ANALYSIS OF IEEE 802.11 STANDARD FROM SECURITY STANDPOINT AND FINDING SOLUTION TO PS-POLL BASED DOS ATTACK

By

Zaffar Iqbal Qureshi

Submitted to the Faculty of Information Security
National University of Sciences and Technology, Rawalpindi in partial fulfillment for the requirements of M. S Degree in Information Security
MARCH 2009

ABSTRACT

The proliferation of networking across the world continues to grow at an incredible rate. In the past decade the growth of Wireless Local Area Networks (WLAN) was even more astounding. The Institute of Electrical and Electronics Engineers (IEEE) standard 802.11 for WLAN, ratified in 1999 was widely accepted by the industry. Due to the scarcity of battery power in portable devices operating in WLANs, 802.11 directly addressed the need of Power Saving (PS). It defines a mechanism allowing stations (STA) to go into sleep mode without losing information.

Identification of flaws in security mechanism of 802.11 led to amendments / enhancements in the standard, but availability issues persisted. Even in the latest IEEE security standard 802.11i, management and control frames are unprotected. Thus the possibility of identity theft exposes WLAN to Denial of Service (DoS) attacks thereby compromising availability. DoS attacks have high success rate in PS mode, as portable mobile devices recurrently operate in this mode to conserve battery power. Moreover, at the time when attack is being perpetrated, the legitimate user is quiescent and thus oblivious to this malicious activity on the network.

IEEE 802.11 standard has been analyzed for identity vulnerabilities. Attacks have been studied to identify the niche of DoS attacks in PS mode. A solution for this persisting vulnerability has been proposed and analyzed for its effectiveness by simulation. The solution is effective, efficient and robust. It can be incorporated in wireless stations by just firmware upgrades, not needing any additional hardware.

Dedicated to

My Beloved Parents

ACKNOWLEDGEMENTS

First and foremost, I am most humbly thankful to ALLAH Almighty. I thank him for creating me. I thank him for giving me each day; without him sustaining the universe nothing would exist.

I am very thankful to my thesis advisor, Dr Younus Javed. His sage advice and patient encouragement aided the publication of papers and writing of this thesis in innumerable ways. I am also thankful to my committee members, Jawad Habib, Athar Mohsin and Faisal Amjad for their valuable feedback and comments on my research. I am especially thankful to my colleagues; Baber and Atta Ullah for their guidance and their time, spent in protracted discussions about mathematical problems and simulation functions. Without their support, this work would not have seen conclusion.

I am extremely grateful to Information Security Department and all my teachers for providing a healthy, yet competitive learning environment. My sincere gratitude goes to Military College of Signals and National University of Sciences and Technology for the provision of research facilities and making the whole learning experience worthwhile.

I am indebted to my mother, whose prayers have always knocked on correct doors, granting me courage to sail through tough times. My family, especially my wife deserves particular thanks for her patience and care. My daughter Eesha and sons Aashan and Fayzaan also deserve special gratitude, just for being there to light me up with their radiant smiles. Last but not the least my sister; whose constant supply of tea and coffee kept me going during final days and nights of this research.

TABLE OF CONTENTS

Chapter Caption Page

LIST OF FIGURES

LIST OF TABLES

Table **Caption** **Page**

LIST OF PUBLICATIONS BASED ON THESIS WORK

.

1. Zaffar I. Qureshi, Baber Aslam, Athar Mohsin, Yonus Javed, "A Solution to Spoofed PS-Poll Based Denial of Service Attacks in IEEE 802.11 WLANs," presented at *ICCOM'07: The 11th WSEAS International Conference on Communications*, Vol. 11, Agios Nikolaos, Crete Island, Greece, pp. 7 –11, July 2007.

2. Zaffar I. Qureshi, Baber Aslam, Athar Mohsin, Yonus Javed, "Using Randomized Association ID to Detect and Prevent Spoofed PS-Poll Based Denial of Service Attacks in IEEE 802.11 WLANs," *WSEAS TRANSACTIONS on COMMUNICATIONS*, Issue 3, vol. 7, pp. 170–179, March 2008.

Chapter 1

INTRODUCTION

1.1 Overview

The proliferation of networking across the world continues to grow at an incredible rate. In the past decade the growth of Wireless Local Area Networks (WLAN) was even more astounding. Devices connected over wireless networks provided an opportunity to the networking world to free itself from the restrictive, inflexible and expensive web of network cables and wires. IEEE standard 802.11 [1] was first developed in 1997. After ratification in 1999 it was widely accepted as the defacto wireless standard and got its commercial name “Wireless Fidelity” or simply WiFi. This standard defines the Media Access Control (MAC) and Physical (PHY) layers for a LAN with wireless connectivity.

The rapid growth in the use of WLANs can be attributed to the prolific innovation in portable mobile devices. The complete range of devices like laptops, Personal Digital Assistants (PDA), mobile phones and sensors show a propensity towards miniaturization. With miniaturization came the issues of computing and power efficiency. In battery operated mobile devices, battery power is a scarce resource. Current wireless devices do not manage their energy usage well and thus quickly drain their batteries. A fact established from prior research was that a large part of power drain can be attributed to the wireless LAN card. Powering down the transceiver can lead to great power savings in wireless networks [2, 3]. IEEE standard 802.11 achieves power conservation by minimizing the time spent in active state and maximizing the time in sleep state. However, IEEE 802.11 accomplishes this without sacrificing connectivity. It defines a whole mechanism called Power Saving (PS) mode to allow connected stations (STA) to go into sleep mode for long periods of

time without losing information. Simultaneously, new techniques were being explored to propose even more efficient battery power conservation mechanisms [4, 5, 6].

However, the key concern with IEEE 802.11 WLANs has always been security. WLANs add an extra level of security complexity compared to their wired counterparts. Security risks in WLAN are sum of the risks of operating a wired network, new risks introduced due to portability of wireless devices and risks due to the unrestrictive nature of wireless transmission. Unintended recipients such as potential attackers can pick up wireless signals with very little expertise and amateur level effort. This can compromise the confidentiality, integrity and availability of information in a network which are the three main concerns of any security specification.

The security specifications of IEEE 802.11 known as Wired Equivalent Privacy (WEP), failed to address the issues of confidentiality, integrity and availability. The security vulnerabilities are well known [7, 8, 9]. To address these security concerns, new standards were introduced. The related standards are IEEE Standard 802.1x [10] and IEEE Standard 802.11i [11]. The IEEE 802.1x, a port-level access control protocol provides a security framework for networks, including wired and wireless both. The IEEE 802.11i standard was created for wireless specific security functions that operate with IEEE 802.1x. With these standards IEEE proposed a secure architecture called Robust Security Network Architecture (RSNA). However, even in IEEE 802.1x, design flaws were identified and it was noted that this framework too does not provide solutions to many security vulnerabilities making DOS attacks possible [12]. Although RSNA did address the issues of authentication, data confidentiality and integrity but it failed to resolve the compromise of availability which is the first causality in a DoS attack.

