile nodes in a MANET.
- AODV only request a route when needed or demanded.
- It retains only routes recently used and does not maintain routes to destinations that are not actively used in communications. Also, as long as there is no request

or the on-going communication has valid routes to each other, it does not play any role.

- It supports multicast routing and mitigates the Bellman Ford "counting to infinity" problem utilizing destination sequence numbers.
- A node in AODV routing, updates its path information only if the destination sequence number of the current packet received is greater than the last destination sequence number stored in the route entry at the node [55].
- The AODV algorithm uses different messages to discover and maintain route links. They are:
    - It broadcasts a Route Request (RREQ) to all its neighbors when a node wants to find a route to another node.
    - It uses hello messages broadcasted periodically in the form of special Route Reply (RREP) to immediate neighbors. These hello messages serve as advertisements to indicate the continued presence of the node.
    - In the event of a link failure or topology change, a Route Error Packet(RERR) is used for link failure notification and sent to the affected set of nodes.
- Each node maintains in the routing table, one entry per destination hence no multiple paths are stored or available.
- A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use or have used that entry to route data packets.
- AODV keeps track of recently traversed routes by entering them in the routing table. The route entries has the following information:[67]
    - Destination IP Address – The IP address for the destination node
    - Destination Sequence Number
    - Hop Count – Number of hops to the destination
    - Next Hop – The designated neighbor to forward packets to the destination for the route entry
    - Lifetime – The time period which the route entry is considered valid (renewed if route is used)

- Active Neighbor List – Neighbor nodes which actively use this route entry
- Request Buffer – Used to ensure that a request is only processed once

- It has a characteristic of minimal space complexity whereby the algorithm makes sure that the nodes that are not in the active path do not maintain information about a requested route. When a node receives the Route Request Packet (RREQ), sets a reverse path in its routing table and propagates the RREQ to its neighbors, if it does not receive any Route Reply Packet (RREP) from its neighbors for that request, it deletes the routing information that it recorded.

2.5.2 Route Discovery

When a source node needs or has data packets to send to some destination, it first checks whether it already has a route entry to the destination in its route table. If a route entry exists, it will then use the route for the data packet transmissions. However, if it does not find a route in its routing table, it must initiate a route discovery procedure to find a route. To start route discovery, the source node will create a *Route Request Packet (RREQ).* In the packet, it enters the destination node's IP address, the last known sequence number for that destination, and the source IP address and current sequence number. The RREQ will also contain a hop count, initialized to zero, and a Route Request ID (RREQ ID) also known as broadcast ID.

The RREQ ID or broadcast ID is a per-node identity number with an increasing counter that is incremented each time the node initiates a new RREQ. Therefore, the source IP address together with the RREQ ID, uniquely identifies a RREQ and can be used to detect duplicates and identify the most recent. After the creation of the Route Request Packet, the source node broadcasts the RREQ to its neighbors.

After forwarding the RREQ, a neighboring or intermediate node, on receipt of the RREQ, first creates a *Reverse Route* to the source node. It records the *reverse route* as an entry in its route table of the source node from which the first copy of the request came. Also the node from which it received the RREQ is then designated as the next hop to the source node and the hop count in the RREQ is incremented by one to get the hop distance from the source. If additional copies of the same RREQ are later received, these packets are

discarded. The node then checks its own routing table to determine if it has an unexpired route to the destination. If it does not have a valid route to the destination, it simply rebroadcasts the RREQ, with an incremented hop count value to its neighbors. Hence, in this manner, the RREQ floods the network in search of a route to the destination. Figure 2.3(a) below illustrates this procedure [34].

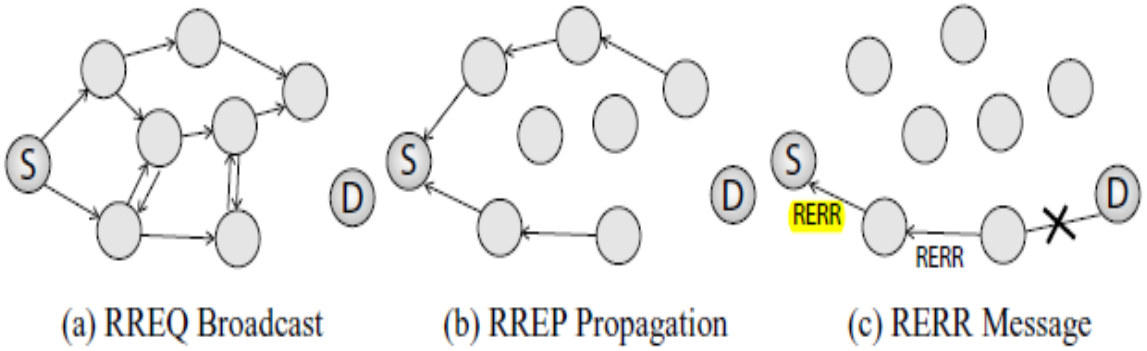


Figure 2.3 AODV Route Discovery and Maintenance

However, when a node receives a RREQ and after checking whether it has an unexpired or valid route to the destination, if it does have such a route, a condition has to be fulfilled for the node to generate a reply message containing the route to the destination. The condition is that this node's route table entry for the intended destination must have a corresponding sequence number that is at least equal or greater than the one contained in the route request RREQ.

Condition ---> $dseq_{\mathrm{rt}} \geq dseq_{RREQ}$

When this condition holds, it means that the node's route table entry for the destination is at least as recent as the source node's last known route to the destination. This condition ensures that the most recent route is selected and also guarantees loop freedom. Once this condition is met, the current node can then create a *Route Reply Packet (RREP)* message.

The RREP contains the source node IP address, the destination node IP address, and the destination sequence number as given by the node's route table entry for the destination. In addition, the hop count field in the RREP is set to correspond to the node's distance

from the destination. If the destination itself is creating the RREP, the hop count is set equal to zero. After creating the reply – RREP, the node uni-casts the message to its next hop towards the source node. The node utilizes the *reverse route* it created and recorded in its routing table in forwarding the RREP back to the source node [10].

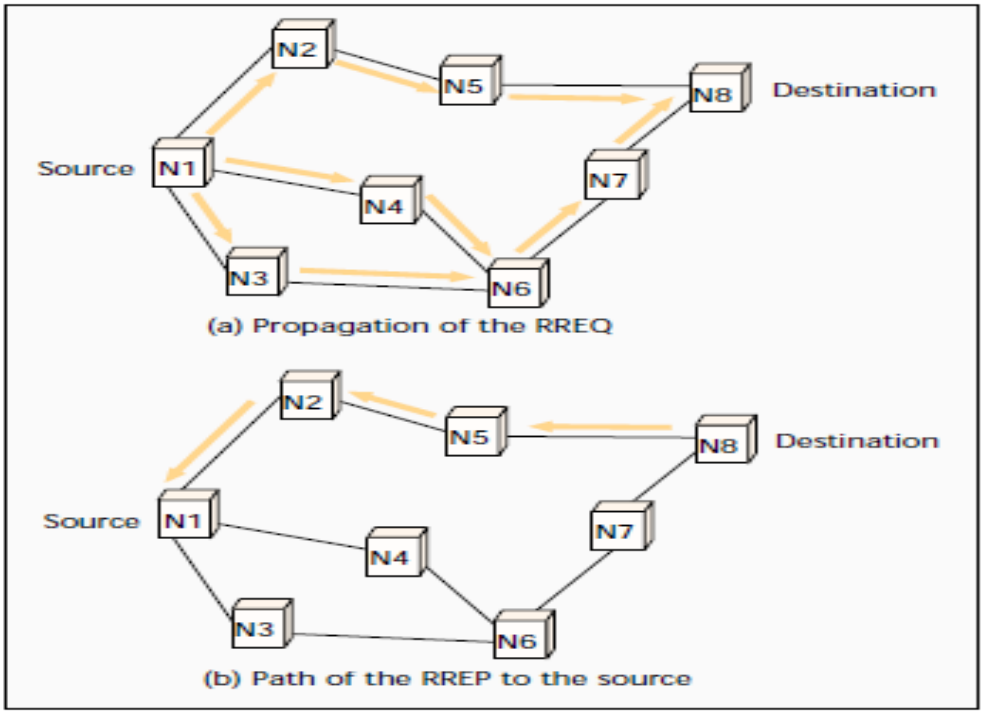


Figure 2.4 AODV Route Discovery

As the RREP is routed back along the reverse path, nodes along this path on receipt of the RREP, first creates a *forward route entry* for the destination node in their route tables which point to the node from which the RREP came. That is, it uses the node from which it received the RREP as the next hop towards the destination node. These forward route entries indicate the active forward route. The hop count for that route is the hop count in the RREP, incremented by one. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used within a specified lifetime. This forward route entry for the destination is for utilization if and when the source selects this path for data packet transmissions to the destination. On creating the *forward route entry*, it forwards the RREP to the destination node. Because the RREP is forwarded along the path established by the RREQ, AODV only supports the use of *Symmetric* links as the

route reply packet follows the reverse path of the route request packet. The RREP is then forwarded hop by hop to the source node as indicated in the figure 2.4(b) above [34].
On receipt of the RREP by the source node, it then utilizes the path for the transmission of data packets. If more than one RREP is received, the source node selects the route with the greatest sequence number and smallest hop count. It is then established and entered into the routing table, maintaining it as long as it is needed and recently used. A route that has been recently utilized for transmission of data packets is called an *active* route. Hence a route is considered *active* as long as there are data packets periodically travelling from the source to the destination along that path. Each node maintains in the routing table one entry per destination. Therefore, multiple paths are not stored or available in AODV.

2.5.3 Route Maintenance

Routes are maintained as follows. If a source node moves, it is able to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its upstream neighbors will notice the move or link failure and propagate a *link failure notification* message (which is an RREP with infinite metric) to each of its active upstream neighbors to inform them of the erasure of that part of the route. These nodes in turn, propagate the *link failure* notification to their upstream neighbors, and so on until the source node is reached. The source node can then choose to reinitiate route discovery for that destination if needed.

AODV specifies two different ways in which a link break can be detected. An aspect of the protocol route maintenance is through all nodes regularly broadcasting a “hello” message to its one-hop neighbors. Periodic local broadcasts (‘hello’ messages) by a node, is used to inform each of the mobile nodes in its neighborhood, of its presence and continued operation. Hello messages can be used to maintain the local connectivity of a node. This makes it possible for them to verify link operation, immediately identifying link breakage or node dissociation. Also, hello messages may list the other nodes from which a mobile node has heard from, thereby yielding greater knowledge of network connectivity. The second way is detection through a link signaling mechanism when the link is used.

2.5.4 Advantages of AODV

- ✓ It optimizes available bandwidth as it does not require periodic global advertisements.
- ✓ It is a simple protocol to implement in the network and makes the network self-starting. This is with each node behaving as a router, maintaining a simple routing table, and the source node initiating path discovery request.
- ✓ AODV has the advantage of selecting the best routes to a destination node as a result of its usage of both the lowest hop-count and the latest valid path (made possible by its use of the higher destination sequence number).
- ✓ The algorithm is highly scalable because of the minimum space complexity and the broadcasts avoided.
- ✓ Because of its reactive nature, and its efficient route maintenance mechanisms which enables it to respond quickly to broken links, AODV can handle highly dynamic behavior.

2.5.5 Disadvantages of AODV

- × It has a disadvantage of overdependence on broadcast medium. That is, the algorithm expects or requires the nodes in the broadcast medium can detect each other's broadcasts.
- × When compared to other reactive protocols, AODV incurs a higher overhead bandwidth. This comes about from an RREQ when travelling from node to node in the process of route discovery on-demand, it sets up the reverse path with the addresses of all the nodes through which it is passing and then carries all this information all the way.
- × AODV lacks an efficient route maintenance technique as there is limited reuse of routing information and routes are always obtained on demand including for common cases traffic [65].

- It is highly vulnerable to misuse – its messages can be misused and replayed for insider attacks including route disruption, route invasion, node isolation, and resource consumption.
- As it is designed solely to use hop count as metric, it favors long, low-bandwidth links over short, high bandwidth links. Therefore AODV lacks support for high throughput routing metrics.
- As characteristic of reactive routing protocols, AODV does not discover a route until a flow is initiated. This route discovery adds latency and can be quite high in large-scale full mesh networks.

2.6 DSR – (Dynamic Source Routing)

The Dynamic Source Routing protocol (DSR) is simple and efficiently designed specifically for routing purposes in multi-hop wireless Ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure, pre-administration or administration. The DSR protocol provides highly reactive service in order to help ensure successful delivery of data packets in spite of node movement or other changes in network conditions. The key distinguishing feature of DSR is the use of *source routing,* where the sender knows the complete hop-by-hop route to the destination. These routes are stored in a route cache. The data packets carry the source route in the packet header. It comprises of two major mechanisms that work together to allow the discovery and maintenance of source routes in the Ad hoc network: "Route Discovery" and "Route Maintenance". Route Discovery is the mechanism by which a node originating a packet to some destination discovers a source route to that destination if it does not currently have a route to that destination cached. Route Maintenance is the mechanism by which a node sending a packet to some destination learns if the route it used for that packet has broken (i.e. because some node in the route has moved out of wireless transmission range of the previous node in the prior existing route).

The protocol allows multiple routes to any destination (multipath routing) and allows each sender to select and control the routes used in routing its packets which is handy for use in load balancing or for increased robustness. In the IETF rfc 4728, the design specification and provision is for Ad hoc networks up to a couple hundreds of nodes. DSR is an on-demand protocol designed to restrict the bandwidth consumed by control packets in Ad hoc wireless networks by eliminating the periodic table update messages which in contrast is required in the table driven approach and even as found in AODV.

2.6.1 Characteristics of DSR

- DSR makes use of *source routing,* where the sender knows the complete hop-by-hop route to the destination. Instead of being forwarded hop by hop, data packets contain strict source routes that specify each node along the path to the destination. The data packets carry the source route (total hop-by-hop route information to a destination) in the packet header.
- It utilizes a *route cache* for maintaining and tracking routing information instead of a route table. In the route cache, it stores all possible information extracted from the source route contained in a data packet. Entries in the route cache are continually updated as new routes are learned.
- The route entries in the DSR *route cache* need not have lifetimes. That is, once a route is placed in the route cache, it can remain there until it breaks.
- There is no special mechanism needed to detect routing loops as DSR makes very aggressive use of source routing and route caching.
- It makes use of a mechanism called *route salvaging* to repair a link break in the event that its node upstream has a different valid route to the destination in their route cache.
- In DSR, nodes can receive and process data and control packets that were not addressed to them at the MAC layer, using it to gratuitously learn routing information for other network destinations. This option is a characteristic of DSR known as *promiscuous listening*.
- DSR requires no periodic packets of any kind at any layer within the network. Hence it does not use any periodic routing advertisement, link status sensing, or

neighbor detection packets. It also does not rely on these functions from any underlying protocols in the network.

- It is *beacon-less* and does not require *hello* packet transmissions which are used by a node to inform its neighbors of its presence [55].
- It utilizes only event-triggered updates.
- A node sending a packet using DSR, can select and control the route used for its own packets as a result of multiple route information and its multipath support.
- It makes use of a "soft state" approach in routing. Soft state in that the loss of any state will not interfere with the correct operation of the protocol. That is also, that routing information can be discarded without any warning or collaboration with other nodes (as a local decision) and the network could continue to operate. All state is discovered as needed and can easily and quickly be rediscovered if needed after a failure without significant impact on the protocol.
- DSR is capable of routing correctly over networks using *unidirectional* links, since the path over which the Route Reply (RREP) is sent need not be the same as the reverse of the path over which the Route Request (RREQ) was forwarded.
- Host may use its *route cache* to avoid propagating a RREQ received from another host. This is because, on receipt of a RREQ, the node checks its route cache first to check if it has a route to the requested destination and only if it does not, will it forward the RREQ onwards.
- The initiator of a RREQ can specify the maximum number of hops or maximum hop limit for the RREQ to travel.

2.6.2 Route Discovery of DSR

When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination/target node. If it has an unexpired route to the destination, it will use that route to send the packet. On the other hand if the nodes not have such a route, it initiates a *route discovery process* to dynamically determine such a route.

In a route discovery, a node A wanting to send a packet to some node D of which it does not have a route entry to in its route cache, will broadcast a *Route Request Packet (RREQ)*, which is received by nodes within wireless transmission range of D. This *Route Request (RREQ)* contains the IP address of the destination, along with the source node's address and a unique identification number for this route discovery chosen by the source node A. The source node A is referred to as the *originator/source* of the Route Discovery, and node D is referred to as the *target/destination* of the Discovery.

If an intermediate node receives a RREQ for which it is not the target, it checks its route cache to see it has a route to the destination/target of the RREQ. If it does not have an entry in its local route cache, it adds its own IP address to the *route record* of the RREQ packet and then it rebroadcasts the Route Request (RREQ) by forwarding the packets along its outgoing links. This RREQ *route record* comprises a list of intermediate nodes that have forwarded this RREQ up to this point including the source/originator node. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's IP address does not already appear on the route record. When the request (RREQ) reaches the target/destination node, this list of hops *(route record)* in the RREQ will be an indication of the path or sequence of hops along which this copy of the RREQ was forwarded in the Route Discovery in order to reach the target/destination node from the originator/source node. Figure 2.5(a) illustrates the formation of the route record as the route request propagates through the network [10].

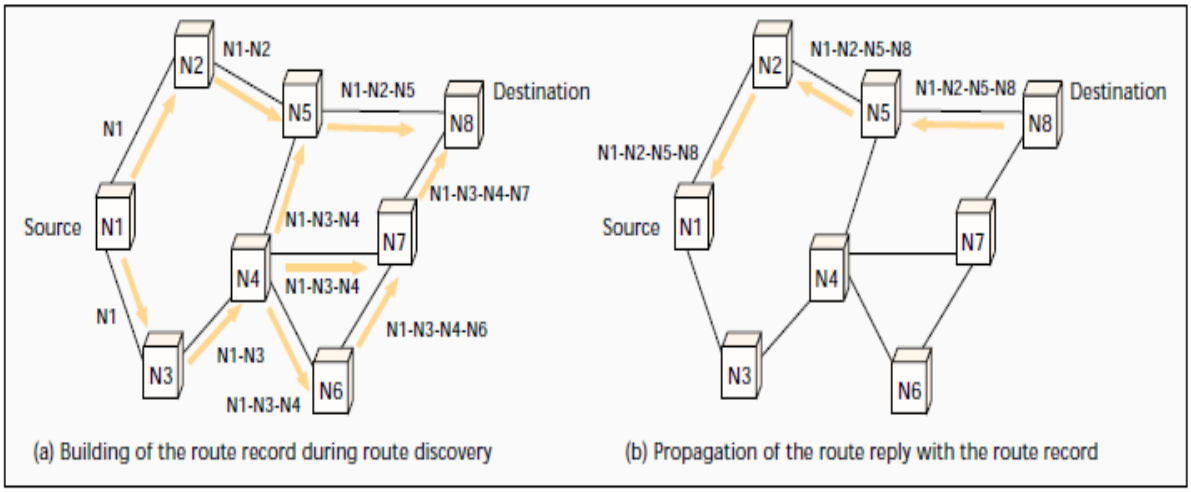


Figure 2.5 Creation of the route record in DSR

A *Route Reply packet* is generated when the route request reaches either the destination itself, or an intermediate node which contains in its route cache an un-expired route to the destination/target. If it is the destination/target node, it places or encapsulates the sequence of hops taken (route record) from the originator to itself (the destination) in the packet header of a unicast *Route Reply (RREP) Packet*. The Route Reply (RREP) can in general be routed along any path independent of the original route that was taken by the Route Request (RREQ) packet to get to the target/destination node. This ability of the Route Discovery in DSR allows *unidirectional links* to be supported (if allowed by the specific MAC protocol in use on that link). The originator or source node on getting this RREP, enters it into its route cache for possible use on subsequent packets while immediately using the path discovered to commence the transmission it wanted to do, of data to that destination/target node.

