“ENHANCEMENT IN EVALUATION PARAMETERS OF WLAN”

DISSERTATION-II

Submitted in partial fulfillment of the

Requirement for the award of the

Degree of

MASTER OF TECHNOLOGY

IN

(ELECTRONICS AND COMMUNICATION ENGINEERING)

By

(PRINCECON BERA)

Under the Guidance of

ASSISTANT PROFESSOR VISHALI SHARMA

PROJECT SUPERVISOR

LOVELY PROFESSIONAL UNIVERSITY

PHAGWARA (DISTT. KAPURTHALA), PUNJAB

(School of Electronics and Communication Engineering)

Lovely Professional University

Punjab

DECEMBER 2014

DECLARATION

I, **PRINCECON BERA** student of B.TECH + M.TECH (DUAL DEGREE) under Department of ELECTRONICS AND COMMUNICATION ENGINEERING of Lovely Professional University, Punjab, hereby declare that all the information furnished in this dissertation report is based on my own intensive research and is genuine.

This thesis does not, to the best of my knowledge, contain any part of my work which has been submitted for the award of degree either of this university or any other university without proper citation.

Date:

PRINCECON BERA
(10904661)

CERTIFICATE

This is to certify that the Thesis titled "***SECURITY ENHANCEMENT FOR WLAN***" that is being submitted by " ***PRINCECON BERA***" is in partial fulfillment of the requirements for the award of **MASTER OF TECHNOLOGY DEGREE**, is a record of bonafide work done under my /our guidance. The contents of this Thesis, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

Vishali Sharma
Assistant Professor
School of Electronics and Communication Engineering
Lovely Professional University
Phagwara, Punjab.

Date:

OBJECTIVES OF THE PROJECT

1. Extensible Authentication Protocol, or EAP, is a universal authentication framework frequently used in wireless networks and Point-to-Point connections.
2. It is defined by RFC 3748. Although the EAP protocol is not limited to wireless LANs and can be used for wired LAN authentication, it is most often used in wireless LANs.
3. To limit the time hopping distance to a limit and make it lesser as possible.
4. EAP provides a security authentication by sending the user a key to verify the key form the back end database for further secure transmission.
5. To find out the shortest path from source to destination to save time.

ACKNOWLEDGEMENT

I hereby take this opportunity to thank all people whose knowledge and experience helped me to bring this report in its present form. It would have been almost a Herculean task for me to compile this report without their help.

I express my sincere thanks and gratitude to **Assistant Professor Vishali Sharma, SECE, LPU** , **Dr. Anil Kumar Mishra (Sc. 'F', Joint Director and HOD), DCRS Deptt. INMAS** , **Assistant Professor Nikesh Bajaj, HOD, SECE, LPU** for coordinating this project and training and giving me an invaluable opportunity to work in a competitive yet amicable atmosphere and providing me with all facilities and paraphernalia required to carry out this project. They made learning so easy that it never seemed that I was new for the whole thing. It was always a new and unique experience working with him.

I strongly record my deep sense of gratitude and thankfulness with utmost respect to **Dr. Abhinav Mittal (Deptt. Of Clinical PET, INMAS)** for providing me valuable data for my project.

I would like to express my gratitude towards **Mr. Lokendra Singh (Senior Tech. Assistant)** for his worthwhile suggestions ever willing and fruitful guidance and also for all knowledge they imparted to me during the course of time.

I express my thanks to **Mr. Akhilesh Yadav (GE)** for his guidance in software and system support.

I am also thankful to all department members for providing me the same opportunity to work.

Finally I would like to express my deep appreciation to **my family and friends** who have been a constant source of inspiration. I am eternally grateful to them for always encouraging and being with me wherever and whenever I needed them.

PRINCECON BERA

ABSTRACT

This work is study of analyze and improve the security of the efficient password-based authentication protocol that has been proposed recently in the Australasian Conference on Information Security and Privacy (ACISP) 2003 and to enhance the parameters of the connection i.e throughput, BER, energy conservation etc. The Extensible Authentication Protocol (EAP) is best considered as a framework for transporting authentication protocols, rather than as an authentication protocol itself. EAP can be used for authenticating dial-up and VPN connections, and LAN ports in conjunction with IEEE 802.1X.The distinct idea is to utilize two generators of a certain cyclic group for efficiency, while the protocol is vulnerable to the server compromise attack on the contrary to the original assumption. The Extensible Authentication Protocol (EAP) is best considered as a framework for transporting authentication protocols, rather than as an authentication protocol itself. EAP can be used for authenticating dial-up and VPN connections, and LAN ports in conjunction with IEEE 802.1X. An ad hoc network forms when a collection of mobile nodes join and create a network by agreeing to route messages for each other. There is no shared infrastructure in an ad hoc network, such as centralized routers or defined administrative policy. All proposed protocols have many security vulnerabilities like Denial of Service attacks and exposures that easily allow for routing attacks. While these vulnerabilities are very common to many protocols, we are focusing on two protocols that are under consideration by the IETF for standardization. This work / analysis is based on the scanning and sniffing of the data transmission of the packets transferred in a particular time period and will show how secure will be the data transmission when we provide a change in the algorithm or the hash key of the protocol.

LIST OF FIGURES

Figure No.	Name of Figure	Page No.
Fig. 1.1	(a) A simple ad hoc network. (b) Another example ad hoc network	13 13
Fig. 1.2	Static string Topology	14
Fig. 1.3	Different Types of Attacks	
Fig. 1.4	The Architecture of DNS	
Fig. 1.5	Taxonomy of AODV protocol vulnerability	21
Fig. 2.1	Summary of the proposed architectures for the 3GPP-WLAN interworking	26
Fig. 2.2	Simulation results for the different TCP versions as a function of SER for mode #2	29
Fig. 2.3	Simulation results for the different TCP versions as a function of the Eb/No (reference value for BPSK) for fixed modes 1 and 2; the maximum 95% confidence interval amplitude for all the curves is +7%.	29
Fig. 2.4	Representation of the famous Man-in-the-middle attack for both wired and wireless networks	
Fig. 4.1	Proposed System Architecture	33
Fig. 4.2	Proposed Internal System Architecture	33
Fig. 4.3	Flow Chart for Adding a New tcl file and compiling it in NS2	31
Fig. 4.4	Logical design of the encryption/decryption system	
Fig. 4.5	NS2 Simulation for Shortest Path	35

LIST OF ABBREVIATIONS

PHY	Physical Layer
MAC	Medium Access Control
NET	Network Layer
ACISP	Australasian Conference on Information Security and Privacy
IETF	Internet Engineering Task Force
AODV	Ad Hoc On Demand Distance Vector
DSR	Dynamic Source Routing
IP	Internet Protocol
NAR	Normalized Acceptance Rates
ZRP	Zone Routing Protocol
TORA	Temporally Ordered Routing Algorithm
CA	Certification Authority
MANET	Mobile Ad Hoc Network
RWP	Random Way Point
RPGM	Random Point Group Mobility
RREQ	Route Request
RREP	Route Relay Packet
IEEE	Institute of Electricals and Electronics Engineers
CTS	Clear to Send
RTS	Request to Send
GPS	Global Positioning System
QOS	Quality of Service
LAN	Local Area Network
WLAN	Wireless Local Area Network
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service
WEP	Wired Equivalency Privacy
ETSI	European Telecommunication Standard Institute
BRAN	Broadband Radio Access Networks
CCF	Charging Collection Function
SEAD	Secure Efficient Ad hoc Distance vector routing protocol

CPU	Central Processing Unit
GPU	Generic Processing Unit
RFID	Radio Frequency Identification
TID	Tag Identification
PRNG	Pseudorandom Number Generator
CRC	Cyclic Redundancy Code
EPC	Effective Passive Clusturing
OSI	Open Systems Interconnection
SACK	Selective Acknowledgement
TCP	Transmission Control Protocol
ACK	Acknowledgement Number
WMM	Wi-Fi Multimedia
USB	Universal Serial Bus
RMS	Root Mean Square
RF	Radio Frequency
PSE	Power Sourcing Equipment
PoE	Power Over Ethernet
PDA	Personal Digital Assistant
PD	Powered Device
PCMCIA	Personal Computer Memory card International Association
PCI	Peripheral Component Interconnect
DCF	Distributed Coordination Function
DNS	Domain Name System
IDS	Intrusion Detection System
ANS	Authorities Name Server

TABLE OF CONTENTS

LIST OF FIGURES……………………………………………………vi to vii

LIST OF ABBREVIATIONS…………………………………………viii to ix

1 Introduction………………………………………………………………………..........13

1.1 WLAN…….………………………………………………………………………..13

1.2 EAP Protocol…………………..…….………………………………………………..14

1.3 Access Control and Authentication..……...……………………………………………15

1.4 Key Management Service……………….…...…………………………………………..17

1.5 EAP Security Issues…………………………...….…………………………………..18

1.6 Security And Node Cooperation……………...…………………………………………18

1.7 Cooperation in Wireless LAN Networks…………...……………………………………...19

1.8 Merging Network……………………………….…………………………………….20

1.9 Access Control...................………………………….……………………………….21

1.10 Internal v/s External Attack……………………….…………………………….....22

1.11 Denial of Service…………………………………………………………………..…23

1.12 Spoofing……………………………………………………………………………...23

1.13 Gray Hole Attack………………………………………………………………………..24

2 Literature Survey……………………………………………………………………………..26

2.1 Improvements in wireless network technology…………………………….………….26

2.1.1 Topology of the network and Sensor Model……………………………………...27

2.1.2 Enabling Technologies………………………………………………………...28

2.1.3 Conclusion and Learning Outcomes………………………………….…….28

2.2 Multipath Routing in Mobile Ad Hoc Networks………………………………….…...28

2.3 Security Aspects of 3G-WLAN…………………………………………………….…….29

2.4 SEAD……………………………………………………………………………………..30

2.5 Gen2-Based RFID Authentication Protocol…………………………………….……...31

2.6 Mobile Ad Hoc Network are Self Configuring Network…...…………………….……32

2.7 Security Alogorithm Towards Secure Communication…………………………………32

2.8 Cross Layer Design Challenges……………………………………………………….33

2.9 Security Overview of Wireless LAN……………………………………………………34

2.10 SSL-TLS Based Authentication for WLAN-3G Internetworking……………………….35

2.11 Spoof Detection for Preventing DOS…………………………………………………...37

3 Research Methodologies……………………………………………………………………..38

3.1 Quality of Service……………………………………………………………………….38

3.2 Denial of Service………………………………………………………………………..38

3.3 Power Consumption……………………………………………………………………..38

3.4 Secure Transmission……………………………………………………………………..39

3.5 BER……………………………………………………………………………………...40

3.6 Different Methodologies/Approaches…………………………………………………..40

3.7 Challenges Faced by Mobile ADHOC Networks……………………………………41

3.7.1 Routing…………………………………………………………………………..41

3.7.2 Mobility…………………………………………………………………………41

3.7.3 Bandwidth Constraint…………………………………………………………41

3.7.4 Hidden and Exposed Terminal Problems…………………………………………..42

3.7.5 Channel Access…………………………………………………………………42

3.8 Analysis of Method……………………………………………………………………...42

3.8.1 CISCO Packet Tracer……………………………………………………………..42

3.8.2 Protocol Used……………………………………………………………………..42

3.8.3 Network Simulator-2……………………………………………………………...43

4 Approach of the Project………………………………………………………………………44

4.1 Flow Chart……………………………………………………………………………44

4.2 Virtual Scenario and Configuration……………………………………………………...45

4.3 Hash Function……………………………………………………………………………45

4.3 Programming Steps……………………………………………………………………...

REFERENCES………...36

BIO DATA…………………………………………………………………………………..38

CHAPTER 1

1 INTRODUCTION

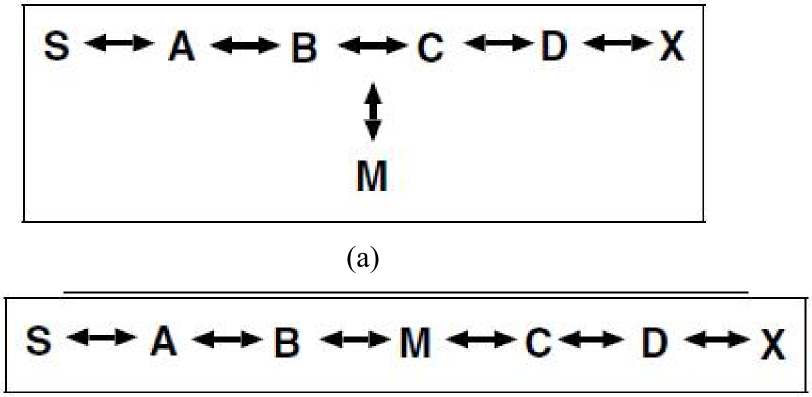
1.1 WLAN

Wireless computing is a rapidly emerging technology providing users with network connectivity without being tethered off a wired network. Wireless local area networks (WLANs), like their wired counterparts, are being developed to provide high bandwidth to users in a limited geographical area. WLANs are being studied as an alternative to the high installation and maintenance costs incurred by traditional additions, deletions, and changes experienced in wired LAN infrastructures. Physical and environmental necessity is another driving factor in favor of WLANs. Typically, new building architectures are planned with network connectivity factored into the building requirements. However, users inhabiting existing buildings may find it infeasible to retrofit existing structures for wired network access. Examples of structures that are very difficult to wire include concrete buildings, trading floors, manufacturing facilities, warehouses, and historical buildings. Interference in wireless communications can be caused by simultaneous transmissions (i.e., collisions) by two or more sources sharing the same frequency band. Collisions are typically the result of multiple stations waiting for the channel to become idle and then beginning transmission at the same time. Collisions are also caused by the "hidden terminal" problem, where a station, believing the channel is idle, begins transmission without successfully detecting the presence of a transmission already in progress. Interference is also caused by multipath fading, which is characterized by random amplitude and phase fluctuations at the receiver. The reliability of the communications channel is typically measured by the average bit error rate (BER). Devices connected to a wired network are powered by the local 110 V commercial power provided in a building. Wireless devices, however, are meant to be portable and/or mobile, and are typically battery powered. Therefore, devices must be designed to be very energy-efficient resulting in "sleep" modes and low-power displays, causing users to make cost versus performance and cost versus capability trade-offs. The capacity of WLANs should ideally approach that of their wired counterparts. However, due to physical limitations and limited available bandwidth, WLANs are currently targeted to operate at data rates between 1–20 Mb/s. To support multiple transmissions simultaneously, spread spectrum techniques are frequently employed. Currently, there are two emerging WLAN standards: the European Telecommunications Standards Institute (ETSI) High-Performance European Radio LAN (HIPERLAN) and the IEEE 802.11 WLAN. Both draft standards cover the physical layer and medium access control (MAC) sublayer of the open systems interconnection (OSI) seven-layer reference model. The