1.2 Problem Statement

Different modes in which devices operate within a network, present different vulnerabilities, exploiting which, the confidentiality, integrity and availability of information in a network can be compromised. Identity theft due to unprotected management and control frames, which is a persistent flaw in WEP and IEEE 802.11i, leaves a window open for attackers to launch successful DoS attacks. High rate of success of these attacks in PS mode is mainly due to two reasons. Firstly, portable mobile devices recurrently operate in PS mode to conserve their scarcest recourse i.e. battery power and secondly, at the time when the attack is being perpetrated, the legitimate user is sleeping and thus oblivious to this malicious activity on the network.

The primary objectives of enhancements introduced by IEEE appear to be confidentiality and integrity. Availability despite being the major concern of any business network was ignored, leaving many DoS vulnerabilities. As these vulnerabilities escalate in PS mode so it is important to analyze PS Mode of IEEE 802.11 wireless LAN for identity vulnerabilities and find a software / firmware upgrade solution to DoS attacks based on these vulnerabilities.

1.3 Approach

During the course of studies, WLAN was identified as the area of interest for research. IEEE 802.11 and other related standards for WLAN were studied, with special emphasis on security specifications defined in these standards. The exchange of information in PS mode of 802.11 and the transfer of different management and control frames was diligently explored. The technicalities of DoS attacks exploiting loopholes in security were understood. A detailed research of earlier efforts to identify vulnerabilities and problems in WLANs was carried out. The persisting identity vulnerabilities were focused and their exploitation by attackers was explored. Prior

attempts to solve the problem of DoS attacks in PS mode were studied in detail to understand their methodologies. Exploitation of identity vulnerabilities in PS mode of IEEE 802.11 standard was identified as the projected area for the research.

Having identified the problem area, a thorough review of standards and detailed research of prior work was done. This revealed that the niche of PS-Poll based DoS attacks had not been explored in due significance. Thereafter, solutions to this problem were constructed and the most efficient was identified. The solution was then analyzed for its viability and strength. The solution was also analyzed for its performance by simulation using MATLAB, which is a high-level technical computing language and interactive environment for simulations, algorithm development, data visualization and data analysis.

1.4 Objectives

The objective set for this research was to analyze 802.11 security specifications thereby identifying the vulnerabilities exploited by attackers to launch DoS attacks and find a viable solution. A solution that is robust, effective and simple in implementation. It should be efficient in functioning and low on computing and power resources. A solution that is implementable as a software or firmware upgrade on wireless STAs and Access Points (AP) without needing additional hardware devices.

To achieve this objective certain goals were identified which were; a detailed study of IEEE 802.11 protocol with special emphasis to its security mechanisms, extensive research on PS mode of this protocol due to its extensive usage, analysis of identity vulnerabilities causing compromise of availability of network, and proposal of a software / firmware upgrade solution for DoS attacks in PS mode of IEEE 802.11 based WLANs.

1.5 Organization of Thesis

Thesis has been organized in eight chapters. Chapter one is the introduction, covering the background of problem, problem statement, approach carried for research, objectives of research and organization of rest of the thesis. Chapter two is the literature review with a brief overview of IEEE 802.11 standard and an understanding of MAC layer functions and frame formats. In chapter three, the evolution of security is discussed, highlighting strengths and weaknesses of various security specifications of 802.11. Chapter four elaborates upon the power management functions of the protocol and the frames exchanged in PS mode.

Chapter five analyzes the identity vulnerabilities persisting in the protocol despite security enhancements and explains DoS attacks which exploit these vulnerabilities. The prior work done to solve the issue of DoS attacks in general and DoS attacks in PS mode of 802.11 based WLANs in particular is also recognized in this chapter. The proposed solution and its basic principle to solve the problem of PS-Poll based DoS attack is explained in chapter six. The implementation and validation of solution is done through simulation in chapter seven. Chapter eight concludes the thesis giving the summary of the work done including the achievements, limitations and future work.

Chapter 2

OVERVIEW OF IEEE 802.11

2.1 Introduction

An overview of IEEE 802.11 standard is given in this chapter. The two supported topologies in which the standard operates are explained. The logical architecture with relation to other IEEE 802 standards and its correlation with OSI model is recognized. The network services defined in the protocol are also discussed in this chapter. The types of frames used in the protocol and their subtypes are explained. As the research focus is manipulation of MAC frames to find an answer to the security vulnerabilities; therefore, various frames used at this layer and exploited by attackers are the highlight of this chapter.

2.2 The 802.11 Topology

The IEEE 802.11 topology consists of components interacting to provide a wireless LAN that enables mobility, transparent to higher protocol layers. An 802.11 node (AP or STA) is any device containing functionality of 802.11 protocol. Various combinations of these nodes define the topologies in which a WLAN operates. The standard supports Independent Basic Service Set (IBSS) topology and Extended Service Set (ESS) topology.

2.2.1 Ad hoc Mode – IBSS

In this topology at least two wireless STAs operate and communicate in a standalone mode with no backbone infrastructure. This type of network is often referred to as operating in a peer-to-peer mode as shown in Figure 2.1. Typically, IBSS are composed of a small number of STAs setup for a specific purpose and for a short period of time.

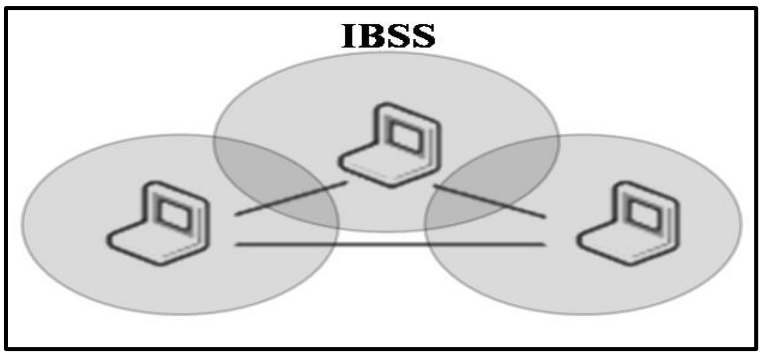


Figure 2.1: Wireless Clients in Ad hoc Mode of 802.11 (IBSS)

2.2.2 Infrastructure Mode – ESS

802.11 defines this topology to satisfy the needs of large coverage networks of arbitrary size and complexity. In this mode, another entity called AP is added to the topology through which all STAs communicate. To allow for mobility, APs of multiple BSSs are interconnected by the Distribution System (DS), which interconnects BSSs within the ESS via APs, as shown in Figure 2.2.