But if a Route Request (RREQ) reaches an intermediate node that has a route entry to the target/destination node in its route cache, this intermediate node can reply, sending a Route Reply (RREP) with a route to the target back to the originator/source. The intermediate node will append it's cached route to the route record and then generate the route reply (RREP). By replying using the route from its route cache, the new route is returned to the originator sooner, and the overhead of Route Discovery is reduced since the RREQ need not be rebroadcasted. To return the route reply, the responding node must

have a route back to the originator/source node. If it has a route to the source node in its route cache, it may use that route. Otherwise, if symmetric links are supported, the node may reverse the route in the route record. If the symmetric links are not supported, the node may initiate its own route discovery and piggyback the route reply on the new route request. Figure 2.6(b) shows the transmission of the route reply with its associated route record back to the source node [10].

A node may also update its route cache based on source routes or other routing information that it may glean from forwarding the packets it forwards for other nodes by optionally operating its network interface hardware in a promiscuous receive mode.

There are a number of optimizations that improve the performance of this basic Route Discovery mechanism detailed above. An example is the *expanding ring* searches. This is a mechanism by which Route Requests (RREQ) may be limited by the Time To Live (TTL) field in the IP header of the packet, control the extent of propagation of RREQ, first from the local or one-hop immediate neighbors to larger areas.

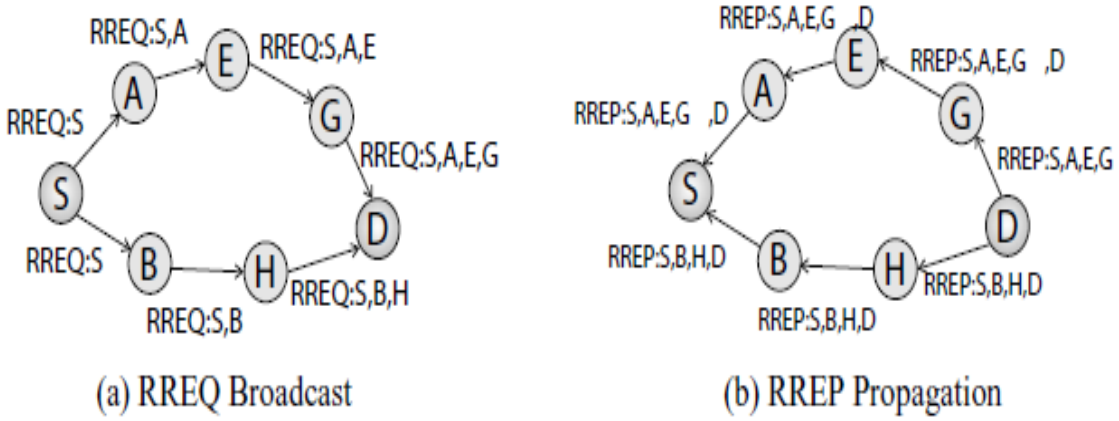


Figure 2.6 DSR route discovery [34]

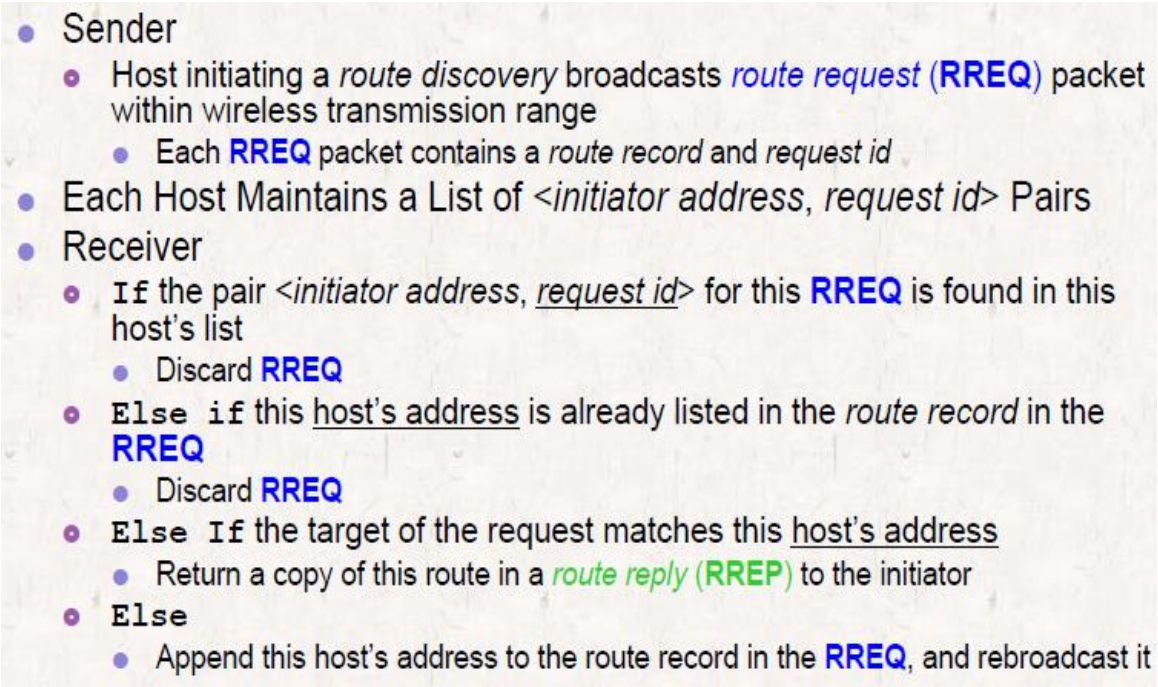


Figure 2.7 Breakdown of DSR Route Discovery [36]

2.6.3 Route Maintenance

After Route Discovery, a source node originating a packet, in the header of the packet, lists a route, with a complete list of hops through which the packet is to be forwarded. It then sends the packet out to the target/destination. The originator or source node is then responsible to confirm that the packet has been received by the first intermediate hop in the route, retransmitting the packet if necessary until this confirmation is received. It can retransmit until a maximum number of retransmission attempts have been performed. Also, when the intermediate node receives the packet and sends it on along the route, it is responsible in the same way for confirming if the packet has been received by the next node in the packet route. The packet is retransmitted by the intermediate node if necessary, just like the original sender.

This confirmation of receipt of the sent packet by the next hop can be obtained in two ways. Confirmation can be achieved through a *passive* acknowledgement using the link-level acknowledgement present in many wireless MAC protocols including IEEE 802.11 [8, 60]. Also, confirmation can be received through an explicit DSR acknowledgement packet from the next hop if necessary.

Route Error packets (*RREP)* are generated at a node when the data link layer encounters a transmission problem. Hence, if confirmation is not received after a limited number of retransmission attempts for the packet, the link from this node to the next hop will be considered to have broken and a *Route Error (RERR) Packet* identifying and notifying about this broken hop is returned to the originator/source node. When a route error packet (RREP) is received, the hop in error is removed from the source node's route cache and all routes containing that hop in error are truncated at that point. It will then use an alternate route to the same destination/target to re-send the packet or for subsequent packet transmissions, if it has the alternate route already in its route cache. If no other route exists in its route cache to the destination, it will invoke Route Discovery to discover a new source route to the destination. In addition to route error messages, *acknowledgements* are used to verify the correct operation of the route links. Such acknowledgments include *passive* acknowledgements, where a mobile is able to hear the next hop, forwarding the packet along the route.

As with Route Discovery, there are a number of optimizations that improve the Route Maintenance performance of the protocol [5, 25]. One of which is a case where, an intermediate node detects a broken link and returns a Route Error (*RERR)* to the source node sender of a packet, the intermediate node may attempt to *salvage* the packet if it has in its own route cache an alternate valid route to the packet's target/destination. To salvage, the intermediate node replaces the path in the original packet route with the alternate route it has in its cache and then transmits the packet to the new next hop node. Another optimization supported by DSR which helps in efficient Route Maintenance is *automatic route shortening.* This allows source-destination routes in use to be shortened when possible, for example, in a case, when nodes move close enough together so that one or more intermediate hops are no longer necessary. Here, if a node is able to promiscuously listen to a packet not intended for it as the next hop, but for which its own node is listed in the unused portion of the packet's source route, then this node can return a *Gratuitous Route Reply* to the original sender of the packet (source node). This *gratuitous RREP* will give the shorter route through that intermediate node that omits one or more of the original intermediate nodes listed in the route been used for the transmission, therefore offering a shorter path to the intended destination.

2.6.4 DSR Optimizations

Several additional optimizations exist in the DSR protocol specifications. They are:

(i) *Salvaging:* This is in the event of link failure or node dissociation. Here, an intermediate node can use an alternate route from its own cache, to successfully transmit data to a specified destination when a data packet encounters a broken link on its source route.

(ii) *Gratuitous repair:* Also this is a route or link repair optimization for greater efficiency. Normally, in DSR, a source node is solely notified by a Route Error Packet (*RERR)*, when a link fails during the transmission of data from the source node to a destination node. *Gratuitous route repair* enhances the process by ensuring a source node, on receiving a RERR packet sends the RERR back along the same path which it came to traverse the same routes. This helps clean up the caches of other nodes in the network that may have the failed link in one of their cached source routes.

(iii) *Promiscuous listening:* This is the ability of nodes to overhear can receive and process data and control packets that were not addressed to them at the MAC layer, using it to gratuitously learn routing information for other network destinations. Also, listening helps a node to learn different routes without directly participating in the routing process.

(iv) *Gratuitous Route Reply (RREP):* This optimization utilizes the promiscuous listening feature. From the information a node gleans using the promiscuous listening mode feature, it checks whether the packet could be routed via itself to gain a shorter route. If so, the node sends a gratuitous RREP to the source of the route with this new, better route.

2.6.5 Advantages of DSR

- There is a higher efficiency and reduced latency as a result of its support of multipath routing, hence, in the event of a link breakage or route going invalid, the source can utilize alternate routes from the route cache if available to prevent another route discovery hence also conserving bandwidth.

- Advantages of DSR include easily guaranteed loop-free routing, operation in networks containing unidirectional links, and very rapid recovery when routes in the networks change.
- Load balancing can be done using DSR as it allows the sender node to select and control the route used for its own packets made possible by its support for multiple routes. Also as the sender node can avoid duplicate hops in the routes selected, all routes used are easily guaranteed to be loop-free.
- The number of overhead packets caused by DSR is scaled all the way to zero when all nodes are approximately stationary with respect to each other and all routes needed for current communication have already been discovered. This is enabled by its lack of usage of any periodic routing advertisement or dependence on any underlying protocols in the network.
- It utilizes only soft state in routing which allows the routing protocol to be very robust to problems such as dropped or delayed routing packets or node failures. A node in DSR that fails and reboots can easily rejoin the network immediately after rebooting and if the failed node was involved in forwarding packets for other nodes as an intermediate hop along one or more routes, it can resume this forwarding immediately after rebooting, with no or minimal interruption to the routing protocol.
- In an Ad hoc network, the use of source routing provides many advantages including simplicity and flexibility [21].
- Differentiated treatment of different types or classes of packets for Quality of Service (QoS) is possible since by having the source route in a packet's header, all routing decisions for a packet are made by the sender of the packet. It is possible for the sender to use different routes for different packets (QoS), without requiring coordination or explicit support by the intermediate nodes.

2.6.6 Disadvantages of DSR

- As the current specification [45] for DSR does not contain any mechanism for route entry invalidation or route-prioritization when faced with a choice of multiple routes, this leads to stale cache entries, particularly at high mobility.
- DSR has the disadvantage of increased per-packet overhead. This is as a result of source routing where the size of each packet is increased in order to carry the source route of hops through which the packet is to be forwarded. The extra network overhead caused by the presence of the source route is incurred not only when the packet is originated, but also each time it is forwarded to the next hop. This extra network overhead decreases the bandwidth available for transmission of data, and consumes extra battery power in the network transmitter and receiver node.
- Loss of data packets and wastage of network bandwidth exists in DSR as a result of having no expiration of routes. Without an effective mechanism to remove excessively old (stale) entries, route caches may contain broken or non-minimum hop routes.
- There is also the security risk pertaining to DSR's route maintenance mechanism. A malicious node may misroute data packets without risking detection under the guise of data salvaging optimization.
- DSR is not very scalable to large networks. Also, it requires more processing resources as each node must spend more time processing any control data it receives, even if it is not the intended recipient (promiscuous listening).

2.7 COMPARISION BETWEEN AODV AND DSR

According to protocol properties, we compare and contrast the characteristics and mechanisms of AODV and DSR. This is detailed in table 2.1 and 2.2 below.

Table 2.1 Comparing Protocol Properties of AODV and DSR

Protocol Property	**Ad-hoc On-Demand Distance Vector (AODV)**	**Dynamic Source Routing (DSR)**
Multi-Path/ Multiple Route capability	***NO*** – Does not support Multipath/Multicost routing	***YES*** – Supports multipath/multicast routes
Uni-directional Link	***NO*** – Does not support Unidirectional link routing	***YES*** – Supports unidirectional link routing
Scalability	***YES*** – Scalable to large networks	***NO*** – Not scalable to large networks, best suited for smaller networks
Distributed	***YES***	***YES***
Multicast	***YES***	***NO***
QoS Support (Quality of Service)	***NO***	***YES***
Route Reconfiguration	It adopts the use of *SEQUENCE NUMBERS* for route maintenance & freshness	Erases route and notifies source
Route Information Record	Uses *ROUTE TABLES*	Uses *ROUTE CACHE* entries to maintain routing information
Protocol Type	*REACTIVE* (using Distance-Vector routing features)	*REACTIVE* (using purely Link State routing features)
Critical Nodes	*NO*	NO
Updates transmitted to	Neighbor Nodes	Neighbor Nodes
Route Update Mechanism	*HELLO & ROUTE BROADCASTS* – which contains destination IP address, number of hops & sequence number	*BEACONLESS* – Does not require hello transmissions.

Frequency of Updates	*PERIODIC AND EVENT TRIGGERED*	*EVENT TRIGGERED*
Multicast capability	*YES*	*NO* - Uses unicast transmissions more
Optimization	Concept of *Expanding Ring Search* & *Local repair of links*	Concept of *Promiscuous listening,* salvaging, gratuitous and replies
Design and Definition Standards Proposal	Uses *RFC 3561* as its specification standard	Uses *RFC 4728* as a standard
Routing Philosophy	*FLAT*	*FLAT*
Routing Metric	*HOP COUNT* using freshest and shortest path	*HOP COUNT* using shortest path

Table 2.2 Differences between AODV and DSR

DSR	**AODV**
Uses *Source Routing*	Uses a *Table-Driven* routing framework
It utilizes a *Soft State* approach in routing	Mainly *Hard State* routing
Features based on *Link State Routing* algorithm	Mainly features from *Distance Vector* algorithm
It stores/records route information using multiple route cache entries for a destination	Stores/records route information as one entry per destination route
Does not support timer-based states	Each routing table entry has an associated lifetime value
Does not support hop by hop routing, instead the packet carries the complete path from source to destination, to be traversed	For routing transmission, it uses intermediate nodes (hop by hop) and next hop information corresponding to each flow for packet forwarding
A set of predecessor nodes is maintained as a list called *route record* in the headers of Route Request Packets (RREQ)	A set of predecessor nodes is maintained for each routing table entry indicating neighboring nodes that use or have used that route to forward packets
Route Error Packets (RERR) are used to inform the source node exclusively about a route/link failure	Route Error Packets (RERR) are used to inform all nodes using a link when the link fails
DSR replies to all requests reaching a destination from a single request cycle	In AODV on the other hand, the destination replies only once to the request arriving first and ignores the rest
DSR has access to a significant amount of routing information using both its source routing and promiscuous listening mechanism. With a single request-reply cycle, the source can learn different routes to each intermediate node on the route in addition to the intended destination.	AODV can gather only a limited amount of routing information in the absence of source routing and promiscuous listening. This makes AODV to rely on route discovery flood more often, which causes a significant network overhead.

CHAPTER THREE
EVALUATION OF MANET ROUTING PROTOCOLS AND REVIEW OF EXISTING WORK

3.1 EVALUATION OF ROUTING PROTOCOLS

This section summarizes and compares the results regarding existing research work done on the routing protocols DSR, AODV and DSDV. In the existing work we used for the evaluations here, the Network Simulator (NS-2) and above were predominantly utilized in carrying out the researches. Comparing the results in the papers directly will not be entirely accurate since the test environments and used protocol features do vary. However, with that in mind, we ensure that the protocol behavior and performance metrics is consistent between the works used for our evaluation. This will further give credence to the results as the research, experiments and simulations where carried by different people at different places and environments but ensuring the performance metrics used are constant and the models employed relatively consistent. Distributed *Constant Bit Rate (CBR)* sources were mostly used in all the existing studies evaluated here with the *random waypoint model* as mobility model. The routing protocols are compared on the metrics:

(i) Throughput, (ii) Delay, (iii) Routing Overhead,
(iv) Energy Efficiency,

3.2 PERFORMANCE METRICS

3.2.1 Throughput

Defined based on a desired outcome, throughput can be explained as a ratio between transmitted packets and delivered packets. Basically presented, it is the number of bits transmitted between source and destination per unit time [59]. It is a measure of how successful a protocol is in delivering packets from source to destination.

$$Throughput\ \% = \frac{\sum_t^n CBR\_received}{\sum_t^m CBR\_sent}\ x\ 100 \qquad \text{…….} \quad \text{(i)}$$

Where n = number of received packets, and m is the number of sent packets and CBR = Committed Bit Rate

3.2.2 Delay

This packet transmission protocol property is useful for establishing the responsiveness of applications. There are however, two problems with the delay measurements. First, the delay can only be computed using successfully received messages/packets (throughput received) i.e. the throughput has to be acceptable for delay to be accurately considered. Secondly, only the average delay is reported. Therefore, to be able to judge the usefulness of delay when routing for delay sensitive applications (i.e streaming voice and video), distribution of delay is worth considering too if feasible [59].

