Utilising Fuzzy Logic to Detect False Access Points in Wi-Fi Networks

A Thesis submission in fulfilment for the degree of

Master of Science (Honours)

Ali Naqvi
School of Computing, Engineering and Mathematics
University of Western Sydney
AUSTRALIA
This thesis entitled:

“Utilising Fuzzy Logic to Detect False Access Points in Wi-Fi Networks”

Written by

Ali Naqvi

Has been approved for the School of Computing, Engineering and Mathematics

Supervised:

Dr Weisheng Si

Signed: ………………………………………. Dated: ………………..

Dr Zhuhan Jiang

Signed: ………………………………………. Dated: ………………..

The final copy of this thesis has been examined by the signatory, and I find that both the content and the form meet acceptable presentation standards of scholarly work in the above mention discipline.
Declaration

I hereby declare that this submission is my own work and to the best of my knowledge it contain no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at UWS or any other education institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by other, with whom I have worked at UWS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project’s design and conception or in style, presentation and linguistic expression is acknowledge.

Signed: .................................   Dated: ..................
Copyright Statement

“I hereby grant the University of Western Sydney or its agents the right to archive and to make available my thesis or dissertation in whole or part in the University libraries in all forms of media, now or here after known, subject to the provision of the Copyright Act 1968. I retain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as article or books) all or part of this thesis or dissertation.

I also authorise University Microfilms to use the 350 word abstract of my thesis in Dissertation Abstract International. I have obtained permission to use copyright material; where permission has not been granted I have applied/ will apply for partial restriction of the digital copy of my thesis or dissertation.”

Signed: …………………………………. Dated: …………………
Authenticity Statement

“I certify that the Library deposit digital copy is a direct equivalent of the final official approved version of my thesis. No emendation of the content has occurred and if there are minor variations in formatting, they are the result of conversion to digital format.”

Signed: …………………………………..  Dated: ………………
Publication arising from this Thesis

Dedication

To

Our Grandparents, Parents and Kids with Love, Respect and Care
Acknowledgement

I searched for the words that could express my gratitude and respect for the person who taught me what I did not know. What I discovered are some feelings that lose their meaning and intensity when tried to be conveyed by words—I acknowledge, with extreme respect, the gift of knowledge and understanding I received from my teachers.
# Table of Contents

1. Introduction.......................................................................................................................... 1
   1.1 Motivation.......................................................................................................................... 6
   1.2 Related work ...................................................................................................................... 10
   1.3 Research objective .......................................................................................................... 15
   1.4 Research outline ............................................................................................................. 17
      1.4.1 Security overview ...................................................................................................... 18
      1.4.2 Accountability .......................................................................................................... 18
      1.4.3 Assurance ................................................................................................................ 19
      1.4.4 Authentication ......................................................................................................... 19
      1.4.5 Authorisation ........................................................................................................... 19
      1.4.6 Availability .............................................................................................................. 20
      1.4.7 Confidentiality ........................................................................................................ 20
      1.4.8 Integrity ................................................................................................................... 20
      1.4.9 Non-repudiation ...................................................................................................... 21
   1.5 CIA Model ....................................................................................................................... 22
      1.5.1 Confidentiality attacks ............................................................................................ 22
      1.5.2 Integrity attacks ....................................................................................................... 24
      1.5.3 Availability attacks ................................................................................................. 28
   1.6 WLAN countermeasure of CIA model .......................................................................... 28
      1.6.1 Validation and access control ................................................................................... 29
      1.6.2 Audit and Intrusion detection ...................................................................................... 31
      1.6.3 Extrusion detection and cryptography ....................................................................... 31
      1.6.4 Firewall and DMZ .................................................................................................. 34
2. Literature review .................................................................................................................... 36
   2.1 Wi-Fi .................................................................................................................................. 37
List of Figures

Figure 1.1: Wireless Network criteria........................................................................................................7
Figure 1.4: Wi-Fi connection stages ........................................................................................................12
Figure 1.5: IEEE 802.11, 4-Way Handshake Algorithm ...........................................................................14
Figure 1.7: Security objective relationships ..............................................................................................21
Figure 1.8: Breach of Confidentiality ..........................................................................................................23
Figure 1.9: Integrity Attacks .........................................................................................................................26
Figure 1.11: Application layer Cryptographic models .................................................................................33
Figure 1.12: Online succession encryption mechanisms .............................................................................33
Figure 1.13: Layered defence strategy with respect to Firewall and DMZ ....................................................35
Figure 2.1: Literature framework ................................................................................................................36
Figure 2.2: Four-Way Handshake protocol .................................................................................................40
Figure 2.3: DoS attack ................................................................................................................................41
Figure 2.4: CIA, DoS and MiM Attacks Vulnerability ..................................................................................43
Figure 2.5: Artificial model of a neuron ......................................................................................................48
Figure 2.6: Fuzzy Neural Network (F2N) concepts and computation .........................................................49
Figure 2.7: F2N Classification .......................................................................................................................50
Figure 4.1: Wireless Access Point with 4m, 40m, 400m model ..................................................................59
Figure 4.2: General Wi-Fi modelling & simulation approach block model .................................................60
Figure 4.3: Representing 4m, 40m, and 400m distance between BS and AP ............................................64
Figure 4.4: Complex envelop with respect to 4m, 40m, 400m ..................................................................64
Figure 4.5: Wireless Model between a transmitter and receiver .................................................................66
Figure 4.7: Wireless model with an embedded False Access Point .............................................................68
Figure 4.8: Channel frequency (MHz) and magnitude of the complex signal (dB) ....................................69
Figure 5.1: DoS attack with respect to proxy timeout ...............................................................................76
Figure 5.2: Four-Way Handshake protocol Fuzzy Set ...............................................................................79
Figure 5.3: Wireless Station Attributes with respect to Wi-Fi protocol ....................................................82
Figure 5.5: Fuzzy logic connection model of Wi-Fi with respect to Figure 5.4 & 5.3 ......... 84
Figure 5.6: Fuzzy Logic Wi-Fi Connection model .............................................................. 85
Figure 5.9: SSWA-Spatial AoD- Sensitivity assessment Fuzzy Logic graph ....................... 93
Figure 6.1 MiM attack; vulnerability for wireless network and wired counterpart .......... 96
Figure 6.2: MiM attack Physical Layer model ................................................................. 98
Figure 6.3. Rulebase architecture for eradicating MiM Attack ........................................ 99
Figure 6.4 SSRN Fuzzy logic model w.r.t. Root access point saddle point. ................. 104
Figure 6.5 Surface plot w.r.t. the SoP of an AP and its PPDU aspects ......................... 105
List of Tables

Table 4.1: Wi-Fi 802.11b BER with respect to transmitter and receiver .......................... 70
Table 4.2: Wi-Fi Mamdani MatLab model ........................................................................ 72
Table 5.1: Fundamental properties of crisp set operation .................................................. 80
Table 5.2: Security Swarm Wireless Access Input/Output parameters ............................. 87
Table 5.3: Security Swarm Wireless Access (SSWA) .......................................................... 89
Table 6.1: MiM tool for False Access Point activity .......................................................... 97
Table 6.2: Security Swarm Root Node Input/Output parameters ...................................... 100
Table 6.3: SSRN a tool for protection against False Access Point (MiM) activity .......... 102
Table 6.3 code w.r.t. that SSRN Fuzzy logic modelling .................................................. 106
Abstract

IEEE 802.11 (Wi-Fi) is the widely-accepted standard for implementing a Wireless Local Area Network today. Its security mechanism is defined in the IEEE 802.11i standard, which describes a Four-Way Handshake protocol for a wireless Access Point to associate to an Access Point (AP). Many researchers have proposed new protocols by modifying the use of some state variables in IEEE 802.11i. However, these new protocols cannot effectively prevent Access Points from associating to False APs when the False APs perform the Denial of Service (DoS) attack or the Man-in-the-Middle (MiM) attack to disguise themselves as the true APs.

Facing the above research challenge, this thesis proposes to utilise Fuzzy Logic to detect such False APs. For this purpose, this thesis presents two algorithms: the Security Swarm Wireless Access (SSWA) algorithm and the Security Swarm Root Access Point (SSRN) algorithm, which can detect whether an AP is a true AP under the DoS attack and the MiM attack scenarios respectively. Both algorithms describe the corresponding attack scenario with a fuzzy logic model, which can derive whether an AP is true. Both algorithms take as inputs the following parameters regarding to Access Points or APs in a Wi-Fi network: the geographic positions, the IEEE 802.11 frames transmitted, the Angles of Arrivals, the Angles of Departures, etc. In both algorithms, the Particle Swarm Optimisation (PSO), a well-known computation technique from bio-inspired computing, is employed to obtain the authenticity of an AP through iterative improvements while Wi-Fi networks are in operation.

Finally, the two proposed algorithms are simulated in the Matlab environment, which already includes the implementation of the IEEE 802.11 physical layer and the Fuzzy Logic tool box. Our extensive simulations validate the effectiveness of the proposed SSWA and SSRN algorithms.
Chapter 1

1 Introduction

Wireless network framework is a network without any tangible wire medium between devices. Wireless network can be classified based on three aspects, such as topology of the architecture, medium of communication and access protocol. The distance and mobility factor plays a pivotal role not only with respect to the performance, but also with respect to security paradigms. These can be divided into two major categories; one with a fixed tail architecture and the other without one. Wireless network security is an imperative dimension for any business’s survival and growth. There are many potential wireless application scenarios for wireless LAN and MAN, covering broadband home-office networking, community wireless networking, building automation networks, high speed metropolitan area network, intelligent transport and business enterprise network. Wireless security threats can be divided into three crisp areas i.e. Denial of Service attack, Impersonation attack and Routing attacks i.e. Man in the Middle (MiM) attack. Rogue network activity is transparent to both client and server wireless systems i.e. base station (BS) and access point (AP) within Wireless Local Area Network (WLAN). False Access Point activity enables an attacker to intercept, to copy network messages activity and thus, launch more sophisticated wireless routing attacks.

The open nature of the Internet has made it possible for service-providing companies to provide services to different sectors of communities. However, some service providers close some parts of their network in order to protect their critical network management infrastructure. Communication network security is generally a product of inconvenience rather than ease for usage. The basic security level model is one that can always have more
value additive features to it. Mitigating all communication risk is next to impossible, as mitigating control criteria has a mirage effect with more remaining risks. Wireless security risk is always an integral effect of these consequences and their occurrence probability. The cost of an information technology security setup solution and Return on Investment (ROI) are not proportional to each other, as controlling a hacking element is not the complete security solution. Existing wireless security systems, including most of Intrusion Detection Systems (IDS), address the problem in depth-first approach. These approaches miss out the span of breadth-first investigation that creates a dark window of opportunity for Man-in-the-Middle (MiM) attack, another active class of creating a False Access Point criterion. A security is best defined as the weakest link in the wireless system. Service Level Agreement (SLA) often fails to provide end-user Confidentiality, Integrity, and Availability of Information Technology (IT) resources. Within the realm of Wireless security, most mitigated security controls fall into at least one of the three categories: (1) Prevention, (2) Detection and (3) Deterrence. A reliable security system is one that targets not merely prevention from failures, but also eliminates these threats if they arise. Security framework can be divided into two major domains, how to protect the freedom of information with its supporting business evolution and how to conserve private, personal, and strategic business information system.

Prior security knowledge for a secure communication between two wireless Access Points to overcome the pitfall of a Rogue wireless network has not been put into effect in a public infrastructure. Therefore the possibility for a wireless Access Point to know that it will not be a part of a rogue network is still unanswered. Wireless standard for access control proposed by IEEE 802.11 does not specifically address the false Access Points security issues. Many researchers have laid emphasis on proposing new protocols against IEEE 802.11, such as Two-Way Handshake and Enhanced 3-Way Handshake; however, these protocols have failed to overcome False Access Point association such as Denial of Service
(DoS) or Man-in-the-Middle (MiM) attacks. Imperative paradigms of wireless security that need to be improved are associated with prior knowledge for any Access Point to know that it will not be part of a rogue network association and activity. Access Point security management and performance criterion within the framework of physical constraints is another area of importance. Designing and analysing security trust-mission parameters are some of the critical elements for a secure association between any two wireless Access Points in communication. Key design architecture components for a wireless security are: (1) Knowledgebase Data Structure, (2) Functional security validation and verification modelling parameters, (3) Security risk assessment and (4) Risk mitigation modelling parameters[1]. These paradigms are some of the important aspects of tracking message-dependency criteria for better security management modelling. Henceforth, predictive modelling can not only detect, but also can prevent any future Trojan data-mining activities. Owing to continuous demand and resource exhaustive wireless applications, the network paradigm requires improved security management. Wireless network standards defined by IEEE; are IEEE 802.11 (IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11 ac, IEEE 802.11ad) for Local Area Network (WLAN) coverage and IEEE 802.16 for Metropolitan Wireless Network Area (WMAN) coverage[2].

Any wireless network is consists of fundamental elements: (1) EU (End User) device, i.e. EU wireless host consisting of a laptop which can be connected with multiple adaptive antennae, palmtops, PDA and desktop computing devices. (2) BS (Base Station) i.e. this is a key part of wireless network infrastructure which is responsible for sending and receiving signals on air. Cell tower and Access Point are two main examples. (3) Wireless Links i.e. a radio connection between wireless devices and a broadcasting base station. These are also referred as a wireless system.
A wireless communication link can have many properties with different signal anatomy. Any wireless network has two major management modes called infrastructure tail mode and ad hoc (mobile ad hoc) mode. In infrastructure tail mode, wireless network management has a controlled and centralized architecture, while in ad hoc/mobile ad hoc mode (MANETs) end users are responsible for catering to their own mandatory requirements. SNR (Signal-to-Noise Ratio) is a relative measure of the transmitted/ received signal strength vs. the noise (background) and is measured in decibels (dB). BER (bit error rate) is the probabilistic ratio between the transmitted bits from a transmitter to a receiver in error at a wireless receiver. SNR is inversely proportional to BER, i.e. by increasing transmission power; we would obtain a lower BER curve. 802.11 uses the CSMA/CA protocol for sending and receiving its data frames between AP (access point) and EU (user end). The transmission is bounded within the framework of RTS (Request to Send) and CTS (Clear to Send). IEEE 802.11 is a Four-Way Handshake protocol, which is the architecture defined in RFC 1042. IEEE 802.11 (Wi-Fi) follows the mandatory criterion defined by ISM (Industrial, Scientific, and Medical) Band i.e. from 6.765 MHz to 244.00 GHz [2-5].

Fuzzy logic and Neuro Fuzzy logic are set-base approximate reasoning methodologies. They represent different granules which are combined to formulate a projection onto the universe(s) of interest. The Fuzzy set framework is a pattern of reasoning under uncertainty involving axioms of Artificial Intelligence (AI). What we intend to do in this research is to have a Function-layer design model using Fuzzy Logic that will provide the Access Point with an ability to take a secure predictive decision against False Access Point association as well as False Access Point activities’. Fuzzy Logic and Neural Network are branches of mathematical science that can be used as inference models with crisp logic (maxima and minima), having a number of inputs and outputs as their Functional solution. This Functional model can provide security for any wireless client, with respect to a wireless
Access point; from which their spatial positioning in any operational time period must be validated prior to any succession. Temporal variables of these Functional models will continue to maintain a valid, verified connectivity. This connection succession will continue with its peer as long as the mandatory aspects of an Access Point in communication holds true in nature.

**Chapters outline**, this section of our thesis gives the outline of the Thesis. Section 1.1 explains the motivation of the thesis. Here we will explain how imperative it is to have a trust paradigm between any two Access Points. These Access Points can be in a wireless client-server role or peer to peer, routing and AAA role. Section 1.2 explains the background knowledge with respect to the motivation of the thesis and research related objective work. Section 1.3 outlines the research work with the approaches that have intended to improve the problem aspects of security and reliability between any two wireless Access Points in communication. Section 1.4 explains the background of the thesis security architecture. Chapter 2 discusses the Literature frame work with respect to the research scope. A major component of this chapter is Wi-Fi and its IEEE architecture. A Fuzzy Logic tool box by using Matlab will conclude the chapter’s literature review. Chapter 3 presents the problem definition. It defines two main Wireless Security Vulnerabilities i.e. Denial of Service (DoS) attack and Man-in-the-Middle (MiM) attack. Chapter 4 presents the methodical approach; with respect to the wireless modelling, wireless security threats and Fuzzy logic Functional model approach in order to curb the shortfalls, with respect to the Four-Way Hand Shake protocol. Chapter 5 presents modelling aspects of Wi-Fi physical layer network. This Matlab model, along with Security Swarm Wireless Access algorithm, improves wireless security paradigm. Chapter 6 provides a solution for improving Wi-Fi security in case of MiM Attack. The Security Swarm Root Node algorithm is proposed for an Access point to curb MiM attack. Chapter 7 provides a brief conclusion and future research directions.
1.1 Motivation

Wireless Sensor Networking (WSN) is very common for corporate organisations and personal individual use. Almost all communication devices have built-in wireless capabilities, from which arise many security issues. Wireless Local Area Network (WLAN) is not only flexible but also a versatile communication network, as compared to its wired network counterpart. Authentication of a resource network user is pivotal in order to detect and prevent misuse of associated resources[6, 7].

WLAN broadcasts and transmits data over the air using radio wave paradigm. Wireless security involves three major issues, such as Authentication, User Privacy with respect to Internet of Everything (IoE) and System Authorizations. IEEE 802.1X Families as represented in figure 1.1. This represents the framework of wireless network architecture paradigm which can be divided into two major sub fields i.e. Infrastructure-based and without Infrastructure (which can be further classified as Mobile Ad-Hoc Network). Furthermore, Mobile Ad-Hoc network classification also inherits the properties of Distributed System (DS) and Extended Service Set (ESS) with respect to Basic Service set (BSS). The standard can further be sub-sectioned on the basis of access method for wired or wireless communication [8, 9] systems.

Mobile Ad-Hoc Networks (MANETs) have their own sets of communication aspects, i.e. each Access Point or wireless node is responsible for managing its own activity but must share common communication aspects; while Wireless tail Infrastructure with Access Points has well-defined architecture in terms of verification and validation. Henceforth, the False Access Point [10] of operation is a vulnerability that persists throughout the wireless communication system. This wireless vulnerability has been curbed by introducing a Fuzzy Logic Function models.
Without formal security implementation, any attack on any wireless internet user, computing machine or network resource can make it temporarily or permanently unavailable for use. The unavailability of an online resource with respect to its internet services is known as Denial of Service attack (DoS) or Distributed Denial of Service attack (DDoS). Perpetrators of DoS attack typically target high profile machines, e.g. Banking Domain Servers, Credit Card Gateways or even Root Name Servers. Common methods are to saturate a target machine with external requests, whence it cannot perform its defined task. Some common methods of DoS attacks are ICMP flooding, SYN flooding, Tear drop attacks, low-rate Denial of Service attack, Peer to Peer attacks, Lack of symmetry of resource utilization in Starvation attack, Permanent Denial of Service attack, Application Level Flooding, Nuke, Distributed attacks, Reflected Spoofed attacks and Unintentional Denial of Service attack. The major reason for any derivative of DoS and MiM attacks (or both) is presence of False
Access Points. A False Access Point or wireless node can also mutate a further complex attack scenario of Man-in-the-Middle (MiM) attack. These unauthorised complexities can be contained within the defined paradigm of Open System Interconnection (OSI) Model. Following figure 1.2 defines the standards with respect to OSI Model layers.

Figure 1.2: OSI Model for Wireless Network

This figure (1.2) also explains the complexity and interconnectivity for wireless standards. Modern networks that are ubiquitous can be further aggravated by their reliance on connectionless oriented protocols, such as IP and other proprietary protocol suites [8, 9, 11-13]. Wireless Network is defined on the basis of bandwidth, throughput and access method such as IEEE 802.11, IEEE 802.15 and IEEE 802.16. These can be further classified with respect to security research activity i.e. IEEE 802.11i (Wi-Fi Security). Wi-Fi security is not only calibrated with respect to service provision and coverage area but also with respect to the security solution framework. In the model represented in figure 1.3, an interesting fact to be noted is that IEEE 802.10, protocol suite does not intersect the boundary of OSI Physical Layer Model. Management frame with respect to MAC header used for probing will have no previous state memory address as an initial reference. Control frame and Data frames thus
became beyond the control of security management and resilience structuring.

Figure 1.3: IEEE standards for communication

Physical Layer Security attacks in IEEE 802.11i are Jamming, Data Traffic Modification, Denial of Service, Man-in-the-Middle attacks with respect to CIA security framework. IEEE 802.11i defines the security standard for Wireless Local Area Network (WLAN), and is designed to eradicate the WEP attacks. It has been further observed that these standards are not capable of defending itself against any DoS/ DDoS attacks. Henceforth, some authors have proposed 3-Way handshake protocol to prevent DDoS attack, which is cost effective in computation. Elliptic curve Diffie-Hellman (ECDH) protocol used for offline directory and internal attacks are thus no effective. However beside attack validation and verification with respect to Protocol Composition Logic (PLC), DoS and MiM attack scenarios still persist. A new Function layer model which we have proposed can improve, eradicate these threats and can also provide reliable security performance in any wireless network infrastructure [14-19].
IEEE 802.11i defines two types of approaches. One is Open/IEEE 802.1X and another one is Pre-Shared Key (PSK) approach. These are a probing mechanism used by supplicant/STA for Authenticator/ AP. An Open approach is a port-based (Service Access Point) approach, without the use of any encryption method or hardware (OSI Physical Layer) cipher.

1.2 Related work

Wireless network user Access Points are becoming increasingly reliant on High Dataflow and Heterogeneous connectivity. Security services are becoming very important with respect to trust validation and verification between them. Wireless networking Paradigm, just like the wired counterpart network, has three main aspects: (1) Network Topologies, (2) Access Methods and (3) Medium of Communication. Thus, the wireless Access Point, the wireless link and the base station are the major elements for a wireless networking system. Wireless network infrastructure can be divided into several architecture layers as described by OSI. The following Table 1 highlights major security threats and vulnerabilities. The focus of our work with respect to False Access Point detection and avoidance will be mainly on lower and more fundamental layers.

Table 1: Wireless network security vulnerabilities.

<table>
<thead>
<tr>
<th>OSI Layer</th>
<th>Wireless Security Threats</th>
<th>Security compromise criterion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Layer</td>
<td>Message Interception</td>
<td>Cryptography or Security key substantiations.</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>Routing Session attack</td>
<td>Resilience to Access Point compromise.</td>
</tr>
<tr>
<td>Data Link Layer</td>
<td>Session Hacking</td>
<td>Collision, Contention, Exhaustion.</td>
</tr>
<tr>
<td>Physical layer</td>
<td>Denial of Service</td>
<td>Frequency Jamming, Access Point Tampering</td>
</tr>
</tbody>
</table>
The main objective for defining IEEE 802.11i security standard is to provide reliable access control management for any WLAN and eradicate attacks against Wired Equivalent Privacy (WEP) as well. IEEE 802.11i has been able to provide a solution regarding confidentiality, mutual authentication, and integrity for WLAN environment. However, it (Four-way Handshake Protocol) has not been able to provide a secure security mechanism against Denial of Service Attack (DoS) and False Access Point identification, such as association and de-association criterion. Two-Way Handshake and 3-Way Handshaking protocols have been proposed, to optimise security by constraining Handshake session but not to secure the functionality of the existing protocol. The main purpose of this work is to improve the security of the existing defined standard and to propose new measures. These measures must not only address previous shortfall but should also provide framework for future directions as well. Security management against DoS and MiM attacks still remains a question where Risk management and vulnerability are not challenged with respect to the axioms of wireless user-Access Points association. In order to provide a secure wireless connectivity over a wireless network, tailed or without, IEEE 802.11 Task group has proposed Wired Equivalent Privacy (WEP), a mechanism for data encryption, authentication between Mobile (MS) and Authentication Centre (AuC) device. To repair the problem with respect to WEP and without any additional hardware cost, Temporal Key Integrity Protocol (TKIP) with keyed cryptographic Message Integrity Code (MIC) mixing function has been proposed.