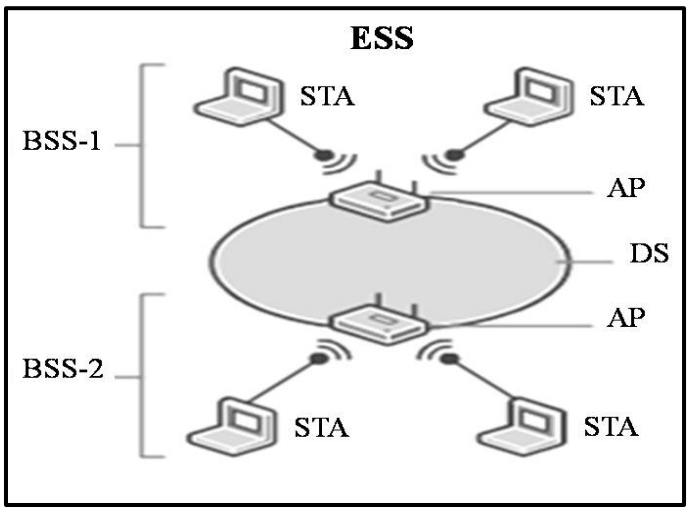


Figure 2.2: 802.11 Infrastructure Mode

2.3 Logical Architecture

The IEEE 802 Standards Committee further partitions the Data Link Layer (DLL) of OSI model into Logical Link Control (LLC) and Media Access Control (MAC) layers [13]. The MAC and PHY layers of IEEE 802 family were organized into a separate set of standards from LLC functions because of the interdependence

between access control, medium and topology. The functions of other layers of OSI model remain same for all other 802 protocols. The family of IEEE 802 standard and correlation of 802.11 to the layers of OSI model is depicted in Figure 2.3.

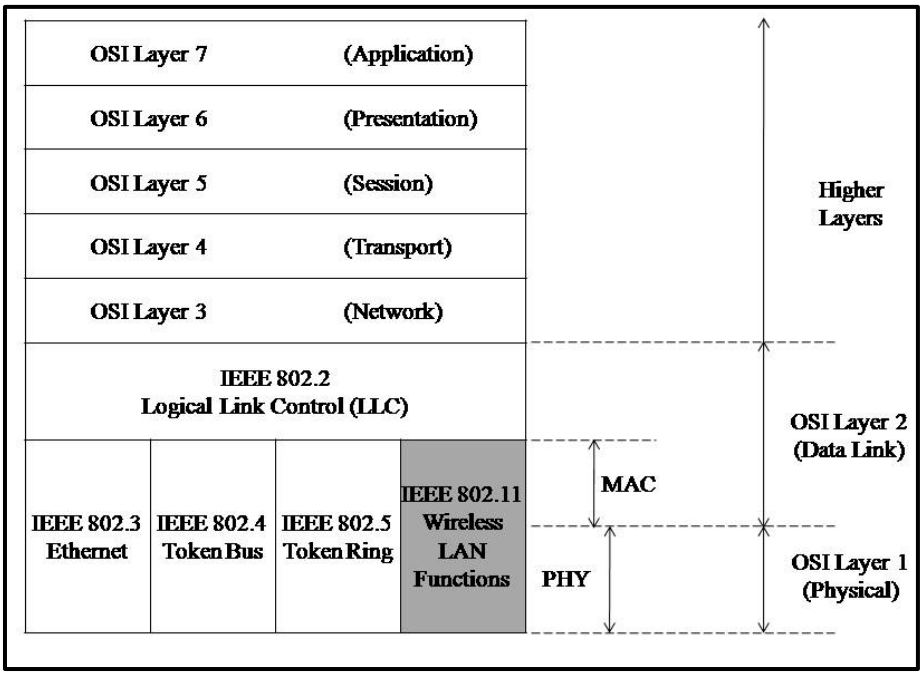


Figure 2.3: 802.11 and OSI Model

2.4 Network Services

The 802.11 standard defines services providing the functions required by LLC layer for sending MAC Service Data Units (MSDUs) between two entities on the network. These services, implemented at MAC layer, fall in the categories of STA Services and DS Services.

2.4.1 STA Services

Authentication, De-authentication, Privacy and MSDU delivery are the STA services of an 802.11network. Authentication services exercise control over LAN access and prevent unauthorized admittance. A STA operating in any mode must use the authentication service prior to establishing a connection (association) with another STA with which it will communicate. When a STA wants to disassociate from another STA, it invokes the de-authentication service. The security level of a wireless

link is seriously affected because of the unrestrictive nature of wireless medium. The standard thus offers a privacy service option based on the 802.11 WEP algorithm. As shown in Figure 2.4, this algorithm is applied to all data frames and some authentication management frames for encryption of messages.

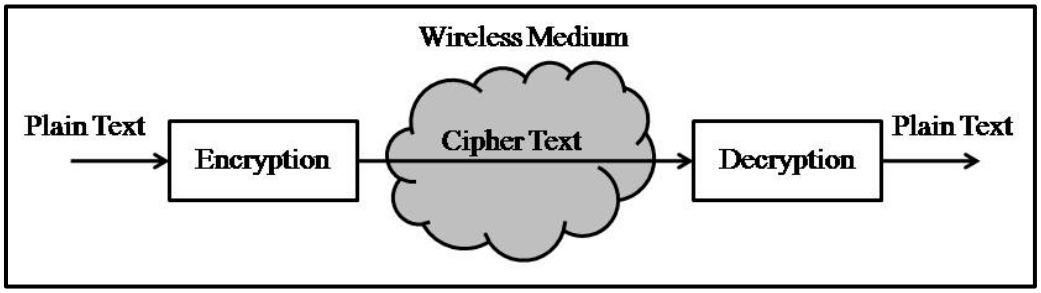


Figure 2.4: Privacy Service Through WEP Algorithm

2.4.2 DS Services

The AP provides DS services including Association, Disassociation, Distribution, Integration and Re-association. The association maps a STA to the DS via an AP and disassociation service terminates it. Each STA can associate with only a single AP, but each AP can associate with multiple STAs. Distribution service is used for sending MAC frames across a DS. The integration service enables the delivery of MAC frames through a portal[1]. The re-association service enables a STA to change its current state of association from one AP to another.

2.5 Frame Formats

In IEEE 802.11 specifications there are three main types of frames, further divided into different subtypes, according to their specific function. The Data Frames are used for data transmission. Control Frames are used to control access to the medium. Management Frames are transmitted the same way as data frames to exchange management information, but are not forwarded to upper layers. To meet the challenges posed by a wireless data link, the MAC layer of 802.11 was forced to

[1] **Portal:** A logical point from where data frames enter and exit to and from 802.11 and non-802.11 LAN. If DS has all 802-type components then Portal and AP becomes same.

adopt several unique features. Each frame consists of three basic components. A MAC header, a variable length frame body and a frame check sequence.