HIPERLAN committee has identified the 5.15–5.30 GHz and 17.1–17.2 GHz bands for transmission. The Conference of European Postal and Telecommunications Administrations (CEPT) have ratified the 5 GHz band for HIPERLAN use. Data rates up to 23.529 Mb/s are projected, and multihop routing, time-bounded services, and power-saving features are expected

1.2 EAP PROTOCOL

In EAP, the party demanding authentication is called the authenticator and the party being authenticated is called the supplicant. The EAP protocol defines four types of packet: request, response, success and failure. Request packets are issued by the authenticator, and solicit a response packet from the supplicant. Any number of request-response exchanges are permitted to complete the authentication. If the authentication is successful, a success packet is sent to the supplicant; if not, a failure packet is sent. The basic EAP packet format is simple. A type field indicates the type of packet, such as a response or a request. An Identifier field is used to match requests and responses. Response and request packets have two further fields. The first, confusingly called type, indicates the type of data being transported (such as an authentication protocol), and the second, type-data, consists of that data. Note that EAP method is anonymous with type, and both are used frequently. The EAP specification defines three 'basic' authentication EAP types (MD5-Challenge, OTP and GTC) and three non-authentication types (Identity, Nak, and Notification). The three 'basic' authentication types are not considered secure for typical use, particularly in wireless environments, and consequently other types, which will be discussed later, should be used. If the supplicant Naks a proposed type, the authenticator may choose to try another, thereby allowing supplicant and authenticator to negotiate a mutually acceptable authentication protocol. The Notification type, which is rarely used, returns a message that must be displayed to the user.



(a)

(b)

Fig 1.1 (a) A simple ad hoc network. (b) Another example ad hoc network.

There is a consideration of a finite population of N nodes (e.g., students on a campus). Each node, depending on its type (e.g., laptop, cell phone etc) is associated with an average power constraint. This constraint can be derived by dividing its initial energy allocation by its lifetime expectation. I have assumed that time is slotted and that each session lasts for one slot. We deal with connection-oriented traffic. At the beginning of each slot, a source, destination and several relays are randomly chosen out of the N nodes to form an ad hoc network (e.g., students in a coffee shop). The source requests the relay nodes in the route to forward its traffic to the destination. If any of the relay nodes rejects the request, the traffic connection is blocked. For each node, we define the Normalized Acceptance Rate (NAR) as the ratio of the number of successful relay requests generated by the node, to the number of relay requests made by the node. This quantity is an indication of the throughput experienced by the node. Then, we study the optimal tradeoff between the lifetime and Normalized Acceptance Rates of the nodes. In particular, given the energy constraints and the lifetime expectation of the nodes, we identify the feasible set of Normalized Acceptance Rates. This provides us with a set of Pareto optimal values, i.e., values of Normalized Acceptance Rates such that a node cannot improve its Normalized Acceptance Rates without decreasing some other node's Normalized Acceptance Rates. By assuming the nodes to be rational, i.e., that their actions are strictly determined by self-interest. The principle behind ad hoc networking is multi-hop relaying in which messages are sent from the source to the destination by relaying through the intermediate hops (nodes). In multi-hop wireless networks, communication between two end nodes is carried out through a number of intermediate nodes whose function is to relay information from one point to another. A static string topology is an example of such network.

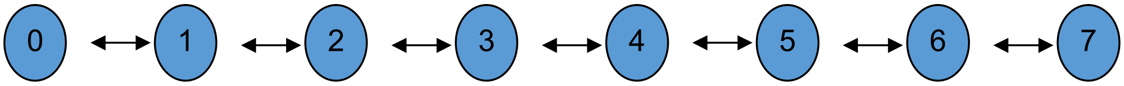


Fig 1.2 Static string Topology

1.3 ACCESS CONTROL AND AUTHENTICATION

A secure routing algorithm always prevents each of the following exploits;

1. Attacks Using Fabrication;

2. Attacks Using Impersonation;

3. Attacks Using Modification;

Extending access control, especially to the wireless world, means a more finely grained authorization; for example, you can allow access to the network and its resources for internal employees and allow Internet access for guests. Employees are also working on federations, so access can be allowed based on the entity's membership in identity federations—for example, intercollege access to researchers, interorganization access based on collaboration on certain projects, and other similar groups and roles.

1. Routing signal can never be spoofed;

2. Fabricated routing messages can never be injected into the network;

3. Routing messages can never be altered in transit, except the signal according to the normal functionality of the routing protocol;

4. Routing loops can never be formed through any malicious action of any software or by any other aspects;

5. Routes cannot be redirected from the shortest path by malicious action. The above requirements comprise the security needs of an open environments. The following additional requirement distinguishes a managed open environment;

6. Unauthorized nodes should be excluded from route computation and discovery.

This requirement does not preclude the fact that authenticated peers may act maliciously as well. Additionally, we assume that the managed-open environment has the opportunity for pre-deployment or exchange of public keys, session keys, or certificates. To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. Routing protocols proposed for ad hoc networks cope well with the dynamically changing topology. However, none of them, to our knowledge, have accommodated mechanisms to defend against malicious attacks. Routing protocols for ad hoc networks are still under active research. There is no single standard routing protocol. Therefore, we aim to capture the common security threats and to provide guidelines to secure routing protocols. In most routing protocols, routers exchange information on the topology of the network in order to establish routes between nodes. Such information could become a target for malicious adversaries who intend to bring the network down. There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce excessive traffic load into the network by causing retransmission and inefficient routing. The second and also the more severe kind of threats comes from compromised nodes, which might advertise incorrect routing information to other nodes. Detection of such incorrect information is difficult: merely requiring routing information to be signed by each node would not work, because compromised nodes are able to generate valid signatures using their private keys. To defend against the first kind of threats, nodes can protect routing information in the same way they protect data traffic, i.e., through the use of cryptographic schemes such as digital signature. However, this 3 defense is ineffective against attacks from compromised servers. Worse yet, as we have argued, we cannot neglect the possibility of nodes being compromised in an ad hoc network. Detection of compromised nodes through routing information is also difficult in an ad hoc network because of its dynamically changing topology: when a piece of routing information is found invalid, the information could be generated by a compromised node, or, it could have become invalid as a result of topology changes. It is difficult to distinguish between the two cases. On the other hand, we can exploit certain properties of ad hoc networks to achieve secure routing. Note that routing protocols for ad hoc networks must handle outdated routing information to accommodate the dynamically changing topology. False routing information generated by compromised nodes could, to some extent, be considered outdated information. As long as there are sufficiently many correct nodes, the routing protocol should be able to find routes that go around these compromised nodes. Such capability of the routing protocols usually relies on the inherent redundancies — multiple, possibly disjoint, routes between nodes — in ad hoc networks. If routing protocols can discover multiple routes (e.g., protocols in ZRP, DSR, TORA, and AODV all can achieve this), nodes can switch to an alternative route when the primary route appears to have failed. Diversity coding takes advantage of multiple paths in an efficient way without message retransmission. The basic idea is to transmit redundant information through additional routes for error detection and correction. For example, if there are n disjoint routes between two nodes, then we can use n - r channels to transmit data and use the other r channels to transmit redundant information. Even if certain routes are compromised, the receiver may still be able to validate messages and to recover messages from errors using the redundant information from the additional r channels.

1.4 KEY MANAGEMENT SERVICE [4]

Employing cryptographic schemes, such as digital signatures, to protect both routing information and data traffic. Use of such schemes usually requires a key management service. It can be done by adopting a public key infrastructure because of its superiority in distributing keys and in achieving integrity and non-repudiation. Efficient secret key schemes are used to secure further communication after nodes authenticate each other and establish a shared secret session key. In a public key infrastructure, each node has a public/private key pair. Public keys can be distributed to other nodes, while private keys should be kept confidential to individual nodes. There is a trusted entity called Certification Authority (CA) for key management. The CA has a public/private key pair, with its public key known to every node, and signs certificates binding public keys to nodes. The trusted CA has to stay on-line to reflect the current bindings, because the bindings could change over time: a public key should be revoked if the owner node is no longer trusted or is out of the network; a node may refresh its key pair periodically to reduce the chance of a successful brute-force attack on its private key. It is problematic to establish a key management service using a single CA in ad hoc networks. The CA, responsible for the security of the entire network, is a vulnerable point of the network: if the CA is unavailable, nodes cannot get the current public keys of other nodes or to establish secure communication with others. If the CA is compromised and leaks its private key to an adversary, the adversary can then sign any erroneous certificate using this private key to impersonate any node or to revoke any certificate. A standard approach to improve availability of a service is replication. But a naive replication of the CA makes the service more vulnerable: compromise of any single replica, which possesses the service private key, could lead to collapse of the entire system.

1.5 EAP SECURITY ISSUES

In general, EAP is a standard that provides an infrastructure for network access clients and authentication servers. EAP does not specify the authentication mechanism itself but the way it is negotiated by the communicating parties. Consequently, EAP has no security issues in itself. Several EAP implementations are vulnerable to dictionary attacks As a consequence of this vulnerability, Cisco developed EAP-FAST to provide better protection against dictionary attacks. However, EAP-FAST is vulnerable to MitM attacks. EAP-GSS is another example of an EAP implementation vulnerable to dictionary attacks. GSS relies on the Kerberos protocol, which is itself vulnerable to dictionary attacks. EAP implementations that rely on clear-text authentication using RADIUS (even within a protected tunnel) are vulnerable to known-plaintext attacks EAP-IKE2 and EAP-TTLS are examples of EAP implementations that may use password-based authentication (PAP) and therefore are vulnerable to this type of attacks . In PAP-based authentication, passwords are transmitted unencrypted. Another EAP implementation vulnerable to MitM attacks is EAP-FAST, the protocol Cisco developed as replacement for LEAP. EAP-FAST was designed to address the vulnerabilities of LEAP while keeping its simplicity and economy.

1.6 SECURITY AND NODE COOPERATION

As the wireless medium is vulnerable to many other attacks and to the eavesdropping attacks. Ad hoc network facility the mobile ad hoc networks intrinsically exposed to internal attacks also known as active attacks. There should be an algorithm/protocol which needs to verify each and every connection between any two nodes before sharing any data so that the data loss/data stealing by the external user should be at least at its highest possibility. Secure communication has an important aspect of any networking environment, and is specially a significant challenge in ad hoc networks. The MANET paradigm seeks to enable communication across networks whose topology and membership change frequently. The main and distinctive feature in secure transmission is that the network nodes needs to collaborate on a peer to peer basis to support network functionality. This is so because every node needs to involve/participate in network functionality so that which is the basic reason every node is not only entitled but also in fact is required to assist in network operation, network establishment and network maintenance. The communication in a LAN network comprises of two phases i.e data transmission and route discovery. Likely, in an adverse environment both the phases are vulnerable to different type of attacks, which could be either active or passive. Moreover in a volatile communication

1.7 COOPERATION IN WIRELESS LAN NETWORKS

Wireless LAN have matured as a viable means to provide ubiquitous untethered communication. In order to enhance network connectivity, a source communicates with far off destinations by using intermediate nodes as. However, the limitation of finite energy supply raises concerns about the traditional belief that nodes in ad hoc networks will always relay packets for each other. Consider a user in a campus environment equipped with a laptop. As part of his daily activity, the user may participate in different ad hoc networks in classrooms, the library and coffee shops. He might expect that his battery-powered laptop will last without recharging until the end of the day. When he participates in these different ad hoc networks, he will be expected to relay traffic for other users. If he accepts all relay requests, he might run out of energy prematurely. Therefore, to extend his lifetime, he might decide to reject all relay requests. If every user argues in this fashion, then the throughput that each user receives will drop dramatically. We can see that there is a trade-off between an individual user's lifetime and throughput. Cooperation among nodes in an ad hoc network has been previously addressed in. In nodes, which agree to relay traffic but do not, are termed as misbehaving. Clever means to identify misbehaving users and avoid routing through these nodes are proposed. Their approach consists of two applications: *Watchdog* and *Pathrater*. The former runs on every node keeping track of how the other nodes behave; the latter uses this information to calculate the route with the highest reliability. In a secure mechanism to stimulate nodes to cooperate and to prevent them from overloading the network is presented. The key idea is that nodes providing a service should be remunerated, while nodes receiving a service should be charged. Based on this concept, an acceptance algorithm is proposed. The acceptance algorithm is used to decide whether to accept or reject a packet relay request. The acceptance algorithm at each node attempts to balance the number of packets it has relayed with the number of its packets that have been relayed by others. The drawback of this scheme is that it involves per packet processing which results in large overheads. In two acceptance algorithms are proposed, which are used by the network nodes to decide whether to relay traffic on a per session basis. The goal of these algorithms is to balance the energy consumed by a node in relaying traffic for others with energy consumed by other nodes in relaying traffic and to find an optimal trade-off between energy consumption and session blocking probability. By taking decisions on a per session basis, the per packet processing overhead of previous schemes is eliminated. We emphasize, however, that all the above algorithms are based on heuristics and lack a formal framework to analyze the optimal trade-off between lifetime and throughput.