IEEE 802.11i was ratified on 24 June 24 2004. The IEEE 802.11i process combines 802.1X authentication with succession key management procedure to generate a fresh Pairwise for data transmission on wireless session.
Figure 1.4: Wi-Fi connection stages

Figure 1.4 depicts the underlying stages for any WLAN, Wi-Fi connectivity. Henceforth, the possibility for any wireless Access Point to know that it is not a part of rogue network Access Point, for secure access, is still in doubt. End-user internet information access with respect to privacy lifeline can forecast its pivotal security needs. Computer, Command, Control, Communication, Intelligence Surveillance and Reconnaissance (C4ISR) application requires uninterrupted and secure channel management. Wireless network security can be divided with respect to the network access method protocol and its Architecture suite.

A False Access Point [20] is an attacker Access Point installed and controlled as well as monitored by an attacker in order to intercept and accept the traffic from wireless clients (wireless system). It disguises itself as a valid Authenticator and thus it can extract and
forward packets to launch further complex network worm attacks. More complex and comprehensive study is required in order to mitigate this attack [21][17].

As a result, possibility for any wireless Access Point to know the fact that it is not part of a rogue network for a secure access is not very well defined. Thus, the Functional model is required for an end-user Access Point, requiring for internet information access with respect to privacy lifeline, can also be protected. The critical threats that today’s Wi-Fi has to encounter are Rogue Roger Rogue Network Access Point (R3N2), Man-in-the-Middle, Eavesdropping, Masquerading, Management Message Modification, Denial of Service attacks.

Figure 1.5 represents the IEEE 802.11i algorithm. It represents the connection and association for current Wi-Fi network associativity. It also shows that any wireless client Access Point prior to an association has no way to predict its true association with respect to prior authentic ethnicity. Figure 1.5 defines the Wi-Fi (Four-Way Handshake protocol) association. It has these following stages:

**Stage 1**: Network Discovery: Supplicant observes and maintains the list networks by monitoring broadcasted frame from AP, and/ or the probe response ACK from APs.

**Stage 2**: IEEE 802.11 authentication and association: Supplication will choose one AP from the probed list, as it has no prior memory, and negotiate the security parameters for association.

**Stage 3**: IEEE 802.1X: At this stage supplicant will choose generated Master succession Key (MSK) for which Pairwise Master Key (PMK) is used. EAP is also used for strong authentication.

**Stage 4**: 4-Way handshake is performed to generate Pairwise Transient Key (PKT) with respect to nonce. ANonce and SNonce are Access Point and supplicant alphanumeric representation respectively, as shown in figure 1.4 as well. Formula for PTK is:
PTK = PRF-n [PMK, “Pairwise Key Expansion”, {min (AA, SPA) ||max (AA, SPA) ℓ}; Where PRF is Pseudo Random Function and n mean number of bits required.

AP = Access Point
ANonce = Once Used Digit from AP
STA = Wireless Station
PMK = Pairwise Master Key
PTK = Pairwise Transient Key 64 Bit
SNonce = Once used Digit from Client Station
GTK = GroupWise Transient Key 32 Bit
MIC = Message Integrity Code
ACK = Acknowledgement

STA
Supplicant (PMK)

AP
Authenticator (PMK)

STA Construct the PTK

{SPA, Snonce, SN, msg2 + MICPTK(SNonce, SN, msg2)}

AP Construct the PTK

{GTK(AA, Anonce, SN+ 1, msg3) + MICPTK(ANonce, SN+ 1, msg3)}

STA Verify PTK

{GTK(AA, Anonce, SN+ 1, msg3) + MICPTK(ANonce, SN+ 1, msg3)}

AP Verify PTK

ACK

Figure 1.5: IEEE 802.11, 4-Way Handshake Algorithm

14
Stage 5: iff supplication requires Group Transient Key (GTK) for multicast key for its multimedia streaming as defined in IEEE 802.11n, IEEE 802.11ac or IEEE 802.11ad.

Stage 6: Data communication renders with respect to PTK/ GTK, between Supplicant and Access Point[17, 21].

The respective steps are also depicted in following page figure 1.5; showing the Four-Way Handshake IEEE 802.11i algorithm. Our main objective is to implement Wi-Fi algorithm with new proposed Functional layer model in order to improve the wireless security aspects of a wireless Access Point in communication.

1.3 Research objective

Is the easiest way to protect a network attack is to close it off completely? The purpose of network is to be service-oriented within the framework of Application Service, Internet Service and Internetwork Service provision. Wireless interconnectivity has been efficient and robust but not very secure. However, these are significantly down sized when security threat severity increases to financial notoriety, theft and damages for all or some applications in its connection scenario. False Access Point associativity provides means to perform crime, with a defined motive and organised opportunities. The role of an adversary as False Access Point, can lead to may complex data-mining-machine-learning, catastrophic scenarios. Wireless networks have serious real time security handshake limitation concerning security, evaluation, prediction and association. Therefore, real-time multimedia applications such as M-Commerce, Mobile-Medicare support, State Emergency Services (SES), POLICE, and other geographical train surveillance with respect to C4ISR, require integrated and robust realtime connectivity[22].
The question remains on the assurance and trust relation for any wireless Access Point prior to its association that it will not be part of a False Access Point activity, as well as how often one must validate or verify these trust parameters before and after its association. The upcoming version of Wi-Fi, i.e. IEEE 802.11 ac and IEEE 802.11ad are more focused with respect to improve bandwidth throughput. Again, the wireless security vulnerabilities are still not addressed adequately. The main objective of the research is to formulate a Function layer model for improving the wireless security [17, 21, 23, 24].

Figure 1.6: Research objective parameters

The pivotal parameter for trusted communication between any two or more wireless Access Points also requires more refined definition. Our research objective is within the framework of Wi-Fi security. Security optimised management of these aspects are defined with in the ISO/IEC Guideline for IT Security Risk Management and Assessment as shown in figure 1.6. It explains framework of wireless network in relation to AI in order to improve security aspects[25].

Our area of focus is Wi-Fi security that is bounded with three parameters of two non-polarized doctrines. First area is associated with Wireless network [23]and how we can improve its Security by using Artificial Intelligence (AI). The two other shadow areas seek
how we can fine-tune these parameters, such as Flexibility of learning and accuracy with respect to implementation. Thus accuracy for any project design is a trade off with respect to its time and space. Complexity of this research is controlled by defining the area of access method that is Wi-Fi wireless network. Furthermore, Fuzzy Logic or/and Neuro Fuzzy Logic are used to control the research area flexibility. Complexity of thesis research area is inversely proportional to Wireless Network, i.e. Space and Time operation relation within the framework of Wi-Fi together. Security and accuracy are also another paradigm which is not directly proportional i.e. Security criteria must be defined in a manner where less is always more, rather the contrary. For example, a very accurate security verification and validation is always required rather than a solution with a diffusely prolong response time. Wireless network has many academic research areas such as Wi-Max, UMTS, LTE-4G and etc.[26-28]; with respect to the coverage and mobility aspects of the system. However, because of imperative aspects of every day and rapidly evolving standards, IEEE 802.11i is the main area of this research objective.

1.4 Research outline

It is progressively becoming difficult to define and maintain a secure network computational environmental framework. Any network infrastructure within the public, private or any government emergency support has threats not only internally but externally as well. Furthermore ROI (return on investment) calculates and defines toll-bypass network operation convergence. In this chapter we will provide an overview of general categories of attacks and countermeasures existing within the paradigm of wireless network computation engineering[29].
1.4.1 Security overview

Information access classification and authorisation is the first principle for deployment of any wireless or wired network. Sometimes information classification is a regulatory requirement. It can be labelled as liability issue but data access validation is deemed an integral component of network security. Following are the key components in comprehensive security architecture for a WLAN: (1) Administrative Controls are largely procedure-and-policies oriented. They are designed based on risk management policies of the system. (2) Technical design, involves electronic hardware devices and there access method. (3) Physical aspect of a system components are associated with the physical environmental operational condition and are generally within the end user area of concern.

Security risk management associated with any wireless network are further classified in to three area i.e. Control Objectives for Information and Related Technology (COBIT), International Standard Organisation (ISO 27002) and Information Technology infrastructure Library (ITIL). COBIT is a supporting toolset allowing managers to bridge the gap between control requirements, technical issues and business risk management. ISO 27002 is well-respected and is associated with security authorisation, security control, and many security information policies. ITIL is a set of practice for IT service management that grasps and aligns IT services and policies.

1.4.2 Accountability

It is a security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. Its objective is to hold accountability for both system users and administrators. Accountability is often an organisation policy requirement and directly supports non-repudiation, deterrence, fault isolation, intrusion detection, prevention and legal action. These aspects are becoming more and more important as businesses are turning their
infrastructure towards online electronic communication media. For example, in an e-business transaction between online user and business store, it maintains a succession of communication, exchange credit card details and receipt. Hence, both the user and store should be accountable for their communication and behaviour.

1.4.3 Assurance

Assurance grounds for confidence that other security goals (including integrity, availability, confidentiality and accountability) have been adequately met by specific implementation. “Adequately met” includes: (1) functionality of correct performance procedure for validating and verification of an electronic event, (2) sufficient protection against unintended errors, i.e. exception handling of errors must be raised properly, and (3) sufficient resistance to intentional penetration or by-pass must be formulated.

1.4.4 Authentication

Authentication is a process of verifying the validity of an instance requesting a transaction, on a resource. Requesting process can be a user, device or a triggering event requesting its access to a system resource. This objective requires that the identity (or the relevant information) of an entity or the originator of data can be verified and assured. Fulfilling this objective can prevent faking or masquerading from happening.

1.4.5 Authorisation

Authorisations are an event of granting or denying access rights to a user, program process or triggering of an event. This objective requires that only a legitimate user can have the right to use certain services or to access certain resources, while the contrary are kept out or restricted. This process is also defined as “access control”. Different IT vendors have various methods for organisation of access control data structure events. Authorisation is often combined with authentication in order to implement system authentication and therefore to
validate the request as a grant or a void. At a higher layer of communication, digital signatures with various succession keys are used to define resource authorisation.

1.4.6 Availability

Availability is a security goal that generates the requirement for protection against incidental or accidental attempts to perform unauthorised deletion of data, or to cause unavailability of service. This objective requires that data and system should be accessed by legitimate users within an appropriate system time slot. Some attacks such as Denial of Service (DoS) attack, Man-in-the-Middle (MiM) attacks, or instability of a system may cause loss of availability[30].

1.4.7 Confidentiality

Confidentiality is the security goal that generates the requirement for protection from incidental or accidental attempts to perform unauthorised data reads. It covers data in storage, and even during processing. Hence, objective is that data must be assessed by the authorised user or program process for which it is intended. Loss of confidentiality generates serious level of privacy breaches and can generate loss or compromise in system data.

1.4.8 Integrity

Integrity can be classified as data integrity and its system association. Data integrity is an objective where data should not be altered or destroyed in an unauthorised manner and therefore keep maintaining its consistency. It also covers data in storage or during processing. System integrity is an objective where system should be free from unauthorised manipulation while performing its intended function in an unimpaired manner.
1.4.9 Non-repudiation

This objective requires that either side of a communication cannot deny the communication later. Important communication exchange must be logged to prevent later denials by any party of transaction. It also relies on authentication to record the identities of entities. Accountability, availability, assurance, confidentiality and integrity are the five major paradigms of a wireless network security.

![Diagram of security objective relationships]

Figure 1.7: Security objective relationships

Figure 1.7 explains the relation between five imperative aspects of wireless network security whenever wireless Access Points are in communication. This figure is system specific. Certain security parameters may conflict during system operation, such as increasing the
availability of a system resource may compromise its confidentiality or integrity level of operation. Therefore, over all security policy are often preferred to an individual security objective.

1.5 CIA Model

The CIA triad (Confidentiality, Integrity, and Availability) is one of the core principles of information security. Any basic security model comprises of benchmarks defined by ISO and HIPAA. CIA paradigm has three basic subset models such as Risk based, Benchmark Based as well as Diligence based.

The security architecture of any organisation depends on the understanding of its culture, experience and commitment to its security objectives. Risk-Based model is driven on qualitative or quantitative and on both elements of security aspects. Benchmark model has not been implemented as a whole model for an organisation; rather certain elements are implemented, such as what are the parameters for secure e-mail transactions’, system configuration with respect to Remote Procedure Call (RPC) or Remote Directory Synchronisations (RDS). The third model i.e. Diligence Based model has main emphases on information assurance with respect to diligence, compliance and enablement of an information system.

1.5.1 Confidentiality attacks

Confidentiality breach is an attempt when an attacker attempts to access reading only-sensitive data. These attacks are very transparent as an attacker can easily copy sensitive information without any trace activity. Network scanning activity is also called as fingerprinting. These are of two types- active and passive. Both can lead to emanations capturing. The main cause of confidentiality breach is mainly due to incorrect data directory access permission. In order to eradicate this, an appropriate directory data access level must
be associated, with respect to user information access. In figure 1.8, an attacker can compromise an exposed web server. That is because of the False Access Point that breached this server and caused it to become exposed for malicious activity. This enabled an attacker to gain full control of the database server [2, 15, 31, 32].

![Diagram of Web Server, Database Server, Internet Connectivity, E-Retailer, Branch Office, and steps of the attack](image)

**Figure 1.8: Breach of Confidentiality**

Such attacks are difficult to curb since attacker has not modified the data within the system. There are many methods to compromise confidentiality. Most common are as following:

i. Packer sniffing: Intercepting and logging traffic that passes over a digital network or a segment of network.

ii. Port scanning: Searching a network host for open ports for any semaphore procedure.

iii. Dumpster diving: Searching through company dumpsters or trash cans looking for information such as phone book, login identities, memos, or other thesis which can be
used as a valuable source of information. Even files in system heap memory areas can be used.

iv. Emanations capturing: Capturing electrical transmission from the equipment of an organisation to deduce information regarding organisation.

v. Wiretapping: Monitoring telephone or Internet conservation of a third party, often covertly.

vi. Social engineering: Using social skill or relationships to manipulate staff or friends inside the network to gain or deduce information to gain network access.

vii. Overt channel: Obvious and visible method of communication. Overt channel can be used for covert communication.

viii. Convert channel: An attempt to hide the coded information in transmission channel, based on different set of data encoding rule sets.

All of the above mentioned classifications are potential methods for Phishing and Pharming. These are attempts to acquire sensitive information with respect to user access such as user name, password or credit card details i.e. masquerading as a trustworthy entity in a form of a disguised False Access Point attempt. Pharming attack is mainly aimed for more aggressive attacks such as Blackhole attack or Wormhole attack where False Access Point also redirects network traffic to another Access Point [33].

1.5.2 Integrity attacks

Integrity violation transpires when attacker attempts to change any sensitive data without proper authorisation, i.e. when an attacker has access to read, write, and execute a memory heap area and detach the former authority from it. Furthermore, the owner might not detect till access is denied. Many organisations consider Integrity attack as a very serious threat against their networked architecture, since sometimes it’s difficult to identify and eradicate these in real time.
For example, a consolidator of credit card transaction proceeds to make a batch transfer to a bank for all the transaction that took place during the previous 12 hours. A hacker could intercept and compromise the resumé of the ongoing transaction. Neither the bank nor the consolidator would have the clue that some of the totals in the totals are compromised. The following are some of the attacks which compromise integrity of a wireless system:

i. Salami attacks: These are series of small attacks where an attacker renders minor data security attacks and inflicts a very large loss for an organisation. A fraud activity in a bank where an employee steals small amount of funds from several accounts is an example of salami attack. It is virtually undetected when a complaint is launched from several bank customers with respect to the stolen funds.

ii. Data diddling: This attack involves the change of transaction before and during the input into a computer. A compromised and unattended application can be used without any alarm.

iii. Trust exploits: It’s an event where an individual can gain trust and can render malicious activity. Passive example would be MiM attack.

iv. Password attacks: It’s an attack which attempts to identify a user account, password, or both. A password attack often uses a method called brut-force attack. However, it can also be employed by using Trojan horse program, IP spoofing, key loggers, packet sniffing, and etc.

v. Succession hijacking: It’s an exploitation of valid computer succession, sometimes also called succession key, to gain unauthorised access to information of services in a computation system. TCP succession hijacking is a common variant of MiM attack[34].
Figure 1.9: Integrity Attacks

Figure 1.9 is an example of integrity attack, where a hacker has gained trust of a database server behind a DMZ. He has previously hacked server A (web server) trust and therefore now has full control of the database. In other words, database server trusts server A, server A trusts every one, resulting in database server trusting everyone. Similar examples can be found in Windows Active directory and Linux default Network Information Service Plus (NIS+). Figure 1.9 also reflects a port re-direction attack by exploiting trust-base attacks. Above figure also shows a standard Firewall with three interfaces - inside, outside, and DMZ. A compromised host at DMZ level can reach out to a target machine in order to create a virtual trunk with single or multiple compromised re-directed ports and thus can violate the
rule base implementer because of an expensive firewall device. Such a procedure is termed as Grayhole attack.

Password attack can be implemented using several methods such as brute-force attack, trojan house applications, IP spoofing, key logger, packet sniffers attacks. Plain text is security risk; hence it’s stored in an encrypted format to overcome this risk. Almost all systems use these stored passwords by using one way hashing function, as one cannot reverse to obtain the plain text. However, hacker can use many techniques to crack the password, such as following:

i. Word List: These programs use list of words, phrases, or other combination of letters, numbers and symbols used by the system. It’s implemented in a form of high speed dictionary attack until a match is found.

ii. Brute force: It is a show process that relies on power and repetition of permutation and combination until a match is found.

iii. Hybrid crack: It is the combination of both the above mentioned operations. Poorly constructed operation can easily be cracked.

Password cracking can be implemented on all those systems that accept authentication including the following:

i. NetBIOS over TCP (port 139)

ii. Direct host (TCP port 445)

iii. FTP (TCP port 21)

iv. Telnet (TCP port 23)

v. SNMP (UDP port 161)

vi. PPTP (TCP port 1723)

vii. Terminal services (TCP port 3389)
1.5.3 Availability attacks

The responsibility of an operation rests on everyone that takes part to keep a network, computer system and its application services online. Any attempt to compromise the availability of a system resource is defined as an availability attack, for example DoS attack. A DoS Attack is an attempt to compromise the availability of a network, host or application[35, 36].

Attacks against the availability have three main objective models i.e. consumption of scare or non-renewable resources, destruction of a resource information as well as physical destruction of network model. Hackers can use many types of attacks to compromise availability of such resources. Some are as following:

i. Botnets

ii. DoS

iii. DDoS[37]

iv. SYN floods

v. ICMP floods

vi. Electrical power

vii. Computer environment

Failure of hosts or applications to handle an unexpected condition such as maliciously input format or crashed link with respect to DMZ links are one of the major causes of above mentioned failure.

1.6 WLAN countermeasure of CIA model

Countermeasure paradigm not only focuses on solving a specific problem, but also number of different classes and domains. The most vulnerable area is wireless network security where confidentiality, integrity and availability are not overlapped. Some authors have proposed
that CIA model for rendering a WLAN security is not adequate; henceforth strategies for better Validation and reliable Disaster Recovery (DR) must also be in places.

1.6.1 Validation and access control

For validation, as a countermeasure for securing a wireless network and its application, it’s imperative that a proper functional and integrated model must be in places at different communication layer sets. These layer sets can be at a physical layer, Network access layer, Operating system layer, including database management, file sharing and online application portals. In the process of validation, one entity proves its identity to another challenging entity. This is a very important aspect of security reliance and service dependencies [38-40].

In a WLAN access method policies are high level guidelines which are pivotal for secure and reliable connectivity and operation. These criteria determine access control and user management roles with respect to the system interface. System login validation access methods can be classified as following three classes:

i. Mandatory Access Control (MAC)
ii. Discretionary Access Control (DAC)
iii. Role Base Access Control (RBAC)

MAC is a process where user Label tags are compared with the sensitivity of the system object Label tags, iff MAC validation is verified, a specific user is granted an access otherwise its denied. Security architecture organised with respect to MAC has three major requirements 1) the protection decision must not be decided by the owner object. 2) Protection decision must always be integrated with respect to POSIX.6 (http://en.wikipedia.org/wiki/POSIX). It also provides object labelling mechanism and 3) user level access interface priorities.
DAC is the most common user level access method. It restricts user object based on identity of the user. User association is often exclusive or within group and tree of an object system. DAC is discretionary in nature and tends to pass access permission level to other user directly or in-directly as well. Access rights of an object in DAC are of read, write, execute and inheritance defined by their operation roles. DAC permissions on system object are files and directories and can be overridden by any super user. Henceforth, it is susceptible to a trojan horse attacks. Usually DAC and MAC are implemented together for improved validation mechanism.

RBAB model is a function approach where role is a permission grant with respect to the authorisation. These are defined according to data object and inheritance of their resources used by the authorised user. This role base model also has the capability to support multiple access control policies and support both MAC and DAC models as well. Validation function in a WLAN is defined and implemented in a matrix format, where numbers of wireless network resources are represented in column and user privileges in rows. Microsoft Windows, Novell NetWare, Digital’s OpenVMS, UNIX- BSD and Linux are some of the examples. Access Control List (ACL) is a method where users and resource objects are arranged in matrix format and where files and directories are objects with the corresponding crossed user privileges. Validation architecture, known as Capabilities, corresponds by row organisation[41]. In this function model when a process presents a capability on behalf of a user, the operating system examines the capability to determine both the object and access a privilege. Its location is encapsulated in the capability. Similarly to ACL, for example if user object is given, what and how many network resources subject elements can be accessed?. Or if a resource is given as a subject, then how many user objects can be accessed at a time?.

Third method for WLAN Security validation is known as Authorisation Table, which has the advantage of both method i.e. ACL and Capabilities. It contains entries specifying which user
or group of users have what access rights to which object. Sorted on object, it becomes a set of ACL, while sorted on subjects it becomes a set of capabilities [22, 42-45].

1.6.2 Audit and Intrusion detection

It is a process of review of an occurred event versus practice standard procedures, in order to validate and control the system. There are two types of audit, Compliance audit and Event audit. Compliance audit is main focus of E-Commerce PKI Glossary (http://en.wikipedia.org/wiki/Information_security). Compliance audit has three major categories, i.e. regulatory audit, internal audit and certified public accountant audit. Event audit with respect to intrusion detection is a continuous behaviour of the system, i.e. what is happening in the system and its analysis. Such type of event audit requires a Knowledgebase system; however detection of a new anomaly cannot be detected in real time. It is also possible to mutate the Knowledge base in favour of new anomaly. Design CPN (http://www.daimi.au.dk/designCPN/) and fizzy neural network are very accurate tools for designing and simulating any modern IDSs’ such as misuse IDS model, anomaly IDS model and specification-base IDS models.