2.6 The MAC Header of 802.11 Frame

In contrast to the MAC header of normal Ethernet 802.3 frame that contains only the destination address, source address and type / length fields, the MAC header of 802.11 generic frame is much more complex. The comparison of both is given in Figure 2.5.

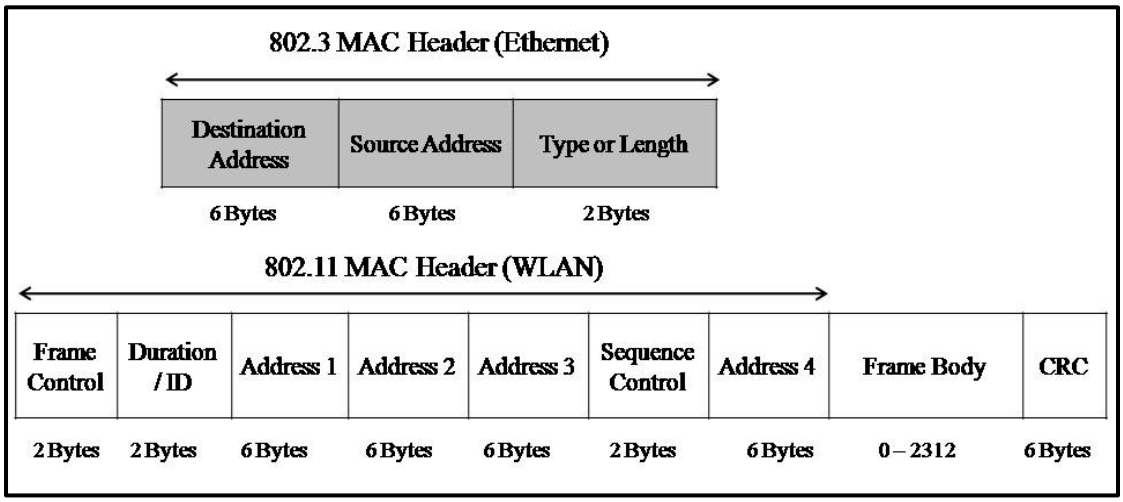


Figure 2.5: Comparison of MAC Headers: 802.3 Ethernet to 802.11 WLAN

2.6.1 Frame Control Field

The Frame Control field illustrated in Figure 2.6 carries control information exchanged between various WLAN entities. These two bytes (16 bits) contain the information required to set different parameters controlling various functions of the entity operating in WLAN.

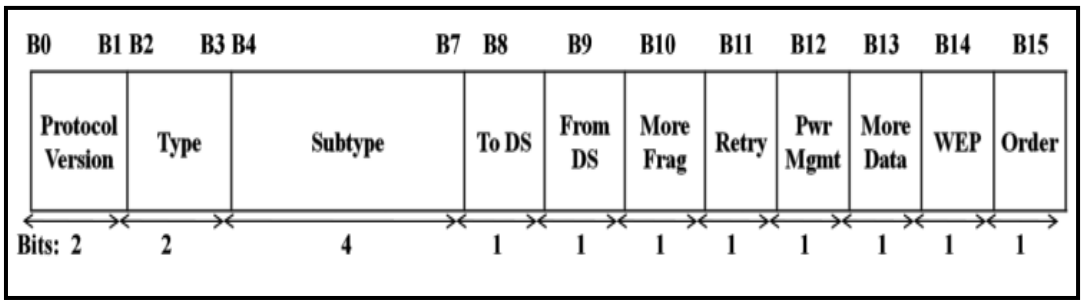


Figure 2.6: Frame Control Field

2.6.1.1 Protocol Version

This field consists of two bits, which are invariant in size and placement across all versions of 802.11 Standard. These bits will be used to recognize possible future versions. In the current version of the standard the value is fixed as “0”.

2.6.1.2 Type and Subtype

The Type field (2 bits) and Subtype field (4 bits) are used in conjunction. These 6 bits define the Type and Sub-Type of the frame. The first two bits (b2, b3) confirm the type as management, control or data frame. The remaining four bits (b4, b5, b6, b7) specify the actual purpose of the frame.

2.6.1.3 ToDS

This is a single bit field. If set to “1”, the frame is addressed to the AP for forwarding it to the Distribution System (including the case where the destination station is in the same BSS, and the AP is to relay the frame). The Bit is set to “0” in all other frames.

2.6.1.4 FromDS

The bit in this field, if set to “0” for all management frames, control frames and the data frames within an IBSS (Ad hoc mode). The bit is set to “1” for all data frames transmitted from a wireless station in an infrastructure network.

2.6.1.5 More Fragments

The bit in this field is set to “1” when there are more fragments belonging to the same frame following this current fragment. When a higher-level packet has been fragmented by the MAC, the initial fragment and any following non final fragments set this bit to “1”. Some management frames may be large enough to require fragmentation; all other frames set this bit to “0”.

2.6.1.6 Retry

From time to time, frames may be retransmitted. Any retransmitted frames set this bit to 1 to aid the receiving station in eliminating duplicate frames. The bit in the Retry field indicates that this fragment is a retransmission of a previously transmitted fragment; the receiving entity to recognize duplicate transmissions of frames that may occur when an Acknowledgment (ACK) packet is lost will use this.

2.6.1.7 Power Management

To conserve battery life, battery operated mobile devices have the ability to power down parts of the network interface. The Power Management mode of an 802.11 node is indicated by the bit in this field. This is used by STAs which are changing state either from Power Save to Active or vice versa. The MAC layer places a “1” in this field if the STA will be in sleep mode (802.11 defines this as PS mode). A “0” in this field indicates that the STA will be in full active mode. A receiving entity can use this information to adjust transmissions to avoid waking up the sleeping STA. In most cases, battery operated devices should be kept in PS mode to conserve battery power.

2.6.1.8 More Data

This bit is also used for Power Management and is used by the AP to indicate that there are more frames buffered for this STA. The STA may decide to use this information to continue polling or even changing mode to Active.

2.6.1.9 WEP

The information that the frame body is encrypted according to the WEP algorithm is indicated by setting the bit in this field. A “1” in this field is an indication that data bits have been encrypted using a Secret Key.

2.6.1.10 Order

Frames and fragments can be transmitted in order at the cost of additional processing by both the sending and receiving MACs. When the "strict ordering" delivery is employed, this bit is set to “1”. It indicates that this frame is being sent using the Strictly-Ordered Service Class 2. This tells the receiving entity that frames must be processed in order.