1.8 MERGING NETWORK

WLAN network is the infrastructure less mobile network which has no fixed gateways (routers). All nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network. Example applications of ad hoc networks are emergency search-and rescue operations, meetings or conventions in which folks wish to quickly share information, and data acquisition operations in inhospitable terrain. A Mobile Ad hoc NETwork (MANET) is an autonomous system of self-organized mobile nodes without relying on any infrastructure. Node mobility is one of the inherent characteristics of MANET. It is also one of the parameters that most critically affect the performance of network protocols (e.g., routing). Conventional mobility models proposed for MANET can be classified into two categories: Entity models and Group models. Entity models are used to represent the movement of an individual mobile node. One such model is the Random WayPoint mobility (RWP) model; perhaps the most popular mobility model used in the literature. Because entity models cannot reflect the interaction between MNs, group mobility models are proposed. A typical group mobility model is the Reference Point Group Mobility (RPGM) model. The shortcoming of conventional models is that they fail in modelling scenarios where groups may be partitioned and merged; these are most likely to be found in ad hoc networks. With AODVR, a source node that wants to send a message to a destination for which it does not have a route broadcasts an RREQ [4] packet across the network. All nodes receiving this packet update their information for the source node. Thus, unlike DSR, this approach does not use route caching. Instead, each node maintains only the next hop’s address in a routing table, and these routing tables are updated all the way along the RREQ propagation path. The RREQ [4] contains the source node’s address, broadcast ID, and current sequence number as well as the destination node’s most recent sequence number. Nodes use these sequence numbers to detect active routes. A node that receives an RREQ [4] can send an RREP [4] if it either is the destination or has a route to the destination with a corresponding sequence number greater than or equal to the sequence number the RREQ [4] contains. In the latter case, the node returns an RREP [4] to the source with an updated sequence number for that destination; otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ [4] source address and broadcast ID, discarding any RREQ they have already processed. As the RREP [4] propagates back to the source, nodes set up entries to the destination in their routing tables. The route is established once the source node receives the RREP. This algorithm also includes route maintenance facilities. For every route in a routing table, a host maintains a list of neighboring nodes using that route and informs them about potential link breakages with RERR messages. Each node also records individual routing table entries and deletes those not used recently.

1.9 ACCESS CONTROL

The access control is an applicable concept also within ad hoc networking, as there usually exist a need for controlling the access to the network and to the services, it provides. Moreover, as the networking approach may allow or require the forming of groups in for instance network layer, several access control mechanisms working in parallel may be needed. In the network layer the routing protocol must guarantee that no authorized nodes are allowed to join the network or a packet forwarding group such as the clusters in the hierarchical routing approach. For example in the battlefield example of the introduction the routing protocol the ad hoc network applies must control so that no hostile node can join and leave the group undetectable from the viewpoint of the other nodes in the group. In application level, the access control mechanism must guarantee that unauthorized parties cannot have accesses to services, for instance the vital key management service. Access control is often related to the identification and authentication. The main issue in the identification and authentication is that the parties can be confirmed to be authorized to gain the access. In some systems, however, identification or authentication of nodes is not required: nodes may be given e.g. delegate certificates with which the nodes can gain access to services. In this case actual authentication mechanisms are not needed, if the nodes are able to present adequate credentials to the access control system. In some ad hoc networks, services may be centralized, while in other networks they are applied in a distributed manner, which may require the use of different access control mechanisms. Moreover, the required security level in access control also affects the way the access control must be implemented. If a centralized ad hoc networking approach with low security requirements is applied - as in the classroom example - the server party with simple means such as user id - password scheme, can manage the access control. In ad hoc network that operate in more difficult conditions without any centralized resources as in the battlefield scenario, the implementation of access control is much more difficult. Either the access to the network, its groups and resources must be defined when the network is formed, which is very inflexible. The other possibility is to define and use a very complex, scalable and dynamic access control protocol, which brings flexibility but is prone to various kinds of attacks and it may even be impossible to apply properly and efficiently.

1.10 INTERNAL V/S EXTERNAL ATTACKS

Internal attacks leads directly on the links and the interfaces between any two nodes. Any external device, any third object, or any other individual does not do these. Internal attacks is based on three different parameters viz availability, authentication, integrity, non-repudiation. If it comes to availability if any one of the nodes is not available for receiving or transmitting any data then it is considered as an internal attack whereas in case of an authentication the node is not verifying the data that is trying to transmit the data it rejects its verification key. That can be considered as an internal attack. Now if I come to external attack the attacker is always aims to cause congestion, propagating fake routing information to the node or disturb the node from providing any kind of services. The attacks are further categorized as shown below.

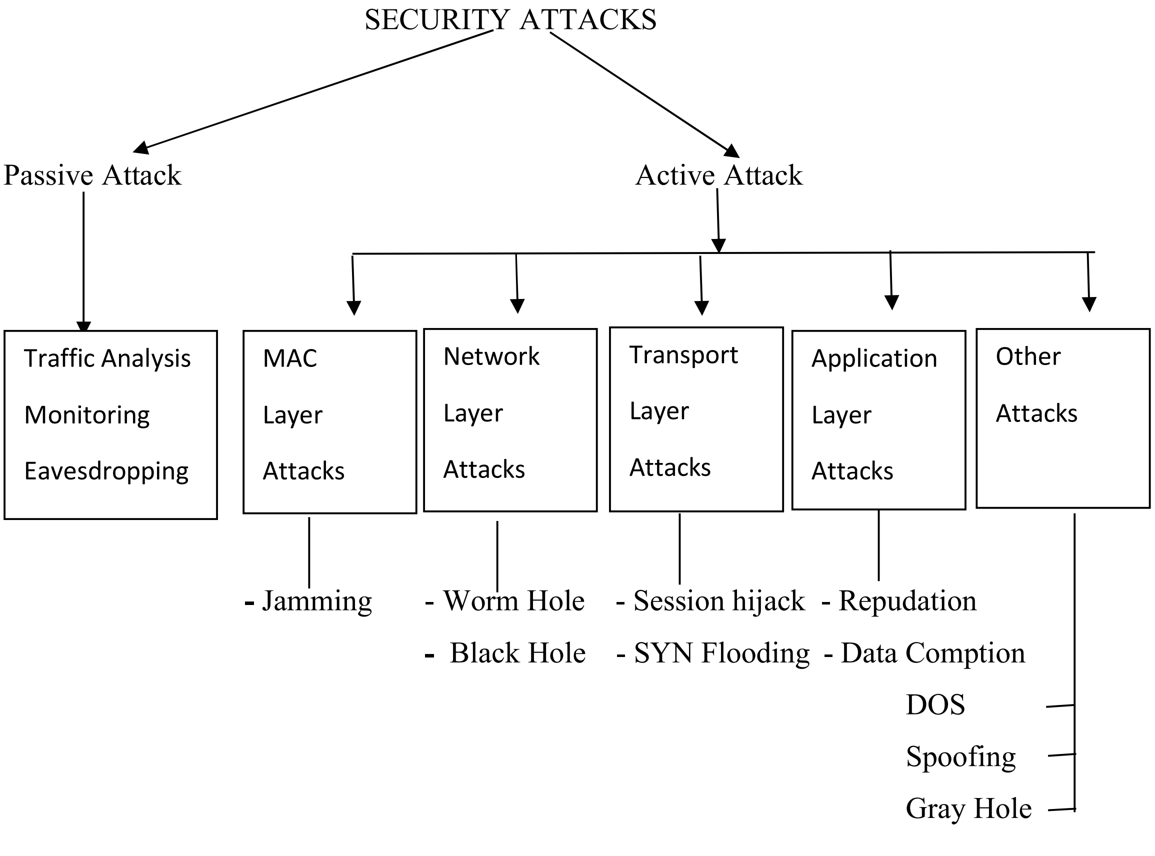


Fig 1.3 Different Types of Attacks

1.11 DENIAL OF SERVICE

Increasingly, network admins are seeking tools to assess end-user patterns and then notify them in the event anomalies occur that suggest a network attack: for example, logins attempted from a different location or by attempts to access different apps. The goal is contextual security that allows systems to sense when something's not right and take proactive steps to protect enterprise assets. There's a tendency among some IT professionals to believe that any technical problem can be solved with the right commercial product. Vendors call them solutions, after all. And at a time when some of the biggest members of the Fortune 500 are getting whacked with massive data breaches, there's a similar tendency to allow panic to override reason. That is why it's important to approach network security as not only a technology strategy because technology definitely plays a critical role but also as an operational one.

- 802.11 Control frames can be used to "busy out" a channel so that no other station can transmit. Entering this continuous transmit mode is known as a Queensland DoS attack.
- 802.11 Deauthenticate frames can be used to disconnect an individual station, or every station associated with a given AP. Sending a continuous stream of these forged frames is known as a Deauth Flood.
- 802.11 Associate frames consume AP resources by creating entries in the AP's association table. Flooding an AP with Associate frames from random station MAC addresses can make the AP too busy to service real users.
- Similar attacks can be launched using forged 802.1X packets -- for example, 802.1X EAP Logoff Flood, EAP Start Flood, and EAP-of-Death attacks.

1.11 SPOOFING

The Domain Name System (DNS) is a critical element of the Internet infrastructure. Even a small part of the DNS infrastructure being unavailable for a very short period of time could potentially upset the entire Internet and is thus totally unacceptable. Unfortunately, because DNS queries and responses are mostly UDP-based, it is vulnerable to spoofing-based denial of service (DoS) attacks, which are difficult to defeat without incurring significant collateral damage. The Domain Name System (DNS) is a critical component of the Internet infrastructure, because most network services and applications require a translation step from domain name to IP address to just send the packets out. As a result, even a small part of the DNS infrastructure being unavailable for a short period of time could have a significant rippling effect on the rest of the Internet. The other attack strategy is to exploit DNS servers to amplify attack traffic. The attacker crafts a DNS request that gets a response significantly larger than the request itself, e.g., a 50-byte request for a 500-byte response. The amplified response is replied to a spoofed third-party victim machine. Under this attack, both the amplifying DNS server's upstream bandwidth and the third-party machine's downstream bandwidth could be exhausted. Due to traffic amplification, an attacker can starve the bandwidth of its victims even if his bandwidth is 10 times smaller. An effective defense against spoofing-based DoS attacks on DNS servers requires source address spoof detection. Assuming a DNS server can distinguish between spoofed requests from real ones, it can selectively drop those spoofed ones with little collateral damage. If a DNS server is sure that the incoming requests use a genuine source IP address, it can use a rate-limiting strategy to drop packets in a fair way.