1.6.3 Extrusion detection and cryptography

Extrusion detection is the analysis of a system activity and its study of an outbound traffic. It is a process to detect and protect system from malicious users, malware, or network traffic that can be a threat. In this method both system and user information is recorded as a baseline data entry. It covers all the hardware and software aspects of the system and later data mining techniques such as association rules, frequency rules, classification analysis, links and sequence analysis are used. Existing extrusion and proper feature behaviours are studied in order to build an operation profile to compare an event of future extrusion detection[46].
Cryptography is a paradigm of encryption and decryption of data. Data transfer security on air is not only tedious process but it’s also relaying on air. Cryptography process is widely used for data protection and securing its content especially on air.

Figure 1.10 depicts that initiator/ sender must encrypt the plain text into illegible cipher text. This text is transmitted over unsecure channel. When this message is received at the receiver end it is decrypted in to plain text again. Encryption and decryption is based on certain algorithms and secrets, which are called “keys”. It is desired that the choice of encrypt or decrypt algorithms and key could fulfil certain criteria such as encryption. Encryption is easy, while decryption without the key should not be possible and other benchmarks must fulfil the organisation Standard Operation Procedure (SOP). Keys can be classified into two main types, symmetric cryptography and asymmetric cryptography key. Symmetric key distribution is also known as shared-key cryptography, thus sharing a common key for both processes of encryption and decryption. In this process Key Distribution Centre (KDC) is often used, which uses a secure channel for the key distribution with respect to encryption and decryption of the message as shown in the following figure 1.11.
Asymmetric cryptography is also known as “public key cryptography”. In this process two keys with a mathematical algorithm (such as DES, RSA, etc.) are generated and are linked together, where one can be used to encrypt data and other is used for decrypting the receiving data. In this process the encrypting key is made public and is used for encryption of the text data while the other key is kept secret and, also represents the owner and known as private key.

As shown in the following figure 1.12; anyone can encrypt the data using the public key but it is the rightful receiver with specific private key who will be able to retrieve the plain text data.
1.6.4 Firewall and DMZ

Firewall is a security mechanism with respect to any inbound and outbound traffic. It is imperative that all the wireless edge devices as well as wireless Access Points have detection and avoidance mechanism with respect to rogue detection and avoidance. Firewall technologies provide both physical and logical protection with respect to network access.

The three main categories called packet filters, proxy servers and state-machines with multilayer access methods[47-49] are as following:

i. Packet filtering firewalls: Packet filtering is the most basic form of firewall security method. In this mechanism each packet is compared with a set of predefined rules. These rules also define the procedure and event log activation criteria as well. It is limited to OSI Network layer. These are also susceptible to IP spoofing.

ii. Proxy servers: It is a security mechanism where hardware plays pivotal aspect. It is generally recommended that proxy servers must be a multi-home piece of a device. Generally proxy servers are succession oriented i.e. these monitor with respect to network address, ports and semaphores. These have two main classes called circuit-level gateway and application-level gateway. Circuit level gateway works at OSI-Succession layer. It provides and secures the web-network cash traffic. Application-level firewall uses the support of circuit level and provides security decision with respect to network applications[50].

iii. State-machine-firewall: This is a set of algorithms that recognize and process application layer data, rather than using an application at Application layer. Set of State-machine-firewall is transparent to the user and resides at all Network and Transport layers. However, these are more complex and require highly competent personals for administration.
Layer defence mechanism in firewall uses combine depth to protect the security integrity. Firewall or DMZ without a knowledgebase is not capable of protecting against rogue network association and connectivity.

Figure 1.13: Layered defence strategy with respect to Firewall and DMZ

Perimeter Security is an example of packet filtration firewall process, while proxy server firewall encapsulates the features of communication layer. Finally with respect to figure 1.13, state-machine firewall is also responsible to deal with and trigger an event of remote disaster recovery paradigm in case of threat log alarm. DMZ is set of corporate servers within the domain of application service provision, accessible for general public. DMZ provides functionality between a combination of untrusted and trusted polices. Policy rule set is also a combination of public and private rules associated with the network and its access methodologies.
Chapter 2

2 Literature review

The objective in this literature review is to briefly explain Wi-Fi networks limitations and vulnerabilities. This section is divided into three sub-areas, namely, wireless network standard Wi-Fi, security threats and utilisation of Fuzzy Logic for improving security performance management of Wi-Fi networks. Figure 2.1 depicts framework outline.

IEEE 802.11i wireless standard is carefully selected[32, 51] with respect to the problem definition and its system complexity. Complexities which have been considered are first point of contact of any wireless Access Point to its surrounding system network architecture.
System security vulnerabilities addressed are the issues of Confidentiality, Integrity and Availability (CIA) attack against acquiring access control. Improving secure measures for wireless network have been proposed by developing various functional models that have mitigated the effects of DoS and MiM attacks. Operation research flexibility has also been frame-worked by carefully considering the domain of Artificial Intelligence i.e. Fuzzy Logic and Neuro Fuzzy Logic. This is a branch of science that deals with the conditional probability with respect to the system’s surrounding and helps the object to choose the best case.

2.1 Wi-Fi

Wireless Local Area Networks (WLAN) are gaining popularities with robust throughputs and relatively easier and simple deployment. They are installed by businesses communities of all walks of life i.e. emergency support institutes, educational institutes and government, etc. The freedom of mobility that WLAN inherits, as compared to its counterpart (a wired network), comes with its own serious security challenges [52].

WLAN has many standards for its area of coverage, data transfer rate and mobility with respect to sensor localised association [53]. Amongst such standards, IEEE 802.11i is popularly known as Wi-Fi standard. The purpose of this standard is to connect and exchange data wirelessly. However, wireless network connectivity has many vulnerabilities. These shortfalls are mainly due to untrustworthiness of an associated service point. Such arbitrary or unpredictable operation of any service providing Access Point can be defined as a False Wi-Fi access point or a Rogue Access Points (RAP) [54, 55]. They are mainly installed by criminal intents of hacking. IEEE 802.11 family of standards have different substandard frequency standards. Higher frequency standard is associated with low area of coverage. With the increased bandwidth throughput such as in IEEE 802.11ac and IEEE 802.11ad [56], the inside and outside threats have a much higher probability of occurrence. The focus of this
thesis is to improve a wireless Access Point against DoS and MiM attacks i.e. how a wireless Access Point can, know the fact that it is not part of a False Wireless Access Point (Wireless node), or its activity. These attacks are the most fundamental aspects with respect to Confidentiality, Integrity and Availability (CIA) attacks on any networked system. Any compromised Wireless Access Point transaction is not only vulnerable to itself but also can be vulnerable to the entire system[8, 57]. These vulnerabilities can have data-mining effects and thus can jeopardize the purpose of any organisation network infrastructure. Table 2 defines the IEEE 802.11 standards with respect to their scopes.

2.2 Wi-Fi architecture

Any wireless network comprises of fundamental elements, such as End User (EU) device, Base Station (BS) and a Wireless Link. EU wireless host can be a laptop, palmtop or desktop computation device. All these EU user devices have the capability to communicate on air and follow the defined protocol of IEEE 802.11 for their functionality. BS is a key part of a wireless network infrastructure. It is also responsible for transmitting and receiving messages from its wireless clients. Wireless link is a radio connection between a wireless client and its BS. Wireless link has many properties with respect to its frequency and magnitude of its communication. IEEE 802.11 or Wi-Fi is a Four-Way Handshake protocol with respect to RFC 1042. For reliable authentication and confidentiality in IEEE 802.11, it defines Robust Security Network Association (RSNA) based on IEEE 802.1X authentication criterion. The paradigm involves three network aspects i.e. a supplicant (Wireless Access Point), authenticator (Access Point) and AAA server. A complete handshake procedure requires connectivity between all three wireless elements of a network.
Table 2: Wireless network IEEE 802.11 network standards

<table>
<thead>
<tr>
<th>IEEE 802.11</th>
<th>Release</th>
<th>GHz</th>
<th>MHz</th>
<th>Mbits/s</th>
<th>MIMO</th>
<th>Range(m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 1997</td>
<td></td>
<td>2.4</td>
<td>20</td>
<td>1,2</td>
<td>1</td>
<td>20</td>
</tr>
<tr>
<td>a Sept 1999</td>
<td></td>
<td>3.5,7</td>
<td>20</td>
<td>6,9,12,18,24,36,48,54</td>
<td>1</td>
<td>35</td>
</tr>
<tr>
<td>b Sept 1999</td>
<td></td>
<td>2.4</td>
<td>20</td>
<td>1,2,5.5,11</td>
<td>1</td>
<td>35</td>
</tr>
<tr>
<td>g Jun 2003</td>
<td></td>
<td>2.4</td>
<td>20</td>
<td>6,9,12,18,24,36,48,54</td>
<td>1</td>
<td>38</td>
</tr>
<tr>
<td>n Oct 2009</td>
<td></td>
<td>2.5,5</td>
<td>20</td>
<td>7.2,14.4,21.7,28.9,43.3,5</td>
<td>4</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>40</td>
<td>7.8,65,72.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15,30,45,60,90,120,135,1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ac Dec 2012</td>
<td></td>
<td>5</td>
<td>20</td>
<td>Up to 87.6</td>
<td>8</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>40</td>
<td>Up to 200</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>80</td>
<td>Up to 433.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>160</td>
<td>Up to 866.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ad Feb 2014</td>
<td></td>
<td>2.4,5,60</td>
<td></td>
<td>Up to 6912</td>
<td></td>
<td>400</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(6.75 Gb/s)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Once the procedure of handshake is completed, it results in generating a Master Succession Key (MSK), and the supplicant along with the MSK generates Pairwise Master Key (PMK). As a substitute, a base station and Access Point may have a preconfigured static Pre-Shared Key (PSK). For further reassociating, a cashed version of the key may be used, which may be vulnerable for wireless Access Point and its associated network. An execution of Four-Way Handshake protocol is imperative for a satisfactory configuration of RSNA.

### 2.3 Four-Way Handshake protocol

Verification of a shared PMK renders the procedure of Four-Way Handshake validation. Therefore Window (operating system) for DoS attack is left unattended if pre-existed cashed copies of PSK are used, especially in case of vertical handoff. Figure 2.2 represents four stages of the protocol sequencing; first message is a communication between Wireless client and Wireless Access Point which is an open broadcast for all. Second message is from a wireless client node to its access point, where upon receiving, it has the mandatory details of
access point such as AA, ANounce, sequencing and sequence number. Wireless client node submits its credentials such as SNounce, sequencing reply number along with Message Integrity Code key.

At this stage, a wireless client has no validation criteria with respect to False Access Point paradigm. Furthermore, the third step is prone to a Man-in-the-Middle (MiM) attack, which can be a potential risk for Denial-of-Service attack. Third message is a reply from Wireless client node to its associating wireless Access Point that has its calculated ANounce, message sequencing number along with its Message Integrity Code. MIC at this stage is a calculated sequence representation. Vulnerability of DoS attack will still persist at this stage because of burlesque of any attempts, as also depicted in figure 2.3.

**Figure 2.3: DoS attack**
2.3.1 Denial of Service attack

A DoS attack is an attempt to impersonate its authenticator; as shown in figure 2.3. It is also known as one message attack. The simplicity of this operation is rendered by PTK inconsistency. As depicted in the following figure, an attacker sends message 1 to the target wireless Access Point client node. This disrupts the sequence of the previous handshake, which will terminate the current succession as its PTK is not the same as the former one [14, 15, 21, 24, 43].

In order to launch any DoS attack, in the time period with respect to the succession messaging, methods like forging message 1 or modest frequency flooding can inflict a False (Wi-Fi) Access Point association. It can also cause serious routing Impersonation and Sybil attacks.

2.3.2 Enhanced 3-Way Handshake protocol

The main emphasis of this protocol is on a generation of a new encryption key based on PMK and PSK. This New Encryption Key (NEK) would be a Message-1 between Supplicant and Authenticator in order to overcome the DoS and Directory attacks, as well as elimination of the fourth Stage of Wi-Fi Protocol. However, this Protocol has failed against Non-repudiation and Freshness between vertical handoff. False Access Point association and detection has not been polarised out [43].

2.3.3 Two-Way Handshake protocol

Mobile Station (MS) with mission critical broadband application cannot sustain its succession within the paradigm of Three-Way Handshake Protocol. A security criterion for a vertical or horizontal handoff for any MS has not been structured. Thus, association with another Access Point (AP) completely disregards IEEE 802.1x-based EAP authentication. Henceforth,
Mobile Stations (MS) are subject to all the attacks as mentioned previously, as well as Mobile Station (MS) having no authority to evaluate the authenticity of the next handover AP.

Two-Way Handshake protocol with two counters (i.e. PMK, PSK) having to encrypt 1st Message by PMK has been proposed against DoS attack but is still vulnerable to directory attacks which are the derivatives of Distributed Denial of Service (DDoS) attacks. The proposed solution is beyond the time and space complexity and still has not addressed any False Access Point detection or avoidance paradigm. Figure 2.4 represents matrix operation of DoS and MiM attack against wireless system CIA vulnerabilities’ [13, 58].

The security complexities with respect to client association for the upcoming IEEE 802.11ac standard are even more crucial as the main focus of the standard is only on the better throughput. The rogue network[59] detection and avoidance within the framework of horizontal handoff between IEEE 802.11ac must have a transient and stable solution. IEEE
802.11n, and its association with the dynamic client topologies that can evolve into multi-hop and can change randomly with unpredicted multilink, requires adaptive security management control and prior Knowledgebase prediction.

2.4 Fuzzy Logic

Fuzzy Logic is a branch of mathematical science i.e. Artificial Intelligence which deals with study of decision theory. Its fundamentals are designed on Graph theory. In this section we will give a brief overview of Fuzzy logic set theory, its control system attributes and decision making attributes[26, 60].

Fuzzy set theology and its membership function suppose that, if U is a universal set having an object, then its members can have continuous and discrete properties. A fuzzy set F in its universe of discourse is formulated by its membership function as: $\mu = (x) \in X \rightarrow [0,1]$

Where 0= Complete Non-Membership degree and 1= Complete Membership degree.

Fuzzy meta-scheduler [61, 62] that follows the classical schema of Mamdani Fuzzy logic system is represented such as: a) Triangular b) Trapezoidal and (c) Gaussian membership functions.

2.4.1 Triangular membership function

If there is a triangular fuzzy number i.e. F in R, where a, b, c, x $\in R$, then membership function, $\mu_R : R \rightarrow [0,1]$ is:

$$ \mu_R(x) = \begin{cases} 
(x - a)/(b - a), & a \leq x \leq b, \\
(c - x)/(c - b), & b \leq x \leq c \\
0, & otherwise 
\end{cases} $$

---------------------------------------------(2.1)
2.4.2 Trapezoidal membership function

If there is a trapezoidal fuzzy number i.e. F in R, where a, b1, b2, c, x ∈ R, then membership function, \( \mu_R : R \rightarrow [0,1] \) is:

\[
\mu_R(x) = \begin{cases} 
(x-a)/(b_1-a), & a \leq x \leq b_1, \\
1, & b_1 \leq x \leq b_2, \\
(c-x)/(c-b_2), & b_2 \leq x \leq c, \\
0, & \text{otherwise.}
\end{cases}
\]

\[\text{(2.2)}\]

2.4.3 Gaussian membership function

The main focus for Gaussian membership is because of its smooth projections between different sets of defined membership area. The function can be formulated as:

\[
\mu_{R(x_m)}^i(z) = \frac{1}{\sigma_i(x_m) \sqrt{2\pi}} \exp \left\{ -\frac{(z - \tau_i(x_m))^2}{2\sigma_i(x_m)^2} \right\} \{z \in R \mid z \leq 1\}
\]

\[\text{(2.3)}\]

where, \( \tau_i(x_m) \) and \( \sigma_i(x_m) \) are mean and standard deviation of the defined function. Henceforth the rule set can express mathematically as:

\[
R_i = \left\{ \mu_i^{(x_1)}(x), \mu_i^{(x_2)}(x), \mu_i^{(x_3)}(x), \ldots, \mu_i^{(x_n)}(x), \Omega_i \right\}
\]

\[\text{(2.4)}\]

Where \( \mu_i^{(x)}(x) \) is a Gaussian membership function and \( \Omega_i \), are input set, output set and rule weights.

2.4.4 Fuzzy set linguistic variables

Fuzzy set linguistic variable is a quintuple \((x, T(x), U, G, M)\); whence \( x \) is a variable name, \( T(x) \) is a term sets of variable \( x \) defined on \( U \); \( G \) is the syntax rule of the variable \( x \) and \( M \) is the semantic rule for the assigned variable \( x \).
2.4.5 Fuzzy relations

Fuzzy relation $R$ with respect to $U=\{x\}$ and $V=\{y\}$ is a Cartesian product $U \times V$, defined as function; $\mu_R(x,y) \rightarrow [0,1]$

2.4.6 Rule base system

Fuzzy Rule base system defines the semantic and syntax between input variables and output variables of the system. These can be classified such as:

i. the Mamdani fuzzy rule-base system

ii. the Sugeno fuzzy models

iii. The Tsukomoto fuzzy models

For our methodology we have been using Matlab i.e. Mamdani fuzzy rule-base system. It consists of four function layers as follows:

i. A Knowledgebase consists of fuzzy IF-Then rules and Fuzzy set database members used as Knowledgebase axioms.

ii. A decision-making unit function defines its performance interface operations. For example for any given relation $R$ from $U$ onto $V$ is defined as $B=A \circ R$

i.e. $\mu_B(y) = \max_x [\min \{\mu_R(x,y), \mu_A(x)\}]$  \hspace{1cm} \text{--------------------------(2.5)}

iii. A Fuzzyfication is an interface that performs parameter matching of any crisp nature to its corresponding discourse of universe linguistic values.

iv. Defuzzification is the process of finding the crisp values from a defined fuzzy interface set. There are two main techniques for extractions of defuzzification: a) maximum and b) centroid. Maximum values define the output and its gravity or Center Of Area (COA) is calculated from its respective scalar value. As shown in figure 6.6
where \( \mu \) is the aggraded output function with respect to figure 5.6 in chapter 5.

2.5 Neuro Fuzzy Logic

Fuzzy Neural Network is a branch of science which deals with the logical axioms of associated network places and their respective transaction. For a given content of a network to its memory, one gets the appropriate outcome. This outcome is bounded by fuzzy logic theology. Henceforth, it is the interaction between microscopic and macroscopic phenomena of the system. A system such as Wi-Fi, if it is considered as a microscopic system of access method, then its users, such as wireless clients or different communicating Access Points processes, are the macroscopic paradigm. Application of Fuzzy Neural Networks (F2N) includes area such as Hyphenation algorithms, Signal prediction, its forecasting, image processing, sonar target recognition, noise removal from time series signals and etc. The neural systems with the following characteristics are called regular (F2N) fuzzy neural network:

i. The topological architecture is identical with ones of conventional multi-layered feed-forward neural network.

ii. The input signal, connection training weight and threshold (biases) are fuzzy sets in \( F(\mathbb{R}) \);

iii. The internal operations are based on Professor Zadeh’s Fuzzy arithmetic.

Figure 2.5 represents Fuzzy Neural Network model i.e. artificial (Mathematical) model of human neuron.
The input output behaviour of F2N, as shown in above figure, is represented where dendrites of input signals lines are represented by variable $x_i$, which represents the presence or absence of training pulse i.e. $x_i(t) = 1$ or $x_i(t) = 0$, respectively. And the variable $w_i$ is called the weight of the input line $i$.

$$y(t + \tau) = \begin{cases} 1 & \text{iff } \sum_{i=1}^{n} w_i x_i(t) > -w_0 \\ 0 & \text{Otherwise} \end{cases} \quad \text{(2.7)}$$

The Threshold $T = -w_0$, the weights, $w_i$ and delay $\tau = \theta$ represent no feedback.

In the words of Professor Lofi A. ZADEH, “Fuzzy Sets Engineering should be on the desk of anyone who has a serious interest in applying fuzzy logic- singly or in combination with neurocomputing and genetic algorithms to the conception and design of intelligent systems”. As represented in the following figure 2.6 (following page),
The basic aspect of fuzzy set connectivity with respect to the logic algebra is collection of input dendrites i.e. $x_i$ where $i=1,2,3,..n$ arranged in a vector form and viewed as the element of unit hypercube, $x \in [0,1]^n$. The representation of these can have layered architecture. The intermediate layers between input and output layers carry some referential progressing with respect to fuzzy logic axioms. F2N can be divided in two major classifications; aggregative and referential neuron. Prior is the logic algebra with universal operators and the latter is Referential processor operators depending on Match, Difference, Inclusive or Dominance relationships. As depicted in figure 2.7, referential neuron follows the aggregation parameterised operation called Ordered Weight Average (OWA) operations.
The Referential process is an implementation of logical approximation between the systems hypercubes. Its paradigm is focused on mapping referential aspects between systems input and output spaces.

![Figure 2.7: F2N Classification](image)

Where Aggregated Neurons follows the frame of Boolean linear algebra and Referential Neurons follows partial differential algebra rules for its optimisation.
Chapter 3

3 Problem Definition

This chapter presents a detailed description of problem cases addressed by this thesis. In-depth introduction of the problem involves a discussion on False Access Point detection and avoidance. Furthermore, a branch of Artificial Intelligence i.e. Fuzzy Logic[60] and its derivatives [63] have been utilised for improving a wireless (Wi-Fi) security[12, 64, 65] of an Access Point(wireless node) in its system.

3.1 Introduction

A wireless network is a collection of devices communicating wirelessly with each other, spreading on any geographic area subject to a system surrounding effects. It is imperative for any wireless client node (Access Point) to know if the immediate connecting Access Point within a group is reliable or not with respect to its association and authentication. Security is a major concern not only for mobile users but also for every day work place users. Most common problems are not with mobile computing, rather its reliability as an edge connecting paradigm. Virtual Private Network (VPN) is often considered a secured scenario, however many vendors have provided VPN server products which are still unable to eliminating DoS and MiM attacks, especially in a wireless communication system. VPN Server products can indeed provide a secure virtual tunnelling procedure between any site servers to an end user, but it has not yet addressed the security issues with respect to mobility. Furthermore, a VPN client does not have a secure inherent mechanism for further validating their vertical and horizontal mobile handover authenticity. The most stringent security measure with respect to Wi-Fi is to have a security functional trust model at both ends of a wireless network capable of periodic validations and verifications.
ISO/ IEC 2382-8[66] has defined security as “the protection of data and resources from accidental or malicious act, usually by taking appropriate action”. Figure 3.1 shows the persistence of False Access Point vulnerabilities at different stages of wireless client node communication succession. These False Access Points activities may/can take place without any clear authentication within Wireless Local Area (WLAN). False Access Point activity also enables an attacker to intercept, accept or copy network messages and thereby launching more sophisticated wireless routing attacks. One of the proposed solutions for Wi-Fi networks is IEEE 802.11i, which uses WPA2 standard for security and reliable data transfer. It introduces a Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) and also a newly introduced AES-base encryption method. These methods are designed to encrypt data, but these can be decrypted fairly easily if cipher hardware is known. Vulnerabilities like rouge access point can leads to any Black hole, Worm hole i.e. Man-In-Middle (MiM) attacks. We have formulated a functional layer model that has improved a wireless security operation within the realm of Wi-Fi paradigm.