2.6.2 Duration / ID

This field has two meanings depending on the frame type as shown in Figure 2.7. In PS Poll messages, bits 14 and 15 are both set to “0”. Mobile stations may elect to save battery power by turning off antennas. The AP in the meanwhile keeps storing the messages addressed to the STA in PS mode.

Dozing stations must wake up periodically. To ensure that no frames are lost, stations awaking from their slumber transmit a PS-Poll frame to retrieve any buffered frames from the access point. Along with this request, waking stations incorporate the association ID (AID) that indicates which BSS they belong to. The AID is included in the PS-Poll frame and may range from 1 to 2,007. Values from 2,008 to 16,383 are reserved and not used. In all other frames this is the duration value used for the network allocation time.

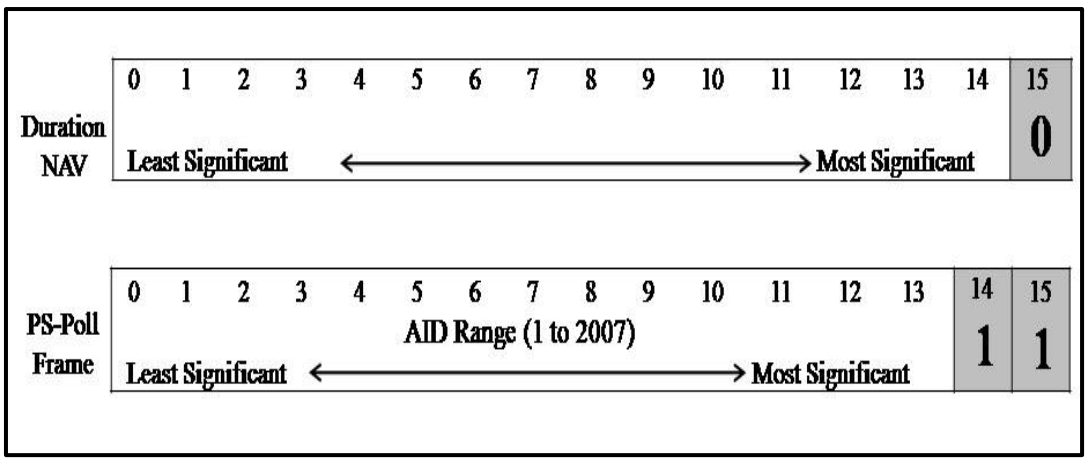


Figure 2.7: Duration / ID Field

2.6.3 Address Fields

A frame may contain up to four Addresses depending on the ToDS and FromDS bits defined in the Control Field. Table 2.1 summarizes the usage of the different addresses according to the ToDS and FromDS bits setting.

Table 2.1: Usage of Different Addresses

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	**0**	**DA**	**SA**	**BSSID**	**N/A**
0	**1**	**DA**	**BSSID**	**SA**	**N/A**
1	**0**	**BSSID**	**SA**	**DA**	**N/A**
1	**1**	**RA**	**TA**	**DA**	**SA**

2.6.4 Sequence Control

The Sequence Control Field is used to represent the order of different fragments belonging to the same frame, and to recognize packet duplications; it consists of two subfields Fragment Number, and Sequence Number, which define the frame and the number of the fragment in the frame.

2.7 Frame Body

This field has a variable length payload and carries information that pertains to the specific frame being sent. MAC management and control frames may include specific parameters in the frame body that pertain to the particular service the frame is implementing.

2.8 CRC

The MAC layer at the sending STA calculates a 32-bit Frame Check Sequence (FCS) using a Cyclic Redundancy Check (CRC) code and places the result in this field. The receiver implements a CRC to check for transmission errors in the frame.

2.9 Station States and Corresponding Frame Types

Figure 2.8 shows the states existing between a source and destination STA.

This governs which IEEE 802.11 frame types the two STAs can exchange. To keep track of STA state, each STA maintains an Authentication State, which has the values of Unauthenticated and Authenticated. The second state maintained is the Association State which as the values of Unassociated and Associated.

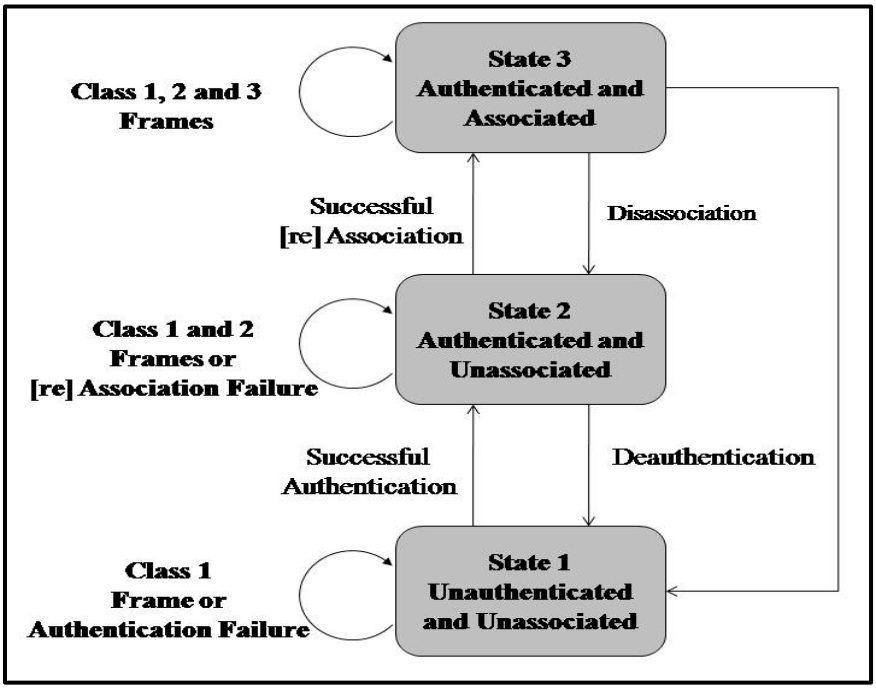


Figure 2.8: STA States and Corresponding Frames

2.10 Conclusion

In this chapter an overview of IEEE 802.11 standard has been given to build the necessary background for subsequent chapters. The logical architecture and operating modes in which wireless networks can be deployed have been discussed. The services provided in different states are also explained to build the basic understanding of the protocol. This was important because in the following chapters, these concepts will be used and referred to. The structure of frames in general and an in depth analysis of the fields in MAC header was given. The states maintained by WLAN entities in which they operate were explored. The main focus of this research work is MAC sub layer of Data link layer because it defines and controls the security services provided by IEEE 802.11.

Chapter 3

EVOLUTION OF SECURITY

3.1 Introduction

A wired network can be secured at its edges by restricting physical access and installing firewalls. A wireless network with the same measures in place is still vulnerable to eavesdropping. This chapter presents a few basic concepts of communications security, and then describes the three main generations of security specifications in 802.11 WLANs. Different security features of these specifications have been explained followed by their flaws / shortcoming which lead to amendments / enhancements in the standard from time to time. Open issues and vulnerabilities in existing final standard are also highlighted.