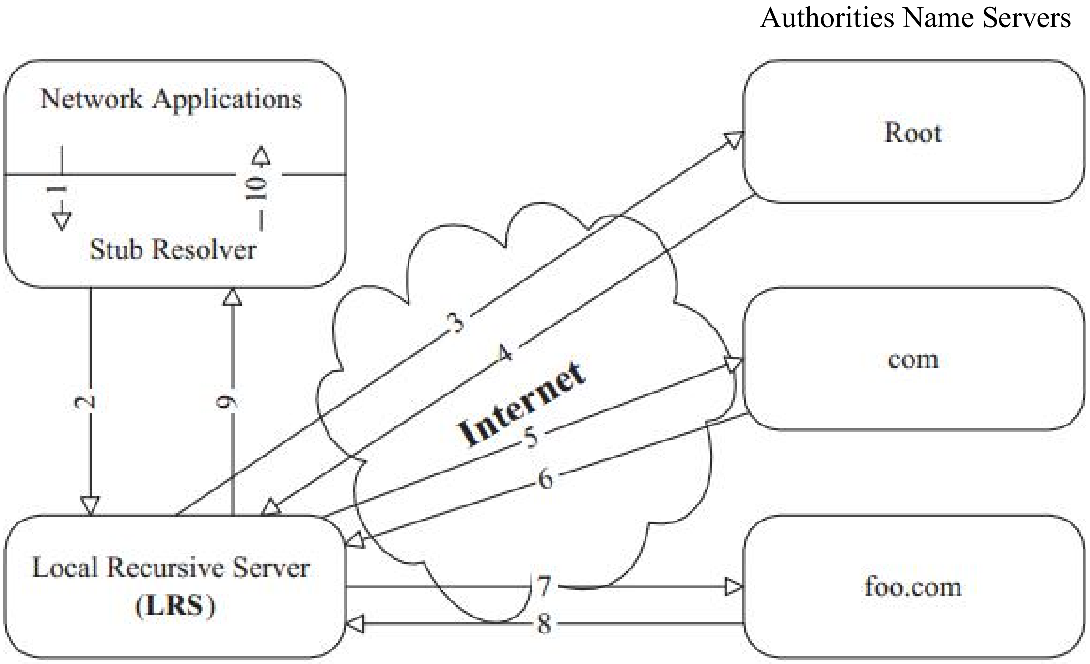


Fig 1.4 The Architecture of DNS

1.13 GRAY HOLE ATTACK

Mobile ad hoc networks are self-configuring network which are connected by the wireless links which forms a random and a different topology of mobile nodes. Topology of these networks changes rapidly and are not able to be predicted by anyone. Due to lack of infrastructure support each node acts as a router and any nodes can join and leave the network at any time. Providing security to these networks is a challenging issue because these type of networks suffer for various kinds of malicious attacks. One of the attacks, which are more difficult to detect in the Mobile ad hoc network, is Gray Hole attack. A Gray hole may exhibit its malicious behavior in various techniques. It simply drops packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Gray Hole node behaves like maliciously for some time duration by dropping packets but may switch to normal behavior later. A Gray hole may also exhibit a behavior, which is a combination of the above two, thereby making its detection even more difficult. For example, whenever the source node wants to transmit data to Destination node, the source node initially broadcasts a Route request (RREQ) packets to its neighbors in order to find a fresh route to the desired destination. The neighbor nodes subsequently checks to see in its routing table whether it is the destination or it has the route to destination. The route to the destination is indicated by the freshness of destination sequence number (Fig.3.) attached to it. The neighbor node thus checks whether it has a valid route to the destination. When the malicious node overhears this information it indicates that it has the fresh route to the destination (i.e., highest sequence number). The malicious node unicasts a RREP [4] (route reply) message back along the saved path to the source node. So the source node starts communicating through the path .But later the Gray Hole node drops the packets at a particular frequency. The Gray hole node does not drop all the packets coming to it. Either it may drop RREQ [4], RREP [4] packets.

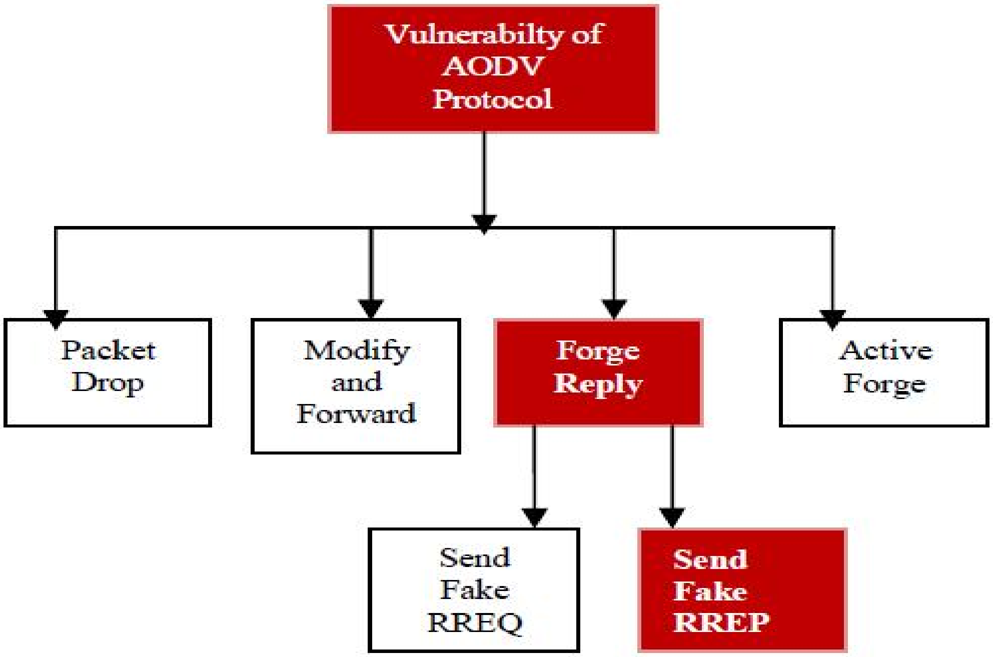


Fig 1.5 Taxonomy of AODV protocol vulnerability

CHAPTER 2

2 LITERATURE SURVEY

2.1 *Seapahn Meguerdichia*-[1]*, Farinaz Koushanfa*[1]*, Miodrag Potkonjak*[1] of University of California suggested in their IEEE research paper as published on 2011 that our personal computing era evolves into ubiquitous computing one, there is a need for a world of fully connected devices with inexpensive wireless networks. [1]Improvements in wireless network technology interfacing with emerging micro-sensor based on micro electro machines technology , is allowing sophisticated and inexpensive sensing, storage, processing, and communication capabilities to be unobtrusively embedded into our daily physical world. Different embedded web servers can be used to connect to the physical world of sensors and actuators and analyzers to the virtual world of information content, utilities and services. The increasing trend in research efforts in the areas referred to as Smart Spaces or Pervasive Computing are directly related to many problems in sensor networks. Although many researchers in the sensor network area have mentioned the critical motion of coverage in the network, according to their knowledge this is the first time that an algorithmic approach combined with computational geometry construction was adopted in ad-hoc sensor networks which has described a general systematic method for developing an advanced sensor network for monitoring the complex network systems such as those found in any nuclear power plant and any aviation bases where data transmission is effected due to the interference from the different mobile stations nearby but does not present any general coverage algorithm because no algorithm has been present in the security of ad Hoc networks which can prevent hundred percentage of security and provide no interference between any two nodes. [2]The Art Gallery as described in their paper is a problem that deals with determining the number of observers necessary to cover an art gallery room such that every point can be seen by at least one observer so to receive and send by enhancing the CTS(Clear To Send) and RTS(Request To Send). They have found several applications in many domains such as the optimal antenna placement problems for wireless communication. The Art Gallery problem was solved optimally in 2D and was shown to be NPhard in the 3D case proposes heuristics for solving the 3D case using Delaunay Triangulation [5]. Sensor coverage for detecting global ocean color where sensors observe the distribution and abundance of oceanic phytoplankton is approached by assembling and merging data from different satellites at different earth stations at different orbits. One of the fundamental issues that arises in sensor networks, in addition to the location calculation, tracking, and deployment, is coverage. Due to the large variety of sensors and applications, coverage is subject to a wide range of interpretations. In general, coverage can be considered as the measure of quality of service of a sensor network. For example, in the previous fire detection sensor networks example, one may ask how well the network can observe a given area and what the chances are that a fire starting in a specific location will be detected in a given time frame. Coverage formulations can be implemented to find weak points in a sensor field and suggest any future deployment or reconfiguration schemes for improving the overall quality of service in the data transmission. In most sensor networks, two seemingly and contradictory, yet related viewpoints of coverage exist: worst and best case coverage. In worst-case coverage, attempts are made to quantify and quantize the quality of service by finding areas which are of lower observability from sensor nodes and detecting the breach regions. In best-case coverage, we will find the areas of high observability from sensors and identify the best support and guidance regions which are of primary concern. Our main objective is the design of robust, efficient and scalable algorithms which is to be used in wireless sensor and multi-sensor integration. From the conceptual and algorithmic point of view, the main contribution which has been provably optimal polynomial time algorithm for coverage in sensor networks. We will now combine existing computational geometry techniques and constructs such as the Voronoi diagram[1], with graph theoretical algorithmic techniques. The use of Voronoi diagram, efficiently and without loss of optimality, transforms the continuous geometric problem into a discrete graph problem. Furthermore, it enables direct application of search techniques in the resulting graph representation.

2.1.1 Topology of the network and Sensor Model

Generally, wireless sensor networks are always been targeted to the extremes of miniaturization, availability, accuracy, reliability, and power savings. This requires a very networked infrastructure with small physical nodes, low power consumption, and low cost, that in turn limit the communications to the immediate proximity of each node. There are several existing models of sensor behavior each having different degrees of complexity. However, most of the models share only one thing in common in that is generally the sensing ability which is directly dependent on the distance between the sensor and the receiver/transmitter. Consequently, in all our subsequent discussions, we assume that sensor coverage decreases as distance from sensors increases.

2.1.2 Enabling Technologies: Sensor Location Technology and Algorithms

The idea of having a smarter way of keep a check on the environment has fostered a growing interest in the location aware systems and services. Obtaining a reliable information on the exact or the approximate location is an enabling component to many other location aware basic tasks in sensor networks such as coverage, tracking and mobility management. The geolocation with GPS is an unattractive solution due to cost, power, and accuracy constraints. Since our coverage algorithms rely on geolocation information, we have implemented the location procedure as the initial step before the coverage algorithm. In this geolocation approach, a few of the sensor nodes called beacons know their coordinates in advance, either from satellite information (GPS) or pre-deployment. The geolocation scheme then relies on signal strength information embedded in the inherent radio frequency communication capabilities of the nodes in approximating neighbor distances. Each node that can hear from a minimum of three beacon neighbors can determine its own location by trilateration and become a beacon. Iterative trilateration's are then used to locate as many nodes as possible.

2.1.3 Conclusion and Learning outcomes

Several interpretations and formulations of coverage in wireless ad-hoc sensor networks were presented. An optimal polynomial time algorithm that uses graph theoretic and computational geometry constructs was proposed for solving for best and worst case coverage's. Experimental results show several applications of the theoretic coverage formulations and algorithms specifically for solving for Maximal Breach Path, Maximal Support Path, and additional sensor deployment heuristics to improve coverage, and stochastic field coverage.

2.2 *Stephen Mueller, Rose P. Tsang, and Dipak Ghosal Department of Computer Science, University of California, Davis, CA 95616* suggested a research paper on Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges which proposed that load balancing is of a special importance in MANETs because of the limited bandwidth between the two or more different nodes. Due to the limitation in the transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network. Routing protocols are like conventional wired networks which are usually based upon either distance vector or link state routing algorithms. Multipath routing has also been addressed in different data networks which are always been an intended to support connection-oriented service with QoS. In packet-oriented networks, like the internet the multipath routing could be also be used to alleviate congestion by using a congestion window by routing the different packets from highly utilized links to links which are less highly utilized. Dynamic topology is the topology in an ad hoc network may change constantly due to the mobility of nodes. As nodes move in and out of the range of each other, some links break down while the new links between the other nodes are created which comes in process. If the source does not have a route to the destination in its original route cache, then it broadcasts a different route request (RREQ) message specifying the destination node for which the route has already been requested. The learning outcome and the conclusion after reading this paper is found out to be that as packet drops increase due to congestion or degraded network conditions, enhancement layer packets are dropped at the source in favor of retransmitted base layer packets. Some ad hoc networks may contain some heterogeneous nodes, where some nodes are more reliable than other available nodes. For an instance, like in a battlefield, low powered sensors or the handhelds which may be deployed in the field, with high-powered, reliable, and secure nodes located in tanks or large vehicles which will be very much able and reliable to data transmission and receiving where we can be easily preventing any loss of the data.

2.3 *Geir M. Køien and Thomas Haslestad, Telenor R&D* [6]*, Norway* did a research on Security Aspects of 3G-WLAN Interworking and found out that WLAN systems are very great for hotspot and large area coverage, while 3G systems provide a global coverage to multi users and the necessary network and management infrastructure which cater the security, roaming, and charging requirements. WLAN on one side get high bit rates and hotspot coverage at a reasonable cost and on the Security-wise the interworking is mostly unproblematic, but there are areas which need to be identified that contain the weaknesses of WLAN. The present 2.5G systems like GSM/GPRS are capable of delivering IP services on a very valuable mode, but current cellular systems are still mostly used for speech services not for the long range data transmission and location tracking services. Third-generation (3G) systems will improve data capacity and offer data rates up to 2 Mb per second and above, but it is very unlikely that the user will be offered with the full theoretical capacity since deployment cost is high and the present chips and IC’s are not available in such a way to receive large amount of data in a particular time span or time slot. This is in contrast to the wireless LANs (WLANs) [6], which provide affordable services and bit rates that easily exceed 3G/3.5G bit rates. IEEE Project 802.11 has provided with the current WLAN 802.11b [6] standard. 802.11b is the standard for 2.4 GHz which provides bit rates up to 11 Mb/s on a physical and application medium. IEEE 802.11 also has the different 802.11a standard which has a frequency for the 5 GHz band (UNII-band) that provides bit rates up to 54 Mb per second. The proposed scheme given by the IEEE 802.11b deploys confidentiality and integrity protection through a scheme called Wired Equivalency Privacy (WEP). This can be understood in a much better way in fig 4. The work in ETSI BRAN [6] resulted in two fundamentally different solutions regarding the level of interworking. The two solutions were termed tight and loose interworking according to the level of integration required between the systems. The work done in ETSI BRAN [6] resulted in the two different fundamental solutions in regarding the level of interworking used. The two solutions which were found were termed as tight and loose interworking according to the level of integration required between the systems.