Figure 3.1 also identifies that quantitative and qualitative measures against rogue Access Point paradigm have not been addressed adequately. This is represented as an occurrence in all layers of communication protocols. False Access Point activity persists in the form of MiM or DoS Attacks. These attacks can further mutate in the form of more complex attacks such as Trojan data mining activities. Henceforth, it is imperative to take measures at all levels. In this research we have designed functional layer security methods which will be helpful to identify threats against vulnerabilities such as False Access Points.
3.2 Problem Case 1

As a general trend we have observed an exponential growth of WLANs due to vendors coming up with a rapid and cost effective deployment solution. With such a demand and supply, it is imperative to adhere to mandatory rules encapsulating verification and validation security aspects. Within network environment such rules are defined as Usage Rules. Any wireless network client node which has ceased to abide by these rules is defined under the category of a False Access Point. Whence False Access Point detection or avoidance, on the basis of validation and verification, is an essential paradigm of any secure communication.

Problem Case 1 targets[67] the following question, with three sub-questions. The primary objective is to formulate a methodology, which not only detects but also identifies False Access Point in a system, thus avoid being its counterpart.

1. How can a wireless client node evaluate if it is part of a False Access Point association?
2. What are the fundamental criteria for a Wireless client node to validate its association?
3. What are the parameters which should/must be inspected by any Wireless client node with respect to a False Access Point activity evaluation?
4. How often should these parameters be monitored by a Wireless client node in order to check False Access Point evaluations?

The scope of problem case 1 is focused on identifying and reporting a False Access Point activity. It is bounded within the framework of rudimentary detection and successive examination of these criteria. Many researchers have proposed different methodologies for addressing the above mentioned problem statement such as a methodology based on MAC/IP address filtering with respect to address spoofing. However, it is not definite since it lacks prior knowledge distribution or deductive reference knowledge to establish trusted wireless communication. Even when captured a WLAN trace it would not resolve a False Access Point problem.
Fundamental criteria for validation are all the wireless network temporal elements, which are mandatory for Usage Rule of a wireless, with respect to the Surface of Position (SoP)[68] of the Access Points in communication. Violation of these round robin monitoring aspects will trigger a trust violation alert. These parameters must always be inspected prior to and after sending any message activity and its acknowledgement must be validated.

Figure 3.1: Wireless False Access Point vulnerabilities
3.3 Problem Case 2

Fuzzy logic is a form of universal logical axioms. It deals with the logical reasoning paradigm, based on approximation instead of a fixed or exact value. The basic machinery for Fuzzy logic set theory has been proposed. According to the Fuzzy set theory, a Fuzzy set A in a non-empty set X is characterized by its member function which is defined as:

\[ \mu = (x) : X \longrightarrow [0,1]. \]  

............... (3.1)

Where 0 = Complete Non-Membership degree;

1 = Complete Member degree;

Fuzzy control system can be applied to various systems, such as linear and non-linear systems respectively. The operation modules of Fuzzy logic system are as following:

i. Fuzzification is the process of finding the membership function called crisp values. Rule Base or knowledgebase are set of rules used for inferencing a Fuzzy logic system.

ii. Inference of a knowledgebase can be further subdivided into two classes; minimum inferencing and product inferencing.

iii. Defuzzification is process of finding the crisp value from a defined inference Fuzzy set. There are two techniques for extraction of defuzzification; maximum and centroid. Maximum value is chosen as an output variable and gravity value is calculated from scalar values respectively.

\[ \overline{X} (centroid) = \frac{\int_{a}^{b} x \mu(x) dx}{\int_{a}^{b} \mu(x) dx}. \]  

............... (3.2)

Where \( \mu(x) = \) membership degree of element \( x \) with limit [a, b].
Problem Case 2 targets the following questions with two sub-questions. The primary objective is to formulate a methodology using fuzzy logic tool box supplied with Matlab in order to improve wireless activity of a Wireless client node and Wireless Access Point in communication.

1. How can Fuzzy Logic be utilised to improve security of a wireless network?
2. What are the Fuzzy logic model parameters which must be evaluated in order to detect and avoid malicious Access Point activity?
3. What is a possible Fuzzy logic Functional model which can be used for identifying False Access Point with respect to Wi-Fi networks?

3.4 Conclusion

The problem of False Access Point detection and avoidance, its validation and verification of False Access Point association, has formally been presented in this chapter. This problem is formulated as a security Functional model which will enable a Wireless client node to not only detect, but also avoid associating with any False Access Point activity. These problem cases will be formulated by utilising an AI axiom of Fuzzy Logic. However, Surface of Position (SoP) [69] and Zenith Augmented tracking [23, 70, 71] and evaluation for its integral functionality is beyond the scope of this thesis; but we will consider some fundamental principles of Global Positioning System (GPS)[72].
Chapter 4

4 Application of Methodology

This chapter explains the research methodology, formulated by different theories and research methods, already explained briefly in previous chapters.

MATLAB (Matrix Laboratory) [73] is a multi-paradigm numerical computing environment and fourth generation programming language developed by MathWorks. Matlab allows matrix manipulation, plotting of function and data, implementation of algorithms, creation of user interface, and its interfacing with other high level programming languages. Matlab, a high level language, is also capable of data analysis, algorithm development, visualisation and numerical computing. Therefore, these capabilities have helped us to design, simulate and remodel communication systems. Matlab modelling tool boxes have been used for our research work, specifically Systems Communication, Simulink, Fuzzy Logic, and Fuzzy Neural Network tool boxes. In our approach, we have presented a wireless communication model and have further developed it using Simulink and Fuzzy Logic tool boxes. Thus, Matlab, as a high level programming language, is designed for systems simulation for all engineering and medical system modelling, and thus has a capability to cater the requirement of many different researchers[74].

4.1 Wireless LAN framework

The ISM frequency bandwidth is appropriate with respect to its coverage area and application framework. It can be used for point-to-point and point-to-multipoint with channel signal timing and its frequency variation. The wireless channel as its counterpart also provides distortion i.e. white noise between any two Access Points in a wireless communication system. Current WLAN systems are being deployed in 2.4GHz and 5GHz with Rice series
distribution or Rayleigh series distribution criteria for indoor and outdoor modelling respectively. Thus, behavioural study requires Matlab modelling of a Wireless Access Point communication system with distance and signal timing strength. The process of signal studying at application layer is known as the studies of a complex envelope series signalling magnitude. Once these models are stabilized, we have used Fuzzy logic tool box in order to eliminate the False Access Point (DoS and MiM attacks) scenario, which will help us to improve wireless network security. These aspects on the basis of sensitivity analysis can predict the validation of the incoming succession[12].

Henceforth, to overcome the above mentioned challenges, we have tried to resolve gaps in workflow implementation, dynamic system level performance and their integration with respect to Fuzzy logic applications. Matlab and its toolboxes have helped us overcome these.

Digital signal processing, with the knowledge of linear algebra, has enabled us to develop Wi-Fi communication system models. In our framework, we have developed [75]a simple Wi-Fi model in Matlab and have progressively added other components such as Frequency Division Duplexing (FDD), Time Division Duplexing (TDD), Single Mode, Single Input Single Output (SISO), Single user multi model, Single Input Multiple Output (SIMO), Multi model multi user and Multiple Input Multiple Output (MIMO). These models are tested with respect to the relative distances between wireless sources and sink model. Observations of the Wi-Fi scenarios have been studied at 4m, 40m and 400m apart, as shown in figure 4.1. The distance is taken in a 2D context with respect to the observation. The respective Matlab code and other timed throughput vs. distance travelled are attached ans can be found in Appendix 8.1 respectively.
4.2 Matlab and Simulink simulation features

Simulink is an overlay tool box of Matlab, and has the capability of designing a multi model base design for embedded and dynamic systems. Its library block set has the capability to study the systems behaviour graphically, which has enabled us to move back and forth through our simulation process for conclusive results. Simulink has provided tool box components for hierarchical system modelling and System data modelling, with respect to Wi-Fi systems and other communication scenarios, such as Wi-Max, Bluetooth, etc. Figure 4.2 describes the general methodological approach for the system/ Wi-Fi modelling paradigm. Some of the succinct or concise accounts of Wi-Fi modelling are as following:

i. Controlled system: Any system that is bounded by controlled input and generates a desired output signal is referred to as a controlled system. This must be guarded by boundary preambles.

ii. Control elements: These are the subsystem elements of the system that control the behaviour of the system. For example, Modulation of a wireless signal.

iii. Control signal: Controlled sub-element produces control signals to procure a controlled system.
iv. Feedback elements: These are responsible for defining a relationship between controlled/desired output and feedback response. Sometimes referred to as a bias.

v. Controlled output: These are the state variable output function. These can also be used to define a relationship for triggering the next event.

vi. Primary feedback signal: These define the relationship between system feedback element and controlled output. For example, stating the priority of any activity path.

vii. Reference input: This is also referred as signalling summing point or the summation junction for signal activities.

viii. Actuating signals: These are the outbound signals from a junction to any controlled element of a system.

ix. Disturbance: This is also defined as the background noise or white noise of a system.

Thus, the complexity of the sub-system must be defined in the same order as that of its system. However, its boundaries and modularity must be controlled with the series of feedback or feedforward/gain elements [66, 75-78].
4.3 Methodology features

Pivotal aspects of our Wi-Fi security research modelling are as following:

System signal: This requires a detailed analysis of time and frequency i.e. transmission through Linear Time Invariant (LTI), auto correlation and spectrum analysis. The magnitude of the complex envelop signal is represented by the following equation with real and imaginary parts as shown in equation 4.1.

\[ A\cos(\omega_0 m + \alpha) + jA\sin(\omega_0 m + \alpha) \]  

\[ \omega_0 = 2\pi \frac{F_0}{F_s} \] = Digital frequency radius

\[ A = \text{Amplitude of the frequency} \]

\[ F_0 = \text{Originating frequency} \]

\[ F_s = \text{Sampling frequency} \]

\[ \alpha = \text{Phase} \]

4.3.1 Baseband Transmission:
All the digital signals must be transmitted in analog format. The baseband modulation and demodulation over non-noisy or noisy with Additive White Gaussian Noise (AWGN) channel process is used for communication between two wireless Access Points in communication.

4.3.2 Analog Modulation:
The purpose of analog modulation is to transmit a digital signal over transmission channel. The amplitude, frequency, or phase of the signal must be modulated according to the transmitting medium of communication.
4.3.3 Analog to digital conversion or vice versa:
This includes the process of signal sampling and quantisation mechanism, with Pulse Coded Modulation (PCM) theory.

4.3.4 Digital Modulation or vice versa:
Digital modulation is a process of conversion from digital bit stream to an analog. Most fundamental types are based on “keying”; such as BPSK, while demodulation is the opposite case.

4.3.5 Link Budget Analysis:
This is also known as the communication link analysis, with respect to the signal and channel noise ratio, and is given by the following formula for the modelled Wi-Fi wireless network channel:

\[ A \cos(\omega_0 n + \alpha) = \frac{A}{2} e^{j(\omega_0 n + \alpha)} + \frac{A}{2} e^{-j(\omega_0 n + \alpha)} \quad \text{.... (4.2)} \]

\[ \omega_0 = 2\pi F_0 F_s = \text{Digital frequency radius} \]

\[ A = \text{Amplitude of the frequency} \]

\[ F_0 = \text{Originating frequency} \]

\[ F_s = \text{Sampling frequency} \]

\[ \alpha = \text{Phase} \]

This also includes the study of transmitted and received power at both the ends. Equation 4.3 represents a system SNR paradigm. It has been observed that SNR calculation, with respect to the distance between sender and receiver, is not the only mechanism to predict...
the presence of False Access Point activity or its association. In any case, the analysis must fulﬁl the Shannon information theory.

\[
SNR = \left( \frac{F_s}{B} \right) \left( \frac{E_s}{N_o} \right) = N_b \left( \frac{F_s}{B} \right) \left( \frac{E_b}{N_o} \right)
\] ........................................... (4.3)

Where

\( F_s \) = symbol rate (1/sec)

\( B \) = bandwidth (Hz=1/sec)

\( N_o \) = noise power spectral density

\[
E_s = \int_{-\infty}^{+\infty} |g(t)|^2 dt = \int_{-\infty}^{+\infty} |G(F)|^2 dF
\]

Energy per symbol

\( E_b \) = Energy per bit (joule)

\( N_b \) = bits per symbol (joule)

\[
P_T = \frac{E_s}{T_s} \approx E_s \times F_s = \text{Transmitted power}
\] ........................................... (4.4)

Figure 4.3 represents the three modelling criteria where sensor base stations are 4m, 40m, and 400m apart. The following figures i.e. 4.4, 4.5 and 4.6 have clearly reﬂected that the signal envelop, with respect to the distance between Base Station (BS) and Access Point, is not only a pivotal criterion for deﬁning and predicting a False Access Point association or authenticity, but also imperative for validating any further horizontal handover veriﬁcation.
4.3.6 Spectrum Analysis:
This is the study of the technique that permits multiple accesses, through multiple terminals with the same or different frequencies (e.g. IEEE 801.11n, IEEE802.11ac and IEEE 802.11ad). MIMO is a process where special diversity is achieved through more than one antenna in an Access Point (AP).

4.3.7 Fading Channels and its aspects:
This is the analysis of obstruction between transmitter and receiver antennae of AP and BS respectively. OFDM can mitigate the fading effect.
Above, figure 4.4 shows the signal magnitude when these are at 4m, 40m, 400m apart, with respect to the model presented in figure 4.3; whence clearly distance is not the only deciding factor that can validate a False Access Point association.

4.4 Modelling aspects of Wi-Fi network using Matlab

Designing a Wi-Fi network in Matlab or using one of its tool box i.e. Simulink, requires a comprehensive knowledge of digital and analog domain. For example, in any Wi-Fi network we have source information from digital media that need to be transmitted on wireless i.e. analog media, for its propagation. On the receiving end of the wireless Access Point, this information is De-Modulated and converted in to the binary information again. However, there are many effecting factors involved which can add a white noise during the process of demodulation. These effecting factors are controlled and filtered out by digital gain filter parameters. Figure 4.5 shows a very fundamental model of wireless communication between a transmitter and a receiver. For generating the information pattern of binary information, we have used a simulink block i.e. Bernoulli Binary number generator. This is a part of discrete time domain, with the help of a defined symbol set and quantization criteria. These are converted into a pulse form for a transmitter to transmit on a defined wireless channel. This whole criterion is defined in a DBPSK Modulation Baseband simulink block set. It uses differential binary phase shift keying method and the resultant output is the modulated baseband signal. With respect to Wi-Fi connectivity, we have used AWGN and Rayleigh Fading Block set for Rice series distribution and Rayleigh series distribution respectively.
AWGN (Additive White Gaussian Noise) adds a white Gaussian noise to real or complex input signals depending on the input format of the signal. If the input signal is real and complex in nature, then the output magnitude is a complex envelope signal having both the real and imaginary part, also as shown in figure 4.4 and figure 4.1. AWGN also provides an insight to Signal-to-noise ratio (SNR) per input sample and Ratio of bit energy to noise power spectral density (EbNo), as well as Ratio of symbol energy to noise power spectral density (EsNo).

DBPSK De-Modulation Baseband Block set converts the information from continuous time domain into discrete time domain by comparing the current and previous symbols i.e. mapping of phase shift difference of $\phi$ and $\pi + \phi$ to 0 and 1 respectively. Next block in figure 4.5 is Error Rate Calculation. It has two inputs. First, Tx is reference from the digital, discrete time source of information and the other, Rx, is from the de-modulated baseband. This block can have two to four input ports depending how they are addressed in a dialog box. It is important to have the same input format. The output data port can describe the error rate, total number of errors and total number of comparisons the block has made. The block set of Discrete-Time Scatter Plots shows the channel distortions or pulse
shape of the signal. The above figure 4.5 also shows the input in a MatLab workspace i.e. TX_Out and RX_IN, for further plot analysis and its comparisons with Time Scope of the signals. The above figure has significantly high SNR results and an error free communication. SNR in a mobile wireless device is an adaptive feature often related with the battery life. Higher SNR means more costly battery operation. The Lower Control Link (LCL) and Upper Control Link (UCL) mean graph shown in figure 4.6 is an activity of its corresponding model. This graph is the physical layer representation of data between two wireless Access Points. We have designed and simulated many models with respect to physical layer data transmission between wireless transmitters and receivers, and have found that the relation of throughput at the physical layer is always linear, in relation with the number of data send with respect to the time in seconds.

![Figure 4.6: Wireless Model with Physical Layer Control graph](image)

In the next section we have modelled a physical layer Wi-Fi model; the Figure 4.7 represents a Wi-Fi model with true and False Access Point criterion, the BER model and respective figure represents the signal magnitude. It is impossible to predict from the signal output that which one should be trusted at the receiving end for the reliable communication.
4.5 IEEE 802.11b Physical Layer Model

The model presented in figure 4.7 is an example of Direct Sequence Spread Spectrum (DSSS) Wi-Fi system with the data throughput capacity of 1Mbps, 2Mbps, 5.5 Mbps and 11 Mbps respectively. MAC sublayer Protocol Data Unit (MPDU), from a wireless transmission Access Point, is transformed into PHY layer Protocol Data Units (PPDU).

Figure 4.7: Wireless model with an embedded False Access Point

This transformation is padded with PLCP headers. In the next phase, this wireless PPDU is modulated and de-modulated by using MatLab/ Simulink toolbox of DBPSK Modulation Baseband block set. Prior to its transmission, it is applied through Root Raise Cosine Pulse Shaping (RRCPS) filter and then transmitted to the wireless channel. AWGN Channel block mimics the wireless channel of a Wi-Fi scenario. At the receiving end of the wireless

68
channel, when this transmitted signal reaches the respective or designated receivers, it is again processed with RRCPS filters and de-modulated with DBPSK MatLab/ Simulink toolbox. The anatomy of the model consists of one standard transmitter and three receivers, where the last two receivers have a path loss model of 40 dB and 16 dB, at receiving ends. The receiver with higher path loss i.e. 40dB, is constructed as a False Access Point, while Access Point with 16 dB is also a trusted Access Point like the first Access Point with no path loss model.

Table 4.1 represents the compression with respect to the BER error estimations, and the probability of error and number of errors and number of errors with respect to the defined frame format of Wi-Fi (figure 4.7). We have considered a three wireless Access Point system. A True Access Point is defined at a path loss of 1dB to 20dB, and a False Access Point at a path loss of 40db and 60dB, as well as a shadow True Access Point at a path loss of 70db to 80dB. The table 4.1 concludes the number of bits transmitted to all the three receiving wireless receivers. It displays the probability of error, number of errors and their defined received frame format structure with respect to Preambles, Headers and PSDU observations as also shown in figure 4.8[79].

Figure 4.8: Channel frequency (MHz) and magnitude of the complex signal (dB)
The calculated probabilistic outcome in the following table (Table 4.1) has also shown that any receiving Wireless client node has almost equal probability that it will consider a False Access Point as a true Access Point.

Henceforth, a False Access Point can mutate itself to have may features. For example, an attack against Privacy is of three major types that are traffic analysis, eaves dropping, as well as impersonating. The impersonating attack can further take the form of address spoofing, device cloning, or False Access Point with false routing activity. Thus, Man-in-the-Middle attacks have options of Greyhole or Blackhole attacks and DoS attack scenarios. These two security threats are the main causes for launching any serious attempt to compromise or hack a wireless Access Point system.

Table 4.1: Wi-Fi 802.11b BER with respect to transmitter and receiver

<table>
<thead>
<tr>
<th>Path Loss</th>
<th><strong>Preamble</strong></th>
<th></th>
<th><strong>Header</strong></th>
<th></th>
<th><strong>PSDU</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Probability of error</td>
<td></td>
<td>Probability of error</td>
<td></td>
<td>Probability of error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Number of errors</td>
<td></td>
<td>Number of errors</td>
<td></td>
<td>Number of errors</td>
<td></td>
</tr>
<tr>
<td>1dB</td>
<td>0.4648</td>
<td>33</td>
<td>0.2826</td>
<td>13</td>
<td>0.5001</td>
<td>4096</td>
</tr>
<tr>
<td>10dB</td>
<td>0.4648</td>
<td>33</td>
<td>0.4565</td>
<td>21</td>
<td>0.5001</td>
<td>4096</td>
</tr>
<tr>
<td>20dB</td>
<td>0.4648</td>
<td>33</td>
<td>0.2609</td>
<td>12</td>
<td>0.5001</td>
<td>4096</td>
</tr>
<tr>
<td>30dB</td>
<td>0.4848</td>
<td>33</td>
<td>0.3913</td>
<td>18</td>
<td>0.5001</td>
<td>4096</td>
</tr>
<tr>
<td>40dB</td>
<td>0.4648</td>
<td>33</td>
<td>0.4130</td>
<td>19</td>
<td>0.5001</td>
<td>4096</td>
</tr>
<tr>
<td>50dB</td>
<td>0.4648</td>
<td>33</td>
<td>0.4348</td>
<td>20</td>
<td>0.5001</td>
<td>4096</td>
</tr>
<tr>
<td>60dB</td>
<td>0.4648</td>
<td>33</td>
<td>0.4130</td>
<td>19</td>
<td>0.5001</td>
<td>4096</td>
</tr>
<tr>
<td>70dB</td>
<td>0.4648</td>
<td>33</td>
<td>0.4348</td>
<td>20</td>
<td>0.5001</td>
<td>4096</td>
</tr>
<tr>
<td>80dB</td>
<td>0.4648</td>
<td>33</td>
<td>0.3043</td>
<td>14</td>
<td>0.5001</td>
<td>4096</td>
</tr>
<tr>
<td>100dB</td>
<td>0.4648</td>
<td>33</td>
<td>0.3696</td>
<td>17</td>
<td>0.5001</td>
<td>4096</td>
</tr>
</tbody>
</table>
Figure 4.8 shows the communicating channel frequency graph, with respect to a transmitter, true receiver, False Access Point receiver and a shadow true receiver respectively (as modelled in figure 4.7). It is evident that besides the channel frequency, the variation in signal complex magnitude should not be considered as an important aspect in deciding the False Access Point process activity in any system. Henceforth, it is imperative to consider the spatial positioning of a wireless Access Point in any verification and validation criterion. Security aspects such as wireless VPN tunnelling must not be implemented prior to its spatial validation establishment.

4.6 Wi-Fi Fuzzy logic

Designing and analysing security trustmission parameters are some of the critical elements in order to secure any association between any two wireless Access Points. The key design architecture components for a wireless security are Knowledgebase datastructure, Functional security validation, Security verification modelling, sScurity risk assessment and mitigation modelling. These paradigms are some of the important aspects for tracing message-dependency criteria for achieving better security management and performance.