Generally, higher mobility and higher traffic load increase the delay. Also congestion brings about higher delays even at low mobility. With congestion, delay can be higher at low mobility than at medium mobility. Major part of the delay comes from queuing at congested nodes. However, according to the existing comparison works done, we will be evaluating delay as an average end-to-end delay of data packets. *Average end-to-end delay* of data packets includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, propagation and transfer times.

$$Average\ Delay\ \% = \frac{\sum_t^n (CBR_{sent_{time}} - CBR_{receive\_time})}{\sum_t^n CBR\_received}\ x\ 100 \qquad \text{……} \quad \text{(ii)}$$

Where n = number of received packets, and CBR = Committed Bit Rate

3.2.3 Routing Overhead

Routing protocols generate traffic as a result of their control packets which is needed to get and maintain routes and network information. There are two common ways to measure this traffic: (a) Number of packets and (b) Number of bytes. The cost to gain access to the media dominates relative to the per byte transmission cost in contention

based media access including wireless. That means, it is more important to reduce the number of routing packets than the absolute routing data size.

Hence, Routing overhead can be said to be the ratio between the total numbers of routing or control packets transmitted to data packets. That is, the number of routing packets transmitted per data packet delivered at the destination. The routing load metric evaluates the efficiency of the routing protocol.

$$Routing\ Overhead = \frac{\sum_t^k Routing\_packets}{\sum_t^n CBR\_received}\ x\ 100 \qquad \ldots\ldots\ldots\ldots \qquad \text{(iii)}$$

Where n = number of received packets, and k is the number of routing packets.

3.2.4 Energy Efficiency

In real life systems, energy consumption is a major issue. For many Ad hoc networks, the nodes are usually small and portable thereby imposing stringent constraints on the battery size and power available. The source of energy consumption for each node in an Ad hoc network is mainly the transmission and reception of both control and data packets. Since the Ad hoc routing protocol determines which nodes will forward the packets and the amount of routing overhead each node needs, the type of protocol definitely affects the energy performance of the system. Other means of energy consumption such as when the node is in listening mode or when the node is caching and filtering route information were assumed equal and taken as constants [17, 18].

Throughput and Delay metrics are among the most important metrics for best traffic forwarding. The routing load metric is an indication of the efficiency of a routing protocol. However, it should be noted that these metrics are not completely independent but rather do have a correlation to one another. Take for an example, a larger overhead may cause lower throughput and longer delay. On the other hand, a shorter delay may not necessarily imply a higher throughput, since delay is only measured on those successfully delivered packets. Also of note is that the existing performance comparison work evaluated here was tested and analyzed based on a random situation using random way point traffic model. Real-world scenario Ad hoc networks usually do have special traffic and mobility models. As different networks and applications have different scenarios, it is difficult getting a model to satisfy exactly the varying scenarios.

3.3 REVIEW OF EXISTING WORK MANET ROUTING PROTOCOLS

Considering performance of routing protocols can be based on various mechanisms which lead to differences in performance and operation, each routing protocol reacts differently when evaluated using metrics and a mobility model. The mobility model of the work utilized by the existing research work compared here is the *random way point* mobility model. Also, the source of packets employed for those simulations are *Constant Bit Rate (CBR)* sources.

According to Sabina Barakovic et al. [69] and the results of their simulation, the Reactive Protocols (AODV & DSR) delivers over 95% of packets in all cases the considered. Hence has a much higher throughput than Proactive Protocols. This is because proactive protocols (i.e. DSDV) because of its table driven approach, is not as adaptive to route changes that occur under high mobility as AODV and DSR protocols are. Between AODV and DSR, DSR delivered the highest percentage of its packets hence has a higher throughput for DSR under low mobility and significantly less under high mobility.
Also in all cases they considered in their simulation, regardless of mobility or source number, DSR protocol generates significantly *less routing load* than AODV, OLSR and DSDV protocols. Analyzing average end to end delay, they came to the conclusion that DSR routing protocol outperforms AODV and DSDV protocols. This is attributed to its use of source routing, aggressive caching and no dependence on periodical activities. Overall, according to Sabina Barakovic et al [69] in high mobility cases, DSR protocol performs better than AODV and DSDV protocols regardless of number of sources in the network.

Azzedine Boukerche in [33] ascertained from his results that DSR has a very high throughput, the highest amongst the protocols. In the delay studies, AODV outperforms others delay-wise by exhibiting a very short end-to-end delay of data packets. Furthermore, DSR was shown to have the smallest routing overhead than AODV, OLSR and DSDV.

From the works of Samyak Shah et al in [52], they showed that proactive protocols like DSDV because of its table-driven approach is not as adaptive to the route changes that occur hence are not suited perfectly for MANET which is a highly dynamic network. Both AODV and DSR (reactive protocols) perform better under high mobility simulations than DSDV. The general observation from their simulation is that for application-oriented metrics such as throughput or packet delivery fraction and delay, AODV outperforms DSR in more 'stressful' situations (i.e. smaller number of nodes and lower load and/or mobility) with the performance gap widening with increasing stress(eg. More load, higher mobility). The slightly poorer performances of DSR in those regards were mainly attributed to a lack of any mechanism to expire stale routes or determine the freshness of routes when multiple choices are available. DSR, however, consistently generates less routing load than AODV. The major contribution to AODV's routing over-head is from route requests and periodic transmissions (hello), while route replies constitute a large fraction of DSR's routing overhead.

According to I.Vijaya et al in [59], both reactive protocols (AODV & DSR) performed well in high mobility scenarios than proactive protocols as proactive protocols fail to respond fast enough to changing topologies. In terms of throughput, DSR performs better than AODV when the number nodes is less but its performance declines with increased number of nodes due to more traffic in the network. The performance of AODV is relatively consistent. For average end-to-end delay, the performance of DSR and AODV are almost uniform with AODV having significantly the higher performance in delay as the size of the network increases. They also deduced from their simulation results that DSR consistently generates less routing load than other protocols (i.e AODV and DSDV).

Reactive protocol, DSR with the aggressive use of cache memory from the performance evaluation of the routing protocols in [43] performs better than all the other protocols. P.Chena Reddy et al [43] states from their simulation results, that in throughput, DSR outperforms AODV and DSDV. In delay, AODV has the best (lowest) delay performance with delay in DSR increasing under higher mobility conditions. Here also, DSR is also stated to have the least routing overhead compared to AODV and DSDV.

From [66], V.B. Narsimha concludes that received packets (throughput) for DSR are much higher than that of DSDV and AODV. Higher throughput efficiency for the routing protocols in descending order is – DSR, OLSR, AODV and DSDV. AODV is attributed with the best delay (lowest latency) especially during higher network entropy. Also, DSR is attributed with displaying the least routing overhead.

Charles E. Perkins, Elizabeth M. Royer et al [16] in their comparison of on-demand routing protocols, also stated that DSR outperforms AODV for application oriented metrics such as delay and throughput but mainly in low mobility and less congested situations. AODV however outperforms DSR as the number of nodes in the networks increases and with higher mobility. They agreed that DSR is consistent in having the least routing load in all situations when compared to AODV.

One important aspect of Ad hoc networks that was ignored by many studies is energy efficiency. Energy consumption and efficiency is a major issue for mobile Ad hoc networks as the nodes have energy limitation due to their need for mobility and lack of infrastructure. Cano and Manzoni[14] studied the routing energy consumption of the protocols using the NS-2 simulator. In [14], they quantified the amount of energy used for the routing overhead of AODV, DSR, TORA and DSDV under different scenarios. Their simulation results showed that DSR outperforms AODV and DSDV in conservation or energy efficiency. This can be attributed to its aggressive approach in promiscuous listening and caching coupled with the ability to have little or no activity when not forwarding data (no periodic/hello transmissions). In their research, it should be of note that only the routing overhead energy used by the different protocols was compared while still using the random way point mobility model and constant bit rate traffic generation.

Chandra S.R. Putta et al in [55] evaluated the performance of reactive (i.e. DSR and AODV) and proactive (i.e. OLSR) routing protocols in 802.11 Ad hoc network environment. They noticed that proactive protocols offer better performances for constant bit rate (CBR) sources (e.g. Voice services) given that it guarantees lowest delay albeit in a very low mobility network. However it consumes much more bandwidth performing badly in throughput and routing overhead. The reactive routing protocols are more

adapted for data services (file transfer). There was no clear winner among DSR and AODV in throughput.

3.4 MODEL AD HOC ROUTING PROTOCOL

Taking into cognizance, the evaluation and comparison of reactive (AODV, DSR) Ad hoc routing protocols, it can be seen from the mechanisms and characteristics of the respective protocols coupled with the evaluation experiments and simulations carried out in existing works, that reactive (on-demand) routing protocols due to their on-demand nature are best suited for the dynamism and mobility associated with MANETs.

DSR is purely an on-demand routing protocol unlike AODV which although on-demand, still possess some proactive properties. DSR makes use of source routing which makes it the best suited for the mobility and dynamism that comes with MANETs. Also apart from the characteristics, advantages and disadvantages of each routing protocol which we discussed in detail in the earlier sections, comparative experiments and simulations conducted strongly favor DSR as exhibiting the better performance on major MANET performance metrics (better throughput, lower delay and lower routing overhead).

Therefore, DSR is used as our model MANET routing protocol in this work.

CHAPTER FOUR
SECURITY

4.1 INTRODUCTION

Security in a MANET is an essential component for basic network functions like packet forwarding and routing. The network operation can be easily jeopardized if countermeasures are not embedded into the basic network functions at the early stages of their design. Unlike conventional networks, the Ad hoc networks carry out basic support functions like – packet forwarding, routing and network management of all of the available nodes without having support of dedicated nodes and also the data has to travel through an open medium [40].

Hence, security is an indispensable need for wireless network communications. In contrast to wire-line networks, wireless networks pose a number of unique challenges to security solutions due to their, unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints etc.

In Ad hoc network, security is not a single layer issue but a multilayered one. A scrutiny reveals that security concerns in MANETs involve two separate problems: secure routing discovery and secure data transmission over the MANETs [50].

4.2 SECURITY CHALLENGES IN AD HOC NETWORKS

One of the main challenges of MANETs comes from their open peer-to-peer architecture. However, security challenges faced in Ad hoc Networks are possible because of [48]:

- ***Vulnerability of Channels***: Ad hoc network is like any wireless network. Because of the medium which is of a wireless or radio spectrum, it is devoid of physical

security. Hence basically, Ad hoc networks from the on-set, is at a disadvantage of having negligible to zero physical layer protection ability. Therefore, the wireless channel is accessible to both users and attackers. Use of wireless links, renders an Ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. An adversary can easily eavesdrop, delete messages and inject fake messages thus violating availability, integrity, authentication, and non-repudiation security goals of a network, without the difficulty of having physical access to network components.

- ***Vulnerability of Nodes**:* Ad hoc network nodes usually are mobile and unlike traditional wire-line networks are not contained in physically protected places. With relatively poor physical protection, nodes have a high probability of being captured or compromised by an attacker. Therefore, this brings about that we should not only consider malicious attacks from outside the network, but highly take into account the likelihood of attacks being launched from within the network by compromised nodes. Therefore, to achieve high survivability and availability, Ad hoc networks should have a distributed architecture with no central entities. Introducing any central entity into a security solution could lead to significant vulnerability because if that centralized node is compromised, the entire network is undermined.

- ***Absence of Infrastructure***: Ad hoc networks are devoid of pre-existing infrastructure and are supposed to operate independently of any fixed infrastructure. This makes the traditional and classical security solutions not quite applicable as they have to be adapted to the dynamism and infrastructure-less of the network. Also, this lack of support infrastructure may prevent the application of standard techniques for key agreement.

- ***Dynamically Changing Topology**:* As a result of the mobility expected of Ad hoc networks, the constant changes in topology require sophisticated routing protocols of which securing the already complex protocols is an additional challenge. A highly noteworthy difficulty is that incorrect routing information can be generated

by compromised nodes or as a result of some topology changes and it is hard distinguishing between the two cases. Also because of the dynamism (i.e nodes frequently join and leave the network), trust relationships among nodes also change frequently and maybe too frequently to be valid and of use. Hence, it is desirable for security mechanisms here, to adapt on the fly to these changes. Finally, due to dynamically changing topology, the availability is not always guaranteed.

- ***Scalability****:* An Ad hoc network can consist of hundreds or even thousands of mobile nodes. Although scalability is not directly related to security but, it is a very important issue that has a great impact on security services. Security mechanisms should be scalable to handle such a large network. Also as resource constraints on nodes in Ad hoc networks limit the cryptographic measures that are used for secure messages. Otherwise, the newly added node in the network can be compromised by the attacker and used for gaining unauthorized access of the whole system [56].

Table 4.1 Grouping Security Issues for MANETs into Layers of the OSI Model

Layer	**Security Issues**
Application Layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport Layer	Authenticating and securing end-to-end communications through data encryption
Network Layer	Protecting the Ad hoc routing and forwarding protocols
Link Layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

4.3 SECURITY MEASURES OR SERVICES REQUIRED IN MANET

There are no ultimate solutions and remedy to all active and passive attacks as a unified or end-to-end security solution. Most security threats and breaches are dealt case-by-case. Security services are needed to be employed in securing a MANET. Security services include the functionality required to provide a secure networking environment. The security schemas that can solve the open challenges present in MANETs need to do so within the stringent resource limitations in terms of computation capability, memory, communication capacity, and energy supply. To secure an Ad hoc network, we consider the following services: Availability, Confidentiality, Integrity, Authentication, and Non-repudiation [13].

Availability:

This ensures the survivability of network services and making the resources of the network available to other legitimate nodes regardless of the attacks that target the network, especially denial of services or the existence of selfish nodes. A DOS attack could be launched at any layer of an Ad hoc network. Frequency/Channel jamming can be employed at physical and data link layers (Media Access Control sub-layer), to interfere with communication on the physical channels which in the case of Ad hoc network is radio wave spectrum. On the network layer, a malicious attacker could disrupt or hijack the routing protocol operations and disconnect the network. For the higher layers, such target can be the key management service, which is an essential service for any security framework. Because communication in MANETs is based on cooperation and coordination, the ability to reach all other nodes in a network is imperative.

Table 4.2 Threats to Availability

Threats to Availability	Black Hole Attack	
	Malware	
	Broadcast Tampering	
	Spamming	
	Greedy Drivers	
	Denial of Service	Consuming the Node Resources
		Jamming the Channel
		DDoS

Confidentiality:

Ensures that data/information transmitted over the network is kept secret and not disclosed to unauthorized entities. Leakage of information in the network can be disastrous, be it control information or data information. Routing information must also remain confidential because the control information can be used maliciously in identifying, locating and controlling of target nodes. Certain information like passwords or keys must have a defense mechanism to protect them and encryption is a more popular technique to achieve confidentiality. Confidentiality can be achieved by using different encryption techniques such that only legitimate users or nodes can analyze and understand the transmission.

Integrity:

It refers to prevention of any compromises that may happen to packets when they are transmitted between nodes. The function of integrity control is to assure that the data is received verbatim as sent, by the authorized party. This is a guarantee that the message transmitted was not tampered or corrupted hence contains no modification, insertion or deletion. Integrity offers little or no tolerance to any passive or active attacks that might target the packets. For instance, a packet cannot be dropped, altered or replaced without detection. As with confidentiality, integrity can apply to a stream of messages, a single

message or selected fields within a message. The destruction of data is also covered under integrity service. Therefore, it can be said to address both message stream modification and denial of service (DOS).

Authentication:

Authentication is the ability to know the actual identity of other nodes. This service verifies a user's identity and assures the recipient that the message is from the source that it claims to be from. It is also used to ensure a node's identity when communicating or about to communicate with a peer node. Without authentication, an adversary could masquerade as a node, thus gaining unauthorized access to resources and information. Impersonating to gain access to secured information is made futile by authentication. A reliable authentication mechanism detects any impersonation and identifies all non-malicious nodes and messages, which is a fundamental security requirement. Authentication can be provided using encryption along with cryptographic hash functions, digital signatures and certificates [1]. Authentication can also be used as a form of access control of either a resource, host system or an application.

Table 4.3 Threats to Authentication

Threats to Authentication	Masquerading
	Replay Attack
	GPS Spoofing
	Tunneling
	Sybil Attack
	Message Tampering
	ID Disclosure

Non-repudiation:

This ensures that the origin of a message sent or received cannot be denied. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender while the sender can also prove that the message was received by the alleged receiver. This is especially useful for detection and isolation of compromised nodes.

4.4 ATTACKS IN MANETS

Mobile Ad hoc Networks depend heavily on the active cooperation of all nodes in order to establish and operate the network. The basic assumption in such a setup is that all nodes are well behaving and trustworthy. However, due to dynamic, distributed infrastructure-less nature of MANETs, and lack of centralized authority, the Ad hoc nodes are vulnerable to being compromised and open to various kinds of attacks. There is a classification of attacker behavior into three major groups: [62] (i) Insider/Internal versus Outsider/External; (ii) Malicious versus Rational; (iii) Active versus Passive (based on methodology).

There are two levels of attacks to MANETs. Attacks on the basic functionality of the MANET, such as routing and attacks on the information on transit.

4.4.1 Vulnerability of Existing Protocols

The main network layer operations in MANETs are Ad hoc routing and data packet forwarding, which interact with each other and fulfill the functionality of delivering packets from the source to the destination. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination. All of the routing protocols in MANETs depend on active cooperation of nodes to provide routing between the nodes and to establish and operate the network. As they are the backbone of any network, they are most targeted by attacker and very vulnerable due to the challenges faced by Ad hoc networks. Malicious and selfish nodes are the ones that fabricate attacks

against physical, link, network, and application layer functionality [31]. Current routing protocols are exposed to two types of attacks: Passive and Active.

In **passive attacks**, the attacker does not send any message, but just listens to the channel. Passive attacks are non-disruptive but they are information seeking which is also sensitive and critical. A passive attacker listens to the channel and packets containing secret information (e.g. IP address, data, location of nodes etc.) may be stolen, which violates confidentiality. In a wireless environment, it is very difficult to detect passive attacks as it does not produce any new traffic in the network and hardly alters any [58]. Passive attacks are done by selfish nodes that aim to preserve energy for themselves by not being involved in passing messages hence might cause partitioning of the networks and decreased performance level of the networks.