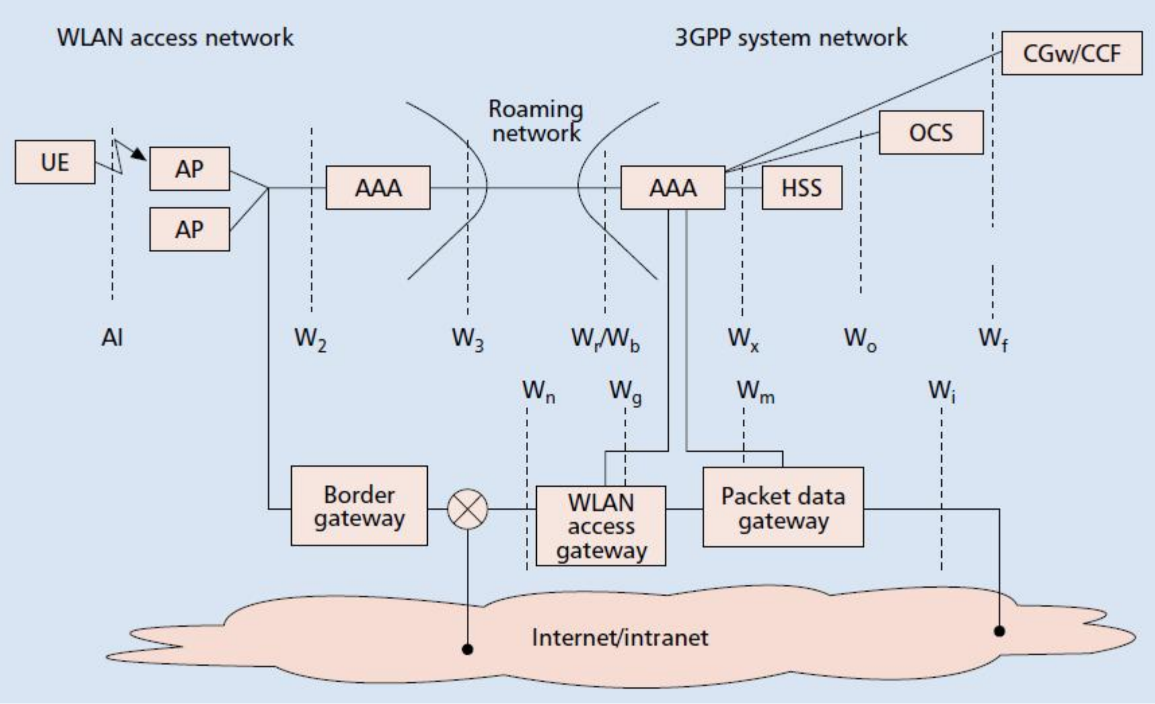


Fig 2.1 Summary of the proposed architectures for the 3GPP-WLAN interworking [6].

AI: Air interface as defined within [1–3]

W2: Defines the interface between the WLAN functions and the interworking functions

W3: Defines the interface between the interworking functions and the external network

Wr /Wb: The reference point connects the WLAN Access Network to the 3GPP network

Wx: This reference point provides communication between AAA infrastructure and HSS

Wn: For further study within 3GPP

Wg: An AAA interface between the 3GPP AAA proxy and the WAG. For provisioning of Information related to the routing enforcement functions for authorized users

Wo: This is used by a 3GPP AAA server to communicate with the online charging system (OCS) for charging related information

Wf: Provides communication between 3GPP AAA server and charging gateway function (CGF)/charging collection function (CCF) for charging information

Wi: Reference point between the packet data gateway and a packet data network (external public or private)

2.4 *Yih-Chun Hu, David B. Johnson, Adrian Perrig of Carnegie Mellon University, Pittsburgh, PA 15213, USA and Rice University, Houston, TX 77005, USA* did submitted their IEEE research paper on SEAD in 2003 which says that in order to support the use with nodes of limited CPU and GPU processing capability and to guard against Denial of Service attacks in which an attacker attempts to make the other nodes to always consume the excessive or extra network bandwidth or the extra processing time. To prevent this DOS attack they have used efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol which will prevent the attacker from finding the hash and this will lead to the non-decoding of the hash to find out what is the data that has been send through the nodes or the data that the node is currently transmitting or receiving. SEAD performs well over the different range of scenarios and is very much robust against multiple uncoordinated undefined attackers creating an incorrect routing state in any other undefined node, even in spite that is there any active attackers or compromised nodes are present in the network. A distance vector routing protocol always finds the shortest paths between different nodes in the network through a distributed implementation of the classical Bellman - Ford algorithm [7]. Distance vector routing protocols are simple, but they cannot guarantee not to produce routing loops between different nodes for some destination. The primary improvement for ad hoc networks made in DSDV over standard distance vector routing is the addition of a sequence number in each routing table entry. When a node detects a broken link to a neighbor, the node creates a new routing update for that neighbor as a destination, with an ‘‘infinite’’ metric and the next odd sequence number after the even sequence number in its corresponding routing table entry. The learning outcome of this paper was that A one-way hash chain is built on a one-way hash function. Like a normal hash function, a one- way hash function, H, maps an input of any length to a fixed-length bit string. Using SEAD, any attacker cannot create a valid advertisement with larger (better) sequence number that it received. If each node corresponds to a single hash tree chain value (γ=1), the attacker is forced to advertise metric at best *m + 1*. Otherwise, the attacker is forced to advertise metric at best *m + 1* with high probability, and otherwise cannot advertise with metric better than *m*. Hence the SEAD protocol that is used is a better way for the security authentication in Ad Hoc networks which will also help in preventing the DOS attacks because in the current era of the wireless communication technology access denied services are the major problem which are faced by the users.

2.5 *Hung-Min Sun and Wei-Chih Ting* did research on the cryptanalysis of the security authentication protocol and published a paper on A Gen2-Based RFID Authentication Protocol For Security and Privacy. EPC global Class-1 Generation-2 specification (Gen2 in brief) has been approved as ISO18000-6C for global use, but the identity of tag (TID) is transmitted in plaintext, which makes the tag traceable and clonable. Several solutions have been proposed based on traditional encryption methods, such as symmetric or asymmetric ciphers, but they are not suitable for low-cost RFID tags. An RFID application contains three basic roles, i.e. tag, reader and back-end database. Each tag contains a unique identification, often called the tag identification (TID). The reader reads the tagged TID and send it to back-end database for further verification that it is the original one or the duplicate one. DOS is an effective attack against some RFID systems, which utilize locking or killing approach as their protection. Even though this is the weakest test when designing secure protocols, there exist many other simpler ways toward denial of service. A Gen2 tag contains a Pseudorandom Number Generator (PRNG) and protects message integrity via Cyclic Redundancy Code (CRC-16). The memory space is separated into four banks: Reserved memory, EPC memory, TID memory, and User memory. It harvests power from readers through the antenna, and hence, cannot perform complex computations. The conclusion of doing an analysis on the Gen2 protocol is that we proposed a lightweight authentication protocol based on Gen2 to resist various attacks. The proposed tag uses no cryptographic function, and hence, is suitable for low-cost RFIDs. Without changing the protocol flow of Gen2, the existing reader can read both Gen2 tags and Gen2$^+$ tags. Gen2$^+$ provides sufficient security level for real-world settings.

2.6 *G.Usha, Dr.S.Bose of Dept. of Computer Science and engineering, Anna University, Chennai, India has* written in their paper Mobile adhoc networks are self-configuring network connected by wireless links, which forms a random topology of mobile nodes. Topology of these network changes rapidly and unpredictably. Due to lack of infrastructure support, each node acts as a router and any nodes can join and leave the network at any time. Providing security to these networks is a challenging issue because these type of networks suffer for various kinds of malicious attacks. One of the attacks which are more difficult to detect in the Mobile adhoc network is Gray Hole attack. In this paper first an analytical approach to detect Gray Hole attack is developing for AODV protocol. Second,a simple algorithmatical framework is created for generating attacks. Third, experiments are simulated for Gray Hole attacks under variety of adhoc network conditions such as packet delivery ratio, dropped packets. Overhead normalized routing load in order to understand the severity of this attack.

2.7 *Mrs. E. Hemalatha Jai Kumari, Research Scholar Associate Professor Bharathiar University Dept. of Computer Applications ,Coimbatore ,Coimbatore Institute of Technology* has done work on the analysis of security algorithms towards secured communication in wireless networks which has the analysis of all the security algorithms which are required for a secure communication between any wireless network. Wireless network provides a mechanism forconnecting adhoc users in a wireless mode. The connecting nodes has specific standards like IEEE 802.1 to allow the nodes to connect and exchange information. The standards vary with generations and provide facility for improving the communication among the users. The roaming among the users can be internal or external roaming.The wireless nodes connect using access point in a seamless manner. The data to be exchanged among the users can vary from basic data to high level information including multimedia content. A wireless network can also be adhoc network in design level. In market there are lot of IEEE standards that exist for wireless communication. IEEE introduced a port based network access control standard 802.1x to authenticate and authorize devices interconnected various IEEE 802 LANs. 802.1x only defines authentication not the actual authentication method which allows the developers to construct their own algorithm and consequently a lot of wireless vendors implemented their own 802.1x adaptation such as MD5 Message Digest 5, TLS (Transport Layer Security), TTLS (Tunneled TLS), PEAP (Protected Extensible Authentication Protocol), LEAP (Lightweight Extensible Authentication Protocol) and others

2.8 *Sastri L. Kota Harris Corporation of GCSD* 1 134 E. Arques Avenue Sunnyvale, CA 94 as witten in his paper on Cross-Layer Design Challenges For Quality Of Service Guarantees In Satellite Networks suggested that Satellite Communications plays a significant role in supporting next generation IP-based heterogeneous communication network infrastructure for broadband fixed and mobile services. Emerging media streaming, mobile broadcasting, content delivery and distribution, and broadband Internet access require Quality of Service (QoS) guarantees. New satellite system architectures are being envisaged to be fully IP-based. The ISO/OSI reference model and the Internet protocol suite (i.e. TCP/IP) are based on a layering paradigm. Each layer protocol solves a specific problem by using the services provided by modules below it and giving a new service to upper layers. IP packets lost due to errors induced by wireless channel are interpreted as signals of congestion at the TCP level, thus lowering the bit-rate (congestion window, cwndc). The cross-layer design requires interfaces between non-adjacent layers, thus violating the classical abstraction levels of the Internet protocol stack. Another improvement to deal with multiple losses is the Selective Acknowledgement (SACK) in which the receiver informs the sender about the successfully received segments. The sender can re-transmit only the lost segments. SACK [12] can be implemented with both fast recovery and fast retransmit algorithms of the TCP New Reno. The SACK scheme is started by a 'SACK permitted' message sent by the sender to the receiver in a SYN segment. Then, the receiver uses the SACK in the TCP header when it sends an ACK [12] that does not acknowledge the highest sequence number in the received sequence. They have implemented the network simulation model described in Figure 4 under the ns-2 environment. Fig 5 compares the TCP good put performance of different TCP versions as a function of SER [12] for transmission mode #2, a similar behavior could be obtained in the case of mode #1. We note that for low SER values, Westwood achieves the highest goodput performance, whereas as SER increases TCP Hybla turns out to have a better performance. The results in Fig 5 clearly highlight that different TCP versions have a different 'resilience' to the presence of channel errors.[11]

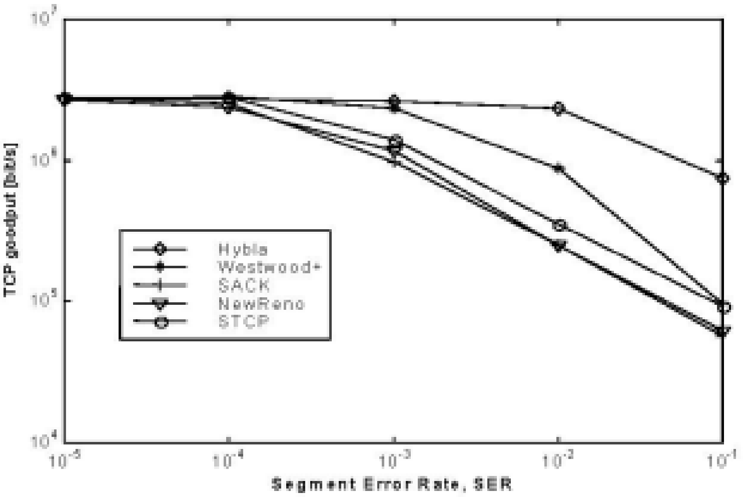


Fig 2.2 Simulation results for the different TCP versions as a function of SER for mode #2.[12]

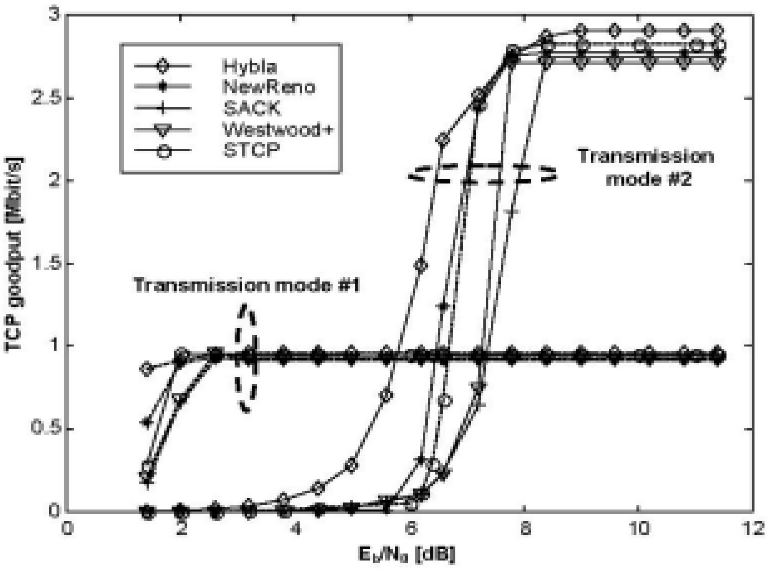


Fig 2.3 Simulation results for the different TCP versions as a function of the Eb/No (reference value for BPSK) for fixed modes 1 and 2; the maximum 95% confidence interval amplitude for all the curves is +7%. [12]

2.9 *Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen, Sultan Qaboos University, Oman* had written in their IEEE published paper on security overview of wireless LAN that Wireless Local Area Networks (WLANs) are cost effective and desirable gateways to mobile computing. They allow computers to be mobile, cable less and communicate with speeds close to the speeds of wired LANs. These features came with expensive price to pay in areas of security of the network. This paper identifies and summarizes these security concerns and their solutions. Broadly, security concerns in the WLAN world are classified into physical and logical. The paper overviews both physical and logical WLANs security problems followed by a review of the main technologies used to overcome them. It addresses logical security attacks like man in-the-middle attack and Denial of Service attacks as well as physical security attacks like rouge APs. Wired Equivalent Privacy (WEP) was the first logical solution to secure WLANs.