Henceforth, techniques such as the Fuzzy logic based predictive-modelling paradigm addresses this problem by not only detecting a False Wi-Fi Access Point or Rogue Access Point (RAP) activity, but also by preventing any future Trojan data-mining activities as well. Fuzzy logic is a set-base approximate reasoning methodology. It is used to represent different granules of knowledge, which are combined to formulate a projection onto the universe of interest. The fuzzy set framework is a pattern of reasoning under uncertainty involving axioms of Artificial Intelligence. The following MatLab code, presented in Table 4.2, is a representation of verification vulnerabilities that exist in any Wi-Fi system.
Table 4.2: Wi-Fi Mamdani MatLab model

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Name</td>
</tr>
<tr>
<td>2</td>
<td>Type</td>
</tr>
<tr>
<td>3</td>
<td>Inputs/Outputs</td>
</tr>
<tr>
<td>4</td>
<td>NumInputMFs</td>
</tr>
<tr>
<td>5</td>
<td>NumOutputMFs</td>
</tr>
<tr>
<td>6</td>
<td>NumRules</td>
</tr>
<tr>
<td>7</td>
<td>AndMethod</td>
</tr>
<tr>
<td>8</td>
<td>OrMethod</td>
</tr>
<tr>
<td>9</td>
<td>ImpMethod</td>
</tr>
<tr>
<td>10</td>
<td>AggMethod</td>
</tr>
<tr>
<td>11</td>
<td>DefuzzMethod</td>
</tr>
<tr>
<td>12</td>
<td>InLabels</td>
</tr>
<tr>
<td>13</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>OutLabels</td>
</tr>
<tr>
<td>15</td>
<td>InRange</td>
</tr>
<tr>
<td>16</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>OutRange</td>
</tr>
<tr>
<td>18</td>
<td>InMFLabels</td>
</tr>
<tr>
<td>19</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>OutMFLabels</td>
</tr>
<tr>
<td>26</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>InMFTypes</td>
</tr>
<tr>
<td>29</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>OutMFTypes</td>
</tr>
<tr>
<td>36</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td></td>
</tr>
<tr>
<td></td>
<td>InMFParams</td>
</tr>
<tr>
<td>---</td>
<td>---------------------</td>
</tr>
<tr>
<td>38</td>
<td>[-3.579 -0.3786 0.4214 3.621]</td>
</tr>
<tr>
<td>39</td>
<td>[1.021 5.021 9.021 0]</td>
</tr>
<tr>
<td>40</td>
<td>[6 10 14 0]</td>
</tr>
<tr>
<td>41</td>
<td>[0 0 1 3]</td>
</tr>
<tr>
<td>42</td>
<td>[0 2 2 5]</td>
</tr>
<tr>
<td>43</td>
<td>[4 5 7 10]</td>
</tr>
<tr>
<td>44</td>
<td>[7 8 10 10]</td>
</tr>
</tbody>
</table>

The next chapter presents an approach to improve the wireless security communication between any two Access Points. False Access Point association can also mutate to a DoS or MiM attack aspect. This can lead to a situation where the entire associated wireless network can be compromised.
Chapter 5

5 Solution for Problem Case 1: Detecting DoS attack

Over the history of wireless network communication, Denial of Service (DoS) attacks have emerged as one of the devastating threats to communication network, for both wired network and wireless network. The scale of this sophisticated attack is not only limited to critical lifeline infrastructures, but to public social infrastructures as well. DoS attacks can have many definitions and mutations. The most precise definition of DoS is provided by International Telecommunication Union (ITU-T). It defines X.800, (http://en.wikipedia.org/wiki/Security_service_(telecommunication) as, “The prevention of authorized access to resources or the delaying of time critical operation”. These attacks can be a result of malicious or benign attempts that can be locally or remotely triggered. The communication wireless bandwidth, wireless access point, or any other communication network infrastructure can be a victim of this attack. Thus, the ultimate goal of False Access Point DoS attack is to compromise the availability of the service [80]. For example, the presence of False Access Point among wireless network at any stock-exchange trading floor can bring devastating circumstance, such as DoS attack in the form of nano second window, where the request for desired stock share can be blocked for a nano second, and resulting in a loss of share[81, 82].

Cyber space is narrowly defined as the collection of networked computing devices. Our dependency for obtaining information somewhere in cyber-space is growing day by day; for example, cloud computing. The difference between the traditional network and wireless network threats elevate by increasing speed, diffusion and complexity. Unsurprisingly, the devil’s footprint logs can be found in the details such as the challenged attributes, the calculation of damage, the security login log of critical infrastructure, its ethics and
responsibility of system jurisdiction, and much more. Thereforth, security of wireless architecture, with respect to cloud access for any Internet of Everything (IoE) transaction, must be secure with respect to the Surface of Position (SoP) of any wireless Access Point.

5.1 Introduction

It is imperative for any wireless network elements such as client node and Access Point to know the authenticity of its association. Any False Access Point association can seriously compromise, not only the wireless Access Point, but the entire wireless network as well. Many researchers have proposed protocols to overcome this issue. However, these protocols do not effectively solve the False Wi-Fi assess point or rogue network issue. Therefore, we propose the Security Swarm Wireless Access (SSWA) Algorithm, which is a Functional layer model that utilises Fuzzy logic. Our algorithm improves the security of the wireless associations of a wireless client node in a False Access Point scenario. Wireless application technologies are gaining importance every day and societies are becoming more reliant on them. Wireless communication technologies such as Wi-Fi (or Wi-Max) have enabled numerous wireless applications to achieve their defined goals and objectives for both paradigms i.e. the Wireless Local Area Network (WLAN) and Wireless Metropolitan Area Network (WMAN) networks. Wireless technology has evolved to cover broadband home-office networking, community wireless networking, high speed metropolitan area network, intelligent transport, business enterprise networks and others. However, this exploitation of technology comes at a price. Wireless network Security plays a pivotal role among all the mission-critical applications. Securing wireless networks has attracted lot of attention from research committee. Most of the academic work on security in WLAN can be subdivided into three crisp areas: (1) the Impersonation attacks, (2) Routing attacks and the (3) Denial of
Service (DoS) attacks. Figure 5.1 shows where a resource connection has been blocked for even a very short duration of time.

Figure 5.1: DoS attack with respect to proxy timeout

A successful DoS attack can lead to various problems in the network and the associated Wireless client node itself. To prevent DoS attacks, detection of False Access Point activities is of high importance. A False Access Point’s activity enables an attacker to intercept and copy the network message’s activity, which might lead to more sophisticated wireless routing attacks. A common rogue network activity is invisible to both a client and Wi-Fi, Access Point. For instance, rogue network activities might be hidden from a base station or Access Point in a Wireless Local Area Network (WLAN) setup. Thus, techniques for detecting rogue network (RN) are of prime significance. Consequently, it is imperative to construct security knowledge between Wireless client node and the Access Point in order to secure the communication. This security knowledge should maintain a record of prior connections establishment based on some knowledge parameters. Building this security profile allows the detection for a RN activity and its associations. Therefore preventing a wireless client node or Access Point from joining a RN is a problem that hasn’t been fully addressed. Wireless
standards for access control proposed by IEEE 802.11 do not fully address the False Access Points security issues. Many researchers have laid emphasis on proposing new protocols against IEEE 802.11, such as the Two-Way Handshake and the Enhanced 3-Way Handshake. These protocols have failed to provide an effective False Access Point detection solution. This, in turn, makes a WLAN vulnerable to other attacks, such as the DoS and Man-In-The-Middle attacks.

A wireless security management and performance criterion within the framework of physical constraints is another area of importance. Designing and analysing security trustmission parameters are some of the critical elements needed to secure the association between any two Access Points. The key design architecture components for a wireless security are Knowledgebase data structure, functional security validation, security verification, modelling, security risk assessment and mitigation modelling. These paradigms are some of the most important aspects for tracing message-dependency criteria to achieve better security management and performance. Therefore, techniques such as the fuzzy logic based predictive modelling paradigm address this problem by not only detecting a RN activity, but by preventing any future Trojan data mining activities [1, 2] as well. Fuzzy logic is a set-base approximate reasoning methodology. It is used to represent different granules of knowledge which are combined to formulate a projection onto the universe of interest. The Fuzzy set framework is a pattern of reasoning under uncertainty involving axioms of Artificial Intelligence.

5.2 Fuzzy Logic

There has been a vague or blurred literature concept for Artificial Intelligence (AI) and its probabilistic modelling with respect to defined mathematical doctrine. Fuzzy Logic is a
branch of science that explains the degree of relationship between the system’s degree of truth and surrounding uncertainties.

The main difference between probability and possibility theory is that probability is the summation of all the outcome of probabilistic events, while possibility is that maxima of possibilities that depicts an event. Together, both quantify the degree of uncertainty of the system verses the system surrounding. Thus, under vagueness aspects of Fuzziness theory all those approaching statements are true to some degree if they are in context of a true space set. For example, wireless access point signal perception, where one cannot exactly define the strength of access point signal, but rather can perceive to some degree. Therefore, such statements involve so-called vague Fuzzy predicates. Furthermore, Fuzzy logic is based on logical operators and their relationships.

Crisp Sets to Fuzzy Sets is a conceptual mapping of variables from classic sets to fuzzy sets. For example, \( X \) denotes the universal set containing all possible elements of concern with respect to context. The power set, denoted \( 2^A \), of a set \( A \subseteq X \), is the set of subsets of \( A \), i.e. \( 2^A = \{B \mid B \subseteq A\} \). Sets are often defined by specifying a property satisfied by its members in the form as; \( A = \{x \mid P(x)\} \), where \( P(x) \) is a statement of the form “\( x \) has property \( P \)”, that is either true or false for any value \( x \in X \).

**Example 5.1.** Let \( X \) is a universal set with subsets \( A, B \in 2^X \) where

\[
X = \{x \mid x \text{ is a WirelessStation}\}
\]

\[
A = \{x \mid x \text{ is a AccessPoint}\}
\]

\[
B = \{x \mid x \text{ is a access point and has its wireless station LinkLife is equal to less than 10 meters Indore}\}
\]

The thought process behind the modelling is to raise awareness with respect to the wireless network insecurities; that is any un-attended or un-associated Wireless client node is
prone to False Access Point association, unless it have has some prior association knowledgebase data structure. Example 5.1, as shown in figure 5.2, has two input functional variable and one output functional variable. Together they have explained the cause and effect relation of a wireless network.

Figure 5.2: Four-Way Handshake protocol Fuzzy Set

Henceforth, in the above figure 5.2, we have a case where $B \subseteq A \subseteq X$, i.e. the characteristics function, denoted, $\mathbb{N} A$ which is a set of $A \subseteq X$ is a function mapping elements of $X$ into $\{0, 1\}$, has the characteristic function elements, $\mathbb{N} A : x \rightarrow \{0, 1\}$ and is defined as following:

$$\mathbb{N} A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases};$$

where $A \subseteq B$ iff $\forall x \in X \bullet \mathbb{N} A(x) \leq \mathbb{N} B(x)$  

$\subseteq, 2^X$ are Boolean algebra lattice, the fundamental aspects are shown in the table 5.1; Elements of Table 5.1 formulate the fuzzy statements such as, low, medium, high are also
known as fuzzy concepts. The most commonly used range of membership functions are between set of [0,1]. A membership function $A$ is defined as:

$$\mu_A : X \rightarrow [0,1]$$

Where $0$ = Complete Non-Membership degree;

$1$ = Complete Member degree;

<table>
<thead>
<tr>
<th>Operation</th>
<th>Fuzzy crisp relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Involution</td>
<td>$\overline{\overline{A}} = A$</td>
</tr>
<tr>
<td>Idenpotence</td>
<td>$A \cup A = A, A \cap A = A$</td>
</tr>
<tr>
<td>Commutativity</td>
<td>$A \cup B = B \cup A, A \cap B = A \cap B$</td>
</tr>
<tr>
<td>Associativity</td>
<td>$(A \cup B) \cup C = A \cup (B \cup C), (A \cap B) \cap C = A \cap (B \cap C)$</td>
</tr>
<tr>
<td>Distributivity</td>
<td>$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$</td>
</tr>
<tr>
<td>Absorption</td>
<td>$A \cup (A \cap B) = A, A \cap (A \cup B) = A$</td>
</tr>
<tr>
<td>Identity</td>
<td>$A \cup X = X, A \cup \emptyset = A, A \cap \emptyset = \emptyset, A \cap X = A$</td>
</tr>
<tr>
<td>Law of Contradiction</td>
<td>$A \cup \overline{A} = \emptyset$</td>
</tr>
<tr>
<td>Law of excluded middle</td>
<td>$A \cup \overline{A} = X$</td>
</tr>
<tr>
<td>De Morgan’s rule</td>
<td>$\overline{A \cup B} = \overline{A} \cap \overline{B}, \overline{A \cap B} = \overline{A} \cup \overline{B}$</td>
</tr>
</tbody>
</table>

The fuzzy control system can be applied to various systems, such as linear and non-linear systems. The operation modules of fuzzy control system are as following:
i. **Fuzzification** is the process of finding the membership function called crisp values.

Rule Base or knowledgebase are the set of rules used for inferencing a fuzzy logic system.

ii. **Inference of a Knowledgebase** can be further subdivided into two classes: minimum inferencing and product inferencing.

iii. **Defuzzification** is the process of finding the crisp value from a defined inference fuzzy set. There are two techniques for extraction of defuzzification: maximum and centroid. A maximum value is chosen as an output variable, and gravity value is calculated from scalar values respectively.

\[
\bar{X}(\text{centroid}) = \frac{\int_{a}^{b} x\mu(x)dx}{\int_{a}^{b} \mu(x)dx}, \quad \text{------------------------------------}(5.2)
\]

Where \( \mu(x) \) = membership degree of element \( x \) with limit \([a, b]\).

This process involves Fuzzy set theory and Fuzzy control system to compute the multimetric system. The optimum outputs of fuzzy decision making \( x_{op} \Rightarrow X = \{x_{i} | i = 1, \ldots, m\} \) represent the finite set for decision options; and \( G = \{g_{i} | i = 1, \ldots, m\} \) represent the finite sets of goals.

**Example 5.2:** Considers wireless station with access method with respect to a Wi-Fi protocol; attributes are as following, (also shown in figure 5.3.)

\( X_1 = \text{ProbeNoConnect} \); an attribute where a wireless Access Point is probing its radius.

\( X_2 = \text{ProbeSubConnect} \); an attribute where a wireless Access Point selects a desired probe signal.

\( X_3 = \text{ProbeRequestConnect} \); an attribute where a wireless Access Point sends its credentials to the defined Access Point for connection.
\( X_3 = \text{AckRequestConnect} \); an attribute where a wireless Access Point confirms its association.

Figure 5.3: Wireless Station Attributes with respect to Wi-Fi protocol

We may define Wi-Fi, attributes w.r.t. corresponding membership function as following:

\[
\mu_{\text{WirelessStation}}(X_1) = \begin{cases} 
1 & \text{iff}(X_1) \leq 1 \\
(3 - X_1)/2 & \text{if}(X_1) \in [1,3] \\
0 & \text{if}(X_1) > 3 
\end{cases} \quad \text{--------------------------(5.4)}
\]

\[
\mu_{\text{WirelessStation}}(X_2) = \begin{cases} 
0 & \text{if}(X_2) \leq 0 \\
(X_2)/2 & \text{if}(X_2) \in (0,2] \\
(5 - X_2)/3 & \text{if}(X_2) \in (2,5] \\
0 & \text{if}(X_2) > 5 
\end{cases} \quad \text{--------------------------(5.5)}
\]

\[
\mu_{\text{WirelessStation}}(X_3) = \begin{cases} 
0 & \text{if}(X_3) \leq 4 \\
X_3 - 4 & \text{if}(X_3) \in (4,5] \\
1 & \text{if}(X_3) \in (5,7] \\
(10 - X_3)/3 & \text{if}(X_3) \in (7,19] \\
0 & \text{if}(X_3) > 10 
\end{cases} \quad \text{--------------------------(5.6)}
\]
As pointed out previously, the definition of membership function depends on the context, i.e. the definition of Wireless Access Point indoor signal strength may vary with respect to the system’s surrounding. However, the behaviour of Wireless Access Point in a Wi-Fi protocol is explained in figure 5.4.

**Example 5.3:** Considers another wireless access point wireless succession. Where:

\[ Y_1 = \text{ANounce-Offer} + \text{Idle}, \text{ is a first initial attempt for probing any Wireless Access Point.} \]

\[ Y_2 = \text{ANounce} + \text{SNounce} + \text{MICi}, \text{ is an establishment interface with a Wireless Access Point.} \]

\[ Y_3 = \text{GTK} + \text{SNounce} + \text{MICi}, \text{ is an established connection between itself and the Wireless Access Point.} \]

And we may define their corresponding membership function as following:

\[
\mu_{\text{WirelessStation}}(X_4) = \begin{cases} 
0 & \text{iff } (X_4) \leq 7 \\
(X_4 - 7) & \text{iff } (X_4) \in (7, 8] \\
1 & \text{iff } (X_4) > 8 
\end{cases}
\]

\[(5.7)\]

![Figure 5.4: Access Point with respect to Wi-Fi protocol access method](image-url)
The above defined memberships function are the depiction of an access point within any wireless network (Wi-Fi system).

**Example 5.4:** Considers the wireless network connection (Wi-Fi) as a connection between any Wireless client node and its corresponding Access Point. The following figure 5.5 represents the wireless link life between a wireless node (wireless client device) and wireless Access Point (Wi-Fi assess point that can also act as a Wireless server).

![Fuzzy logic connection model of Wi-Fi with respect to Figure 5.4 & 5.3.](image_url)

Figure 5.5: Fuzzy logic connection model of Wi-Fi with respect to Figure 5.4 & 5.3.

\[
\mu_{\text{AccessPoint}}(Y_1) = \begin{cases} 
1 & \text{iff } (Y_1) \leq 1 \\
(3.75 - Y_1) / 2 & \text{iff } (Y_1) \in (0.75, 3.75] \\
0 & \text{iff } (Y_1) > 3.75 
\end{cases} 
\]  

(5.8)

\[
\mu_{\text{AccessPoint}}(Y_2) = \begin{cases} 
0 & \text{iff } (Y_1) \leq 1 \\
(Y_2 - 1) / 3 & \text{iff } (Y_2) \in (1, 5] \\
(9 - Y_2) / 4 & \text{iff } (Y_2) \in (5, 9] \\
(10 - X_3)/3 & \text{iff } (X_3) \in (7, 19] \\
0 & \text{iff } (X_3) > 9 
\end{cases} 
\]  

(5.9)

\[
\mu_{\text{AccessPoint}}(Y_3) = \begin{cases} 
0 & \text{iff } (Y_3) \leq 6 \\
(Y_3 - 6) / 4 & \text{iff } (Y_3) \in (6, 10] \\
1 & \text{iff } (Y_3) > 10 
\end{cases} 
\]  

(5.10)
We have defined the LinkLife corresponding memberships function as following:

\[
\mu_{\text{LinkLife}}(Z_1) = \begin{cases} 
0 & \text{iff } (Z_1) \leq 0 \\
\frac{Z_1}{5} & \text{iff } (Z_1) \in (0, 0.5] \\
\frac{(10 - Z_1)}{5} & \text{iff } (Z_1) \in (0.5, 10] \\
0 & \text{iff } (Z_1) > 10 
\end{cases}
\] (5.11)

\[
\mu_{\text{LinkLife}}(Z_2) = \begin{cases} 
0 & \text{iff } (Z_2) \leq 10 \\
\frac{(Z_2 - 10)}{5} & \text{iff } (Z_2) \in (10, 15] \\
\frac{(20 - Z_2)}{5} & \text{iff } (Z_2) \in (15, 20] \\
0 & \text{iff } (Z_2) > 20 
\end{cases}
\] (5.12)

Figure 5.6: Fuzzy Logic Wi-Fi Connection model
The above defined Equations. 5.11, 5.12 and 5.13, represent the link life activity between and Wi-Fi network respectively. The figure 5.6 is the 3D Graphical representation of the system with its fuzzy logic axioms. It is very interesting to notice that the true maximum of wireless link is a 20.2. But, the vulnerability for any wireless client node in a Wi-Fi scenario exists even before its request for connectivity with any appropriate access point. Henceforth, we have proposed a novel approach to define such type of vulnerability. In Table 5.2, the Security Swarm Wireless Access (SSWA)\cite{1} verifies the wireless network inconsistencies and errors. It identifies the windows of interests for a wireless client against False Access Point association.

5.3 Fuzzy particle framework for DoS attack

Fuzzy rule based system has the ability to acquire knowledge with respect to its surrounding. System state vagueness and uncertainties are continuously calibrated to have the best case output. Henceforth, Fuzzy Logic Rule Base Systems (FRBS) that incorporate fuzzy rule axioms, Fuzzy Database and linguistic rules for accurate validation and verification are a class of Genetic Algorithms (GA). Such GA can also provide quasi-optimal solution sets. These quasi FRBS can be classified into two approaches i.e. Pittsburgh (Smith, 1980) and Michigan approach (Booker et al., 1989; Carse et al., 1996). In the Pittsburgh approach, the whole FRBS is considered as a whole Rule-Base and as one entity, while in the latter each FRBS is a set of distributed entities that interacts to have a best case. Both approaches have proven to be effective, however their NP-Complete have different bounds. Swarm Intelligence \cite{83} is a population based stochastic optimisation technique in which system is
initialized with a population of random solutions and learn to find the optimal output. The optimal potential solution is called Particle. Thus, Particle Swarm Optimisation (PSO) [84] solution always keeps track of system components, such as spatial position, velocity, and different weights with respect to its surrounding. Thus, the proposed SSWA algorithm/Functional model, is an adaptive heuristic approached model. The basic principle of such algorithms has initially been proposed by John Holland (1975).

Table 5.2: Security Swarm Wireless Access Input/Output parameters

<table>
<thead>
<tr>
<th>Input Variables</th>
<th>Description</th>
<th>Abstraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_k$</td>
<td>Particle matrix w.r.t. Fuzzy Solution Set</td>
<td>$k = [i, j]$</td>
</tr>
<tr>
<td>$a_{j,k}^i$</td>
<td>Antecedent parameters i.e. Spatial coordinates w.r.t. Fuzzy Solution Set</td>
<td>Prior Knowledge Fuzzy Solution Set</td>
</tr>
<tr>
<td>$b_{j,k}^i$</td>
<td>Consequent parameters i.e. Spatial coordinates w.r.t. Fuzzy Solution Set</td>
<td>Next Event Knowledge Fuzzy Solution Set</td>
</tr>
<tr>
<td>$c_{j}^{i}$</td>
<td>Connector Space Search w.r.t. the matrix of antecedent and consequent</td>
<td>Markov Chain Fuzzy Solution Set properties</td>
</tr>
<tr>
<td>$V_k$</td>
<td>Velocity matrix (assumed as zero w.r.t. access point velocity)</td>
<td>Cluster velocity aspects</td>
</tr>
<tr>
<td>$I_k$</td>
<td>Wireless Virtual Local Area Network</td>
<td>Link initiation aspects</td>
</tr>
<tr>
<td>$\xi_{k'}$</td>
<td>Media Access Control Protocol Data Unit (MPDU)</td>
<td>Signature aspects</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Output Variables</th>
<th>Description</th>
<th>Abstraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I_k$</td>
<td>Wireless Virtual Local Area Network (In order to prevent DoS attack)</td>
<td>Link initiation aspects Temporal condition w.r.t. False Access point Connectivity</td>
</tr>
</tbody>
</table>
The input and out aspects have been defined in table 5.3 in out modelling we have not proposed any new protocol to replace the deficiencies, however with SSWA we have improved the security aspects, as WVLAN with no prior security knowledge is more prone to malicious vulnerabilities.