Active attacks on the other hand involve actions performed by malicious nodes that are destructive and have intrusive capabilities. The action of an active attacker includes: injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes which violates availability, integrity, authentication, and non-repudiation paradigm. However, contrary to passive attacks, active attacks can be detected and eventually avoided by the legitimate nodes that participate in an Ad hoc network [57].

4.4.2 Active Attacks:

- *Denial of Service:* It aims at the complete disruption of the routing function and therefore, the entire operation of the Ad hoc network. The attacker floods the nodes by constant advertisements or broadcasts, preventing the normal operation of nodes to participate in the scheme. The flooded node will look unreachable from the legitimate others. Specific instances of denial of service attacks can include the *routing table overflow* and the *sleep deprivation attack.*

- *Black Hole Attack:* In this attack, the adversary or malicious node injects false route replies (RREP) in response to the route requests it receives, advertising itself as having the shortest path to the destination node whose packets it wants to intercept. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets. Additionally, an attacker can advertise a zero metric for all destinations causing the entire node's neighbors to route packets through the attacker because of its best metric thinking it has the best or closest route. Then the attacker will just drop the packets and not forward them on.

  Also, Black Hole attack is carried out due to a node exhibiting selfishness. A selfish node wants to preserve its own resources while using the services of others and consuming their resources. This can endanger the network by the node in a bid to be selfish, will not participate in the operation of the MANET by not executing packet forwarding instead just dropping packets routed through it, hence a black hole attack.

- *Gray Hole:* This is where a node in an established MANET routing topology, selectively drops packets with certain probability causing network distraction. It can drop some specific ones while forwarding all the packets for other nodes. It may also behave maliciously for some time period by dropping packets but switch back to normal behavior later. A gray hole may also exhibit a behavior which is a combination of the above two.

- *Byzantine Attack:* This is a network layer attack which occurs as a lack of authentication and packets integrity. These attacks are perpetrated by a group of intermediate nodes that compromise their intentions within a network, deteriorating routing services through packet dropping, forwarding to invalid paths, or just creating routing loops.

- *Partition:* Partition divides the network into two sets, by breaking one group of nodes from the other. In this network attack, the malicious node or group of nodes, aims to partition the network to prevent one group of nodes from contacting the other group, through injecting unreliable routing packets and making the route busy until the partition is completed.

- *Node Isolation Attack:* This is an attack against the OLSR protocol [42]. The purpose of this attack is to isolate a given node from communicating with other nodes in the network. This is achievable by attackers preventing link information of a specific node or a group of nodes from being spread to the whole network. Therefore, other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes.

- *Wormhole Attack:* This involves cooperation between two or more attacking nodes. It is also referred to as *Tunneling Attack.* A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short circuit the normal flow of messages in the network and controlled by the two or more colluding attackers. Simply stated, the colluding malicious nodes create a tunnel or a shortcut between them to be able to forward a packet to each other. A wormhole shows a valid route to the destination but it always tunnels the packet to its malicious partner's node. These tunnels are extremely difficult to detect.

- *Session Hijacking:* This is a transport layer attack. It focuses on TCP and takes advantage of the frequency of the TCP (3 way) handshake. In MANETs, TCP authentication only happens at the start of a session, so an attacker takes advantage of the absence during the session and hijacks it to get an unauthorized access to confidential information

- *Malicious Code:* It is an attack on the application layer. It includes injecting of viruses, spywares and worms to achieve goals of harming other nodes or getting access to confidential information. This slows the network and finally damages it.

- *Jellyfish Attack:* The malicious node intrudes into the forwarding group in the network and then unreasonably delays data packets for some amount of time before forwarding them. It results in significantly high end-to-end delay and delay jitter, therefore it degrades the performance of real-time applications.

- *Spoofing:* This is where a malicious node takes the identity of another. It alters the vision of the network topology.

- *Sybil Attack:* Attacker pretends to have manifold identities or nodes. A node can act as if it were a multiple number of nodes either by impersonation or simply claiming false identities. Hence, sending messages containing different fabricated source identities.

- *Replay Attack:* An attacker that performs a replay attack injects into the network, routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to determine poorly designed security solutions.

- *Blackmail / Black list Attack:* This attack is relevant and propagated against routing protocols that use mechanisms for the identification of malicious nodes and use a list (black list) to keep record of suspected malicious nodes. Nodes usually keep information of perceived malicious nodes in a blacklist. Here, an attacker may fabricate messages reporting a particular node as malicious to others in the network in a bid for that particular node to be added to other nodes blacklists hence isolating a legitimate node from the network [13]. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated.

Table 4.4 Summary of Active and Passive Attacks on a MANET

Type	Name	Description	Target
Active Attacks	Denial of Service	Network bandwidth or resources are consumed by data floods triggered by malicious nodes [61]	Data link layer
	Spoofing	Malicious nodes disguised as another, which give them advantages they don't deserve	N/A
	Black hole	Malicious nodes declare they have a right path for packets. The packet in the route gets consumed and intercepted	Network layer
	Byzantine	Routing loops might be made, packets forwarded to bad routes or dropping packets by intermediate nodes	Network layer
	Rushing	A wormhole is formed between two attackers then they rush route request packets to the nodes that receive the packet	Network layer
	Partition	When fake routes are created by a malicious nodes to prevent nodes from communicating	Network layer
	Wormhole	Setting a shortcut by two or more malicious nodes that keep forwarding packets	Network layer
	Sybil attack	When a malicious node represents one of multiple identities	N/A
	Session Hijacking	Session hijacking happens because authentication happens only at the start of business	Transport layer
	Malicious Code	Operating system or user application gets attacked by viruses, Trojan horse, worms, spywares which damages network	Application layer

Passive Attacks	Eavesdropping	Attacker aims to get confidential information during the communications	Physical layer
	Interference and jamming	Attacker sends malicious data along with the same signals to be communicated	Physical layer
	Traffic Analysis	Protocol engaging and provoked communication between nodes	Data link layer

4.4.3 Passive Attacks:

- *Eavesdropping:* This occurs on the physical layer. Nodes eavesdrop to obtain confidential information about other nodes (eg. Passwords, public, and private keys), without authorization. This attack is hard to detect in the MANET environment.

- *Interference and Jamming:* It attacks the physical layer by sending signals with same frequency as those between two specific nodes to create many errors and random noise.

- *Traffic Analysis:* This is an attack on the data link layer where the attacker obtains information about the network such as location of nodes and their roles, the topology of the network and the message routes. Through this attack, the privacy requirements of an Ad hoc network are compromised.

4.5 ATTACKS TARGETING DSR ROUTING PROTOCOL

With our focus on vulnerabilities and exposures that result from the specification of the Ad hoc routing protocols and not from problems with the IEEE 802.11 [21,22,85]. The current standard routing protocols for mobile Ad hoc networks allow for many different types of attacks. Though, the same attacks exist in wire-line networks [5], but they are more easily defended against by the infrastructure present in a wire-line network.

Also, as trivial denial of service attacks based on interception and non-cooperation are possible in all Ad hoc routing protocols, they are not achieved through destabilization or undermining of the routing protocol. However, all attacks targeting Ad hoc routing protocols can be broadly classified into *Modification, Impersonation,* and *Fabrication.*

4.5.1 Attacks Using Modification

Malicious nodes can cause redirection of network traffic and DoS attacks by altering control message fields or by forwarding routing messages with falsified values. As an example, in the network in the figure below, a malicious node M could keep traffic from reaching X by advertising a shorter route to X than the route to X that C advertises.

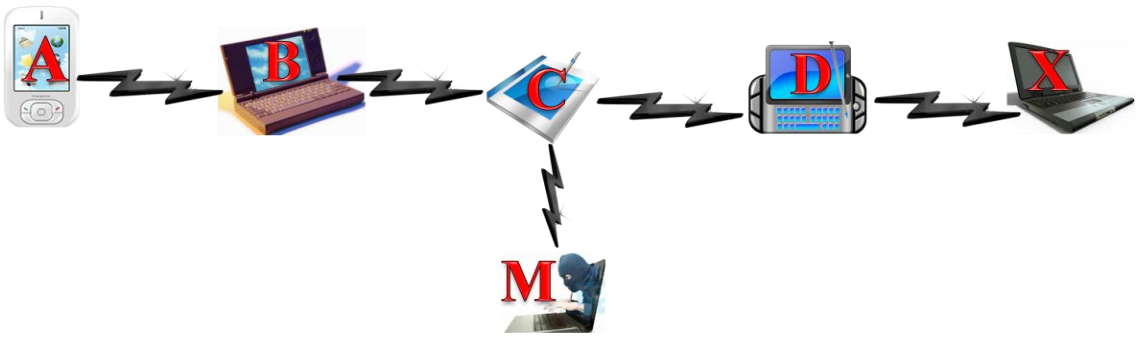


Figure 4.1 A Simple Ad hoc Network

- ***Redirection with modified hop counts*:** This attack is possible by modification of the hop count field in route discovery messages. DSR uses hop count field as a metric to determine the shortest path. In DSR, malicious nodes can tamper and modify the hop count field of the RREQ during route discovery. As DSR uses source routing, keeping track of nodes traversed, a malicious node on passing through can modify the RREQ header, inserting or removing nodes to accomplish a diversion and routing through another route.

- ***Denial of Service with modified source routes:*** As DSR utilizes source routes which explicitly states routes traversed or to be traversed in the packets headers, a simple denial of service attack can be launched in DSR by altering the source routes in packet headers as these routes lack integrity check mechanisms. From the figure 4.2, assuming the path from S to X is the shortest path, and that M is a malicious node attempting a denial of service attack. When S wants to communicate with X and S has an unexpired route to X in its route cache, S will transmit a data packet toward X, with the source route S→A→B→M→C→D→X contained in the packet's header. When *M* the malicious node receives the packet, it can alter the source route in the packet's header inserting or even deleting for instance D from the source route. This brings about that on C receiving the altered packet and attempting to forward the packet to X, it will not find a next hop node on the source route contained in the packet header and subsequently will have to drop the packet making the transmission unsuccessful.

Figure 4.2 Another Example of an Ad hoc Network

Although DSR provides a route maintenance mechanism which is that a node forwarding a packet is responsible to confirm that the packet has been received by the next hop along the route path and if no confirmation of receipt is received, there should be a retransmission of the packet a specified maximum number of times. If still, there is no confirmation of receipt from the next hop, this node should return an error message RERR to the source node. Therefore, in the case of fig 4.2, C would send a route error message to S, but since M would be the first

hop the RERR message takes on its way back to the source node S, M can continue its denial of service attack by dropping this route error message. This assumes that C only knows of the erroneous route to X, of which the DoS attack can be totally successful. This assumption is as a result that DSR has a route maintenance mechanism called *route salvaging* for the recovery from broken links along a path by the node immediately upstream checking its route cache for a different route to the destination. Also, modifications to source routes in DSR can introduce loops in the specified path.

- ***Tunneling:*** As already discussed, a tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes while giving a false representation of the routing path. Figure 4.3 illustrates such a tunneling attack where M_1 and M_2 are malicious nodes carrying out a tunneling attack by collaborating to misrepresent available path lengths by tunneling route request packets (RREQ in DSR source routing). The darker solid lines denote actual paths between nodes, the thin colored lines denote the tunnel and the dotted lines denote the path falsely claimed by M_1 and M_2 is between them.

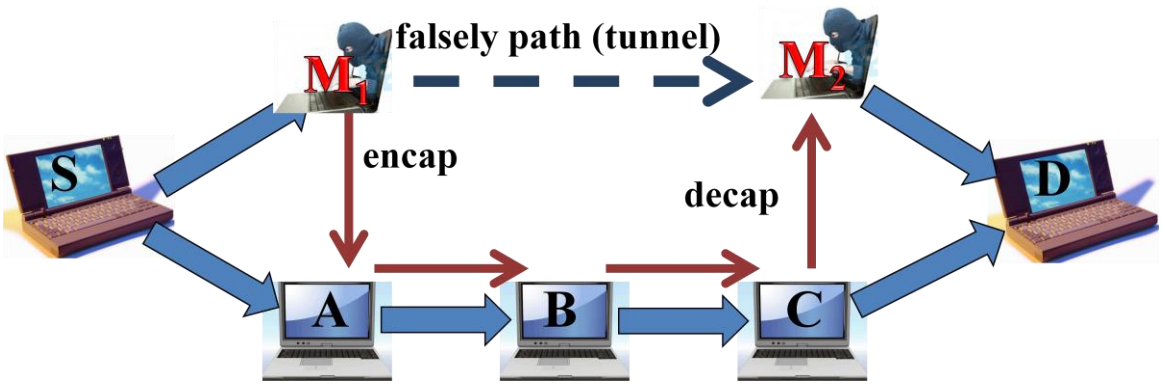


Figure 4.3 Path Lengths Spoofed By Tunneling

Here, a node S wishing to send or communicate with a destination node D, initiates a route discovery. The source node S, sends out RREQs to its immediate neighbors. When M_1 receives a RREQ from S, M_1 encapsulates the RREQ and tunnels it to M_2 through an existing data route, in this case $\{M_1 \rightarrow A \rightarrow B \rightarrow C \rightarrow M_2\}$. When M_2 receives the encapsulated RREQ, it forwards the RREQ onto D as if it had only travelled through this path $\{S \rightarrow M_1 \rightarrow M_2 \rightarrow D\}$. Neither M_1 nor M_2 will update the packet header to reflect that the RREQ also traveled through the path $\{A \rightarrow B \rightarrow C\}$. After route discovery, it appears to the destination that there are two routes from the source node S to the destination D, of unequal hop length – $\{S \rightarrow A \rightarrow B \rightarrow C \rightarrow D\}$ and $\{S \rightarrow M_1 \rightarrow M_2 \rightarrow D\}$. Hence S would erroneously consider the path to D via M_1 a better choice (in terms of hop counts) than the path to D through A.

4.5.2 Attacks Using Impersonation or Spoofing

This attack occurs when a node misrepresents its identity in the network. This can be by altering its MAC or IP address in egress packets and can be easily combined with modification attacks.

- ***Routing Loops by Spoofing:*** Using figure 4.4, assuming paths exists between the five nodes illustrated towards a remote destination, X, and also amongst themselves as shown. In this illustration, A can hear B and D; B can hear A and C; D can hear A and C; and C can hear B, D, and E. While, M can hear A, B, C, and D; with E hearing C and the next hop on the route toward X.

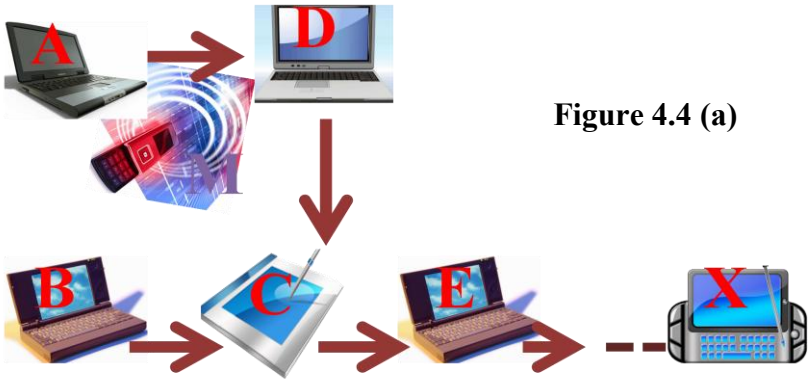


Figure 4.4 (a)

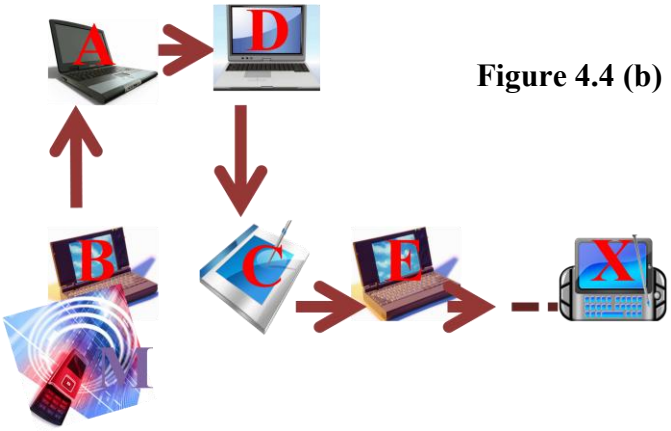


Figure 4.4 (b)

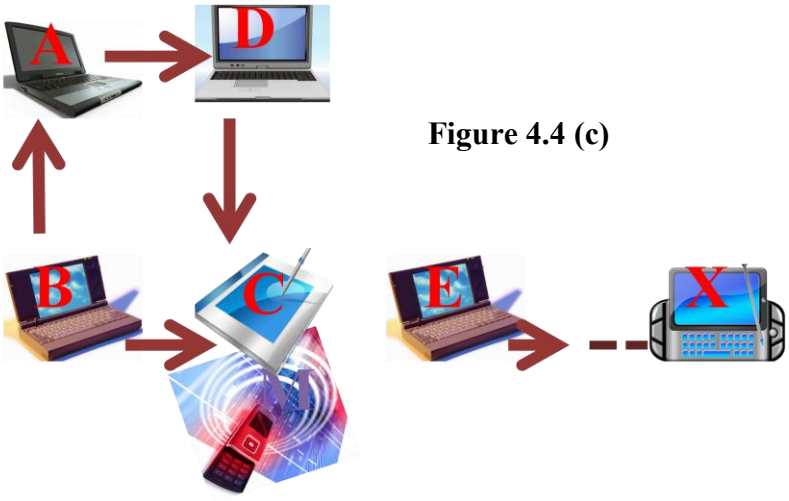


Figure 4.4 (c)

Figure 4.4 A sequence of events that form loops by spoofing of packets

In DSR, as a result of the *promiscuous listening* optimization, a malicious attacker, M, can learn this topology by gleaning information from the

RREQ/RREP exchanges during route discovery. To deploy a looping attack, M moves out of range of node A while moving closer to node B, then changes its MAC address to match A's MAC. It will then send an RREP to node B that contains a hop count to X that is less than the one sent by C (i.e a metric/hop count of zero). Finding a route with a lower hop count, B therefore will change its route to the destination, X, to go through A as illustrated in fig 4.4(b). Having achieved that, M will then change its MAC address to match B's while out of range of B and closer to C. It will then send to C an RREP with a hop count of X lower than what was advertised by E. C then routes to X through B, as shown in figure 4.4(c). At this point a loop is formed and X is unreachable from the four nodes.

- ***Partition Attack through Spoofing:*** This is carried out exactly as discussed in the routing loops by spoofing section. The network becomes inadvertently divided into partitions as illustrated in figure 4.4(c).