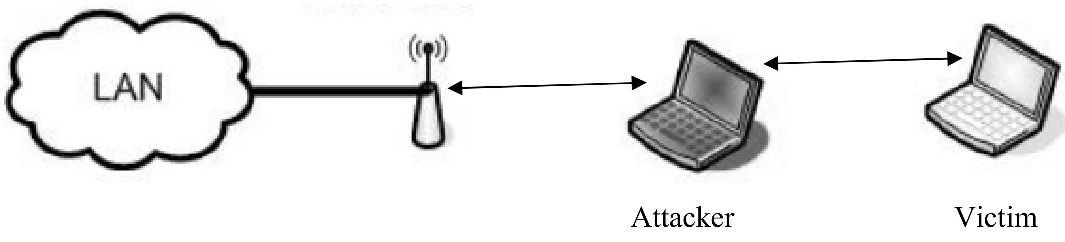


Fig 2.4 Representation of the famous Man-in-the-middle attack for both wired and wireless networks

2.10 *G. Kambourakis, A. Rouskas, G. Kormentzas and S. Gritzalis* published a research paper on Advanced SSL/TLS-based authentication for secure WLAN–3G interworking which motivated the fact that SSL protocol has always been proved its effectiveness in wired IP networks. Although Wi-Fi networks present security deficiencies, they manage to penetrate the wireless market to a great degree due to their low cost, easy administration, great capacity, IPoriented nature, etc. Existing problems related to authentication and key agreement (AKA) procedures and the extensible authentication protocol (EAP)-AKA, as they appear in the latest 3G and integrated 3G/ Wi-Fi specifications, are discussed. It is proposed how EAP-TLS, combined with public key infrastructure (PKI) elements, can be used to overcome these inefficiencies in a hybrid WLAN–3G heterogeneous environment, in order to provide strong authentication and end-to-end security to the mobile user. Emerging or B3G architectures are envisaged to involve an IP-based core network, whereas the access network can be based on a variety of heterogeneous wireless technologies depending on the nature of the access cell. Focusing on picocell environments in such future architectures, where coverage is limited within the buildings, Wi-Fi networks are emerging as the most promising access technology. The anticipated provision of many uncoordinated Wi-Fi picocells will bring to the foreground many open issues concerning authentication and security, mobility management, roaming, and billing of mobile users moving among different Wi-Fi settings. EAP-TLS [14] is based on SSL version 3. 0, and the SSL handshake is performed over EAP, whereas on the Internet the handshake is carried out over TCP. As EAP-TLS performs mutual SSL authentication, each side is required to prove its identity to the other using its certificate and its private key. Other methods similar to EAP-TLS suitable for deployment with wireless LANs are the EAP tunnelled transport layer security (EAP-TTLS) [15] and protected EAP (PEAP) [16] methods. Both were developed in response to the public key infrastructure (PKI) barrier in EAP-TLS and consequently use other non-certificate based methods for user authentication. PEAP is almost identical to EAP-TTLS, relying on the same server-side certificates to authenticate the network and exchange encryption keys. The main difference is that instead of setting up a complete tunnel, it selectively encrypts the client's authentication credentials. The TTLS protocol was also under consideration in the 3GPP to support 3G and WLAN integration, but as it is explained in it was vulnerable to man-in-the middle attacks. Many organizations need to develop a wireless security policy to define what is and what is not allowed with wireless technology, e.g. who gets what, when and how much. On the other hand, the wireless network should be designed with the proper architecture to minimize risk. The WLAN security policy should address several issues among them: basic field coverage, base stations treatment and configuration policy, authentication techniques, Media Access Control (MAC) address filtering, base station discovery, wireless client protection and traffic encryption. For example, the wireless clients should be assessed for having the following security technologies: firecell (distributed personal firewalls) to lock down who can gain access to the client; Virtual Private Network (VPN) to add another layer of encryption and authentication beyond what 802.11 can provide; intrusion detection to identify and minimize attacks from intruders, worms, viruses, Trojans and backdoors, and desktop scanning to identify security misconfigurations on the client. The proposed multiagent-based system directs the operations of the WLAN security products for use in WLAN vulnerability checks and responds quickly to security demands threats. The "new" is the management of these security products using a multiagent-based approach. The purpose is to provide a way to inspect the enforcement of the WLAN security policy and to provide the administrators with an efficient way to revise any steps to ensure a powerful security scheme for their wireless networks. The multiagent-based system correlates the different security threats to their proper security layers. Misconfiguration and client-to-client attacks can be addressed at Layer 1. Jamming, interception and monitoring wireless traffic belong to Layer 2, and the insertion attacks can be addressed at Layer 3. Also, WLAN security policy elements can be correlated to WLAN security layers. For instance, the policies for basic field coverage, users authentication and base station configurations can be enforced at Layer 1. That's because these policies are intended to prevent unauthorized users from gaining access to the WLAN resources. Traffic encryption policy that is utilized to prevent capturing traffic traversing the WLAN can be enforced at Layer 2.

2.11 *Fanglu Guo Jiawu Chen Tzi-cker Chiueh Computer Science Department Stony Brook University, NY 11794* proposed a research paper on Spoof Detection for Preventing DoS Attacks against DNS Servers in which he has shown the attacks done by spoofing in a DNS server. There are two possible DoS attack strategies against DNS servers. The first is to send a large number of requests to a DNS server to overload it. Because a standard DNS server cannot distinguish between spoofed and non-spoofed requests, it has no choice but to handle all of them when it can, and starts to drop requests indiscriminately when it becomes overloaded. However, legitimate requesters interpret request drops as a sign of congestion and back off its timer for retransmission, thus drastically decreasing the amount of legitimate requests served by the overloaded servers. The paper presented a comprehensive study on spoof detection strategies for DNS requests. In all these strategies, a DNS server sends a distinct cookie to each requesting host, and the requester associates each request it sends to the DNS server with the server's corresponding cookie. By checking the cookie that comes with each incoming request, it is possible to determine if a DNS request indeed originates from source address indicated in the packet. However, how to introduce these cookies in a way that is transparent to the existing Internet infrastructure and incurs minimal performance overhead is the design challenge. If any of the DNS server could be prevented from overloading then the attackers will not be able to reset the server hence there would be a secure transmission of data.

CHAPTER 3

3 PROGRAMMING METHODOLOGIES

3.1 Quality of Service

Methodology proposed for its future work on enhancing the performance of the Ad Hoc Networks as found out by the analysis and experiments performed by them on NS-2. The node in ad hoc networks can be attacked in many possible ways. A detailed simulation is being carried out in NS-2. Proposed scheme mainly handles the service attacks, the defects in the link failure, and the effects in the Quality of Service, bogus routing or misrouting. The bogus routing or the misrouting deals with the effect that sending messages to incorrect route, the monitor when finds that there is an ICMP [13] destination unreachable message received but there is no corresponding RERR [13] message to find out the broken link in the transmission.

3.2 Denial of Service

SEAD [7] journal proposed in its work on secure efficient distance vector routing for mobile wireless ad hoc networks by finding the nodes in an ad hoc networks. When the nodes in an ad hoc network are unable to verify asymmetric signatures quickly enough, these protocols may not be suitable and may create Denial-of-Service attacks [7], these protocols also generally require more network bandwidth than does SEAD with its hash values. The researchers have designed a secure on demand routing protocol for ad hoc networks, called Ariadne. The mechanisms they have used for security in Ariadne are end-to-end in nature, whereas their approach here for SEAD which operates on a hop-by-hop basis due to the basic operation of distance vector routing. Furthermore, unlike Ariadne [7], the techniques presented here do not rely on a Message Authentication Code to authenticate routing table entries, but instead directly use elements from a one-way hash chain to provide authentication for both the sequence number and the metric in each entry.

3.3 Power Consumption

Since a wireless network is idle most of the time, it is not necessary to keep the WLAN card fully powered all the time. Software intelligence can be added to put the WLAN card hardware into a low-power "sleep" mode whenever possible while maintaining high data transfer performance. To sustain network connectivity, the WLAN card must have power to listen for traffc, including beacons, periodically. However, the circuitry responsible for sending and receiving packets can be turned of or set to "sleep" when there is no traffic to send or receive. This can lead to considerable power savings. In fact, this is how power saving works in current WLAN cards. When power save is enabled, the WLAN card will follow a periodic "sleep awake-sleep awake” pattern to minimize the power drawn by the card. When the WLAN card is sleeping, incoming packets will be buffered at the AP. Periodically, the card wakes up to listen to beacons from the AP [20], which the AP uses to tell the card if incoming traffic is queued. Once the card notices incoming traffic is available, it tells the AP to deliver the traffic. After that, the card goes to sleep again. The penalty for saving power via sleep is greater latency on the delivery of new incoming packets. Moreover, depending upon the implementation, if only a few packets are delivered before the card goes to sleep again, the data rates will be significantly reduced. More sensitivity carrier sense threshold causes more unnecessary processing Power level adjust method influences the power saving performance. False packet detections of sampling waste power Symbol rate and throughput tradeoff. Higher power radiation causes higher interference level. The IEEE 802 specifications define the family of standards for LANs that deal with the two lowest layers of the ISO Open System Interconnection Reference Model, namely physical and data-link layer. Consequently, the 802.11 standard includes the definition of the 802.11 MAC and various physical layers. The initial version of the standard, called also release 1999, included following physical layers: infrared, Frequency-Hopping Spread Spectrum (FHSS) (both now completely abandoned) and Direct-Sequence Spread Spectrum (DSSS). Later revisions added additional physical layers. The 802.11b extension defined high rate DSSS with data rates up to 11Mbps in the 2.4GHz band. Devices compliant to that standard started to appear already in 1999, and thanks to their enormous popularity form an important part of the evaluation presented in this report. Shortly after, the 802.11a extension was released, that defines a physical layer based on Orthogonal Frequency Division Multiplexing (OFDM) with data rates up to 54Mbps in the 5GHz band. OFDM was also brought to the 2.4GHz band with the 802.11g standard, published in 2003. More recently, further improvements to the physical layer were proposed with the 802.11n standard that incorporates Multiple-Input/Multiple-Output (MIMO) enhancements in both 2.4 and 5GHz band.

3.4 Secure Transmission

IEEE802.11 defines two types of authentication methods used to access WLANs, open-system and shared key [14]. In the open-system method all communications between the STA and the AP are in the clear (i.e. visible and not hidden). In this method it does not matter if the WEP keys used to access the WLAN are correct, the AP will allow accessing the WLAN even if the keys used are invalid, the only requirement here is the network SSID (section 3.2). However, APs broadcast their SSID by default so using open-system authentication is totally insecure. In the shared key method, the AP sends a challenge text to the STA; this challenge is encrypted by WEP keys then it is returned back to the AP to either grant access to the WLAN or not. The AP will decrypt the received challenge and compare it with the original challenge it stores. If the decrypted challenge found identical to the original challenge then it implies that the AP and the STA are using the same WEP key; hence the STA can be authenticated. In this scenario, the authentication of STAs is mandatory while AP authentication is not important [14]. This means that a legitimate STA can connect to an illicit AP. SSID is a network identifier number broadcasted by Aps [24]. Without knowing the SSID number, STAs can not access the etwork. This seems fine but the problem with SSID is that it is actually broadcasted by the AP. Unauthorized stations can capture the SSID of a WLAN and use it to gain access. It is useful to stop SSID broadcast, this means that wireless stations have to actively search for the SSID correspondent to the WLAN they want to access to. It is also recommended to change the value of the SSID frequently but that will overload network administrators if many APs exist in a WLAN with the absence of central management scheme to control all of them at once. SSID is not a very efficient access control technique; however, it is one hurdle that could be tuned to make it difficult for non-skilled attackers to access the WLAN.