![SSWA Fuzzy Logic Model](image)

Figure 5.7: SSWA Fuzzy Logic Model

With respect to the SSWA functional model, described in table 5.2, we have presented a verification approach by integrating model validation paradigm using Matlab, simulink and fuzzy logic block sets. The learning procedure is based on the Particle Swarm Optimisation (PSO) technique.
Table 5.3: Security Swarm Wireless Access (SSWA)

<table>
<thead>
<tr>
<th>SECURITY SWARM WIRELESS ACCESS</th>
</tr>
</thead>
</table>

Given: $P_i$, $a$, $b$, $c$, $V_i$, $I_t$, $\xi$

Where $P_i =$ Particle matrix with FS inputs
  - $a_{i,j}$ = antecedents
  - $b_{i,j}$ = consequent
  - $c_{i,j}$ = connector space search
$V_i =$ Particle Velocity matrix with associated FS
$I_t =$ Succession Initiation
$\xi =$ MPDU vector

1: Initialization $P_i \equiv$ spatial coordinates, $V_i$ and MPDU $\xi$

2: While ($I_t \neq 0$) do
   For $\forall$ spatial coordinates $\in \{ P_i, V_i \}$ from $j$ to $k$
      Compute $|a_{i,j}| \in [-FS_{min}, FS_{max}]$
      Compute $|b_{i,j}| \in [-FS_{out}, FS_{out}]$
      Compute $c_{i,j} \in (\land, \lor)$
      Compute $V_{i,j} \in [-V_{min}, V_{max}]$
   End for
   Update $P_i$ as $P_i$
   Decrement ($I_t$)
   End while

3: Compute $P(t+1) = P(t) \oplus V(t)$

4: Validate for $\Delta P = P - P_0$.
   If $P_i = P_0 + \Delta P$ then goto step 2.
   Else verify MPDU $\xi$ noise ($\xi = \xi$).

5: While (MPDU $\xi = \xi$)
   Establish succession
   Maintain succession.
   End while.

6: Stop scanning $\xi$ and Exit.
Within this approach, the swarm consist of $P_i$ particles i.e. the wireless Access Points including access points and base stations. Each particle $P_i$ depicts a set of Rule Base (RB). Every RB within the system is defined in the equation 5.14 to Equation 5.19: With respect to the above mentioned functional model in table 5.2, we have presented a verification approach by integrating model validation paradigm using Matlab, simulink and fuzzy logic block sets. The learning procedure is based on the Particle Swarm Optimisation (PSO) technique. The underlying principle is based on the individual solution set, and these chromatic features of the solution set can be mapped with any number of binary spars matrix. Its positive outcome is known as “fitness degree of goodness” with respect to its chromatic components. Within this approach, the swarm consists of $P_i$ particles, i.e. the wireless Access Points including access points and base stations. Each particle $P_i$ depicts a set of Rule Base (RB). Every RB within the system is defined in Equations 4.14 to 5.19.

$$P_i = \begin{bmatrix} a_{i,1}^i & a_{i,2}^i & \ldots & a_{i,n}^i & b_1^i & c_1^i \\ a_{2,1}^i & a_{2,2}^i & \ldots & a_{2,n}^i & b_2^i & c_2^i \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ a_{m,1}^i & a_{m,2}^i & \ldots & a_{m,n}^i & b_m^i & c_m^i \end{bmatrix}_{---(5.14)}$$

where each row represents fuzzy logic axioms such as:

a) Antecedent- $a_{j,k}^i$, Fuzzy Set (FS) with $n$ and $m$ as input variables and rules respectively.

b) Consequent- $b_{j,k}^i$

c) Connector space search- $c_{j,k}^i$.

Henceforth they can be expressed as follows:

$$a_{j,k}^i \in [-FS_{in}, FS_{in}] \forall j \in \{1,2,3,\ldots,m\} \quad k \in \{1,2,3,\ldots,n\} \quad \text{---(5.15)}$$

$$b_{j}^i \in [-FS_{out}, FS_{out}] \forall j \in \{1,2,3,\ldots,m\} \Rightarrow FS_{in}, FS_{out} \in F \quad \text{---(5.16)}$$
The Velocity matrix \((V_i)\) with respect to the PSO logic can be defined as follows:

\[
V_i = \begin{bmatrix}
    v_{1,1}^i & v_{1,2}^i & \cdots & v_{1,n}^i & v_{1,n+1}^i & v_{1,n+2}^i \\
    v_{2,1}^i & v_{2,2}^i & \cdots & v_{2,n}^i & v_{2,n+1}^i & v_{2,n+2}^i \\
    \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
    v_{m,1}^i & v_{m,2}^i & \cdots & v_{m,n}^i & v_{m,n+1}^i & v_{m,n+2}^i
\end{bmatrix}
\]

where \(V_{j,k}^i\) is the fuzzy logic spatial input axiom such as:

\[
V_{j,k}^i \in [V_{\text{min}}^i, V_{\text{max}}^i] \forall j \in \{1, 2, 3, \ldots, m\} \quad k \in \{1, 2, 3, \ldots, n+2\}
\]

The Security Swarm Wireless Access (SSWA) proposed a heuristic approach to solve the best set action in an unbounded criterion. SSWA requires a polynomial search and is lower than exponential exhaustive search. NP-Completeness can be adhered to initialisation of the
algorithm, with respect to optimal defined criterion of OSI; Physical Layer aspects. SSWA needs to update its particle matrix space, with respect to its system spatial coordinates. Velocity vector must also adhere to the boundary conditions and to $\xi$, i.e. IEEE 802.11 WLAN-Beacon Frame, Message Protocol Data Unit (MPDU), and then wireless probe signals. Step 2 of the algorithm reveals and validates its next swarm matrix position and also compares its MPDU parameters. SSWA initiates and maintains the communication succession as long as the MPDU threshold elements are aligned, or else the succession is terminated and it is no longer secure to continue. Figure 5.8 is a Fuzzy logic graphical representation of a Physical Layer Wi-Fi model with respect to table 5.2.

5.4 Summary
This section presents a functional layer of a fuzzy logic model. The SSWA discovers the wireless network inconsistencies and errors. It identifies the windows of interests for a wireless client against False Access Point association. SSWA has input parameters such as an Angle of Arrival (AoA), Angle of Departure (AoD), and spatial matrix associated with observed MPDU. The purpose of the model is to eliminate the possibility of DoS attack, which is the most common cause of any compromised wireless transaction. As shown in Figure 5.8, the output parameter is spatial AoD, which can help a Wireless client node in its communication to know whether it is associating to a False Access Point association. The Sensitivity Analysis [85, 86] involves the following steps:

i. Calculate the final defuzzified value of the Spatial-AoD (output case $j=1,2,..,m$) i.e. $y_c(j)$

ii. Recalculate by removing the sensitive input aspect of the algorithm. i.e $y'_c(j)$, Calculate $\Delta_j = \sum_{j} |y'_c(j) - y_c(j)|$
Henceforth the $\bar{\Delta}_i = \left\lfloor \frac{88.9 - 68.7}{4} \right\rfloor = 5.05$

The $\bar{\Delta}_i = 5.05$; shows the imperative aspects of the input. The greater the value of the parameter, the higher the significance. Figure 5.8 represents the graphical activity, with respect to the wireless receiver spatial AoD and MPDU frequency activity i.e. the observed frequency at defined spatial coordinate must be always adhered for secure communication. Figure 5.9 shows the sensitivity analysis graph that reflects the blur or dubious parameter that any Wireless client node must have to have prior expert system with respect to its knowledgebase architecture.

This chapter presents the functional layer algorithm referred to as the SSWA algorithm. It helps in the detection and protection from any False Access Point association. The SSWA algorithm can be used as a verification tool for verifying the authenticity of any wireless access point.
6 Solution for Problem Case 2: Detecting MiM attack

Man-in-the-Middle (MiM) attacks have been one of the most initial plans of vector attacks for quite some time, especially since the advent of smart mobile devices. The basic concept is not new, but innovative methodologies for this planned attack continue to surface. In short, the concept of the technology changes with the advancement of applied science in time i.e. actesriaa mutates with the advancement of the technologies. Thus, MiM attacks are the act of unauthorised individuals or parties placing themselves in the path of communication (wireless or wired) in order to Eavesdrop, Intercept, and Compromise Legitimate communication sessions. Examples of these attacks and succession aspects data back for centuries.

MiM attacks are also known as succession hijacking or TCP (Transmission Control Protocol) hijacking; thus impersonating attacks in a wireless medium, are irrespective of network topologies i.e. Mobile Ad hoc networks (MANets) or Basic Service Sets (BSS) with tail network architectures. These network topologies are always prone to more complex attacks such as GreyHole[87] or BlackHole[88] attacks. These vulnerabilities, with respect to an attack, involve an attacker intercepting and monitoring network traffic or client authorisation credentials and use it to gain complete access and control. The anatomy of attack is by listening to the ARP request replies. Spoofing the MAC address of any legitimate Wireless client node or sending an unsolicited ARP replies to an access point and thus access point can launch MiM attacks or its derivatives i.e. the attacker impersonates the receiver with respect to the sender; and the sender with respect to the receiver. Thus Wireless Security Management is the most critical component in designing a security protocol system, especially in any wireless network.
A critical issue at wireless application layer with respect to MiM attacks is an application of public key technology paradigm for user transaction authentication and verification. Since public key is not owned by the wireless node in communication with its peer; thus an adversaries have a window of escape to impersonate any wireless node by claiming its public key and launch a MiM attack. For example, a malicious wireless node C, can impersonate wireless node B while having communication with wireless node A. It can also impersonate wireless node A as being that of wireless node, since wireless node A and wireless node B cannot verify each other public keys. Thus wireless node C can act as an invisible False (Wireless Access point) router. A conventional solution is a use Certificate Authority (CA), but again in case of impersonating attack an advisory may use the copy of the well-known corresponding certificate authority and still be able to launch an attack. Implementation of public key algorithm in WSN is an expensive exercise as it requires a group of trusted Access Points, especially in MANets. Merkle tree [89, 90] is an approach that can work with the virgin WSN Access Points. Whence, a true parent is a hash of the concentration of its children’s. SoP can also help to improve the Wireless network security since, as a reference to another wireless node certificate authentication; it can also involve the true position of their parents’ wireless network nodes.

Figure 6.1 explains the anatomy of the wireless network False Access Point (FAP), where the fundamental concepts are independent of any network operating system. In other words, if the true Wireless networked node has, all the current and updated security certificate patches; this attack would have, virtually no reliance on a wireless network node or its network operating systems. The figure 6.1 also presents abstract vulnerability issues with respect to confidentiality and integrity for a wireless network theology.
Figure 6.1 MiM attack; vulnerability for wireless network and wired counterpart.

The above figure also reflects that the MiM attack is the prerequisite of a DoS attack, as most of access points are not the part of Internet of Everything (IoE) with respect to the system of reference.

6.1 MiM attack and wireless network.

Man-in Middle attacks can be accomplished by a variety of paradigm; aspects rely on the target protocol, network topology and access method. As reviewed it occurs when any False Access Point place itself between one or more communication edges and mutate to create a communication junction. Ultimate objective of any MiM attack is to place a Cyclic False Node (CRN) junction between legitimate communication network infrastructures. Thus an attacker can have capabilities of performing various attacks, such as sniffing network traffic,
command injection, malicious worm code injection, and public-key cryptosystem attacks in order to fulfill their objective. Table 6.1 provides example of some common tools which can facilitate MiM attack and are not network platform dependent.

Table 6.1: MiM tool for False Access Point activity.

<table>
<thead>
<tr>
<th>MiM tools</th>
<th>Wireless Security Threats.</th>
</tr>
</thead>
<tbody>
<tr>
<td>o DSniff</td>
<td>Sniff Network Layer and Application Layer protocol packets</td>
</tr>
<tr>
<td></td>
<td>{<a href="http://en.wikipedia.org/wiki/DSniff%7D">http://en.wikipedia.org/wiki/DSniff}</a></td>
</tr>
<tr>
<td>o Wireshark</td>
<td>Network monitoring and can sniff the system register contents</td>
</tr>
<tr>
<td></td>
<td>{<a href="http://en.wikipedia.org/wiki/Wireshark%7D">http://en.wikipedia.org/wiki/Wireshark}</a></td>
</tr>
<tr>
<td>o SSLStrip</td>
<td>Compromise the HTTP security by striping SSL aspects for a session</td>
</tr>
<tr>
<td></td>
<td>{<a href="http://en.wikipedia.org/wiki/Moxie_Marlinspike#SSL_stripping%7D">http://en.wikipedia.org/wiki/Moxie_Marlinspike#SSL_stripping}</a></td>
</tr>
<tr>
<td>o TCPkill</td>
<td>An AI oriented tool for blocking host, network ports or their combinations for any Session Hacking</td>
</tr>
<tr>
<td></td>
<td>{<a href="http://en.wikipedia.org/wiki/Tcpkill%7D">http://en.wikipedia.org/wiki/Tcpkill}</a></td>
</tr>
<tr>
<td>o Ettercap</td>
<td>Open source for capturing traffic between different subnetworks. ARP poising and password capturing tool for all OS. Platforms</td>
</tr>
<tr>
<td></td>
<td>{<a href="http://en.wikipedia.org/wiki/Ettercap_(software)%7D">http://en.wikipedia.org/wiki/Ettercap_(software)}</a></td>
</tr>
</tbody>
</table>

The above-mentioned tools are not operating system specific and can be launched by an advisory. However, we have proposed a Functional layer interface model that can actively counteract the paradigm of MiM attack.
6.2 MiM Physical Layer wireless model.

Matlab is a fourth generation programming paradigm with strong mathematical and engineering science integral capabilities’. Figure 6.2, matlab wireless model w.r.t. MiM attack have the following aspects,

i. Symbol Data rate sampling in Hz = Fs = 20e6,
ii. FFT Sample size = N = 64,
iii. Cycle Prefix sample size = L = 16,
iv. Carrier frequency in GHz = FC = 5.0,
v. Speed in km/h = v = 5,
vi. Doppler frequency in Hz = FD = v * FC = 25,
vii. Time delay matrix in seconds = tau = [0, 5, 10, 15] * 1e-6,
viii. Attenuation in dB = P = [0, -2, -4],
ix. Signal to Noise Ration = SNR = 20 dB

Figure 6.2: MiM attack Physical Layer model
An interesting fact about the above mentioned model that is without any spatial verification and validation in any wireless protocol it is vulnerable with respect to CIA attack. Henceforth, in order to improve the security aspects against MiM attack for any network protocol paradigm, a supervisory model is imperative for both or any number of Access Points in communication.

Figure 6.3. Rulebase architecture for eradicating MiM Attack
### Table 6.2: Security Swarm Root Node Input/Output parameters

<table>
<thead>
<tr>
<th>Input Variables</th>
<th>Description</th>
<th>Abstraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>$CN_i$</td>
<td>Maximum number of wireless client access points</td>
<td>Number of slave wireless nodes</td>
</tr>
<tr>
<td>$SP_i$</td>
<td>Saddle point</td>
<td>RSSI aspects w.r.t. spatial coordinates</td>
</tr>
<tr>
<td>$\Delta SP_t$</td>
<td>Accumulated saddle point for all the access points</td>
<td>Aggregated RSSI w.r.t. individual spatial coordinates</td>
</tr>
<tr>
<td>$SN_\xi i$</td>
<td>Spatial node PPDU frequency vector</td>
<td>Frequency Vector matrix w.r.t. spatial coordinated</td>
</tr>
<tr>
<td>$SN_{\xi \text{max}}$</td>
<td>Spatial node with Max Primary TXOP, PPDU frequency vector</td>
<td>Aggregated Frequency Vector matrix w.r.t. individual spatial coordinates</td>
</tr>
<tr>
<td>$SS_i$</td>
<td>Spatial Stack for initial surveillance</td>
<td>Stack Datastructure w.r.t. initial location</td>
</tr>
<tr>
<td>$SS_j$</td>
<td>Spatial Stack for next surveillance</td>
<td>Stack Datastructure w.r.t. next validation spatial location</td>
</tr>
<tr>
<td>$SS_{\text{MiM}}$</td>
<td>Spatial Stack for MiM vector/ MiM Reconnaissance</td>
<td>Stack Datastructure w.r.t. abnormal spatial location for a wireless node</td>
</tr>
<tr>
<td>$SBAVL_Tree$</td>
<td>Spatial Beam Adelson-Velskii &amp; Lands’ Tree</td>
<td>Spatial AVL Tree Datastructure</td>
</tr>
</tbody>
</table>

\[
M = \frac{\partial_i}{\partial I} = \sum_{k=1}^{N} \frac{M_k \Delta_k}{\Delta} \text{ gain between } \in_i \text{ and } I
\]

\[
\in_i \text{ Output of node } I \text{ of the recurrent error-propagation with in SPAVL Tree }
\]

\[
I \text{ Input quantity ( forward error control) }
\]

\[
N \text{ Total number of forward paths from } I \text{ to } \in_i
\]

\[
M_k \text{ Gain of the } k^{th} \text{ forward path }
\]

\[\Delta M_i \text{ Accumulated gain of the Tree Network}
\]

\[P_{mr} \text{ Gain product of } m^{th} \text{ possible combination of } r, \text{ non-sharing loops}
\]

\[\Delta_k \text{ Error propagation with non-sharing input forward path}
\]

\[TP_i \text{ Temporal Particle position in SBAVL Tree}
\]

<table>
<thead>
<tr>
<th>Output Variables</th>
<th>Description</th>
<th>Abstraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiM_Flage</td>
<td>Boolean flag (the root master can halt the operation).</td>
<td>Flag value will define that after, reconnaissance how many malicious nodes ( spatial position) are a rendering Man-in-the-middle attack.</td>
</tr>
</tbody>
</table>
A position-oriented controlled Functional layer solution requires robust and tracking accuracy measurement. It requires position tracking and its continuous application syntheses. The proposed Functional layer model is used, in order to eradicate MiM attack because of False Access Point has PSO and FLC, as the architecture framework blocks. PSO algorithms provide the scaling factor for Fuzzy interface system modelling. Figure 6.3 explains some of the axioms that can improve the security aspects of a MiM attack with respect to the defined model in figure 6.3. Because of spatial coordinates and its associating spatial-aspects MiM-flag can improve the awareness level from white to black region where grey region is a transition phase due to any MiM activity.

Table 6.2; depicts the input and out aspect of the function layer algorithm (i.e. table 6.3). Some of the features are as following:

i. Purpose of the Algorithm is to detect and improve resilience against, MiM attacks by create Spatial Beamforming AVL Balance tree.

ii. Root saddle point will evaluate the root node and its children’s node frequency tree.

iii. Entire communication tree is validated based on the Temporal Particle Position w.r.t. the Spatial Beam Adelson-Velskii & Lands’ (SPAVL) Tree.

iv. Main aspect of the algorithm is to know the spatial position of each wireless node (Access Point) in the communication tree.

v. Stack data structure is used to store and validate the wireless network node position. Saddle points represent a mature spatial value between their maximum and minima.

vi. Upon the discovery the new root node frequency tree vector; it will re associate its entire Tree Structure and store the spatial location of the new tree node with respect to the previous node and may put AP to sleep.

vii. The pivotal feature of is based on non-sharing recurrent loops.
Table 6.3: SSRN a tool for protection against False Access Point (MiM) activity.

<table>
<thead>
<tr>
<th>SECURITY SWARM ROOT NODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given: $CN_i$, $SP_i$, $ΔSP_i$, $SAP\xi_i$, $SAP\xi_i$, $SS_i$, $SBAVL$, $M_i$, $i$, $N$, $M_k$, $ΔM_t$, $Δ$ , $P_{mr}$, $Δ_k$, $TP_i$</td>
</tr>
</tbody>
</table>

Where

$CN_i$ = Maximum number of wireless Client Access Points

$SP_i$ = Saddle Point

$ΔSP_i$ = Accumulated Saddle Point of all the Access Points

$SN\xi_i$ = Spatial node (AP, Wireless Client) PPDU frequency vector

$SN\xi_{max}$ = Spatial node with Max Primary TXOP, PPDU frequency vector

$SS_i$ = Spatial Stack for initial surveillance

$SS_j$ = Spatial Stack for next surveillance

$SS_{MiM}$ = Spatial Stack for MiM vector

MiM_Flag = Boolean flag

$SBAVL$ _Tree = Spatial Beam Adelson-Velskii & Lands’ Tree

$M = \frac{∂e_i}{∂I} = \sum_{k=1}^{N} M_kΔ_k$ = gain between $\xi_i$ and $I$

$\xi_i$ = Output of node $i$ of the recurrent error-propagation with in SPAVL Tree

$I$ = Input quantity (for error control)

$N$ = Total number of forward paths from $I$ to $\xi_i$

$M_k$ = Gain of the $k^{th}$ forward path

$ΔM_t$ = Accumulated gain of the Tree Network

$Δ = 1 - \sum_{m} P_{m1} + \sum_{m} P_{m2} + \sum_{m} P_{m3} + ....$

$P_{mr}$ = Gain product of $m^{th}$ possible combination of r, non-sharing loops

$Δ_k$ = Recurrent error propagation network with non-sharing $k^{th}$ forward path

$TP_i = (ΔM_t + ΔSP_k) - SP_i = $ Temporal Particle position in SBAVL Tree.

1: Initialize $TP_i \forall SN\xi_i$ and $SN\xi_{max} \in SBAVL$ Tree

MiM_Flag = = false
2: For i = 0 to k
   Compute $SN_x^i$ // spatial node frequency i.e. 80 MHz or 160 MHz
   if $SN_x^i \geq SN_x^{max}$ then $SN_x^{max} = SN_x^i$
   do
     ∀ CN_i compute $SN_x^i$
     ∀ CN_i compute $SP_i$ // calculate the saddle point
     ∀ CN_i compute $M$ // calculate the Mason’s gain for re-current error propagation
     $SP_i = \text{push (SS)}$ // save all the elements in stack data type
     $\Delta SP_i = SP_i + +$ // total accumulated saddle weight
     $\Delta M_i = M_i + +$ // total accumulated Mason’s weight
     While (i != k)
     End do
   End for

3: Initialize i // re-initialise for exact stack operation
   While (i != k) do
     $SP_i = \text{pop (SS)}$ // restore elements from stack
     calculate $TP_i$ // calculate SBAVL Tree Access Points
     insert into SBAVL ($TP_i$) Tree // create SBAVL Tree
     validate SBAVL Tree // Balance Tree by determining Left or right rotations
     if (SBAVL Tree != balance) then Rotate (SBAVL Tree) Left or Rotate (SBAVL Tree) Right.
     End if
   End while

4: Compute $SN_x^{root}$ // re scan spatial node frequency from the root node
   If ($SN_x^{root} \neq SN_x^{max}$)
   Then
     CN_i = $SP_{MiM}$ // save the previous vector w.r.t. MiM node spatial position aspects
     CN_i compute $SP_i$ // calculate new saddle point
     CN_i compute $M$ // calculate new Mason’s gain for re-current error propagation
     calculate $TP_i$ // calculate new root SBAVL Tree node weight
     SBAVL ($TP_k$) Tree = SBAVL ($TP_i$) Tree // iff new frequency > current frequency change root SBAVL Tree root Spatial position
   End if

5: Put the previous SBAVL Tree = sleep
6: MiM_Flag = true and Exit // conserve frequency bandwidth to validate the threat level
The following sections explain CIA, vulnerability with respect to MiM attack, a fuzzy logic model [91] simulation within the framework of table 6.2. The models have four framework inputs and a pilot output framework. The output variable defines the validity of a root wireless node (Wi-Fi, Access Point) within the realm SoP.