3.2 Security Requirements

The security requirements or level of security for wireless networks are important for determining which security protocols to employ. Specific wireless network applications may require only a few security features against casual intruders, while some may require elaborate security defenses against determined and capable adversaries. Important security operational parameters include authentication, confidentiality, integrity and availability.

3.2.1 Authentication

Authentication enables a node to ensure the identity of peer node with which it is communicating. Without authentication, an adversary could act as a legitimate node, thus gaining unauthorized access to resources and sensitive information. Key management protocols are usually applied when an authentication procedure is necessary. In addition, some security protocols use authorization as well as authentication.

3.2.2 Confidentiality

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies / adversaries could have devastating consequences. To protect information from unauthorized disclosure, encryption is usually used.

3.2.3 Integrity

Integrity, or soundness, guarantees that a message being transferred is never corrupted, or if it is, that it can be identified as being corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network. Information that needs to be constant or information that must only be modified by a certain authorized set of users must have the guarantee that it will not be modified by an unauthorized user. This can be accomplished through the use of cryptographic hashes or message digests.

3.2.4 Availability

A commonly overlooked aspect of security is availability. While most people know that authentication and encryption are vital for security of a service or network; availability an equally important pillar of security is usually ignored. Every service is useless if someone can disrupt its operation. The criterion of availability ensures the survivability of network services despite DoS attacks.

3.3 IEEE 802.11 Security Specifications

Due to RF signal nature of wireless network, it is very difficult to keep a control on devices which are receiving the wireless network signals, thereby making 802.11 based networks an attractive target for potential attackers. In order to provide security equivalent to its predecessor, i.e. wired network, Wired Equivalent Privacy

(WEP) security standard was specified in the original 802.11 standard. Subsequent research demonstrated some basic flaws in 802.11 encryption mechanisms and authentication protocols. This led to extensive research in this domain, resulting in creation of a series of protocol extensions and replacements.

3.4 Wired Equivalent Privacy — WEP

When the first IEEE 802.11 WLAN standards were being developed, the designers faced many trade-offs. Though they recognized the need for enhanced security, they also wanted the products based on the new standard to be exportable from the United States. As due to restrictions, strong encryption would have prevented 802.11 WLAN equipment from being granted export licenses; therefore, designers settled on a very modest and optional authentication method and encryption scheme called WEP [14].

3.4.1 Specifications

Key management in WEP environment is not defined in [1], so it was left up to vendors. The simplest scheme is to distribute the keys manually. It is assumed that the user has the correct secret key “k” to access the network.

When a station wants to send a frame, it first computes the Integrity Check Value (ICV) over the plaintext data, and adds it to the end of the plaintext data. It then generates an Initialization vector (IV), then concatenates the key with IV and uses this as input for the Rivest’s Cipher 4 (RC4) [15]. The RC4 function outputs an arbitrary long key stream, which is then XOR-ed with the data portion of the frame and the CRC checksum. As the IV is different for each frame sent, therefore each frame is encrypted with a different key. The IV is then appended to this encrypted data and sent. The IV is viewable by anyone, as it is not encrypted so that the receiver knows which IV to use when decrypting. The process is illustrated stepwise in Figure 3.1 and

Table 3.1 provides a summary of the various parameters used in the WEP encryption.

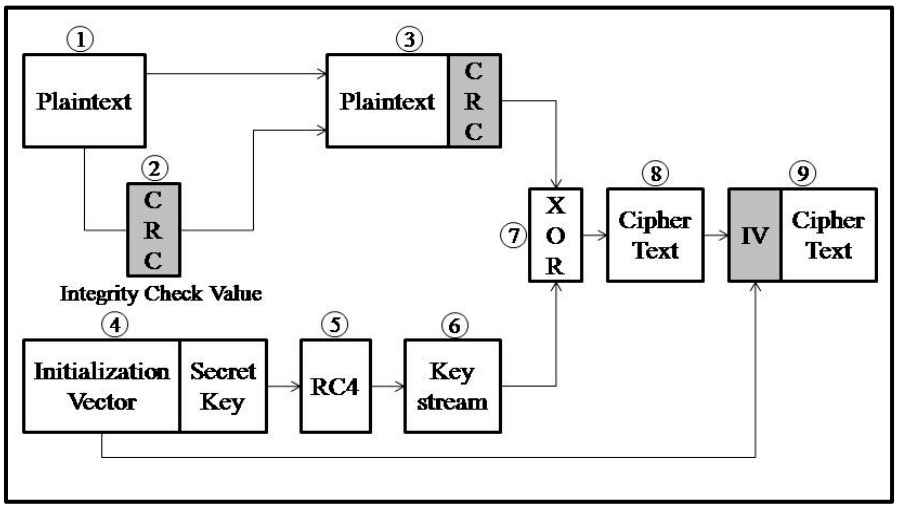


Figure 3.1: WEP Encryption Process

Table 3.1: Parameters used in WEP

PARAMETER	PROPERTIES
Secret key, k	40 bits (used in early versions of WEP) 104 bits (current standard)
Initialization Vector, IV	24 bits
Integrity Checksum	32 bit CRC
Encryption Algorithm	RC4 Stream Cipher

3.4.2 Vulnerabilities of WEP

It was not long before the inherent weaknesses of WEP were noted, analyzed, exploited, and the results published. WEP combines its 40 / 104-bit key with 24-bit Initialization Vector (IV). Small IV space, regardless of key length, opens vulnerability of IV reuse [16, 17]. Moreover, WEP has no protection against weak keys, which can be used to recover secret key [18], this vulnerability was demonstrated and successfully exploited to break the WEP key [19].

Attack tools such as Airsnort [20], Aircrack [21] and WepLab [22] use these vulnerabilities to crack WEP keys. Further, CRC is a linear function that can be used for error detection but not for data integrity [23, 24, 25]. Authentication also has its flaws; Open System Authentication is in essence no authentication and Shared Key

Authentication uses challenge / response system that rests on the knowledge of secret shared key. Both the challenge (plain text) and response (encrypted challenge) are sent in clear management frames, which can easily be exploited for finding key stream [7].

Besides these vulnerabilities, many management and control frames are neither encrypted nor authenticated. So an attacker can spoof the MAC address of a legitimate user / node and request services on its behalf. The worst are DoS attacks based on spoofed PS-Poll, disassociation and de-authentication messages. DoS attack tools such as Airjack [26], KisMAC [27], Void11 [28] exploit this vulnerability.