3.5 Bit Error Rate

ARQ is one of many mechanisms developed to correct errors of packet-based wireless transmissions over unreliable channels. When combined with the channel coding, it results in the so-called hybrid ARQ (HARQ). Various types of HARQ were devised and analyzed [23], differentiated with respect to the retransmission content and the way the receiver deals with multiple replicas of the original packet. In ARQ, it is done using *packet combining* or *code combining* [4], which allows for storage and combining of the received signals. We consider a slightly suboptimal metrics calculation, based on the addition of metrics obtained in different retransmissions. BER is the error rate, which defines how many bits are lost or affected during transmission or receiving.

3.6 Different Methodologies/Approaches Suggested

Based on the design of SEAD in part on the DSDV [15] ad hoc network routing protocol[14], and in particular, on the DSDV-SQ version of the protocol, which has been shown to outperform other DSDV versions in previous detailed ad hoc network simulations [15,16]. For security, we use efficient one-way hash functions and do not use asymmetric cryptographic primitives. Consequently, SEAD is efficient and can be used in networks of computation- and bandwidth-constrained nodes. SEAD actually outperforms DSDV-SQ in terms of packet delivery ratio, although it does create more overhead in the network, both due to an increased number of routing advertisements it sends, and due to the increase in size of each advertisement due to the addition of the hash value on each entry for authentication. There is one more different method where this operation/simulation could be performed that is the Cisco Packet Tracer as provided by the cisco networking systems where a virtual scenario could be developed to just find out whether the data is properly transmitted or it is having a delay in data transmission, if there is any other node or the user who is just consuming the energy or there is a live attacker which is attacking on the DOS attack of the nodes.

3.7 CHALLENGES FACED BY MOBILE WLAN NETWORKS

3.7.1 Routing

The presence of mobility implies that inks made and break often and in an indeterministic fashion. We use the Bellmen-Ford algorithm to sort out the issue to find out the shortest path to move from a source to a destination. While distance-vector-based routing protocol is not actually designed for wireless networks it is still applied to the cable of packet radio networks since the rate of mobility is high. Existing distance-vector and link state-based routing protocols are unable to catch up with frequent link changes in ad hoc wireless networks, resulting in poor route convergence and very low communication throughput. So new and advanced protocols is to be needed.

3.7.2 Mobility

The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes, hence an ongoing session suffers frequent path breaks. Such situations do not arise because of reliable links in weird networks where all the nodes are stationery. Even though the wired network protocols find alternate routes during path breaks, their convergence is very slow. Routing protocols for ad hoc networks must be able to perform efficient and effective mobility management. Routing efficiently in wireless ad-hoc networks poses many challenges. Some commonly studied problems are: How to handle the frequent changes in the network topology due to mobility of the users, failure of wireless links caused by obstruction or fading of signals.

3.7.3 Bandwidth Constraint

Abundant bandwidth is available in wired networks due to the advent of the fiber optics and due to the exploitation of wavelength division multiplexing (WDM) technologies. But in a wireless network the radio band is limited and hence the data rates it can offer as much less that what a wired network can offer. Due to the frequent changes in the methodology maintaining consistent topological information at all the nodes involves more control overhead which in turn results in more bandwidth wastage. As efficient routing protocols in wired networks required the complete topology information they may not be suitable for routing in the ad hoc wireless networking.

3.7.4 Hidden and Exposed Terminal Problems

The hidden terminal problem refers to the collision of the packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver. Collision occurs when we two nodes transmit at the same time but both nodes are not aware of transmitting the signal at the same time.

3.7.5 Channel Access

The routing table may not be able to converge but the routing loop may still exist. Current wired routing uses shortest path metric to transfer the data form one node to the other. The channel faces a very important issue that is the quality of the service that is to be supported by the channel. The packet collisions are so hard that they are not been able to support by the channel. Each packet radio is supported by the CSMA.

3.8 ANALYSIS OF THE METHOD

3.8.1 CISCO Packet Tracer

The CISCO packet tracer that is to be used in the project has a 30% use as the tracer is to be used for creating a virtual scenario of any graphical 2D or 3D environment. The cisco further known as the CCNA guide is hereby used for the networking aspects and the designs so that before applying it to hardware part and before the codes and the programs can be fixed for the networks a pre applied scenario can be checked to find out whether it will be a success or not. A network is simply defined as something that connects things together for a specific purpose.

3.8.2 Protocol Used

The term network is used in a variety of contexts, including telephone, television, computer, or even people networks. A computer network works on the protocols i.e ZRP, DSR, AODV, EAP etc. ZRP works in particular zone only. DSR works when it needs to transfer the data from a particular distance to another. AODV protocol is the base of all protocols on which all protocols works but it has some issues which needs to be fixed. Then comes the EAP protocol, it has many functions that it works upon like key exchange, secure routing, TTLS.

3.8.3 Network Simulator - 2(NS 2)

NS-2 is an open source system that is developed using C++ and Tool Control Language TCL. Researchers can freely add new components to the system to server their own purposes. The latest version of NS-2 is version 2.28. Within this version, most of the standard protocols supported. You can find protocol from media access layer protocols such as CSMA/CD up to application protocols as FTP and HTTP. For routing protocols, there are unicast and multicast routing protocols for wire network and DSR, DSDV, AODV for wireless ad-hoc networks. Most of these protocols were developed by researchers and adopted into standard version of NS-2. In order to experiment security features for network, we need to add security functions into NS-2. Of course for specific experiments there are specific requirements. The purpose of this project is only to illustrate a way to add security functions into NS-2.

CHAPTER 4

4 APPROACH OF THE PROJECT

4.1 FLOW CHART

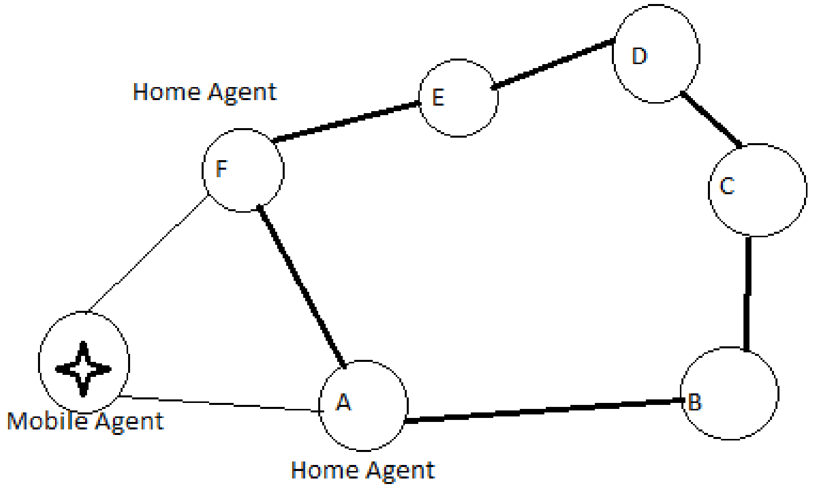


Fig 4.1 Proposed System Architecture Outline

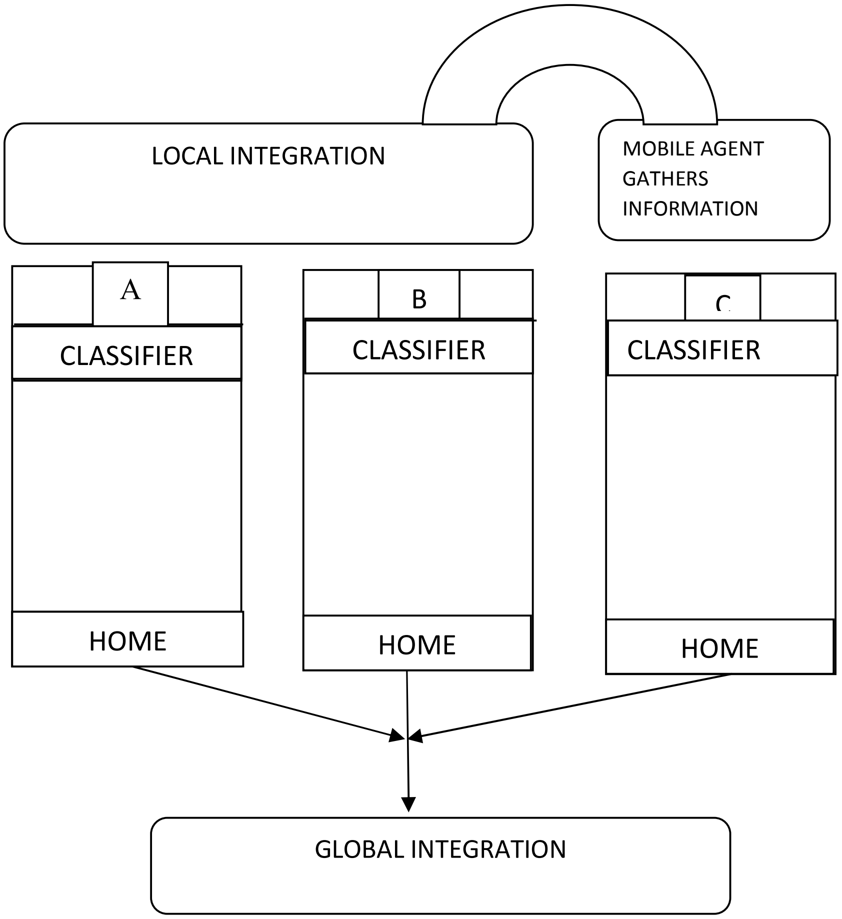


Fig 4.2 Proposed Internal System Architecture

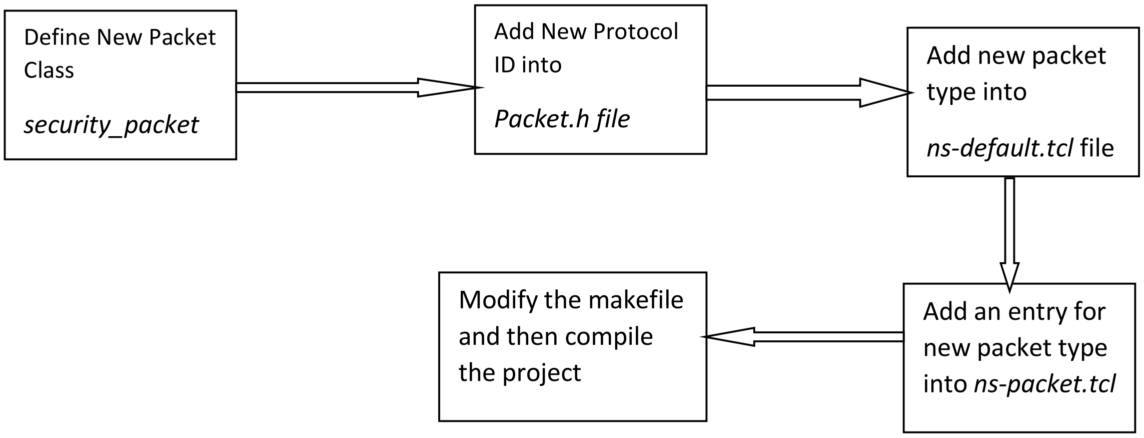


Fig. 4.3 Flow Chart for Adding a New tcl file and compiling it in NS2

4.2 Virtual Scenario and the Configuration of the Tool Used

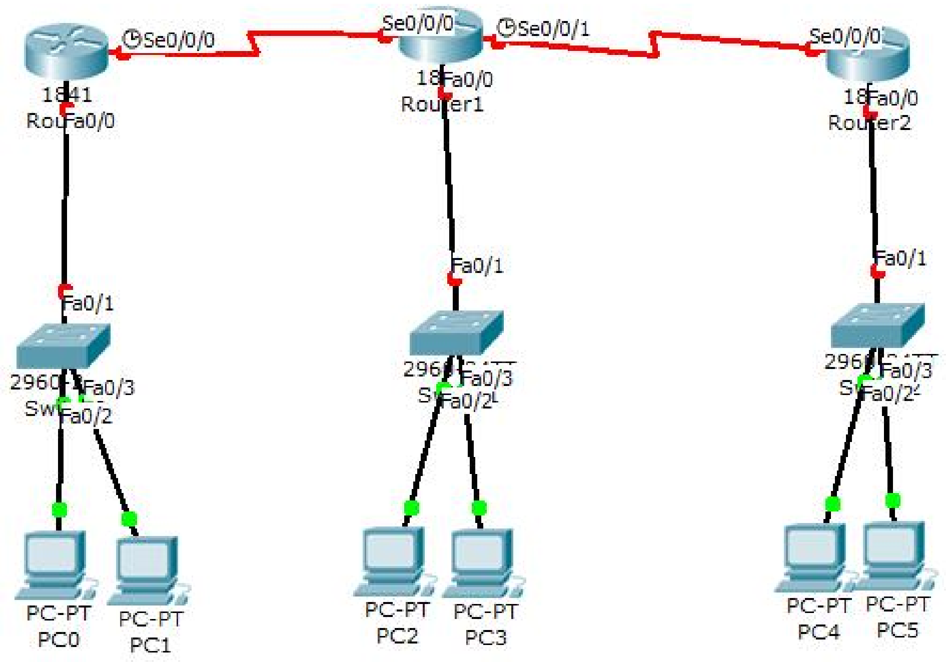


Fig 4.3 Virtual Scenario of the Whole Network

4.3 Hash Function

Using a simple hashing algorithm to get hashed value from a string of plain text. The hash value will be attached to packet header for data integrity checking. At the other end of communication, after decryption, the decrypted text will be hashed again to get new-hashed value. This new-hashed value will be compared to the value attached within packet header. If they are equal, the data integrity is ensured and decrypted text is accepted; otherwise the packet is discarded. In either case, an acknowledge packet will be sent back to sender to inform of the status of the packet. The algorithm for the hash function can be any kind of algorithm like SHA-1, MD5.