6.3 MiM Fuzzy logic Model

The Fuzzy logic Functional model and its Sensitivity analysis can improve security aspects with respect to a MiM attack. The Figure below depicts some of the critical Functional layer components, as also explained in figure 6.4 and table 6.2.

Figure 6.4 SSRN Fuzzy logic model w.r.t. Root Node saddle point.
Above figure 6.4 defines the pivotal aspect of a system Root node (Access point) which can be a system wireless (Wi-Fi) access point. South and East input variables represents the zenith-angle[92, 93] coordinates of the Root node (Access Point). These aspects are a pivotal factor for any wireless system not only to protect but to detect also attacks such as a MiM. The third input model parameter is the MiM- Flag is a trapmf [94]. Its value holds true as long as all the other aspects of the system are true. This model component is an imperative aspect with respect to the validation of the Wireless network node authenticity. If any new Wireless network node intends to be a part of the pre-defined SBAVL tree, then it will change the solution set of the Root Node (Wireless Access Point). The detailed axioms with respect to the Functional model are explained in table 6.3, are formulated in figure 6.3 also.

Figure 6.5 Surface plot w.r.t. the SoP of an AP and its PPDU aspects

105
The architecture of the Functional modelling is formulated by using aspects of Fuzzy logic where the foundation component is mamdani [95]. The basic components have union, min and max together with a universal logic component set of And, Or and Not. For the quality of the fuzzy controller modelling with respect to SSRN functional layer, SBAVL tree is found to be better against MiM attack. Figure 6.5 define the Sensitivity analysis with respect to the Table 6.2.

Table 6.3 code w.r.t. that SSRN Fuzzy logic modelling

<table>
<thead>
<tr>
<th>SSRN Fuzzy logic modelling</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Name</td>
</tr>
<tr>
<td>2. Type</td>
</tr>
<tr>
<td>3. Inputs/Outputs</td>
</tr>
<tr>
<td>4. NumInputMFs</td>
</tr>
<tr>
<td>5. NumOutputMFs</td>
</tr>
<tr>
<td>6. NumRules</td>
</tr>
<tr>
<td>7. AndMethod</td>
</tr>
<tr>
<td>8. OrMethod</td>
</tr>
<tr>
<td>9. ImpMethod</td>
</tr>
<tr>
<td>10. AggMethod</td>
</tr>
<tr>
<td>11. DefuzzMethod</td>
</tr>
<tr>
<td>12. InLabels</td>
</tr>
<tr>
<td>13.</td>
</tr>
<tr>
<td>14.</td>
</tr>
<tr>
<td>15.</td>
</tr>
<tr>
<td>16. OutLabels</td>
</tr>
<tr>
<td>17. InRange</td>
</tr>
<tr>
<td>18.</td>
</tr>
<tr>
<td>19.</td>
</tr>
<tr>
<td>20.</td>
</tr>
<tr>
<td>21. OutRange</td>
</tr>
<tr>
<td>22. InMFLabels</td>
</tr>
<tr>
<td>23.</td>
</tr>
<tr>
<td>24.</td>
</tr>
<tr>
<td>25.</td>
</tr>
<tr>
<td>26.</td>
</tr>
<tr>
<td>27.</td>
</tr>
<tr>
<td>28.</td>
</tr>
<tr>
<td>29.</td>
</tr>
<tr>
<td>30.</td>
</tr>
<tr>
<td>31.</td>
</tr>
<tr>
<td>32.</td>
</tr>
<tr>
<td>33. OutMFLabels</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>34.</td>
</tr>
<tr>
<td>35.</td>
</tr>
<tr>
<td>36.</td>
</tr>
<tr>
<td>37.</td>
</tr>
<tr>
<td>38.</td>
</tr>
<tr>
<td>39.</td>
</tr>
<tr>
<td>40.</td>
</tr>
<tr>
<td>41.</td>
</tr>
<tr>
<td>42.</td>
</tr>
<tr>
<td>43.</td>
</tr>
<tr>
<td>44.</td>
</tr>
<tr>
<td>45.</td>
</tr>
<tr>
<td>46.</td>
</tr>
<tr>
<td>47.</td>
</tr>
<tr>
<td>48.</td>
</tr>
<tr>
<td>49.</td>
</tr>
<tr>
<td>50.</td>
</tr>
<tr>
<td>51.</td>
</tr>
<tr>
<td>52.</td>
</tr>
<tr>
<td>53.</td>
</tr>
<tr>
<td>54.</td>
</tr>
<tr>
<td>55.</td>
</tr>
<tr>
<td>56.</td>
</tr>
<tr>
<td>57.</td>
</tr>
<tr>
<td>58.</td>
</tr>
<tr>
<td>59.</td>
</tr>
<tr>
<td>60.</td>
</tr>
<tr>
<td>61.</td>
</tr>
<tr>
<td>62.</td>
</tr>
<tr>
<td>63.</td>
</tr>
<tr>
<td>64.</td>
</tr>
<tr>
<td>65.</td>
</tr>
<tr>
<td>66.</td>
</tr>
<tr>
<td>67.</td>
</tr>
<tr>
<td>68.</td>
</tr>
<tr>
<td>69.</td>
</tr>
<tr>
<td>70.</td>
</tr>
<tr>
<td>71.</td>
</tr>
<tr>
<td>72.</td>
</tr>
<tr>
<td>64.</td>
</tr>
<tr>
<td>65.</td>
</tr>
<tr>
<td>66.</td>
</tr>
<tr>
<td>67.</td>
</tr>
<tr>
<td>68.</td>
</tr>
<tr>
<td>69.</td>
</tr>
<tr>
<td>70.</td>
</tr>
<tr>
<td>71.</td>
</tr>
<tr>
<td>72.</td>
</tr>
<tr>
<td>64.</td>
</tr>
<tr>
<td>65.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>66.</td>
</tr>
<tr>
<td>67.</td>
</tr>
<tr>
<td>68.</td>
</tr>
<tr>
<td>69.</td>
</tr>
<tr>
<td>70.</td>
</tr>
<tr>
<td>71.</td>
</tr>
<tr>
<td>72.</td>
</tr>
<tr>
<td>64. Rule Connection</td>
</tr>
<tr>
<td>65.</td>
</tr>
<tr>
<td>66.</td>
</tr>
<tr>
<td>67.</td>
</tr>
<tr>
<td>68.</td>
</tr>
<tr>
<td>69.</td>
</tr>
<tr>
<td>70.</td>
</tr>
<tr>
<td>71.</td>
</tr>
<tr>
<td>72.</td>
</tr>
</tbody>
</table>
7 Conclusion and future research direction.

An important research topic in Wi-Fi security is how to prevent mobile clients from associating to false (Access Points) APs. The current Wi-Fi security standard, IEEE 802.11i, prevents this by using a Four-Way Handshake. Though this mechanism works very effectively in most scenarios, it cannot detect false APs when the false APs resort to the DoS attack or the MiM attack to pretend to be true APs.

To overcome this limitation of IEEE 802.11i, this thesis proposed to exploit fuzzy logic to make decisions on the genuineness of APs when potential DoS attack or MiM attack exist. Specifically, we first formulated fuzzy logic models to describe the DoS and MiM attacks in Wi-Fi networks, then based on the models, we developed the Security Swarm Wireless Access (SSWA) algorithm and the Security Swarm Root Node (SSRN) algorithm, which decide whether an AP is genuine under the DoS attack and the MiM attack respectively.

We simulated our fuzzy logic models and the proposed algorithms in the MATLAB environment. Our experiments showed that our algorithms perform well in detecting false APs. We choose MATLAB as our simulation environment because MATLAB comes with an implementation of the IEEE 802.11 physical layer and a Fuzzy Logic toolbox. This makes the implementation of our fuzzy logic models and algorithms much easier. The online documentation of MATLAB is a very helpful, which answered most of our MATLAB programming questions.

As a future research direction, we are thinking to apply fuzzy logic to thwart Grey Hole and Black Hole attacks [88] in wireless ad hoc network. The idea will be very similar to what are presented in this thesis. We need to first formulate the fuzzy logic models to describe these two kinds of attacks and then design algorithms to decide whether these two kinds of attacks are present[96].
8 Appendix

8.1 Appendix-1

% Model parameters with respect to the figure 4.1
% Where distance is 4m, 40, and 400m apart between AP and Wireless Access Point.
% Initialize
clear
close all
clc
% basic inputs
fc=2000;
F=8;
V=10;
Nsamples=100;
NSC=100;
alphaPower=0;
% indirect parameters
lambdac=300/fc;
Dx=lambdac/F;
ts=Dx/V;
fs=1/ts;
k=2*pi/lambdac;
a=sqrt(10.^(avPower/10)/NSC)
f=V/lambdac
% max Doppler shift
timeaxis=ts.*[0:Nsamples-1];
% geometric inputs
dBS=4;
ageBS=180;
BSS=dBS*cosd(angleBS)
BSY=dBS*sind(angleBS)
figure;
% Open scenario plot
hold on

% Transmitter geometry
% ==============================================================
N_tx=3;
% Transmitter antennas number.
delta_tx=lambda_c/16;
% Distance between adjacent transmitter antennas (m).
epsilon=0;
% Angle between Y-axis and the transmitter antennas axis (deg).

BS_epaxis=(-(N_tx-1)/2:(N_tx-1)/2)*delta_tx;
BSX=(BS_epaxis*sind(180-epsilon))+BSx;
BSy=(BS_epaxis*cosd(180-epsilon))+BSy;
plot(BSX,BSy,'k^')
% Mobile geometry
N_rx=3;
% No. of MS antennas
delta_rx=lambda_c/16;
% Distance between adjacent mobile antennas (m).
MSyi=(-(N_rx-1)/2:(N_rx-1)/2)*delta_rx;

%==============
%======================================================================
% initial location of receiver (MS) x-coordinate
MSx=MS0+V.*timeaxis;
% MS route along x-axis
MSy=zeros(Nsamples,1);
% MS route along x-axis (y=0)
plot(MSx,MSy,'r')
%===================================================
plot(repmat(MS0,1,length(MSyi)),MSyi,'r.')
%===================================================
MINx=min(min([BSX; MSx]));-200;
MAXx=max(max([BSX; MSx]))+200;
MINy=min(min(min([BSy; MSy])));-200;
MAXy=max(max(max([BSy; MSy])))+200;
axis([MINx MAXx MINy MAXy])
axis equal
% locations of point scatterers ==============================================================
minalpha=0;
maxalpha=360;
D=199;
% radius from origin
alpha=rand(NSC,1)*(maxalpha-minalpha)+minalpha;
% random draw of angles of arrival
SCx=D.*cosd(alpha);
SCy=D.*sind(alpha);
plot(SCx,SCy,'*')
\[ \text{distSCMS}(ii) = \sqrt{(\text{repmat}(SCx,1,Nsamples) - \text{repmat}(MSx,NSC,1)).^2 + (\text{repmat}(SCy,1,Nsamples) - MSyi(ii)).^2}; \]

\[ \text{end} \]

\[ \text{distBSSCMS}=\text{cell}(N_{tx},N_{rx}); \]

\[ \text{for } ii=1:N_{tx} \]
\[ \quad \text{for } jj=1:N_{rx} \]
\[ \quad \text{distBSSCMS} \{ii,jj\} = \text{distBSSCext} \{ii\} + \text{distSCMS} \{jj\}; \]
\[ \text{end} \]
\[ \text{end} \]

\% =======================================================================
\% calculate complex envelope
\% =======================================================================
\[ \text{ray} = \text{cell}(N_{tx},N_{rx}); \]
\[ \text{r} = \text{cell}(N_{tx},N_{rx}); \]
\[ \text{figure, hold} \]
\[ \text{for } ii=1:N_{tx} \]
\[ \quad \text{for } jj=1:N_{rx} \]
\[ \quad \text{ray} \{ii,jj\} = a \times \exp(-j \times kc \times \text{distBSSCMS} \{ii,jj\}); \]
\[ \quad \text{r} \{ii,jj\} = \text{sum} \{\text{ray} \{ii,jj\}\}; \]
\[ \quad \text{plot}(\text{timeaxis},20 \times \log10(\text{abs}(\text{r} \{ii,jj\})),'k') \]
\[ \text{end} \]
\[ \text{end} \]
\[ \text{xlabel('Time (s)')} \]
\[ \text{ylabel('Magnitude of complex envelope (dB)')} \]
\[ \text{title('All transmitters and receivers')} \]
\% =======================================================================
\% convert cell in matrix
\% =======================================================================
\[ \text{H} = \text{zeros}(N_{tx},N_{rx},Nsamples); \]
\[ \text{for } ii=1:N_{tx} \]
\[ \quad \text{for } jj=1:N_{rx} \]
\[ \quad \text{H} \{ii,jj,:,\} = \text{r} \{ii,jj\}; \]
\[ \text{end} \]
\[ \text{end} \]
\% calculate eigenvalues
\% before they were singular values, now eigenvalues
\[ \text{Neigens} = \text{min}(N_{tx},N_{rx}); \]
\[ \text{eigens} = \text{zeros}(\text{Neigens},Nsamples); \]
\[ \text{for } ii=1:N_{samples} \]
\[ \quad \text{eigens}(;,:ii) = \text{svd} \{H(;,:ii)\}; \]
\[ \text{end} \]
\% calculate capacity time-series with equal power assingment to all models
\% Signal to noise ratio in dB
\[ \text{SNR} = 20; \]
snr=10^(0.1*SNR);
CSISO=log2(1+snr.*abs(r{1,1}).^2);
CMIMO=log2(1+snr.*eigens./Neigens);
figure,plot(timeaxis,CMIMO,'k:',timeaxis,sum(CMIMO),'k-',timeaxis,CSISO,'k-')
xlabel('Time (s)')
ylabel('Data Capacity (b/s/Hz)')
legend('MIMO channels ','Overall MIMO','SISO', 'Location', 'Best')
[xMIMO,yMIMO]=fCDF(sum(CMIMO))
[xSISO,ySISO]=fCDF(CSISO)
figure,semilogy(xMIMO,yMIMO,'k',xSISO,ySISO,'k-')
xlabel('Capacity (b/s/Hz)')
ylabel('Probability the abscissa is not exceeded')
legend('MIMO','SISO', 'Location', 'Best')

% calculate RMIMO
RMIMO=zeros(N_tx*N_rx,N_tx*N_rx);
row=1;
col=1;
for ii=1:N_tx
  for jj=1:N_rx
    for mm=1:N_tx
      auxx=corrcoef(r{ii,jj},r{kk,mm});
      RMIMO(row,col)=auxx(1,2);
      col=col+1;
    end
  end
  row=row+1;
  col=1;
end

% save RMIMO RMIMO
% BS side correlations
RBS=zeros(N_tx,N_tx);
for ii=1:N_tx
  for kk=1:N_tx
    auxx=corrcoef(r{ii,1},r{kk,1});
    RBS(ii,kk)=auxx(1,2);
  end
end
RBS
% MS side correlations
RMS=zeros(N_rx,N_rx);
for ii=1:N_rx
  for kk=1:N_rx
    auxx=corrcoef(r{1,ii},r{1,kk});
    RMS(ii,kk)=auxx(1,2);
  end
end
RMS

RMIMOkron=kron(RBS,RMS)
abs(RMIMO)-abs(RMIMOkron)
%======================================================================
fc=2000; %MHz Carrier frequency
F=8; % sampling rate: fraction of wave length
V=10; % m/s MS1 speed
Nsamples=100; % Number of samples
NSC=100; % Number of scatterers
avPower=0; % \sigma^2 Raverage power
%======================================================================
% indirect parameters
%======================================================================
lambdac=300/fc; % m wavelength
Dx=lambdac/F; % m sampling spacing
ts=Dx/V; % s time sampling interval
fs=1/ts; % Hz sampling frequency
kc=2*pi/lambdac; % propagation constant
a=sqrt(10.*(avPower/10)/NSC) % magnitude of echoes
fm=V/lambdac % max Doppler shift
timeaxis=ts.*[0:Nsamples-1]; %======================================================================
% geometric inputs
%======================================================================
dBS=40; % dBs
angleBS=180; % location of transmitter (BS) x-coordinate
BSx=dBS*cosd(angleBS)
BSy=dBS*sind(angleBS) % location of transmitter (BS) y-coordinate
fig=figure; % Open scenario plot
hold on %======================================================================
% Transmitter geometry
%======================================================================
N_tx=3; % Transmitter antennas number.
delta_tx=lambdac/16; % Distance between adjacent transmitter antennas (m).
epsilon=0; % Angle between Y-axis and the transmitter antennas axis (deg).
BS_epaxis=(-(N_tx-1)/2:(N_tx-1)/2)*delta_tx;
BSxi=(BS_epaxis*sind(180-epsilon))+BSx;
BSyi=(BS_epaxis*cosd(180-epsilon))+BSy;
plot(BSxi,BSyi,k^)
%======================================================================
% Mobile geometry
N_rx=3; % No. of MS antennas
114
\texttt{delta_rx=\lambda/c/16;} \\
\% Distance between adjacent mobile antennas (m). \\
\texttt{MSyi=(-(N_{rx}-1)/2:(N_{rx}-1)/2)*delta_rx;} \\
\%=================================================================== \\
\texttt{MS0=-V*timeaxis(end)/2;} \\
\% initial location of receiver (MS) x-coordinate \\
\texttt{MSx=MS0+V.*timeaxis;} \\
\% MS route along x-axis \\
\texttt{MSy=zeros(Nsamples,1);} \\
\% MS route along x-axis (y=0) \\
\texttt{plot(MSx,MSy,'r')} \\
\%=================================================================== \\
\texttt{plot(repmat(MS0,1,length(MSyi)),MSyi,'r.' )} \\
\%=================================================================== \\
\texttt{MINx=min(min([BSxi MSx]))-200;} \\
\texttt{MAXx=max(max([BSxi MSx]))+200;} \\
\texttt{MINy=min(min([BSyi MSy])))-200;} \\
\texttt{MAXy=max(max([BSyi MSy])))+200;} \\
\texttt{axis([MINx MAXx MINy MAXy]) axis equal} \\
\% locations of point scatterers ===============
\% minalpha=0; \\
\% maxalpha=360; \\
\% D=199; \\
\% radius from origin \\
\texttt{alpha=rand(NSC,1)*(maxalpha-minalpha)+minalpha;} \\
\% random draw of angles of arrival \\
\texttt{SCx=D.*cosd(alpha);} \\
\texttt{SCy=D.*sind(alpha);} \\
\texttt{plot(SCx,SCy,'*')} \\
\% three dimension? \\
\texttt{xlabel('Distance (m)')} \\
\texttt{ylabel('Distance (m)')} \\
\%=================================================================== \\
\% calculate distance matrix \\
\texttt{distBSSC=cell(N_{tx},1);} \\
\texttt{distBSSCext=cell(N_{tx},1);} \\
\texttt{for ii=1:N_{tx}} \\
\texttt{distBSSC{ii}=sqrt((BSxi(ii)-SCx).^2+(BSyi(ii)-SCy).^2);} \\
\texttt{distBSSCext{ii}=repmat(distBSSC{ii},[1 Nsamples]);} \\
\texttt{end} \\
\texttt{dist_BSSCMS=cell(N_{tx},N_{rx});} \\
\texttt{for ii=1:N_{tx}} \\
\texttt{for jj=1:N_{rx}} \\
\texttt{distBSSCMS{ii,jj}=distBSSCext{ii}+distSCMS{jj};} \\
\texttt{end} \\
\texttt{end} \\
\%=================================================================== \\
\% calculate complex envelope \\
\texttt{ray=cell(N_{tx},N_{rx});} \\
\texttt{r=cell(N_{tx},N_{rx});} \\
\texttt{figure;hold} \\
\texttt{for ii=1:N_{tx}} \\
\texttt{for jj=1:N_{rx}} \\
\texttt{ray{ii,jj}=distBSSCMS{ii,jj};} \\
\texttt{r{ii,jj}=ray{ii,jj};} \\
\texttt{end} \\
\texttt{end} \\
\texttt{115}
ray(ii, jj) = a*exp(-j*kc*distBSSCMS(ii, jj));

r(ii, jj) = sum(ray(ii, jj));

plot(timeaxis, 20*log10(abs(r(ii, jj))),'k')
end
end

xlabel('Time (s)')
ylabel('Magnitude of complex envelope (dB)')
title('All transmitters and receivers')

% convert cell in matrix
H = zeros(N tx, N rx, Nsamples);
for ii = 1:N tx
    for jj = 1:N rx
        H(ii, jj, :) = r(ii, jj);
    end
end

% calculate eigenvalues
Neigens = min(N_tx, N_rx);
eigens = zeros(Neigens, Nsamples);
for ii = 1:Nsamples
    eigens(:, ii) = svd(H(:, :, ii));
end

eigens = eigens.^2; % before they were singular values, now eigenvalues

calculate capacity time-series with equal power assingment to all models
SNR = 20; % Signal to noise ratio in dB
snr = 10^(0.1*SNR);
CSISO = log2(1 + snr.*abs(r(1, 1)).^2);
CMIMO = log2(1 + snr.*eigens./Neigens);

figure, plot(timeaxis, CMIMO, 'k:', timeaxis, sum(CMIMO), 'k-', timeaxis, CSISO, 'k')
xlabel('Time (s)')
ylabel('Data Capacity (b/s/Hz)')
legend('MIMO channels', 'Overall MIMO', 'SISO', 'Location', 'Best')