4.5.3 Attacks Using Fabrication

Attacks can be carried out in MANETs by generation and propagation of false routing messages. Such attacks can be difficult to verify and isolate from non-malicious routing messages. This is especially tenable in fabricated route error messages RERR that claim a break in communication with a neighbor.

- ***Falsifying Route Errors in DSR:*** DSR implements path maintenance to recover broken paths when the nodes of MANETs move. If it is the source node that moved and the route is still needed, a route discovery is re-initiated with the generation and transmission of route request RREQ messages. However, if it is the destination node or an intermediate node along an active path that moves, the node upstream of the link break will broadcast a *route error* message RERR to all active upstream neighbors while invalidating the route for that destination in its route cache. With no security mechanism in place, this creates vulnerability in the routing operation of the MANET such that false route error messages can be sent.

Using figure 4.5, where a node S has a route to node X via nodes A, B, C, and D. A malicious node M can launch a denial of service attack against X by sending route error messages to B, indicating a broken link between node C and node X, all the while impersonating node C. Node B will then receive the message thinking it came from C. Node B will then delete its routing cache entry for X and forwards the route error message on to node A, who then deletes its routing cache entry. Hence M can successful prevent communications (DoS) between S and X using falsified RERR packets in conjunction with spoofing.

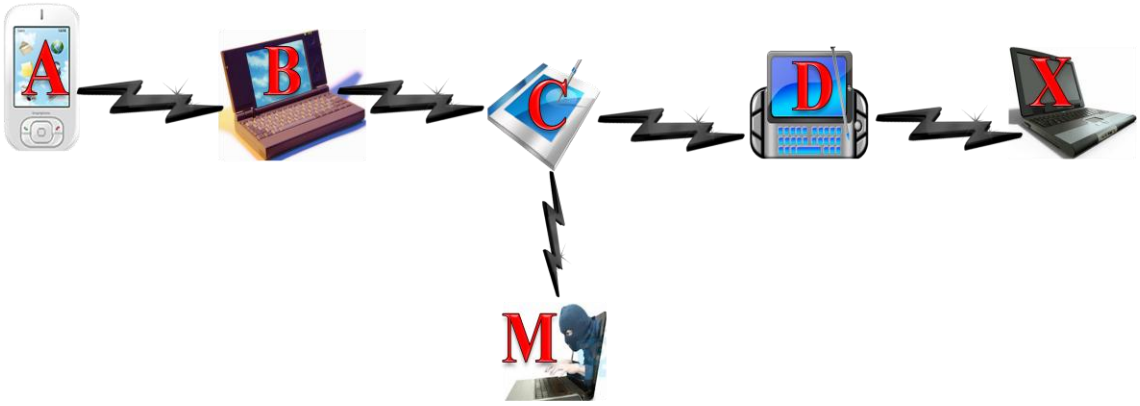


Figure 4.5 Ad hoc Network – Fabrication

- ***DSR Route Cache Poisoning:*** Route cache poisoning which is basically a corruption of the routing state is a passive attack against routing integrity. This occurs when entries or information stored in route caches at the nodes are either, deleted, altered or injected with false information. Although this is obtainable in wire-line networks, but it can often be easily defended against by security measures at the routers due to the existing infrastructure. In DSR, in addition to learning routes from headers of packets that a node is processing along a path, routes in DSR may also be learned through *promiscuous listening.* For example in figure 4.8, of which a path exists from node S to node X via nodes A,B,C, and D. If a packet traveling along the source route from S to X is overheard by another

node, that node may then add the route {S,A,B,C,D,X} to its route cache. This promiscuous method of learning routes could easily be exploited by an attacker to poison route caches. For an instance, if a malicious node M wanted to poison routes to node X, M can broadcast spoofed packets with source routes to X via itself. Neighboring nodes using promiscuous listening, overhears the packet transmission, may add the route to their route cache. As can be observed, this is a vulnerability that can be utilized to corrupt and destabilize the routing operations and state of a MANET.

CHAPTER FIVE
REVIEW OF EXISTING SECURE MOBILE AD HOC NETWORK PROTOCOLS

There exist several proposals that attempt to architect a secure routing protocol for Ad hoc networks to offer protection against security attacks on MANETs. These proposed solutions are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing protocols (eg. DSR and AODV) [26].

A common design principle in all the examined proposals have a trade-off balance between performance and security. Since routing is an essential function of Ad hoc networks, the integrated security procedures should not hinder its operation. Another important part of the analysis is the examination of the assumptions and the requirements on which each solution depends. As can be seen, the design of these solutions focuses on providing countermeasures against specific attacks, or set of attacks.

The existing work done in developing the solutions in the form of secure MANET protocols can be classified into five categories:

- Solutions based on asymmetric cryptography;
- Solutions based on symmetric cryptography;
- Hybrid solutions;
- Reputation-based solutions; and
- A category of add-on mechanisms that provide security for existing Ad hoc routing.

However, this classification is not rigid since many solutions can be classified into more than one category.

5.1 ASYMMETRIC CRYPTOGRAPHY SOLUTIONS

Protocols that use asymmetric cryptography to secure routing in mobile Ad hoc networks require the existence of a certification authority or a universally trusted third party (TTP). The TTP will have a duty of issuing certificates that bind a node's public key with a node's persistent identifier. Also, the TTP can be online in the network or offline. Both approaches have different requirements and advantages. In the use of an online TTP, revocation of the issued certificates is accomplished by broadcasting certificate revocation lists (CRLs) in the network. Asymmetric Cryptography solution category is made up of only one protocol, ARAN. However, many other protocols presented in other categories use asymmetric cryptography in a way or the other, while having similar requirements and limitations.

5.1.1 Authenticated Routing for Ad hoc Networks (ARAN):

The Authenticated Routing for Ad hoc Networks (ARAN) protocol was proposed in [19] as a stand-alone solution for security routing in MANETs in an on-demand routing fashion based on AODV. ARAN achieves security goals of authentication and non-repudiation through the utilization of cryptographic certificates. ARAN can be said to consist of three operational stages.

The first stage is the *certification* process that requires the existence of a trusted certification authority (CA). Each node, before joining the Ad hoc network, must contact the certification authority and request a certificate for its address and public key with an assumption of the protocol believing each node knows a priori the public key of the certification authority.

The second operational stage of the protocol is the *route discovery* process which provides end-to-end authentication. This ensures that the intended destination was reached. The route discovery of the ARAN protocol begins with a node broadcasting a route discovery packet (RDP) to its neighbors. The RDP includes the certificate of the initiating node, a nonce, a timestamp, and the address of the destination node. Also the initiating node signs its digital signature on the RDP. On its way forward, each

intermediate node that receives it, validates the signature with the certificate, updates its routing table with the neighbor from whom it received the RDP, signs it, and forwards it to its neighbors after removing the certificate and the signature of the preceding node (but not that of the initiator's signature and certificate). The signature prevents malicious nodes from injecting arbitrary route discovery packets that alter routes or form loops [37].

The destination node eventually receives the RDP and replies with a reply packet (REP). The REP contains the address of the source node, the destination's certificate, a nonce and the associated timestamp. The destination node digitally signs the REP with its private key prior to transmitting it. The REP is forwarded back to the initiating node by a process similar to the process described for the route discovery (RDP), with the exception that the REP is unicasted not broadcasted along the reverse path. The source node on receipt is able to verify that the destination node actually sent the REP by checking the nonce and the signature.

ARAN ensures end-to-end authentication, replay attack protection, and non-repudiation but at the cost of a slightly higher latency.

5.2 SYMMETRIC CRYPTOGRAPHIC SOLUTIONS

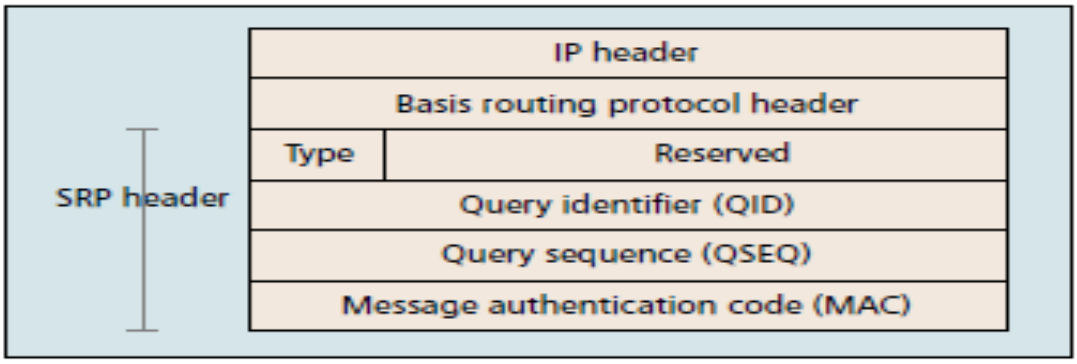
This category is for solutions that rely solely on symmetric cryptography in securing the routing function in MANETs. The most commonly utilized mechanisms are *hash functions* and *hash chains*. A one-way hash function is a function that takes an input of arbitrary length and returns an output of fixed length [38]. Hash functions have the property of being computationally expensive to reverse, i.e. if $h = f(m)$, it will be difficult to compute m such as $f(m) = h$. There are several well-known hash functions that possess these properties including SHA-1 and MD5 [19, 30]. A hash chain can be generated by applying repeatedly a given hash function to a random number which can be called the *root* of the chain. Simply state, in order to generate a hash chain of length n, a hash function is applied n times to a random value p, and the final hash q that is obtained is referred to as the *anchor* of the chain [22]. In order to use a hash chain for authentication purposes, an initial authenticated element of the chain is assumed, usually

the anchor. This is so, because, it is possible to verify the authenticity of the elements that come later in the sequence. Hash functions are especially lightweight when compared to other symmetric and asymmetric cryptographic operations, hence why they have been extensively used in the context of securing Ad hoc routing, and specifically in hop count authentication and integrity.

5.2.1 Secure Routing Protocol (SRP):

The Secure Routing Protocol (SRP) is a set of security extensions that can be applied to any Ad hoc routing protocol that utilizes broadcasting as its route querying method [32]. DSR is particularly favored as the appropriate protocol for incorporating the proposed security extensions by the authors of SRP. The operation of SRP requires the existence of a security association (SA) between the source node initiating a route query and the destination node. A shared secret key between the two (source node and destination) is used by SRP of which the security association (SA) can be utilized in establishing it.
The SRP protocol appends an SRP header to the packet of the base routing protocol. The source node sends a route request with a *query sequence* (QSEQ) number which is used by the destination to identify outdated requests. Also sent is a *random query identifier* (QID) that is used to identify the specific request, and the output of a keyed hash function.

Figure 5.1 SRP Packet Header



The changeable fields of the request, like the accumulated addresses of intermediate nodes, are transmitted in the clear. The query is dropped if it has the same QID with an entry in an intermediate node's routing table. The intermediate nodes after receiving the

query, updates their routing tables then broadcast the query to their neighbors. On receipt, the destination node confirms that the query is not outdated or replayed through the QSEQ, and verifies its integrity and authenticity through the calculation of the keyed hash. In response, the destination node will generate a number of replies with different routes corresponding at most to the number of its immediate neighbors. This is the mechanism employed in SRP as an additional protection against route modification by malicious nodes.

A route reply consists of the path from the source to the destination, the QSEQ and QID numbers. The source node checks the QSEQ and QID numbers of the reply in order to verify that they correspond to the active query, also comparing the IP source route with the reverse of the route in the payload of the reply, and if they match it calculates the MAC.

Route maintenance is achieved in SRP by route error messages that are source-routed. However, this approach is not a guarantee against a malicious node fabricating the route error packets.

5.2.2 Secure Efficient Ad hoc Distance Vector Routing:

This is a secure Ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector (DSDV) algorithm [13]. The SEAD routing protocol employs the use of hash chains to authenticate hop counts and sequence numbers. Creating a hash chain is by applying repeatedly a one-way hash function to a random value. The elements of such a chain are used to secure the updates of the routing protocol. SEAD requires the existence of an authentication and key distribution scheme in order to authenticate one element of a hash chain between two nodes. With this authenticated element, a node is able to verify later elements in the chain [37].

When a node transmits a routing update, it includes one value from the hash chain for each entry in the update message. Moreover, it includes the address of the destination node, the metric and the sequence number of the destination (from its routing table), and a

hash value equal to the hash of the hash value received when it learned the route to the destination. This hash value can be authenticated by the nodes that receive this routing update since they have an already authenticated element of the same hash chain. This mechanism allows other nodes only to increase the metric in a routing update but not to decrease. To avoid denial of service attacks, a receiving node can specify the exact number of hashes it is willing to perform for each authentication.

A node on receiving a routing update verifies the authentication of each entry of the message. The hash value of each entry is hashed the correct number of times and it is compared to the previously authenticated value. From the outcome of the comparison, the routing update is either accepted as authenticated or discarded.

The SEAD routing protocol proposes two different methods in order to authenticate the source of each routing update. The first method requires *clock synchronization* between the nodes that participate in the Ad hoc network, and employs broadcast authentication mechanisms such as TESLA [37]. The second method requires the existence of a shared secret between each pair of nodes. This secret can be utilized in order to use a message authentication code (MAC) between the nodes that must authenticate a routing update message.

In SEAD, elements of the hash chain are used in succession to authenticate the entries in the transmitted routing messages, given that an initial authenticated element exists. The hash chains have a finite size and must be generated again when all their elements have been used.

5.2.3 Ariadne:

It is a secure on-demand Ad hoc routing protocol. Security in Ariadne[68] follows an end-to-end approach, while the SEAD protocol employs hop-by-hop security mechanisms [37]. Ariadne is based on DSR and developed by the authors of the SEAD. It assumes the existence of a shared secret key between the nodes and uses a message authentication code (MAC) in order to authenticate point-to-point messages between these nodes [12].

Also, Ariadne employs the TESLA broadcast authentication protocol to authenticate broadcast messages such as route requests. Therefore, time synchronization is an absolute requirement of Ad hoc networks that use Ariadne.

In a route request, a node includes its own address, the address of the destination node, a number (ID) that identifies the current route discovery, a TESLA *time interval* that denotes the expected arrival time of the request to the destination, a hash chain consisting of its address, the destination address, the ID and the time interval, as well as two empty lists – a node list and a MAC list. A neighboring node checks the validity of the TESLA time interval when it receives the route request. A packet with an invalid time interval is discarded. A valid time interval is one that the time is not too far in the future and its corresponding key must not have been disclosed yet. For a valid time interval, the current node inserts its address in the node list, replaces the hash chain with a new one consisting of its address including the old one while appending a MAC of the entire packet to the MAC list [24]. It then re-broadcasts the route request to its own neighbors. Note that the MAC is calculated using the TESLA key that corresponds to the time interval of the request.

The destination node checks the validity of the route request on receipt of it. The destination generates and broadcasts a route reply packet for every valid route request it receives. A valid route request is one that its keys from the specified time interval have not been disclosed yet, and the included hash chain can be verified. A route reply contains the same fields with the corresponding route request, and additionally it contains a *target* MAC field and an empty *key list.* The reply is forward back to the source node by following the reverse of the route included in the node list, as specified by the DSR protocol. An intermediate node that receives the route reply waits until the specified time interval allows it to disclose its key, which it appends to the key list and forwards the message to the next node. This waiting technique of Ariadne, injects a lot of latency into the process and creates room for the possibility of delay attacks. However, upon receiving the route reply, the source node verifies the validity of every key in the key list, the target MAC and of every MAC in the MAC list. This also increases the cost of Ariadne because of the complexity of this operation.

The Ariadne protocol also specifies a mechanism for securing route maintenance. This is achieved by a node generating a route error message to report broken links while including TESLA authentication details in the message. Therefore, every node that forwards the route error toward the destination of the message is able to authenticate it [27].

5.3 HYBRID SOLUTIONS

The secure routing protocols that fall into this category utilize both symmetric and asymmetric cryptographic operations. The most common approach is the use of digital signatures to provide integrity and authentication and also MAC, hashing and encryption to protect the metric.

5.3.1 Secure Ad hoc On-demand Distance Vector Routing (SAODV):

Secure Ad hoc On-demand Distance Vector (SAODV) is a proposal for security extensions to the AODV protocol [7]. It utilizes digital signatures and hash chains to secure AODV packets. Cryptographic signatures are used for authenticating the non-changeable fields of the messages, while a new one-way hash chain is created for every route discovery process to secure the hop-count field in an AODV message. SAODV requires the existence of a key management mechanism that enables a node to acquire and verify the public key of other nodes.

To facilitate the transmission of the information required for the security mechanisms, SAODV applies changes to the standard AODV message format in the form of extensions. These SAODV extensions consist of the following fields: *hash function* field which identifies the one-way hash function that is used; *Max hop count* which is a counter that specifies the maximum number of nodes a packet is allowed to go through; *Top hash* field is the result of the application of the hash function to a randomly generated number; finally, the *hash* field is that random number. These are shown in figure 5.2 below.

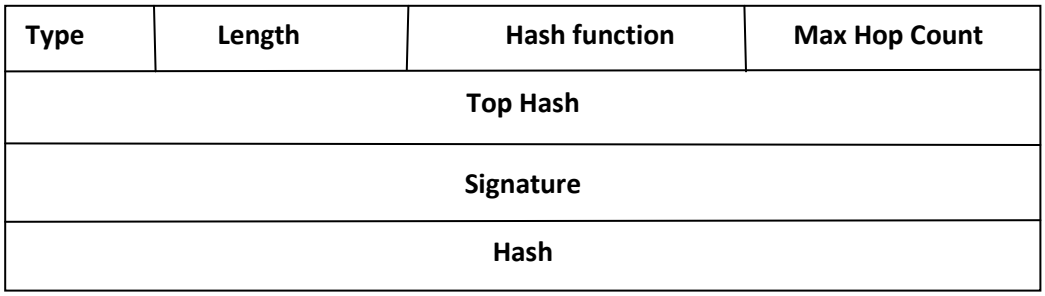


Figure 5.2 SAODV Protocol Header

A node transmitting a route request or a route reply in an AODV packet, sets the max hop count field equal to the time to live (TTL) field from the IP header. It generates a random number and sets the hash field equal to it, then applies the hash function specified by the corresponding max hop count field to the random number and stores the calculated result to the top hash field. The node digitally signs all fields of the message, except the hop count field from the AODV header and the hash field from the SAODV extension header.

On receipt of a route request or route reply by an intermediate node, it must verify the integrity of the message using the digital signature and also verify the hop count AODV field. Before the packet is re-broadcast by the intermediate node, the value of the hash field is replaced by the result of the calculation of the one-way hash of the field itself in order to account for the new hop. Here in SAODV, it still allows for intermediate nodes with fresh routes to reply to a route query on behalf of the destination node only if the reply is signed on behalf of the destination node.