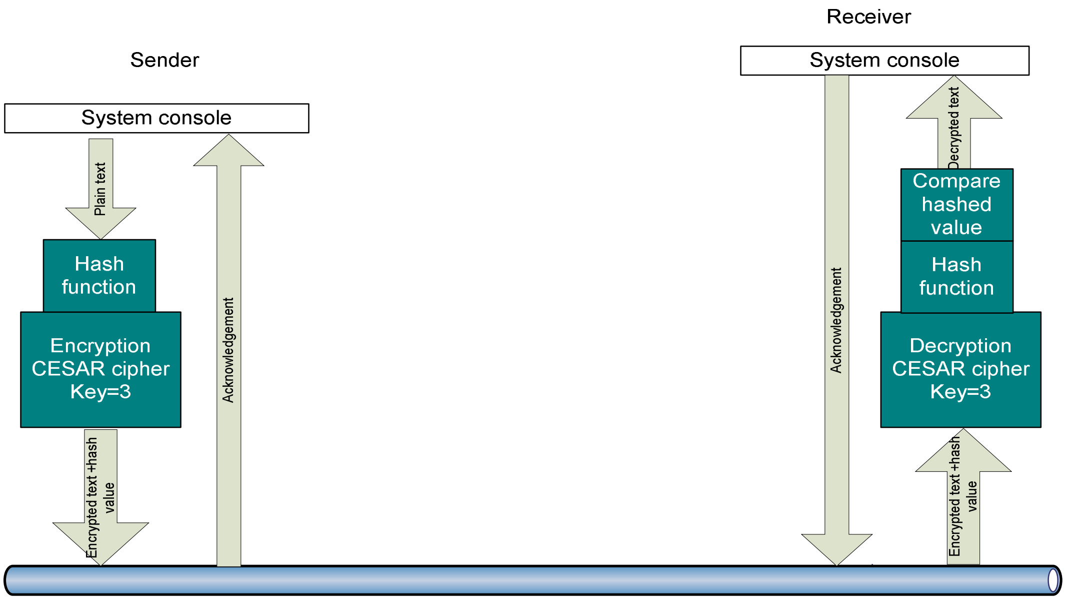
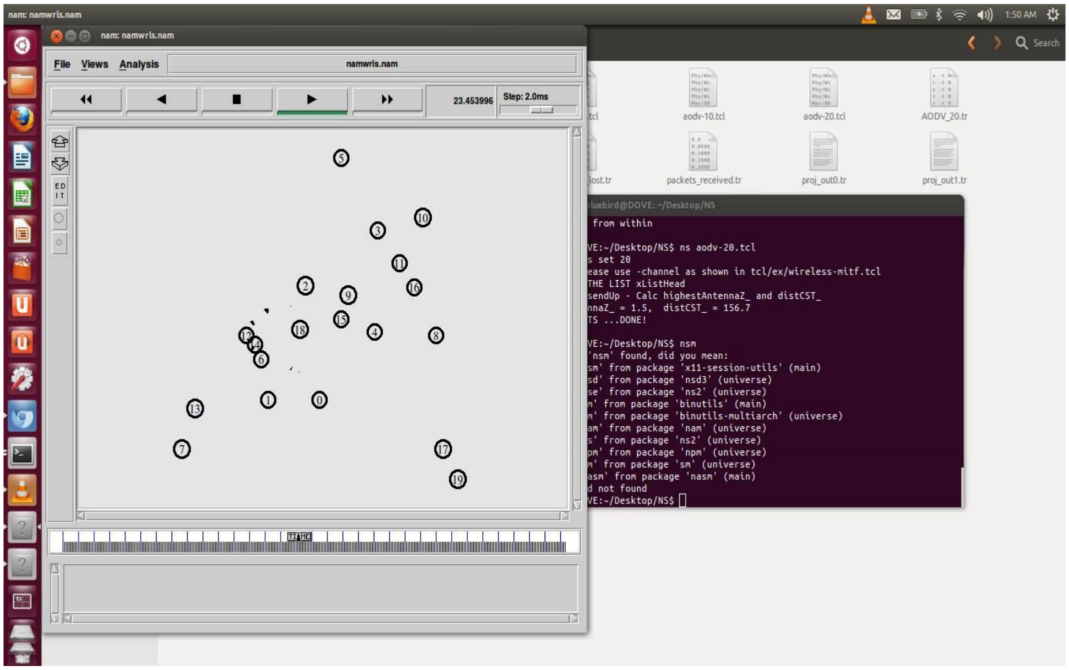


Fig 4.4 Logical design of the encryption/decryption system

4.4 SIMULATION AND RESULTS

4.4.1 Shortest Path From Source to Destination



```
 from within

VE:~/Desktop/NS$ ns aodv-20.tcl
s set 20
ease use -channel as shown in tcl/ex/wireless-mitf.tcl
THE LIST xListHead
sendUp - Calc highestAntennaZ_ and distCST_
nnaZ_ = 1.5,  distCST_ = 156.7
TS ...DONE!

VE:~/Desktop/NS$ nsm
'nsm' found, did you mean:
sm' from package 'x11-session-utils' (main)
sd' from package 'nsd3' (universe)
se' from package 'ns2' (universe)
m' from package 'binutils' (main)
m' from package 'binutils-multiarch' (universe)
am' from package 'nam' (universe)
s' from package 'ns2' (universe)
pm' from package 'npm' (universe)
m' from package 'sm' (universe)
asm' from package 'nasm' (main)
d not found
VE:~/Desktop/NS$ 
```

Fig 4.4 NS2 Simulation for Shortest Path

REFERENCES

[1] Miodrag Potkonjak, Computer Science Department, University of California, Mani B. Srivastava Los Angeles, Electrical Engineering Department, University of California, Los Angeles, Coverage Problems in Wireless Ad-hoc Sensor Networks ,8(2):174–179, 2000

[2] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal, Department of Computer Science, University of California, Davis, CA 95616 ,2011, Sandia National Laboratories, Livermore, CA 94551, Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges

[3] E. Donchin, K.M. Spencer, and R.Wijeshinghe. The mental prosthesis: Assessing the speed of a p300-based brain-computer interface. IEEE Transactions on Rehabilitation Engineering, 8(2):174–179, 2000.

[4] Vikram Srinivasan, Pavan Nuggehalli, Carla F. Chiasserini, Ramesh R. Rao, Cooperation in Wireless Ad Hoc Networks, Department of Electrical and Computer Engineering, University of California at San Diego email: vikram,pavan,rao@cwc.ucsd.edu. 0-7803-7753-2/03 (C) 2003 IEEE

[5] Delaunay Triangulations. Presented by Glenn Eguchi. 6.838 Computational Geometry. October 11, 2001. groups.csail.mit.edu/graphics/classes/6.838/Delaunay/Delaunay2D.ppt

[6] Geir M. Køien and Thomas Haslestad, Telenor R&D, ,2011, Integration Of Wireless Lan And 3g Wireless, Security Aspects of 3G WLAN Interworking ,Norway,IEEE

[7] Yih-Chun Hu, David B. Johnson , Adrian Perrig,Carnegie Mellon University, Pittsburgh, ,Rice University, Houston, 2003, SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks, Ad Hoc Networks 1, 175–192

[8] Neeraj Garg, Atal Chaudhri, Soumya Sankar Basu, "Performance Analysis of MANETS in Scalbility", Proceedings of the 41st Annual National Convention, Computer Society Of India CSI-2006 on Affordable Computing, Science city, Kolkata, pp.51-55, November 2006. ISBN 0-07-062171-3.

[9] Conti M, Giordano S, "Multihop Adhoc Networking: The Theory", IEEE Communications Magazine, Volume 45, Issue 4, pp 78 - 86, April 2007.

[10] A. Narula-Tam, T. MacDonald, E. Modiano, L. Servi, "A Dynamic Resource Allocation Strategy for Satellite Communications," Proceedings of IEEE, October 2004.

[11] C. Caini, R. Firrincieli, "TCP Hybla: a TCP Enhancement for Heterogeneous Networks", International Journal of Satellite Communications and Networking, Vol. 22, No. 5, pp. 547-566,August 2004.

[12] Sastri L. Kota Harris Corporation, GCSD 1 134 E. Arques Avenue Sunnyvale, CA 94085, Cross-layer design challenges for quality of service Guarantees in satellite networks, IEEE, November 2004

[13] Goswami D. N., S.O.S. in Computer Sc. Jiwaji University, Gwalior World Congress on Information and Communication Technologies,2011, IEEE Conference Paper

[14] Gowrishankar.S, SubirKumarSarkar, T.G.Basavaraju , "Analysis of AOMDV and OLSR Routing Protocols Under Levy-Walk Mobility Model and Gauss-Markov Mobility Model for Ad Hoc Networks", (IJCSE) International Journal on Computer Science and Engineering, vol. 02, pp. 979-986, 2010

[15] C.E. Perkins, P. Bhagwat, Highly Dynamic Destination- Sequenced Distance-Vector routing (DSDV) for mobile computers, in: Proceedings of the SIGCOMM _94 Conference on Communications Architectures, Protocols and Applications, August 1994, pp. 234–244. Available <http:// www.cs.umd.edu/projects/mcml/papers/Sigcomm94.ps> (a revised version).

[16] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, M. Degermark, Scenario-based performance analysis of routing protocols for mobile ad-hoc networks, in: Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_99), August 1999, pp. 195–206.

[17] J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, J.G. Jetcheva, A performance comparison of multi-hop wireless ad hoc network routing protocols, in: Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_98), October 1998, pp. 85–97.

[18] H.M. Sun, "An efficient remote use authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 4, pp. 958-961, Nov. 2000.

[19] C.C. Lee, M.S. Hwang, and W.P. Yang, "A flexible remote user authentication scheme using smart cards," ACM Operating System Review, viol. 36, no. 3, pp. 46-52, 2002.

[20] S. Medidi, M. Medidi, and S. Gavini, "Detecting Packet Dropping Faults in Mobile Ad-hoc Networks," In Proc. of IEEE ASILOMAR Conference on Signals, Systems and Computers, volume 2, pp. 1708–1712, 2003.

[21] H.safa,Mirza.O ,Artail.H. A Dynamic Energy Efficient Clustering Algorithm for MANET.IEEE International Conference on Wireless and Mobile Computing, 2008

[22] Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, November 2002.

[23] David B. Johnson, and David A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[24] Y. Zhang, W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," 6th Int'l. Conference Mobile Comp. Net., Mobicom 2000, pp. 275-283, August 2000.

[25] Monis Akhlaq, Baber Aslam, Muzammil A. Khan, John Mellor, M. Noman Jafri, Irfan Awan, Performance evaluation of IEEE 802.1x authentication methods and recommended usage, WSEAS TRANSACTIONS on COMMUNICATIONS , Volume 7 Issue 3 ,March 2008.

[26] G. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X. P. Costa, and B. Walke. The IEEE 802.11 universe. IEEE Comm. Mag., 48:62–70, January 2010.

[27] M. Gast. 802.11 Wireless Networks: The Definitive Guide. O'Reilly & Associates, Inc., Sebastopol, CA,USA, 1st edition, 2002.

[28] Atheros Communications. Power Consumption and Energy Efficiency Comparisons of WLAN Products. http://www.super- g.com/collateral/atheros_power_whitepaper.pdf, 2003.

[29] Notani, S., "Performance Simulation of Multihop Routing Algorithms for Ad-Hoc Wireless Sensor Networks Using TOSSIM," in Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on, vol. 1, 2008.

[30] Varga, A., Hornig, R., "An overview of the OMNeT++ simulation environment," in Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops table of contents. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) ICST, Brussels, Belgium, Belgium, 2008.

[31] X. Yang, D. Wetherall, and T. Anderson, "A DoS-limiting network architecture," in *SIGCOMM '05*. New York, NY, USA: ACM Press, 2005, pp. 241–252.

[32] A. Yaar, A. Perrig, and D. Song, "SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks," in *Proc. of IEEE Symposium on Security and Privacy, 2004*, 2004.

[33] S. Templeton and K. Levitt, "Detecting spoofed packets," in *Proc. of The Third DARPA Information Survivability Conference and Exposition (DISCEX III)2003*, 2003.

[34] K. Rikitake, "A Study of DNS Transport Protocol for Improving the Reliability," Ph.D. dissertation, Graduate School of Information Science and Technology, Osaka University, 2005.

[35] ComputerWire. (2002) DDOS attack 'really, really tested' UltraDNS. http://www.theregister.co.uk/2002/12/14/ddos attack really really tested.

[36]

APPENDIX A

Steps to install NS-2

- Sudo apt-get update
- Sudo apt-get

BIO DATA

NAME: PRINCECON BERA

REGISTRATION NO. : 10904661

SCHOOL OF ELECTRONICS AND COMMUNICATION ENGINEERING

NAME OF SUPERVISOR: VISHALI SHARMA

DESIGNATION: ASSISTANT PROFESSOR

SCHOOL OF ELECTRONICS AND COMMUNICATION ENGINEERING