3.5 Wi-Fi Protected Access — WPA

In order to rectify the security issues in WEP, Task Group-I was formed to develop 802.11i. But due to delays in finalization of standard, Wi-Fi Alliance[2] introduced its interim security specifications known as WPA. The specification was designed to overcome WEP flaws using only software or firmware upgrades in existing hardware.

3.5.1 Specifications

WPA introduces Temporal Key Integrity Protocol (TKIP) for confidentiality, Message Integrity Code (MIC) for data integrity and Pre Shared Key (PSK) / IEEE 802.1x for authentication and key management. TKIP increases the IV size to 48 bits, uses TKIP Sequence Counter (TSC) for key freshness and two-stage key mixing to eliminate weak keys [29]. MIC uses MAC addresses, MIC keys and TSC to generate integrity code [30]. 802.1x [9] is a port based network access control protocol using Extensible Authentication Protocol (EAP) [31] as transport protocol for authentication.

[2] http://www.wi-fi.org. The Wi-Fi Alliance is a non-profit organization, certifying wireless products for interoperability.

3.5.1.1 IEEE 802.1x

The IEEE 802.1x is a port based protocol that provides authentication and authorization for both wired and wireless networks. It was included in the 802.11 standard to remedy the weaknesses in the authentication processes used in WEP. 802.1x defines three entities in the authentication process. *Supplicant* - entity that wants to join a network i.e. a wireless client, *Authenticator* - entity that controls access to the network (in the case of WLANs, this refers to an AP) and *Authentication server* - entity that makes the authorization decisions.

3.5.1.2 Extensible Authentication Protocol – EAP

802.1x is intended to provide strong authentication, access control and key management control, which is not provided in WEP. 802.1x is based on EAP over Local Area Networks (EAPOL). This provides communications and message exchanges between different parties in the authentication process. EAP does not specify the type of underlying authentication method, so any method can be used.

In the authentication sequence using EAP, supplicant sends an EAP-Start message to the authenticator. The authenticator responds with an EAP Request Identity message to determine the identity of the supplicant. The supplicant follows up by sending its identity information using the EAP Response Identity message which is forwarded by the authenticator to the authentication server. The authentication server initiates a series of challenges to the supplicant, which provides responses to each challenge. The authentication server checks them and returns a Success message to the authenticator if the responses are correct. On receiving the Success message from the authentication server, the authenticator grants access to the supplicant. Most current applications use the EAP-TLS (EAP Tunneled Layer Security) method for authentication with an authentication server. EAP-TLS uses a

certificate-based mechanism to perform mutual authentication and key exchange, and is generally considered to be the strongest EAP method [32].

3.5.1.3 Temporal Key Integrity Protocol – TKIP

TKIP is designed to address WEP's weaknesses in data encryption. The current WEP implementation uses a static shared secret key together with a short (24 bit) initialization vector to generate the encryption key stream using the RC4 algorithm. TKIP continues to use the RC4 algorithm for data packet encryption; however, unlike WEP, TKIP uses a temporal key that is changed every 10000 packets. A longer 48 bit initialization vector is also adopted to prevent the reuse of initialization vectors over the life-time of a temporal key. These measures make it much more difficult to break TKIP key, using existing WEP-breaking techniques.

3.5.1.4 Michael Message Integrity Check – MIC

The Michael Message Integrity Check (MIC) is intended to provide protection to data in transit against unauthorized modifications or tampering. The Michael algorithm uses a cryptographic digest of the original message as an integrity checksum. This protects the integrity of data packets on the wireless networks, since any attempt to modify packets will be detected.

3.5.2 Vulnerabilities of WPA

WPA also failed in providing desired security. PSK authentication suffers from key management problem for large networks. Selection of a strong PSK is also very important. Weak PSK can easily be broken using cracking tools like coWPAtty [33]. IEEE 802.1x also has vulnerabilities to various attacks like Man-in-the-middle-attack [12]. Weaknesses in temporal key hash lead to calculation of all keys by compromise of just two or more keys [34]. Besides these WPA is still vulnerable to DoS attacks because of unauthenticated management and control frames [12].

3.6 IEEE 802.11i – WPA2

IEEE 802.11i [11] was ratified in 2004 to rectify the security issues of WEP and WPA. IEEE 802.11i is a Layer 2 specification that focuses on strengthening IEEE 802.11 security at the MAC sublayer. IEEE 802.11i goes beyond the simple and flawed encryption mechanism of WEP, to include specifications on encryption, authentication and key management in a multilayered approach to security.

3.6.1 Specifications

Besides algorithms of WPA, IEEE 802.11i uses Advanced Encryption Standard (AES) [35] in Counter (CTR) Mode for confidentiality and AES in Cipher Block Chaining Message Authentication Code (CBC-MAC) mode for message integrity. Resulting protocol is known as Counter Mode with CBC-MAC (CCMP).

CCMP is the encryption technique in the 802.11i standard. It employs the AES algorithm using the CCM mode of operation. CCM utilizes the Counter (CTR) mode for data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to ensure message authenticity and integrity. CCMP uses the CTR mode in AES to encrypt data for transmission. The basic mechanism for AES CTR mode encryption is shown in Figure 3.2.

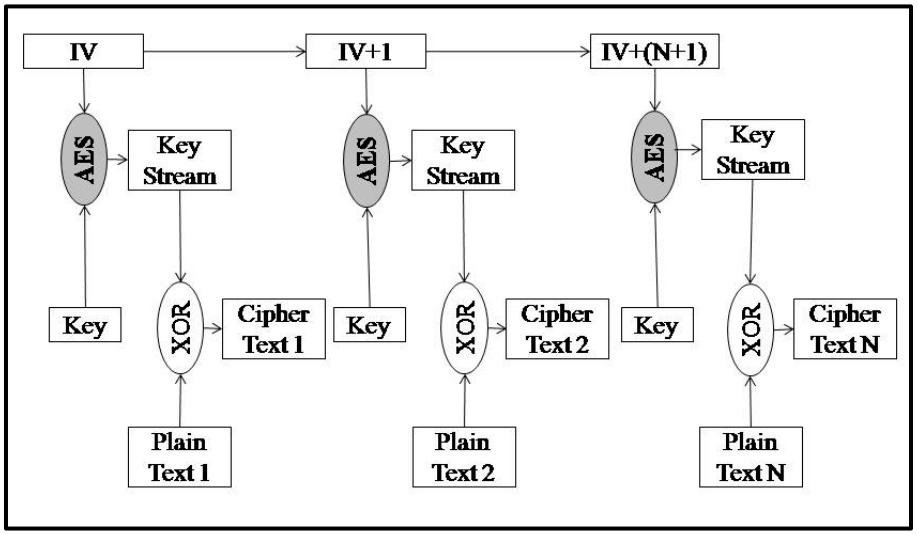


Figure 3.2: AES CTR Mode Encryption Process

A 128 bit temporal key “k” together with a 48 bit IV is used to generate a one-time pad using the AES algorithm “E”. The IV is incremented after generating each one-time pad. A logical XOR operation is then performed with the message plaintext and the corresponding one-time pad.