% calculate RMIMO
RMIMO = zeros(N tx*N rx, N tx*N rx);
row = 1;
col = 1;
for ii = 1:N tx
for jj=1:N_rx
    for kk=1:N_tx
        for mm=1:N_rx
            auxx=corrcoef(r{ii,jj},r{kk,mm});
            RMIMO(row,col)= auxx(1,2);
            col=col+1;
        end
        row=row+1;
        col=1;
    end
end
% save RMIMO RMIMO
% ========================================================================
% BS side correlations
% ========================================================================
RBS=zeros(N_tx,N_tx);
for ii=1:N_tx
    for kk=1:N_tx
        auxx=corrcoef(r{ii,1},r{kk,1});
        RBS(ii,kk)= auxx(1,2);
    end
end
RBS
% ========================================================================
% MS side correlations
% ========================================================================
RMS=zeros(N_rx,N_rx);
for ii=1:N_rx
    for kk=1:N_rx
        auxx=corrcoef(r{1,ii},r{1,kk});
        RMS(ii,kk)= auxx(1,2);
    end
end
RMS
% ========================================================================
% basic inputs
% ========================================================================
fc=2000;
% MHz  Carrier frequency
F=8;
% sampling rate: fraction of wave length
V=10;
% m/s MS1 speed
Nsamples=100;
% Number of samples
NSC=100;
% Number of scatterers
avPower=0;
% sigma^2  Raverage power
% ========================================================================
% indirect parameters
% ========================================================================
lambdac=300/fc;
% m wavelength
Dx=lambdac/F;
% m sampling spacing
ts=Dx/V;
% s time sampling interval
fs=1/ts;
% Hz sampling frequency
kc=2*pi/lambdac;
% propagation constant
a=sqrt(10.^(avPower/10)/NSC)
% magnitude of echoes
fm=V/lambdac
% max Doppler shift
timeaxis=ts.*[0:Nsamples-1];
% geometric inputs
% geometric inputs
dBS=400;
angleBS=180;
BSx=dBS*cosd(angleBS)
% location of transmitter (BS) x-coordinate
BSy=dBS*sind(angleBS)
% location of transmitter (BS) y-coordinate
fig=figure;
% Open scenario plot
hold on
% Transmitter geometry
N_tx=3;
% Transmitter antennas number.
epsilon=0;
% Angle between Y-axis and the transmitter antennas axis (deg).
BS_epaxis=(-(N_tx-1)/2:(N_tx-1)/2)*delta_tx;
BSxi=(BS_epaxis*sind(180-epsilon))+BSx;
BSyi=(BS_epaxis*cosd(180-epsilon))+BSy;
plot(BSxi,BSyi,'k^')
% Mobile geometry
N_rx=3;
% No. of MS antennas
delta_rx=lambdac/16;
% Distance between adjacent mobile antennas (m).
MSyi=(-(N_rx-1)/2:(N_rx-1)/2)*delta_rx;
%===================================================
MS0=-V*timeaxis(end)/2;
% initial location of receiver (MS) x-coordinate
MSx=MS0+V.*timeaxis;
% MS route along x-axis
MSy=zeros(Nsamples,1);
% MS route along x-axis (y=0)
plot(MSx,MSy,'r')
%===================================================
plot(repmat(MS0,1,length(MSyi)),MSyi,'r.')
%===================================================
MINx=min(min([BSxi MSx]));-200;
MAXx=max(max([BSxi MSx]))+200;
MINy=min(min([BSyi MSy]));-200;
MAXy=max(max(max([BSyi MSy']))));+200;
axis([MINx MAXx MINy MAXy])
axis equal
% locations of point scatterers
minalpha=0;
maxalpha=360;
D=199;
% radius from origin
alpha=rand(NSC,1)*(maxalpha-minalpha)+minalpha;
% random draw of angles of arrival
SCx=D.*cosd(alpha);
SCy=D.*sind(alpha);
plot(SCx,SCy,*);
% three dimension?
xlabel('Distance (m)');
ylabel('Distance (m)');
%
% calculate distance matrix
%
distBSSC=cell(N_tx,1);
distBSSCext=cell(N_tx,1);
for ii=1:N_tx
    distBSSC{ii}=sqrt((BSxi(ii)-SCx).^2+(BSyi(ii)-SCy).^2);
distBSSCext{ii}=repmat(distBSSC{ii},[1 Nsamples]);
end
dist_BSCMS=cell(1,N_rx);
for ii=1:N_rx
    distSCMS{ii}=sqrt((repmat(SCx,1,Nsamples)-repmat(MSx,NSC,1)).^2+(repmat(SCy,1,Nsamples)-MSyi(ii)).^2);
end
distBSSCMS=cell(N_tx,N_rx);
for ii=1:N_tx
    for jj=1:N_rx
        distBSSCMS{ii,jj}=distBSSCext{ii}+distSCMS{jj};
    end
end
% convert cell in matrix
H=zeros(N_tx,N_rx,Nsamples);
for ii=1:N_tx
    for jj=1:N_rx
        H(ii,jj,:)=r{ii,jj};
    end
end
% calculate eigenvalues
Neigens=min(N_tx,N_rx);
eigens=zeros(Neigens,Nsamples);
for ii=1:Nsamples
    eigens(:,ii)=svd(H(:,:,ii));
end
eigens=eigens.^2;  % before they were singular values, now eigenvalues
figure,plot(timeaxis,10*log10(eigens),'k')
xlabel('Time (s)')
ylabel('Eigenvalues (dB)')

CDFx=[];
CDFy=[];
for ii=1:min(N_tx,N_rx)
    [x,y]=fCDF(eigens(ii,:));
    CDFx=[CDFx, x'];
    CDFy=[CDFy, y'];
end
figure,semilogy(10*log10(CDFx),CDFy)
xlabel('Eigenvalues (dB)')
ylabel('Probability the abscissa is not exceeded')

SNR=20;   % Signal to noise ratio in dB
snr=10^(0.1*SNR);
CSISO=log2(1+snr.*abs(r{1,1}).^2);
CMIMO=log2(1+snr.*eigens./Neigens);
figure,plot(timeaxis,CMIMO,'k:',timeaxis,sum(CMIMO),'k-',timeaxis,CSISO,'k-')
xlabel('Time (s)')
ylabel('Data Capacity (b/s/Hz)')
legend('MIMO channels ','Overall MIMO','SISO', 'Location', 'Best')

RMIMO=zeros(N_tx*N_rx,N_tx*N_rx);
row=1;
col=1;
for ii=1:N_tx
    for jj=1:N_rx
        for mm=1:N_rx
            auxx=corrcoef(r{ii,jj},r{kk,mm});
            RMIMO(row,col)=auxx(1,2);
            col=col+1;
        end
    end
    row=row+1;
col=1;
end

RBS=zeros(N_t,N_t);
for ii=1:N_t
    for kk=1:N_t
        RBS(ii,kk)=corrcoef(r{ii},r{kk});
    end
end

RBS=corrcoef(r{1,1});
auxx=corrcoef(r{ii,1},r{kk,1});
RBS(ii,kk)=auxx(1,2);
end
end
RBS

% MS side correlations
% MS side correlations
RMS=zeros(N_rx,N_rx);
for ii=1:N_rx
    for kk=1:N_rx
        auxx=corrcoef(r{1,ii},r{1,kk});
        RMS(ii,kk)=auxx(1,2);
    end
end
RMS

% RMIMOkron=kron(RBS,RMS)

abs(RMIMO)-abs(RMIMOkron)

abs(RMIMO-RMIMOkron)
8.2 Appendix-2

% Figure 4.3, %
% %==========================================================================
clear
close all
clc
% basic inputs=================================================================

fc=200;
% MHz  Carrier frequency
F=50;
% sampling rate: fraction of wave length
V=10;
% m/s MS1 speed
NFFT=128;
% Number of points in FFT
Nmeters=4;
% Number of meters in the distance axis.

% geometry inputs=================================================================

BSx=-4;
% location of transmitter (BS) x-coordinate
BSy=4;
% location of transmitter (BS) y-coordinate
MS0=0;
% initial location of receiver (MS) x-coordinate

% locations of point scatterers=================================================================

SC=[100 100
    -100 50
    -40 30
    100 70
    -70 -80
    -30 -60
    5 120
    -40 110
    0 -110
    -60 30
    50 -60
    -80 45
    -45 -80];

SCx=SC(:,1);
SCy=SC(:,2);

NSC=length(SCx);
% Number of scatterers;

figure,plot(SCx,SCy,'*', BSx,BSy,'^'), hold on

% indirect parameters=================================================================
lambdac=300/fc;
% m wavelength
Dx=lambdac/F;
% m sampling spacing
ts=Dx/V;
% s time sampling interval
fs=1/ts;
% Hz sampling frequency
kc=2*pi/lambdac;
% propagation constant
Nsamples=Nmeters/Dx;
% Number of samples

% timeaxis=ts.*[0:Nsamples-1];
distanceaxis=Dx.*[0:Nsamples-1];

% MSx=MS0+V.*timeaxis; % MS route along x-axis
MSx=MS0+distanceaxis;
% MS route along x-axis
MSy=repmat(distanceaxis',1,length(distanceaxis));
% MS routes along x-axis for different y values

for m=1:length(MSy)
    plot(MSx,MSy(m,:),'r')
end
xlabel('Distance (m)');
ylabel('Distance (m)');

MINx=min(min(BSx, SCx))-100;
MAXx=max(max(BSx, SCx))+100;
MINy=min(min(min(BSy, SCy)))-100;
MAXy=max(max(max(BSy, SCy)))+100;
axis([MINx MAXx MINy MAXy])

% calculate distance matrix
distBSSC=sqrt((BSx-SCx).^2+(BSy-SCy).^2);

distBSSCext=repmat(distBSSC,[1 Nsamples Nsamples]);
distSCMS=zeros(NSC,Nsamples,Nsamples);

for jj=1:Nsamples
    for ii=1:Nsamples
        distSCMS(:,:,jj)=sqrt((SCx-MSx(ii)).^2+(SCy-MSy(jj,1)).^2);
    end
end

distBSSCMS=distBSSCext+distSCMS;

% calculate complex envelope
ray=exp(-j*kc*distBSSCMS);
ra=sum(ray);
ra(1,:)=ra(1,:);

figure,surf(distanceaxis,distanceaxis,abs(ra));
xlabel('Distance apart (m)');
ylabel('Distance apart (m)');
zlabel('Magnitude of complex envelope');

%=======================================================================

fc=200;
% MHz Carrier frequency
F=50;
% sampling rate: fraction of wave length
V=10;
% m/s MS1 speed
NFFT=128;
% Number of points in FFT
Nmeters=4;
% Number of meters in the distance axis.

% geometry inputs ==========================================================

BSx=-40; % location of transmitter (BS) x-coordinate
BSy=40; % location of transmitter (BS) y-coordinate
MS0=0; % initial location of receiver (MS) x-coordinate

% locations of point scatterers ===========================================

SC=[100 100
-100 50
-40 30
100 70
-70 -80
-30 -60
5 120
-40 110
0 -110
-60 30
50 -60
-80 45
-45 -80];

SCx=SC(:,1);
SCy=SC(:,2);

NSC=length(SCx);
% Number of scatterers;

figure,plot(SCx,SCy,'*', BSx,BSy,'^'), hold on

% indirect parameters ======================================================

lambdac=300/fc;
% m wavelength
Dx=lambdac/F;
% m sampling spacing
ts=Dx/V;
% s time sampling interval
fs=1/ts;
% Hz sampling frequency
kc=2*pi/lambdac;
% propagation constant
Nsamples=Nmeters/Dx;
% Number of samples
% timeaxis=ts.*[0:Nsamples-1]
distanceaxis=Dx.*[0:Nsamples-1];

% MSx=MS0+V.*timeaxis; % MS route along x-axis
MSx=MS0+distanceaxis;
% MS route along x-axis
MSy=repmat(distanceaxis',1,length(distanceaxis));
% MS routes along x-axis for different y values

for m=1:length(MSy)
    plot(MSx,MSy(m,:),'r')
end
xlabel('Distance (m)');
ylabel('Distance (m)');

MINx=min(min(BSx, SCx))-100;
MAXx=max(max(BSx, SCx))+100;
MINy=min(min(min(BSy, SCy)))-100;
MAXy=max(max(max(BSy, SCy)))+100;
axis([MINx MAXx MINy MAXy])

distBSSC=sqrt((BSx-SCx).^2+(BSy-SCy).^2);
distBSSCext=repmat(distBSSC,[1 Nsamples Nsamples]);
distSCMS=zeros(NSC,Nsamples,Nsamples);

for jj=1:Nsamples
    for ii=1:Nsamples
        distSCMS(:,ii,jj)=sqrt((SCx-MSx(ii)).^2+(SCy-MSy(jj,1)).^2);
    end
end
distBSSCMS=distBSSCext+distSCMS;

% calculate complex envelope
ray=exp(-j*kc*distBSSCMS);
ra=sum(ray);
r(:,:,1)=ra(1,:);
figure,surf(distanceaxis,distanceaxis,abs(r));
xlabel('Distance apart (m)');
ylabel('Distance apart (m)');
zlabel('Magnitude of complex envelope');

% MHz Carrier frequency
fc=200;
F=50;
% sampling rate: fraction of wave length
V=10;
NFFT=128;
\text{% Number of points in FFT} 
Nmeters=4;
\text{% Number of meters in the distance axis.}

\text{% geometry inputs} 
\text{BSx=-400;} \text{ MS1 speed} 
\text{BSy= 400;} \text{ NFFT=128;}
\text{MS0= 0;} \text{ Nmeters=4;}
\text{BMx=4;} \text{ Number of scatterers.}
\text{SC0=1;} \text{ Number of meters in the distance axis.}

% locations of point scatterers 
\text{SC=[100 100} 
\text{-100 50} 
\text{0 50} 
\text{-70 80} 
\text{-30 60} 
\text{5 120} 
\text{-40 110} 
\text{0 110} 
\text{-60 30} 
\text{50 -60} 
\text{-80 45} 
\text{-45 -80];}

SCx=SC(:,1); 
SCy=SC(:,2); 
NSC=length(SCx); 
\text{% Number of scatterers.}

\text{figure,plot(SCx,SCy,'*', BSx,BSy,'^'), hold on}

% indirect parameters 
\text{lambdac=300/fc;} 
\text{\% m wavelength} 
\text{Dx=lambdac/F;} 
\text{\% m sampling spacing} 
\text{ts=Dx/V;} 
\text{\% s time sampling interval} 
\text{fs=1/ts;} 
\text{\% Hz sampling frequency} 
\text{kc=2*pi/lambdac;} 
\text{\% propagation constant} 
\text{Nsamples=Nmeters/Dx;} 
\text{\% Number of samples} 
\text{timeaxis=ts.*[0:Nsamples-1];} 
\text{distanceaxis=Dx.*[0:Nsamples-1];}

% MSx=MS0+V.*timeaxis; 
\text{% MS route along x-axis} 
\text{MSx=MS0+distanceaxis;}

% MSx=MS0+V.*timeaxis; 
\text{% MS route along x-axis} 
\text{MSx=MS0+distanceaxis;
% MS route along x-axis
MSy=repmat(distanceaxis',1,length(distanceaxis));
% MS routes along x-axis for different y values
for m=1:length(MSy)
    plot(MSx,MSy(m,:),'r')
end
xlabel('Distance (m)');
ylabel('Distance (m)');

MINx=min(min(BSx, SCx))-400;
MAXx=max(max(BSx, SCx))+400;
MINy=min(min(min(BSy, SCy)))-400;
MAXy=max(max(max(BSy, SCy)))+400;
axis([MINx MAXx MINy MAXy])

% calculate distance matrix
distBSSC=sqrt((BSx-SCx).^2+(BSy-SCy).^2);
distBSSCext=repmat(distBSSC,[1 Nsamples Nsamples]);
distSCMS=zeros(NSC,Nsamples,Nsamples);
for jj=1:Nsamples
    for ii=1:Nsamples
        distSCMS(:,ii,jj)=sqrt((SCx-MSx(ii)).^2+(SCy-MSy(jj,1)).^2);
    end
end
distBSSCMS=distBSSCext+distSCMS;

% calculate complex envelope
ray=exp(-j*kc*distBSSCMS);
ra=sum(ray);
r(:,:,)=ra(1,:);
figure,surf(distanceaxis,distanceaxis,abs(r));
xlabel('Distance apart (m)');
ylabel('Distance apart (m)');
zlabel('Magnitude of complex envelope');
8.3 Appendix-3

Following table 6.3 provides some problematic aspects with respect to Man-in-Middle; the following issues are with respect to IEEE 802.11 and IEEE 802.16

Table 6.3: wireless MiM; False Access Point attacks table

<table>
<thead>
<tr>
<th>Problem Cause in Wireless Network Access method</th>
<th>Problem Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Max is based on the Data Over Cable Services Interface, Base Line Plus Interface (DOCSIS BPI +); Designed for cable modem.</td>
<td>○Security Handover Issues w.r.t. Mobility.</td>
</tr>
<tr>
<td>Operation Stack house Layer 1 and Layer 2 of OSI Model Wi-Max has no defied solution against Layer 1 attacks as RNG_REQ and RNG_RSP are in a plain text. 48 bit wireless client Mac address for SA and X.509 certificate.</td>
<td>○DoS; ○DDoS.</td>
</tr>
<tr>
<td>Three types of SA (Security Association) 1: Primary SA; Used by wireless client without encryption initially. 2: Static SA; Used by BS (Base Station) for all. 3: Dynamic SA; for mobility factor same as IEEE 802.1j criterion.</td>
<td>○RRRN; ○Mesh Mode attack.</td>
</tr>
<tr>
<td>Network coding w.r.t. each Access Point during handoff succession criterion, it must follow intra flow or inter flow network coding criterion, i.e. within the network flow or across multiple flow respectively; henceforth intelligent knowledgebase routing protocol must be defined. This protocol must be secure and provide real-time multimedia.</td>
<td>○Pollution and Entropy attacks.</td>
</tr>
<tr>
<td>X.509 Certificate exchange with no encryption from client to BS (Base Station).</td>
<td>○Man-in-the-Middle Attack.</td>
</tr>
<tr>
<td>SA defines two type of TEK (Traffic Encryption Key). TEK 1: Used for current operation, TEK 2: Used when TEK1 expires, TEKs life time is arbitrary (b/w 30minutes to 7 days) 2 bit key descriptor for each TEK (00, 01, 10, 11) HMAC (Hashed Message Authentication Code): HMAC=Key XOR Message; Where Key descriptor is 2 bit.</td>
<td>○Open to reply attack where attacker can reuse the expired key. ○Privacy-Preservation during fast handover.</td>
</tr>
<tr>
<td>EAP (Extensible Authentication Protocol) messages are directly encoded into management frames and EAP is dependent upon SIM (Subscriber Identity Module) or USIM (Universal SIM) or Hardcoded digital certificate. Privacy and Key Management = Step 1 + Step 2 Step 1= wireless client authorization and AK exchange; wireless client with no prior Knowledgebase. Step 2= TEK exchange; when TEK 1 expires TEK 2 keep repeating till mobile succession ends.</td>
<td>○IoT; ○Location Privacy Violation. ○Multi and Broad cast attacks. ○Eaves Dropping</td>
</tr>
<tr>
<td>Lack of BS certificates,</td>
<td>○Relies 1 to 1 on IEEE 802.11i ○Duplication of AK can cause RRRN Attack ○Water Torture Attack</td>
</tr>
<tr>
<td>AK is generated by BS for its wireless client, and BS does not have perfect random number generator. DES in CBC mode is insecure after operating (2^{64} = 2^{32}) blocks size, iff block size = 64 bits.</td>
<td></td>
</tr>
<tr>
<td>Centralized security architecture cannot support hop by hop authentication,</td>
<td>○Key Renewal (duplication) is used instead of new authentication whence it is susceptible to RRRN attack. ○Cannot support multicast multi hop mobile multimedia security application w.r.t. MANETs also.</td>
</tr>
<tr>
<td>Security Sub Layer; IEEE 802.16m relies on PKMv3</td>
<td>○When it’s susceptible to RRRN attack. ○And all the physical layer attacks referred in figure 8.</td>
</tr>
<tr>
<td>Wi-Fi, 4- Way hand shake protocols first and last succession criterion is w.r.t. the acknowledgement only</td>
<td></td>
</tr>
</tbody>
</table>
9 References


10 Acronyms
AAA= Authentication Authorisation Accounting
ACK= Acknowledgement
ACL= Access Control List
AES= Advance Encryption Standard
ANonce= One used digit from AP
AoA= Angle of Arrival
AoD= Angle of Departure
AP= Access Point
ARP= Address Resolution Protocol
AuC= Authentication Center
AVL- Tree= Adelson-Velskii Tree
AWGN= Additive White Gaussian Noise
BER= Bit Error Rate
BSS= Basic Service Set
C4ISR= Computer Command Control Communication
Intelligence Surveillance Reconnaissance
CIA= Confidentiality Integrity Availability
COA= Centre Of Area
COBIT= Control Objective for Information and Related Technology
CPN= Color Petri Nets
CSMA/CA= Carrier Sense Multiple Access/ Collision Avoidance
CTS= Clear to Sent
DAC= Discretionary Access Control
DBPSK
DDoS= Distributed Denial of Service
DMZ= demilitarized zone
DoS= Denial of Service
DR= Disaster Recovery
DS= Distributed System
ECDH= Elliptic Curve Diffie-Hellam
ESS= Extended Service Set
EU= End User
FAP= False Access Point
FRBS= Fuzzy Logic Rule Base System
FS= Fuzzy Set
FTP= File Transfer Protocol
GTK= Group Wise Transient Key
HIPAA= Health Insurance Portability And Accounting Act of 1996
ICMP= Internet Control Message Protocol
IDS= Intrusion Detection System
IoE= Internet of Everything
IoT= Internet of Things
IP= Internet Protocol
ISM= Industrial Scientific Medical
ISO 27002= International Standard Organisation for wireless security
ITIL= Information Technology Infrastructure Library
KDC= Key Distribution Centre
LTE-4G= Long Term Evolution Generation Four
MAC= Mandatory Access Control
MAN= Metropolitan Area Network
MANETs= Mobile Adhoc Networks
Mbps= Megabits per second
MIC= Message Integrity Code
MiM= Main-in-The-Middle
MIMO= Multiple Input Multiple Output
MPDU= Message Protocol Data Unit
MS= Mobile Station
MSK= Master Session
NEK= New Encryption Key
NetBIOS= Network Basic Input/output System
NIS+= Network Information Services Plus
NP= Polynomial-time
OFDM= Orthogonal Frequency Division Multiplexing
OSI= Open System Interconnection
PAN= Personal Area Network
PCM= Pulse Code Modulation
PLC= Protocol Composition Logic
PMK= Pairwise Masker Key
PPDU= PLCP Protocol Data Unit
PPTP= Point to Point Tunnelling Protocol
PSK= Pre-Shared Key
PSO= Particle Swarm Optimisation
PTK= Pairwise Transient Key
R3N2= Rouge Roger Rogue Network Access Point
RB= Rule Base
RBAB= Role Base Access Control
RDS= Remote Directory Synchronisation
RFC= Request For Comments
ROI= Return On Investment
RPC= Remote Procedure Call
RSNA= Robust Security Network Association
RTS= request To Sent
RX = Receiver
SBAVL= Spatial Beam Adelson-Velskii & Lands
SES= State Emergency Services
SIMO= Single Input Multiple Output
SISO= Single Input Single Output
SLA= Service Level Agreement
SNMP= Simple Network Management Protocol
Snonce = Once used digit from client station
SNR= Signal to Noise Ratio
SOP= Standard Operation Procedure
SoP= Surface of Position
SSWA= Security Swarm Wireless Access
SYN= Synchronisation
TCP= Transmission Control Protocol
TKIP= Temporal Key Integrity Protocol
TX= Transmitter
UDP= User Datagram Protocol
UMTS= Universal Mobile Telecommunication System
VPN=Virtual Private Network
WEP= Wire Equivalent Privacy
Wi-Fi= Wireless Fidelity
WiMAX= Worldwide Interoperability for Microwave Access
WLAN= Wireless Local Area Network
WMAN= Wireless Metropolitan Area Network
WSN=Wireless Sensor Network