For route maintenance, the route error messages (RERR) generated in SAODV by nodes to inform neighbors of inability to route messages to specific destinations are secured using digital signatures. A node generating or forwarding a route error message signs the whole message, except the destination sequence numbers [7]. Since the destination does not authenticate the destination sequence number, SAODV specifies that a node should never update the destination sequence numbers of the entries in its routing table based on

route error messages. Even with this requirement, route error messages are still useful in SAODV as it allows a node to decide whether to completely remove a route from its routing table or not.

5.4 REPUTATION BASED SOLUTIONS

Reputation based solutions operation usually relies on passive monitoring of transactions and exchange of recommendation or alert messages between nodes that participate in a system. The main purpose of reputation systems is to make decisions regarding trustworthy entities and to encourage behavior that leads to increasing trust [9, 39]. Several reputation mechanisms have been proposed to address the problem of selfish behavior and disruption of the routing process in MANETs including the Watchdog and Path-rater concept.

5.4.1 Watchdog and Path-rater:

This scheme consists of two extensions to the DSR routing protocol that attempt to detect and mitigate the effects of nodes that do not forward packets although they have agreed to do so [11]. This misbehaviour may be due to malicious or selfish intent, or simply the result of resource overload.

The watchdog extension is responsible for monitoring that the next node in the path forwards data packets by listening in promiscuous mode. It identifies nodes that fail to do so as suspicious nodes.

The path-rater assesses the results of the watchdog and selects the most reliable path for packet delivery. One of the base assumptions of this scheme is that malicious nodes do not collude in order to circumvent it and perform sophisticated attacks against the routing protocol.

Every node that participates in the Ad hoc network employs the watchdog functionality in order to verify that its neighbors correctly forward packets. Furthermore, if there is no link encryption employed in the network, the listening node can also verify that the next node did not modify the packet before transmitting it [37]. The watchdog of a node maintains copies of recently forwarded packets and compares them with the packet transmissions overhead by the neighboring nodes. Positive comparisons result in the deletion of the buffered packet and the freeing of the related memory. Every node in the Ad hoc network, maintains a rating, assessing the reliability of every other node from which it can overhear packet transmissions. Therefore, if a node that was supposed to forward a packet fails to do within a certain timeout period, the watchdog of an overhearing node increments a failure rating for the specific node. A node is identified as misbehaving or malicious when the failure rating exceeds a certain threshold bandwidth and the source node of the route that contains the offending node is notified by a message sent by the identifying watchdog [11]. The main issue with this approach is its vulnerability to blackmail attacks.

The path-rater extension to DSR selects routes for packet forwarding based on the reliability rating assigned by the watchdog mechanism. Particularly, a metric for each path is calculated by the path-rater by averaging the reliability ratings of the nodes that participate in the path. This path metric allows the path-rater to compare the reliability of available paths. The path-rater selects the path with the highest metric when there are multiple paths for the same destination node. When the path-rater calculates a path value as negative, this means that the specific path has a participating misbehaving node.
The watchdog and path-rater extensions as discussed facilitate the identification and avoidance of misbehaving nodes that participate in the routing function. The main operational assumption besides the support of promiscuous mode by the participating nodes is that there is no collusion between active attackers in the network. Also, since the system does not use cryptographic methods for securing exchanged messages, Watchdog and Path-rater suffers from the possibility of blackmail attacks.

5.5 ADD-ON MECHANISMS TO EXISTING PROTOCOLS

These are add-on mechanisms that address specific security problems in Ad hoc routing and can be implemented into already existing protocols without modifying the protocols. IPsec has been suggested as a possibility for securing Ad hoc routing.

5.6 COMPARISONS OF THE EXISTING PROPOSED SECURE ROUTING FOR MANETs

As each protocol has a different set of operational requirements and provides protection against different attacks by utilizing particular approaches, a comparison can provide insight regarding the applicability of a particular protocol for a specific application domain. In this section, we present the assumptions and operational requirements of the analyzed protocols, and compare them based on the approaches they utilized.

5.6.1 Requirements and Assumptions of the Existing Proposed Secure Solutions

Certain assumptions and operational requirements form the basis of the proposed solutions by the surveyed protocols. Most of the protocols require the existence of an online trusted third party like a certification authority, in order to facilitate the acquisition and verification of the public keys of the nodes that participate in the Ad hoc network. ARAN, SEAD, and SAODV. The operational requirement of SRP is similar since it needs a pre-established security association between every source and destination node. The SEAD protocol requires the existence of a key distribution scheme for the authentication of one element of a hash chain between two nodes, which can be realized with a broadcast authentication mechanism such as TESLA, hence requiring the nodes of the network to have synchronized clocks. Ariadne requires both shared secret keys between each pair of nodes to authenticate point-to-point messages, and time synchronization in order to use TESLA as a method for authenticating broadcast messages. Finally, the successful operation of the Watchdog and Path-rater protocol

extensions require that no two or more malicious nodes collude to perform routing attacks. Table 5.1 summarizes the results of the comparison.

Table 5.1 Operational Requirements for the existing Secure Ad hoc Protocols

Proposed Solution	**Requirements**
ARAN	Online trusted certification authority. Each node knows a prior the public key of the CA
SEAD	Clock synchronization, or a shared secret between each pair of nodes
SRP	Existence of a security association between each source and destination node. Malicious nodes do not collude within one step of the protocol process
SAODV	Online key management scheme for the acquisition and verification of public keys
Ariadne	Clock synchronization and the existence of a shared secret between each pair of nodes. Also, an authentic TESLA Key for each node and which are distributed via an online key distribution center
Watchdog and Path-rater	No collusion between malicious nodes

Most of the security solutions for Ad hoc routing are based on existing security solutions for Ad hoc routing are based on existing Ad hoc routing protocols. These base or underlying protocols introduce parameters that must be taken into account. Table 5.2 presents a complete set of these.

Table 5.2 Existing Secure MANET Routing Protocols Parameters

Proposed Solution	Routing Approach	Loop freedom	Routing Metric	Shortest path identification	Intermediate nodes allowed to reply to route requests
ARAN	On-demand	Yes	None	Optional	No
SRP	On-demand	Yes	Distance	No	Optional
SEAD	Table-driven	Yes	Distance	No	No
Ariadne	On-demand	Yes	Distance	No	No
SAODV	On-demand	Yes	Distance	No	Optional
Watchdog and Pathrater	On-demand	Yes	Path reliability or distance	Depends	Yes

Ideally, a secure Ad hoc routing protocol should be able to provide protection against all the categories of attacks discussed in this work. However, in reality, with the highly dynamic nature of Ad hoc networks and the different scenarios of their application, it is difficult to design a general solution that can provide adequate protection against all kinds of attacks in all possible application scenarios, possessing acceptable requirements and overhead. Table 5.3 below provides a comparison of the surveyed secure routing solutions with respect to the different attacks.

Table 5.3 Defense Against Attacks

	Protocols					
Attacks	**ARAN**	**SRP**	**SEAD**	**Ariadne**	**SAODV**	**Watchdog and Path-rater**
Location Disclosure	No	No	No	No	No	No
Black Hole	No	No	No	No	No	Yes
Replay	Yes	Yes	Yes	Yes	Yes	No
Wormhole	No	No	No	No	No	No
Blackmail	NA	NA	NA	NA	NA	No
Denial of Service	No	Yes	Yes	Yes	No	No
Routing table poisoning	Yes	Yes	Yes	Yes	Yes	No

CHAPTER SIX
PROPOSED SECURE ROUTING PROTOCOL

6.1 SECURITY REQUIREMENTS OF A SECURE AD HOC ROUTING PROTOCOL

A good secure routing algorithm should prevent each of the attacks presented and discussed in the section above. It must ensure successful and secure route discovery and maintenance with no node prevent or hindering it apart from the possibility of non-participation. A secure Ad hoc routing protocol must satisfy some requirements to ensure the correct and safe functioning of routing operations and path discovery in the presence of malicious adversaries:

1. Routing signaling cannot be spoofed
2. Fabricated routing messages cannot be injected into the network
3. Routing messages should and cannot be altered in transit, except according to the normal functionality of the routing protocol
4. Routing loops cannot be formed through malicious action
5. Routes cannot be redirected from the best path (shortest path) by malicious action
6. Unauthorized nodes should be excluded from route computation and discovery. This does not overlook the fact that already authenticated peers may act maliciously too. However, we assume that in managed –open environment, there is some pre-deployment and exchange of public keys, session key or certificates.
7. The network must never be exposed neither to adversaries nor to authorized nodes by the routing messages. Exposure of the network topology is maliciously utilized by adversaries to even destroy or capture nodes.

6.2 PROPOSED SECURE ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS

The mobile Ad hoc network routing protocols standardized by the IETF (rfc 3501) and (rfc 4728), does not take into serious consideration the security threats and attack out there. Hence the routing protocols for MANETs lack built-in security to mitigate attacks and help secure the vulnerabilities of the mobile wireless Ad hoc networks.

Having conducted extensive research into the existing standard routing protocols for MANETs, noted their security vulnerabilities and that of MANET as a network coupled with the security attacks they face, a secure routing protocol is highly needed for mobile Ad hoc networks to be of practical application in this technological age.

As a result, we hereby put forward "*Authenticated Source Routing for Ad hoc Networks*" (ASRAN), a novel secure routing protocol enhancements for MANET. It is based on DSR, a source-routing on-demand routing protocol. Its use of source routing makes it the best suited for the mobility and dynamism that comes with MANETs. DSR was chosen as the model protocol to use as a backbone for ASRAN because out of the MANET prototypical routing protocols, DSR possesses the best characteristics, exhibited better performance in experiments and simulations conducted as reviewed in earlier sections, and possess mechanisms, which can easily be adapted to include security, while having fewer vulnerabilities.

6.3 AUTHENTICATED SOURCE ROUTING FOR AD HOC NETWORKS (ASRAN)

ASRAN makes use of cryptographic certificates to offer routing security. It builds upon concepts from ARAN (a secure routing protocol adapted using AODV) [19] and also SAODV [7], another proposal for security extensions to the AODV protocol to specifically accommodate source routing as found in DSR.

ASRAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. Route discovery in ASRAN is accomplished by a broadcast route discovery message from a source node with a reply only from the intended destination node, hence intermediate node are no longer required to send a reply on behalf of the destination node, if a route to it exists. The reply is such that the routing messages are authenticated at each hop from source to destination, as well on the reverse path from the destination to the source.

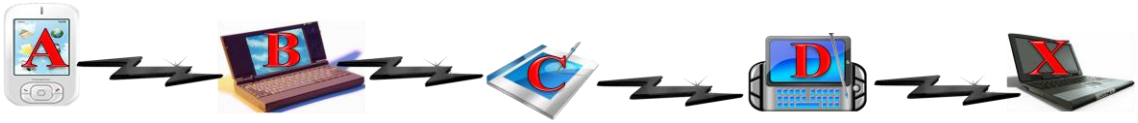


Figure 6.1 Simple MANET Topology Employed to Explain ASRAN

Table 6.1 Notations used for ASRAN

K_{A+}	Public key of node *A*	N_A	Nonce issued by node *A*
K_{A-}	Private key of node *A*	RDP	Route Discovery Packet
$[p]K_{A+}$	Encryption of packet *p* with key K_{A+}	RREP	Route Reply Packet
$[p]K_{A+}$	Packet *p* digitally signed by node *A*	SRR	Source Route Record
$cert_A$	Certificate belonging to node *A*	RERR	Route Error Packet
t	Timestamp	IP_A	IP address of node *A*
e	Certificate expiration time	$\|h\|$	One way hash with input *h*

6.3.1 ASRAN Certification

ASRAN requires the use of a trusted certificate server *T,* whose public key will be known to all valid nodes. They keys are initialized - that is generated and exchanged through an existing, probably out of band relationship between *T* and each node. For a node to join

the Ad hoc network, a certificate must be requested from *T*. Each node receives exactly one certificate after securely authenticating their identity to *T*. We do not go into details in this work in reference to the methods for secure authentication to the certificate server but are left for developers and future work. Details of certificate revocation in ASRAN are explained in the coming section.

After a node *A* requests and receives a certificate from *T,* after securely authenticating their identity to *T*. A node *A* receives a certificate from *T* as follows:

$$T \rightarrow A : cert_A = [IP_A // K_{A+} // t // e] K_{T-} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (6.1)$$

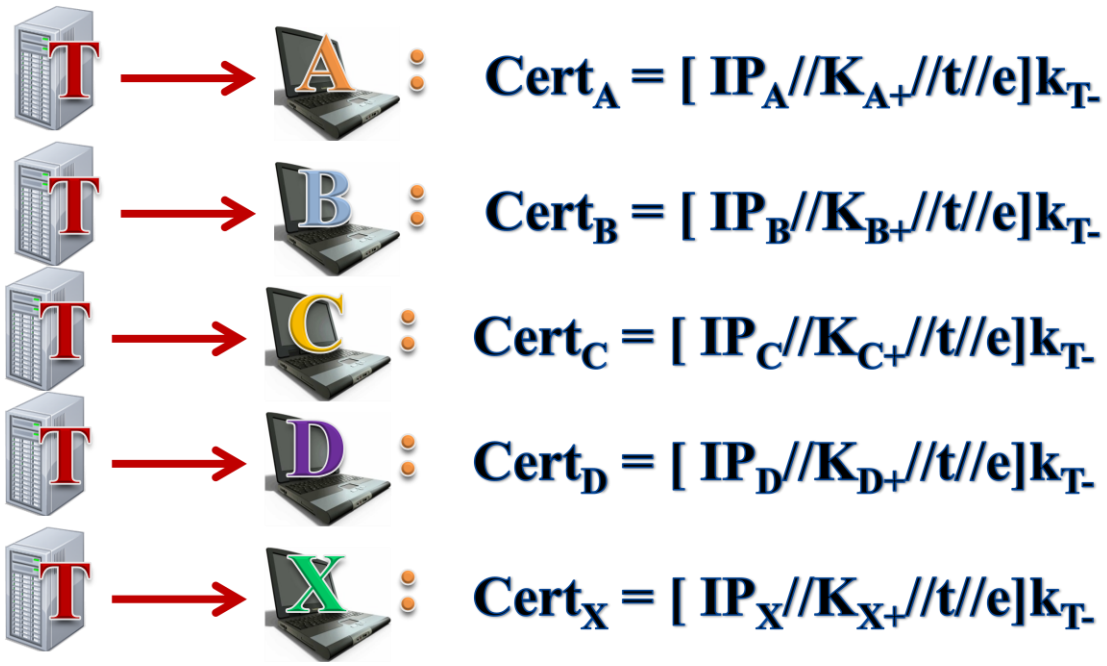


Figure 6.2 ASRAN Certification

The certificate contains the IP address of *A*, the public key of *A,* a timestamp *t* of when the certificate was generated, and a time *e* at which the certificate expires. These variables are concatenated and signed by *T*. All nodes must maintain fresh and current certificates with the trusted server. Nodes use these certificates to authenticate themselves to other nodes during the exchange of routing messages.

6.3.2 ASRAN Route Discovery

The purpose of end-to-end authentication is for the source to verify that the intended destination was reached. We assume a bi-directional link and that the destination node will choose the same route as a return path.

Figure 6.3 Route Discovery Packet (DSR and ASRAN)

Using the topology in figure 6.1, source node *A,* begins route discovery to destination *X* by broadcasting to its neighbors a *route discovery packet (*RDP*)* secured thus:

$$Cert_A \,//\, \{ IP_x \,//\, t \,//\, N_A \}k_{A-} \quad \ldots\ldots\ldots\ldots \quad (6.2)$$

The route discovery packet includes a concatenation of Node A's certificate and the IP address of the destination (IP_x), *A*'s certificate ($cert_A$), a nonce N_A, and the current time *t*, all digitally signed with node *A*'s private key K_{A-}.

Each time node A performs route discovery, it will monotonically increase the nonce. The nonce and timestamp are used in conjunction with each other to determine freshness of message, and also uniquely identify. Other nodes then store the nonce they have last seen for a particular node along with its timestamp.

Once a node receives an RDP message, it sets up a reverse path back to the source by making an entry in its route cache of the neighbor from which it received the RDP. This is used as a verification mechanism on receipt of a reply packet. As we are assuming a bi-directional link, when a response is passed back from the destination to the source, on getting to this node, the node will use its entry to verify that the next hop address contained in the source route header tallies to the one which is in its route cache. *This is an integrity mechanism to ensure that the source route has not been tampered with*.

The receiving node uses *A*'s public key, which it extracts from *A*'s certificate, to validate the signature's authenticity and verify that *A*'s certificate has not expired. The receiving node also checks the (N_A, IP_A) ordered list of elements (tuple), to verify that it has not already processed this RDP. Nodes do not forward messages for which they have already seen the tuple. However, if it has not seen the tuple previously, the node signs the contents of the message, appends its own certificate, and forward broadcasts the message to each of its neighbors. *This signature prevents impersonation and or spoofing attacks that may alter the route or form loops*.

Taking Node *B* to be a neighbor that has received from *A* the RDP broadcast, it then subsequently rebroadcasts thus:

$$Cert_B \,//\, Cert_A \{\{ IP_x \,//\, t \,//\, N_A \}k_{A-}\}k_{B-} \quad \ldots\ldots\ldots\ldots \quad (6.3)$$

On receipt of the RDP, *B*'s neighbor, *C* validates the signature with the enclosed certificate. *C* then strips *B's* certificate and signature, makes a record of *B* as its predecessor, signs the contents of the original message broadcast by *A*, appends its own certificate and forward broadcasts the message. *C* then rebroadcasts the RDP onwards.

$$: Cert_C \,//\, Cert_A \,//\{\{ IP_x \,//\, t \,//\, N_A \}k_{A-}\}k_{C-} \quad \ldots\ldots\ldots \quad (6.4)$$

Thus, these steps of validating the previous node's signature, stripping the previous node's certificate and signature, making an entry of the previous node's IP address into the route cache, signing the original contents of the message while appending its own certificate before forward broadcasting the message is repeated along the path by each node until it reaches the destination node.

The source route within the RDP on reaching the destination node, is secure because the RDP messages were signed at each hop on its way to the destination, hence malicious nodes have no opportunity to redirect traffic with the attack exploits we discussed in the previous section.

6.3.3 ASRAN Route Setup

Eventually, the route request message is received by the destination, *X. The destination, X, replies to the first RDP it receives for a particular source and given nonce.* Hence, it does not depend on the hop count recorded within the RDP but rather that the first RDP to arrive must have traveled through a route with least congestion and delay to arrive first. Therefore, *ASRAN utilizes delay and will prefer a non-congested non-shortest path to a congested shortest path because of the reduction in delay*.

After receiving the RDP, the destination will generate a Route Reply packet (RREP) using a record of the traversed nodes contained in the route request (RDP) packet. This is the complete list of nodes back to the source node or the source route record (SRR). It will then generate a one-way hash of the newly created SRR using as input the complete source route record back to the source node to return a fixed length output → $h|SRR| = f(SRR)$. Having done all this, the destination node *X* will concatenate it into one bundle as a response packet RREP, signing it with it's private key, before unicasting the RREP message along the reverse path through which it came, back to the source node.

Original:

DSR Route Response (REP) :

Modified by ASRAN:

ASRAN Route Response (REP) :

Figure 6.4 Route Response Packet (DSR and ASRAN)

Let the first node that receives the route reply RREP sent by the destination, X be node D. The reply message RREP includes the certificate belonging to X ($cert_x$) concatenated with a hashed SSR ($[|SRR|$), the source route record (SRR), the IP address of A (IP_a), the nonce and associated timestamp sent by A.

$$: \quad Cert_X \,//\, \{ IP_x \,//\, h|SRR| \,//\, t \,//\, N_A \}k_{X^-} \qquad \ldots\ldots\ldots \quad (6.5)$$

Nodes that receive the RREP message validate the authenticity of the node from which it received it using the public key of the node on the digital signature. It checks the source route node list (SRR) to ascertain the next hop it should forward the RREP message, verifying that it is actually the correct route and next hop by checking if it corresponds with the entry it made in its route cache previously for that source node RDP and nonce. If everything tallies, it then signs the RREP and appends its own certificate before forwarding the RREP message to the next hop (back to the predecessor from which the original RDP was received). Each node along the reverse path does the same verification and double-checking with its route cache entry, before signing the REP and appending its certificate, then forwarding it along to the next hop on the way back to the source node.

The verification of next hop in the source route record (SRR) in the RREP packet with the nodes previous entry in the route cache is a mechanism to avoid and detect spoofing and modification attacks.

Let *D's* next hop to the source node be node *C*.

$$: Cert_D \,//\, Cert_X \,//\, \{\{ IP_A \,//\, h|SRR| \,//\, t \,//\, N_A \}k_{X-}\}k_{D-} \quad \ldots\ldots\ldots \quad (6.6)$$

C validates *D*'s signature on the received message, removes the signature and certificate, then signs the contents of the message and appends its own certificate before unicasting the RREP to the next hop *B*.

$$: Cert_C \,//\, Cert_X \,//\, \{\{ IP_A \,//\, h|SRR| \,//\, t \,//\, N_A \}k_{X-}\}k_{C-} \quad \ldots\ldots \quad (6.7)$$

Also, each node checks the nonce and signature of the previous hop as the RREP is returned to the source. This avoids the attacks where malicious nodes instantiate routes by impersonation and replay of *X*'s message. When the source node receives the RREP, it verifies the destination's signature and the nonce returned by the destination. *It also runs a hash of the SRR and compares it to the sent destination hashed value* $|SRR|$ *to ensure the integrity of the source route (SRR)* and that no nodes were fabricated, injected or deleted. *This adds integrity mechanism to ASRAN's* route setup operation.

6.3.4 ASRAN Route Maintenance

ASRAN is an on-demand protocol, where nodes keep track of the recently used entries in the route cache or simply whether the routes are active. If no traffic or usage has occurred during an existing route's lifetime, the route entry is simply removed from the route cache. Route Error (RERR) messages are used by nodes to report links in active routes that are broken due to node movement, shutdown etc. All RERR messages must be signed.

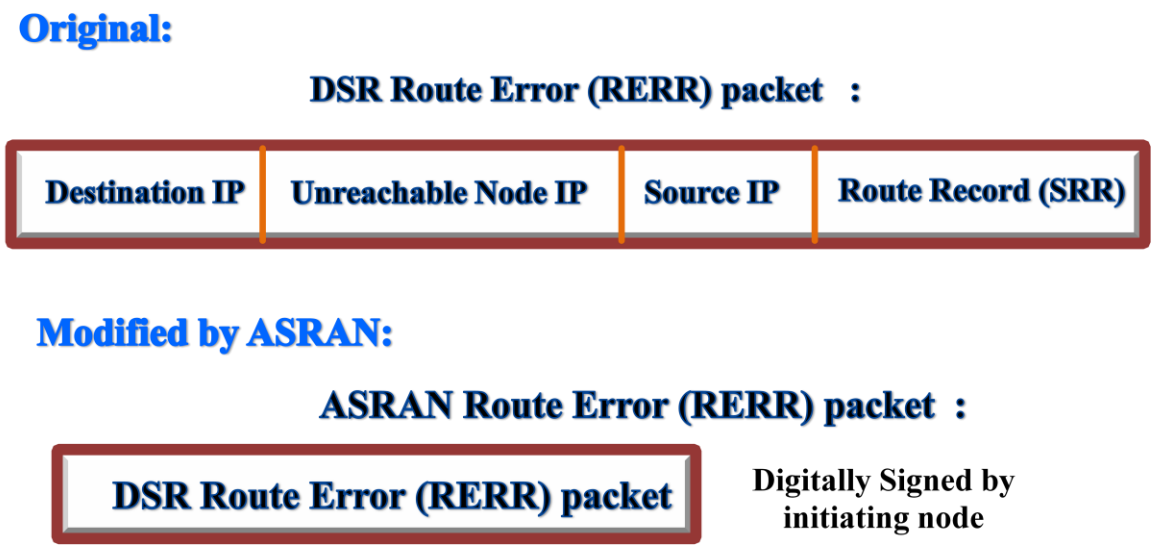


Figure 6.5 Route Error Packet (DSR and ASRAN)

For a route between a source node *A* and destination *X*, a node *B* generates the RERR message for its neighbor *C* as follows:

…… (6.8)

This message is forwarded along the path toward the source without modification. Because messages are signed, malicious nodes cannot generate RERR messages for other nodes, but can for its node. This is because, it is difficult to detect when RERR messages are fabricated for links that are truly active and broken. Also, *the non-repudiation provided by the signed ERR message allows a node to be verified as the source of each RERR message that it sends*. A node that generates and transmits large numbers of RERR messages should be suspected, whether the RERR messages are valid or fabricated.

6.3.5 ASRAN Responses to Erratic Behavior

Erratic behavior can come from a malicious node, but it can also come from a friendly node that is malfunctioning. ASRAN's response does not differentiate between the two

and regards all erratic behavior as the same. Erratic behavior includes the use of invalid certificates, improperly signed messages, and misuse of route error messages. *ASRAN's response to erratic behavior is an area for further work* where an Intrusion Detection System (IDS), Watchdog and Path-rater mechanism [11] and or a trust based mechanism can be integrated to handle responses to suspicious behavior.

6.3.6 ASRAN Key Revocation

A best effort immediate revocation service can be provided that is backed up by the use of limited-time certificates. This is due to the desired low-overhead in wireless networks, hence a trade-off between the standard of security (complexity) and cost.

When a certificate needs to be revoked, the trusted certificate server, *T*, sends a broadcast message to the Ad hoc group of nodes to announce the revocation. Let us call the revoked certificate, $cert_x$, the transmission will appears as:

$$T \rightarrow broadcast : [revoke, cert_r,]K_{T-} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (6.9)$$

On receipt of this message by a node, it will re-broadcast it to its neighbors. Until the revoked certificate's normally expiration time elapses, these revocation notices will be stored. Neighbors of the node with the revoked certificate, on receipt of the revocation notice, will need to reform routing as necessary to avoid transmission through the now un-trusted node. There is a problem with this method that is in the event that the un-trusted node whose certificate was revoked is the sole connection between two parts of the Ad hoc network. Hence there might be a partition of the network, which will last until the un-trusted node is no longer the sole connection between the two partitions.

6.4 SECURITY ANALYSES AND APPRAISAL OF ASRAN

In this section, we provide a security analysis of ASRAN by the evaluation of its robustness in the presence of the attacks we discussed in the section 4.6 above.

- ***Mitigation of Tunneling Attacks:*** Hop count is the metric of DSR which is the underlying protocol on which ASRAN is built on. There is no way to guarantee that one path is shorter than another based solely in terms of hop count. Taking into consideration that tunneling attacks, such as the one presented in the section above are possible in DSR and other prototypical MANET routing protocols, designing a way of determining the best path is of utmost importance. Securing a shortest path cannot be done by any means except by physical metrics such as a timestamp in routing messages. However, according to ASRAN, the best and shortest path is not a function of hop counts only, but mainly that of the least delay as can be deduced from the timestamps. Therefore, malicious nodes will find it difficult carrying out tunneling attacks in MANETs using ASRAN because tunneling attacks normally is as a result of exploiting the vulnerability of a use of hop count as the sole determinant of best route, which is not so in ASRAN. ASRAN equates the best and shortest path as a function of time using timestamps, and responds accordingly. Therefore, ASRAN will prevent most tunneling attacks.

- ***Spoofed Route Signaling:*** Source node messages can only be signed by its own private key. Therefore, nodes cannot spoof other nodes in route instantiation or discovery. Similarly, reply packets include the destination node's certificate and signature, ensuring that only the destination can respond to route discovery. This prevents *impersonation* attacks where either the source or destination node is spoofed.

- ***Unauthorized Participation*****:** ASRAN participant nodes accept only packets that have been signed with a certified key issued by the trusted authority. We did not discuss mechanisms for authenticating users to the trusted certificate authority in this work. There are numerous mechanisms with a significant list provided by Schneier [2]. Also, in ASRAN, having a central trusted authority is vulnerable and a single point of failure. This is an area for future work and improvement. A look into threshold cryptography [38] as a way of achieving a distributed certification

system or multiple redundant authorities as suggested by Zhou and Haas [13] can be used.

- ***Replay Attack:*** Replay attacks are prevented by including a nonce and a timestamp in the routing messages (RDP and REP).

- ***Fabricated Routing Messages:*** As only nodes with certificates can generate messages, hence, messages can only be fabricated by nodes with certificates – meaning valid authenticated nodes that has been hijacked or become malicious. ASRAN does not have provision to mitigate such attacks or those by selfish nodes. However, ASRAN does offer a deterrent by ensuring *non-repudiation* services. A node that continues to inject false messages into the network may be excluded from future route computation.

- ***Integrity and Alteration of Routing Messages:*** ASRAN specifies that all fields of RDP and REP messages remain unchanged between source and destination using an integrity enforcing mechanism. Since both packet types are signed by the initiating node, any alterations in transit would be immediately detected by intermediary nodes along the path resulting in the altered packet subsequently discarded. A further enhancement of security in ASRAN in this respect is that the final node - the source as the case maybe, now has the ability to verify that there were no alterations in the route list by making use of the hashed SRR included in the REP message. It will run the appended SRR through the hashing algorithm in use and compare with the already hashed one transmitted from the destination node. This ensures integrity in ASRAN and corrects a flaw of ARAN, whereby only the intermediate nodes can detect alterations with no provision for the final node to detect it too, enabling a vulnerability which is that the last intermediate node might be able to successfully alter the packet contents as there will be no other intermediate nodes to detect it.

6.5 COMPARISON OF ASRAN TO EXISTING SECURE ROUTING

Here we are going to compare our proposed security enhancement - Authenticated Source Routing for Ad hoc Networks (ASRAN) - to the existing secure routing solutions we have already reviewed in this thesis (chapter 5). The comparison is based on the protection/defense rendered against security threats and attacks facing MANETs.

Table 6.2 Defense against attacks

	Protocols						
Attacks	**ASRAN**	**ARAN**	**SRP**	**SEAD**	**Ariadne**	**SAODV**	**Watchdog and Path-rater**
Location Disclosure	No	No	No	No	No	No	No
Black Hole	No	No	No	No	No	No	Yes
Replay	Yes	Yes	Yes	Yes	Yes	Yes	No
Wormhole	No	No	No	No	No	No	No
Blackmail	NA	NA	NA	NA	NA	NA	No
Denial of Service	**Yes**	No	Yes	Yes	Yes	No	No
Routing table poisoning	Yes	Yes	Yes	Yes	Yes	Yes	No
Spoofing	Yes	Yes	No	No	Yes	No	No
Integrity/Alteration	**Yes**	No	No	No	No	No	No

CHAPTER SEVEN
SIMULATION, CONCLUSION AND FUTURE WORK

7.1 SIMULATION

We implement and run a simulation for ASRAN to verify and validate its performance in varying degree of mobility for a performance metric. The performance metric used is "Route Acquisition Time". We used Network Simulator (NS-2), a discrete event simulator for our simulated experiments.

While Not Empty (*Event Queue*) **Do**

dequeue(*m*) /*earlier event from EventQueue*/

update(*clock*)

simulate(*m*)

enqueue() /* enqueue any events produced */

EndWhile

7.1.1 Performance Metrics

The following performance metrics were used for evaluating the proposed secure routing protocol (ASRAN).

(i) ***Route Acquisition Tim***e: The time it takes a source node to find a route to a destination node.

(ii) ***Pause Time***: This is the degree of mobility of a node.

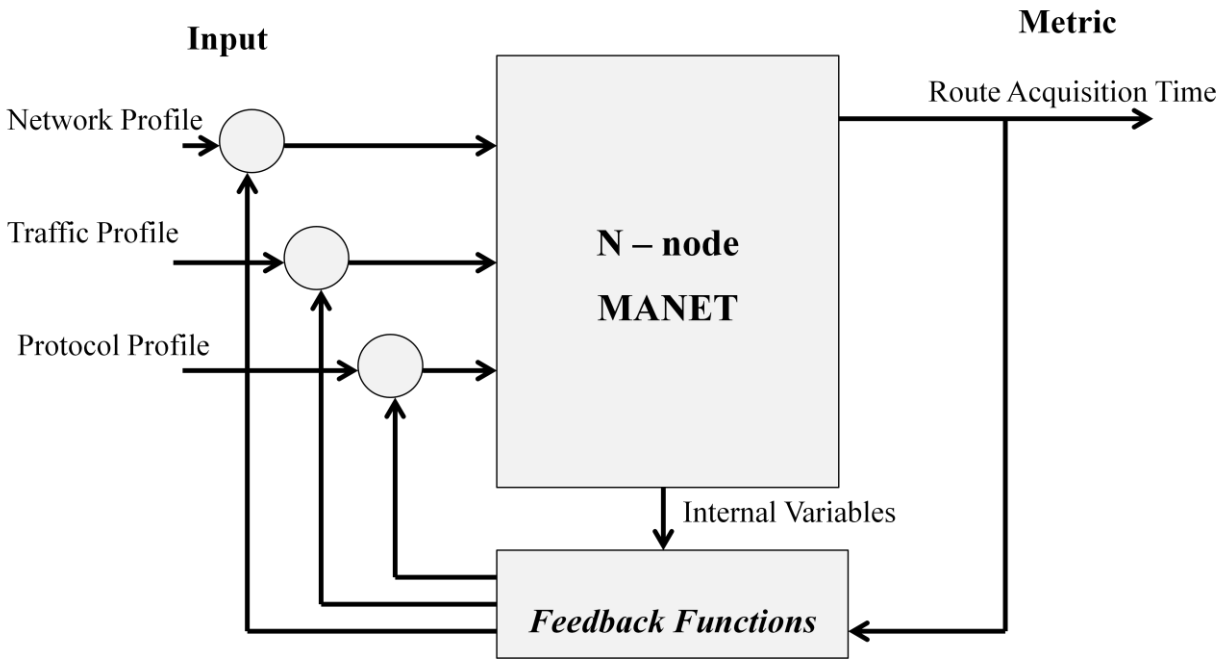


Figure 7.1 Simulation Block Diagram

7.1.2 Simulation Parameters

The different parameters considered for the simulation are shown in Table 6.2 below

Table 7.1 Simulation Test-bed

Parameter	Value
Simulation Software	**Network Simulator (NS-2)**
Node density	20
Maximum velocity	20m/s
Environment Size	1200m x 300m
Traffic Type	CBR (Constant Bit Rate)
CBR (Packet Rate)	4 (kb/s)
Pause Times (mobility)	0 to 500secs (interval time of 100)
Mobility model employed	Random waypoint model
Size of packets	512 bytes
Error Margin	±0.003

7.1.3 Methodology

We correlate the published DSR and our proposed protocol (ASRAN). This is done by modifying the NS-2 Tcl/Tk. We modified the written Tcl/Tk script to take into account the changes and security mechanisms added in the route acquisition process as discussed earlier. The modified Tcl/Tk script implements the proposed ASRAN protocol. The simulation was repeated four times with the same conditions and the mean is shown below.

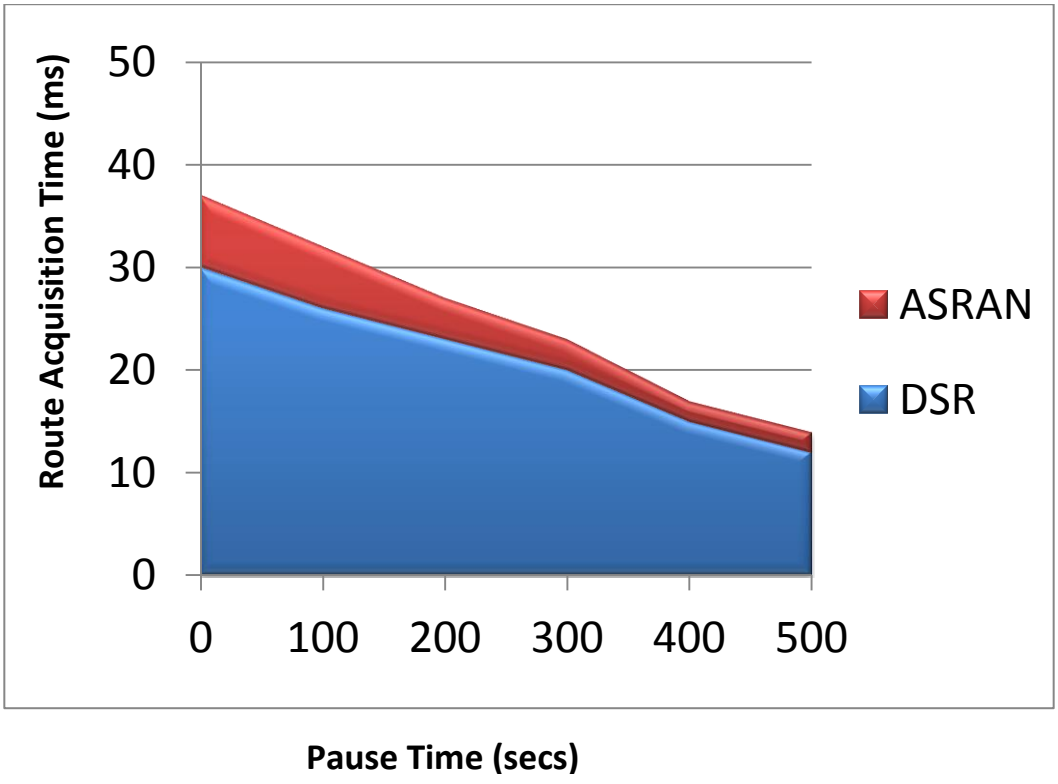


Figure 7.2 Simulation Results

Table 7.2 Simulation result values

Pause Time (seconds)		0	100	200	300	400	500
Route Acquisition Time (milliseconds)	DSR	30	26	23	20	15	12
	ASRAN	37	32	27	23	17	14
Coefficient of Correlation		0.811	0.813	0.852	0.869	0.882	0.857

Mean Coefficient of Correlation → 5.084/6 = 0.847

7.1.4 Discussion

The simulation result leads us to the following observations:

The Route Acquisition Time is increased, indicating that the security additions and implementations introduced some latency.

ASRAN has a higher route acquisition time or delay at higher mobility (lower pause time). This is as a result of a high demand of routes as routes already acquired changes at a higher frequency due to the highly dynamic topology (mobility).

The co-efficient of correlation from the simulation for the route acquisition metric evaluated for both DSR and ASRAN is an indication of the behavior of ASRAN in relation to DSR. The mean coefficient value comes out to be 0.847 which shows that our proposed ASRAN is in close proximity with the published DSR protocol in terms of performance.

Finally, we deduce that the performance (latency) trade-off as a result of security additions and implementations in ASRAN is negligible.

7.2 CONCLUSION

Wireless mobile Ad hoc networks differ in many ways to the conventional wire-line networks. The characteristics of MANET which are – dynamic changing topology; absence of Infrastructure; Limited resources and energy constraints – pose a lot of security challenges for the network. The very basic nature of the mode of communication (radio spectrum) and possibility of high node mobility brings about a lot of vulnerabilities and insecurity. Security is an essential requirement for networks. However, the standard MANET routing protocols published have negligible or no security mechanisms. This makes them and MANET network highly insecure and susceptible to a variety of security attacks. Secure routing in Ad hoc networks is the main focus of our research. Authenticated Source Routing for Ad hoc Networks (ASRAN) routing protocol has been proposed and simulated for performance. We summarize our contributions as follows:

1. We conducted a performance evaluation of various MANET routing protocols of different types, mainly focusing on the flat-routing protocols. The routing protocols were analyzed to assess their relative strength and weaknesses.
2. From our study results, we selected DSR as our prototype protocol as it is the best routing protocol for providing secure routing because there are no periodic beacons, thus resulting in a lesser overhead during communication.
3. We analyzed the various attacks targeting the DSR protocol and MANET at large and reviewed existing work in secure routing protocols.
4. We introduced a novel secure routing protocol termed as "Authenticated Source Routing for Ad hoc Network" (ASRAN). The proposed protocol is a source routing protocol based on DSR and employs certificate. We basically modified the route acquisition process of DSR, adding security mechanism to mitigate the existing vulnerabilities.
5. The proposed algorithm was compared to existing secure routing protocols. Also, we simulated and compared ASRAN to DSR to establish its route acquisition time and correlation of performance.

7.3 FUTURE WORK

This work opens new avenues for future research. The research can be extended in several directions and some of them are summarized below:

1. The proposed protocol, ASRAN, uses a certification server for initialization and administration of certificates. The method for the authentication of the nodes to the certificate server is an area to be researched and developed further.
2. As ASRAN security improvements were mainly in its route acquisition process, securing further the data transmission stage is an area for future work.
3. In the presented work, the selfish nodes are not dealt with; it would be interesting as an area for improvement, the design and integration of security mechanisms capable of mitigating both selfish and malicious nodes activities.

BIBLIOGRAPHY

1. W. Mehuron, "Digital Signature Standard (DSS)," U.S. Department of Commerce, *National Institute of Standards and Technology (NIST),* Information Technology Laboratory (ITL). FIPS PEB 186, 1994.

2. B. Schneier. *Applied Cryptography*: *Protocols, Algorithms and Source Code in C., 2nd Ed.,* John Wiley & Sons, Inc., New York, 1996.

3. David B. Johnson and David A. Maltz. Dynamic Source Routing in Ad hoc Wireless Networks. In *Mobile Computing,* edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153-181. Kluwer Academic Publishers, 1996.

4. Perkins, C and Bhagwat, P.; "DSDV Routing over a Multi-hop Wireless Networks," *In Proceedings of INFOCOM'97,* Kobe, Japan, pp. 754-761, April 1997.

5. F. Wang, B. Vetter, and S. Wu. Secure Routing Protocols: Theory and Practice. Technical report, North Carolina State University, May 1997.

6. IEEE Computer Society LAN MAN Standards Committee. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,* IEEE Std 802.11-1997. The Institute of Electrical and Electronics Engineers, New York, 1997.

7. S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998.

8. J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations". IETF RFC 2501, January 1999.

9. Charles E. Perkins, Elizabeth M. Royer, "Ad hoc On-demand Distance Vector (AODV) routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp. 90-100, February 1999.

10. Royer, E.M.; Chai-Keong Toh; , "A review of current routing protocols for Ad hoc mobile wireless networks," *Personal Communications, IEEE* , vol.6, no.2, pp.46-55, Apr 1999.

11. S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," *Proc. 6th Annual ACM/IEEE Int'l Conf. Mobile Comp. and Net. (Mobicom'00)*, Boston, Massachusetts, pp. 255-65., Aug. 2000.

12. R. Ramanujan, A. Ahamad, and K. Thurber, “Techniques for Intrusion Resistant Ad hoc Routing Algorithms (TIARA),”*Proc. Military Commun. Conf. (MILCOM 2000),* Los Angeles, CA, pp. 660-664, Oct. 2000.

13. Jae-Hwan Chang and Leandros Tassiulas. *Energy Conserving Routing in Wireless Ad-hoc Networks.* INFOCOM 2000. Proceedings of the Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Volume: 1, page 22-31, 2000.

14. Juan-Carlos Cano and Pietro Manzoni. “A Performance Comparison of Energy Consumption for Mobile Ad-Hoc Network Routing Protocols”, Proceedings of the *8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, pp. 57-64, 2000.

15. A. Perrig et al., “Efficient and Secure Source Authentication for Multicast,” *Proc. Symp. Network and Distributed Systems Security (NDSS’01),* San Diego, California, pp. 35-46, Feb. 2001.

16. Perkins, C.E.; Royer, E.M.; Das, S.R.; Marina, M.K.; , "Performance comparison of two on-demand routing protocols for Ad hoc networks," *Personal Communications, IEEE* , vol.8, no.1, pp.16-28, Feb 2001.

17. W. Arbaugh, N. Shankar, and Y.C. Wan. Your 802.11 Wireless Network has no Clothes. Technical report, Department of Computer Science, University of Maryland, March 2001.

18. A. Stubblefield, J. Ioannidis, and A.D. Rubin. Using the fluhrer, Mantin and Shamir attack to break WEP. Technical Report TD-4ZCPZZ, AT&T Labs, August 2001.

19. S. Yi, P. Naldurg, and R. Kravets, “Security-Aware Ad hoc Routing for Wireless Networks,” *Proc. 2nd ACM Symp. Mobile Ad hoc Network and Comp. (Mobihoc’01),* Long Beach, CA, pp. 299-302, Oct. 2001.

20. David B. Johnson, David A. Maltz, and Josh Broach. The Dynamic Source Routing Protocol for Multihop Wireless Ad hoc Networks. In *Ad hoc Networking,* edited by Charles E. Perkins, chapter 5, pages 139-172. Addision-Wesley, 2001.

21. Yih-Chun Hu and David B. Johnson. “Implicit Source Routes for On-Demand Ad hoc Network Routing,” *Proceedings of the 2001 ACM International Symposium on Mobile Ad hoc Networking & Computing (MobiHoc 2001)*, pp. 1-10, ACM, Long Beach, CA, October, 2001.

22. P. Papadimitratos and Z.J. Haas, “Secure Routing for Mobile Ad hoc Networks,” *Proc. Communication Networks Distributed Systems, Modeling and Simulation Conf. (CNDS’02)*, San Antonio, e Texas, pp. 27-31, Jan. 2002.

23. R. Ramanathan, J. Redi and BBN Technologies, “A Brief Overview of Ad hoc Networks: Challenges and Directions,” IEEE Communication Magazine, Volume: 20, pp. 20-22, ISSN:0163-6804, May 2002.

24. M.G. Zapata, and N. Asokan, “Secure Ad hoc On-demand Distance Vector Routing,”*ACM Moblie Comp. and Commun. Review,* vol. 3, no. 6, pp. 106-07, July 2002.

25. Y.C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks,” *Proc. 8th ACM Int’l Conf. Mobile Comp. and Net. (Mobicom’02)*, Atlanta, Georgia, pp. 12-23, Sept. 2002.

26. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure protocol for Ad hoc networks", Proc. ICNP, pp.78 -87, 2002.

27. R. Ogier, M. Lewis, and F. Templin, “Topology Dissemination Based on Reverse-Path Forwarding (TBRPF),”Internet Draft, draft-ietf-manet-tbrpf-08.txt, Apr. 2003.

28. C.E. Perkins, E.M. Royer, and S. Das, “Ad hoc On-demand Distance Vector (AODV),” RFC 3561, July 2003.

29. Fan Bai, Narayanan Sadagopan, Ahmed Helmy, “The Important framework for analyzing the Impact of Mobility on Performance of Routing Protocols for Adhoc Networks”, INFOCOM, 2003.

30. P. Papadimitratos and Z.J. Haas, “Secure Link State Routing for Mobile Ad hoc Networks,”*Proc. IEEE Wksp. Security and Assurance in Ad hoc Networks,* IEEE Press, pp. 27-31, 2003.

31. Yih-Chun Hu, Adrian Perrig, David B. Johnson, “Rushing Attacks and Defense in Wireless Ad hoc Network Routing Protocols,”*In Proc. ACM Workshop on Wireless Security,* 2003.

32. Y.C. Hu, A. Perrig, and D.B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks,” *Proc. 22nd Annual Joint Conf. IEEE Comp. and Comm. Societies (INFOCOM 2003),* IEEE Press, pp. 1976-86, 2003.

33. Azzedine Boukerche. “Performance Evaluation of Routing Protocols for Ad hoc Wireless Networks” In *Mobile Networks and Applications,* vol. 9, pp. 333-342, 2004.

34. Elizabeth M, Belding-Royer, “Routing Approaches in Mobile Ad hoc Networks”, *Mobile Ad hoc Networking, Institute of Electrical and Electronics Engineers (IEEE)*, 2004.

35. S. Basagni, M. Cont, S. Giordano and I. Stojmenovic. *Mobile Ad hoc Networking.* IEEE Press, New Jersey, 2004.

36. David B. Johnson and David A. Maltz, “Dynamic Source Routing in Ad hoc Wireless Networks” Computer Science Department, 2005.

37. P. Argyroudis and D. O'Mahony, "Secure routing for mobile Ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 3,pp. 2-21, 2005.

38. William Stallings. Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, USA, 2005.

39. Adibi, S.; Erfani, S.; , "A multipath routing survey for mobile ad-hoc networks," *Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE* , vol.2, no., pp. 984- 988, 8-10 Jan. 2006.

40. M.C. Govil, D. Gopalani, R. Jain, R. Ladha and S. Sharma, “Evolution of TCP over Wireless Links”, *In Proc. National Symposium on Emerging Trends in Broadband Communication,* April 8-9, 2006.

41. Adibi, S.; Erfani, S.; Harbi, H.; , "Security Routing in MANETs - A Comparative Study," *Electro/information Technology, 2006 IEEE International Conference on* , vol., no., pp.625-630, 7-10 May 2006.

42. B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto and A. Jamalipour, “Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad hoc Networks,” *Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN’06),* pp. 30-35, June 2006.

43. Chenna Reddy, P.; ChandraSekhar Reddy, P.; , "Performance Analysis of Adhoc Network Routing Protocols," *Ad hoc and Ubiquitous Computing, 2006. ISAUHC '06. International Symposium on* , vol., no., pp.186-187, 20-23 Dec. 2006.

44. Pin Nie. “Security in Ad hoc Network”, Helsinki University of Technology, 2006.

45. D. Johnson, Y. Hu, and D. Maltz, “The Dynamic Source Routing Protocol (DSR),” RFC 4728, February 2007.

46. IEEE Standard for 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," *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)* , vol., no., pp.1-1076, June 12 2007.

47. Jeremy Cioara, D. Minutella, and H. Stevenson. CCNA Exam Prep (Exam 640-802) Second Edition. Published by Pearson Education, Inc., USA, 2007.

48. Karan Singh, Rama Shankar Yadav, and Ranvijay. "A Review Paper on Ad hoc Network Security", In *Internatonal Journal of Computer Science and Security,* Volume (1): Issue (1), pp. 52-69, 2007.

49. Tepe, K.E. and Tarique, M., "A new Hierarchical Design for Wireless Ad hoc Network with Cross Layer Design" International Journal of Ad hoc and Ubiquitous Computing, Vol. 2, No. 1/2, pp. 31-35, 2007.

50. Zhongwei Zhang; , "An intelligent scheme of secure routing for mobile Ad hoc networks," *Signal Processing and Communication Systems, 2008. ICSPCS 2008. 2nd International Conference on* , vol., no., pp.1-6, 15-17 Dec. 2008.

51. Geetha Jayakumar and G. Gopinath; "Performance Comparison of Two On-demand Routing Protocols for Ad hoc Networks based on Random Way Point Mobility Model" American Journal of Applied Sciences 5 (6): ISSN 1546-9239, pp. 659-664, 2008.

52. Samyah Shah, Amit Khandre et al. "Performance Evaluation of Ad hoc Routing Protocols Using NS2 Simulation", In *Mobile and Pervasive Computing (CoMPC),* pp. 167-171, 2008.

53. Huapeng Wu; Shushan Zhao; Aggarwal, A.; Shuping Liu; , "A Secure Routing Protocol in Proactive Security Approach for Mobile Ad-Hoc Networks," *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE* , vol., no., pp.2627-2632, March/April 2008.

54. Ertaul, L., and Ibrahim, D., "Evaluation of Secure Routing Protocols in Mobile Ad hoc Networks (MANETs)", In *The 2009 International Conference on Security and Management SAM'09*, Las Vegas, July 2009.

55. Putta, C.S.R.; Prasad, K.B.; Ravilla, D.; Nath, R.S.M.; Chandra, M.L.R.; , "Performance of Ad hoc network routing protocols in IEEE 802.11," *Computer and Communication Technology (ICCCT), 2010 International Conference on* , vol., no., pp.371-376, 17-19 Sept. 2010.

56. Anuj Joshi1, Paa llavi Srivastava and Poonam Singh" Security Threats in Mobile Ad hoc Network" S-JPSET: ISSN: 2229-7111, Vol. 1, Issue 2, 2010.

57. V. Ramesh, Dr. P. Subbaiah, N. Koteswar Rao and M. Janardhana Raju, "Performance Comparison and Analysis of DSDV and AODV for MANET,"(IJCSE) International Journal on Computer Science and Engineering, vol. 02, pp. 183-188, 2010.

58. Agrawal, S., Jain, S. and Sharma. "A Survey of Routing Attacks and Security Measures in Mobile Ad hoc Networks", in *Journal of Computing*, Vol. 3 Issue 1, pp. 41-48, Jan. 2011.

59. Vijaya, I.; Mishra, P.B.; Dash, A.R.; Rath, A.K.; , "Influence of Routing Protocols in Performance of Wireless Mobile Adhoc Network,"*Emerging Applications of Information Technology (EAIT), 2011 Second International Conference on* , vol., no., pp.340-344, 19-20 Feb. 2011.

60. Das, A.; Basu, S.S.; Chaudhuri, A.; , "A novel security scheme for wireless adhoc network," *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on* , vol., no., pp.1-4, Feb. 28 2011-March 3 2011.

61. Al Mazrouei, M.S.; Narayanaswami, S.; , "Mobile adhoc networks: A simulation based security evaluation and intrusion prevention," *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for* , vol., no., pp.308-313, 11-14 Dec. 2011.

62. Farzad Sabahi, "The Security of Vehicular Adhoc Networks", In *Third International Conference on Computational Intelligence, Communication Systems and Networks,* IEEE 2011.

63. N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (visited 07-26-2012).

64. B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad hoc Networks," Department of Computer Science and Engineering, Florida Atlantic University, http://student.fau.edu/jchen8/web/papers/surveybookchapter.pdf (visited 07-29-2012)

65. Krishna Ramachandran. AODV-st. Technical Report, University of California, Santa Barbara, USA. http://www.cs.ucsb.edu/krishna/aodv-st/ (visited 08-06-2012)

66. V.B. Narsimha, "Comparison of Routing Protocols in Mobile Ad hoc Networks", In *Global Journal of Advanced Engineering Technologies*, Vol. 1, Issue 1, pp. 10-12, 2012.

67. Martha Steenstrup, "Routing in Communication Networks". Prentice Hall. ISBN 0-13-010752-2, http://books.google.ca/books?id=GfNSAAAAMAAJ&q=inauthor:%22Martha+E.+Steenstrup%22&dq=inauthor:%22Martha+E.+Steenstrup%22&source=bl&ots=2zTFlSZ5HD&sig=ZFPYPaInXPvBYDjJf0eAzBiF7hA&hl=en&sa=X&ei=5cgnULazOO6I6AHN2IGYDg&ved=0CDMQ6AEwAA (visited 07-29-2012).

68. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks**",** *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, pp. 12-23, ACM, Atlanta, GA, http://www.monarch.cs.rice.edu/monarch-papers/mobicom02.pdf (visited 07-23-2012).

69. NS-2, The NS Manual (formally known as NS Documentation) available at http://www.isi.edu/nsnam/ns/doc (visited 12-01-2012).

VITA AUCTORIS

Soke M. Onyemelukwe was born in the year 1983 in Nigeria. He received his Bachelor's Degree in Electrical and Electronic Engineering from Nnamdi Azikiwe University in 2005. He then went on to work as a Network Engineer for more than 3 years. He has industry recognition and hold certifications by both Cisco Systems Inc. and Microsoft Corporation as a Network Professional (Cisco Certified Internetwork Professional–CCIP, Cisco Certified Network Professional – CCNP and Microsoft Certified Information Technology Professional – MCITP). He is currently a candidate for the Master of Applied Science Degree in the Electrical and Computer Engineering Department at the University of Windsor and hopes to graduate in June 2013.