To provide data integrity, a message integrity check (MIC) is generated for each message packet using CBC-MAC. This is illustrated in Figure 3.3. The MIC is computed over the payload and the header, and the resulting MIC is appended. Encryption is then applied over the payload and the MIC, while the header is sent in the clear. Since the header is included in the computation of the MIC, any unauthorized modification or corruption of the header will also be detected.

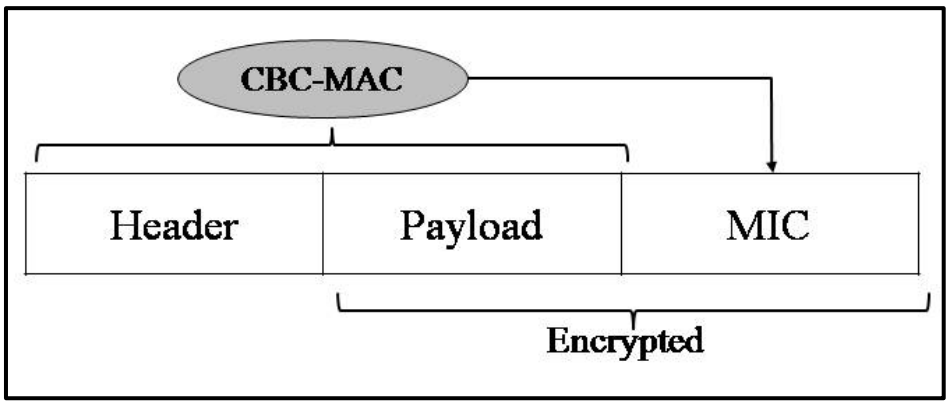


Figure 3.3: Message Integrity Check Using CBC-MAC

3.6.2 Vulnerabilities of WPA2

802.11i being a well designed standard for authentication, data confidentiality and integrity, may provide satisfactory mutual authentication and key management, but is still not the ultimate security solution for WLANs. Since the 802.11i design does not emphasize availability, several DoS attacks are possible. The vulnerabilities have been studied in detail and published [36]. The vulnerability of unprotected management and control frames leaves a window open for experienced attackers to launch successful DoS attacks [37, 38].

IEEE also acknowledges this weakness and is in the process of developing a solution to the persisting vulnerabilities due to unprotected management and control frames in IEEE 802.11i. However, the standard 802.11w [39] is still under development as new proposals and recommendations are being incorporated. It is not expected to be ratified before mid 2009.

A summary of wireless network security methods is given in Table 3.2.

Table 3.2: Summary of Wireless Network Security Methods

	WEP	**802.11i Methods**	
		WPA	**WPA2**
Security Protocol	WEP	TKIP	CCMP
Cipher	RC4	RC4	AES
Key Length	40 or 104 bits	128 bits encryption, 64 bits authentication	128bits
Key Life	24 bit IV	48 bit IV	
Key Generation	Concatenation	Two phase mixing function	Not needed
Data Integrity	CRC-32	Michael	CBC-MAC
Header Integrity	None	Michael	CBC-MAC
Replay Protection	None	Packet Number	
Key Management	None	EAP-based	
Authentication	Open or Shared Key	802.1x or Pre-Shared Key (PSK)	

3.7 Conclusion

IEEE 802.11 is the defacto WLAN standard. It was designed to provide security however it failed to do so. As a result amendments / enhancements were, and are still being made to overcome the flaws by first introducing Wi-Fi Protected Access (WPA) and then IEEE 802.11i. But both these enhancements failed to achieve the desired objectives especially availability. In this chapter, the evolution of security has been discussed in detail highlighting the flaws at each stage.

Chapter 4

POWER MANAGEMENT IN IEEE 802.11

4.1 Introduction

Wireless LANs are typically related to mobile applications, in which, battery power is a scare resource. In this chapter, the elements entailing power consumption in communicating devices are factorized. Power saving techniques defined in various wireless networking standards are also explored. As the research culminates on proposing a solution which addresses vulnerabilities in PS mode of 802.11, so the PS mechanism [40] of IEEE 802.11 is explained by elaborating on the messages / frames exchanged in this mode.

4.2 Elements of Power Consumption

The power consumed by a communicating device can be factored into seven elements contributing towards the drainage of power. First the *Transmission*, which accounts for the energy spent in data packet transmission. Second the *Reception*, accounting for the energy spent by a node in data reception. Third the *Idle Listening*, referring to the power consumed when the radio of the node is waiting to receive potential packets but the media is idle. Fourth is the *Overhearing*, which refers to the power used by a node when it is receiving packets on the media meant for another destination. Fifth factor is the *Control Overhead*, which accounts for the power used to send and receive control packets. *Reliability*, the sixth element pertains to energy consumed in meeting the protocol reliability requirement, i.e., data retransmissions because of bad media, collisions and mobility. *Turnaround Time*, the seventh factor is the time required to switch modes from transmit to receive and vice versa.

4.3 Power Saving Techniques

As the use of wireless LAN grew, innovation in handheld mobile devices

escalated. The devices manufactured focused on light weight and smart design. The heaviest part of a mobile device is its battery. In order to strike a balance between the otherwise inversely proportional factors of smaller batteries and longevity of operation, several power saving techniques [41, 42, 43] were explored and proposed. These techniques, by proposing different combinations of the factors mentioned in the preceding paragraph, strive to minimize the energy consumed by a wireless device. A few of these techniques are summarized in the subsequent paragraphs.

4.3.1 Transmission Power Control — TPC

High transmission power increases the network connectivity. It decreases the signaling overhead needed for route maintenance in high mobility. It however consumes more power and generates interference on the shared radio media. On the other hand low power transmission conserves power and reduces interference but generates high signaling overhead. TPC is most useful in dense networks for efficient media usage while minimizing interference and conserving battery power. Different techniques have been implemented at different layers for TPC [44, 45, 46, 47, 48]

4.3.2 Reduced Control Overhead

Reducing the number of control messages without incurring substantial loss in link quality or accessibility can improve power efficiency. The number of control messages can be reduced both by reducing the control signaling for handshake and controlling the packet flooding in the network [49].

4.3.3 Sleep Awake Mechanism

An 802.11 LAN card consumes 1.65W, 1.4W, 1.15W and 0.045W in transmit, receive, idle and sleep states respectively [50]. Hence maximum power is saved when a device is in sleep mode. It is, therefore, desirable that a wireless device, when not actively communicating, remains in sleep mode also called the PS mode [5].

The challenge lies in estimating when the other devices may have data to send to it and waking up at the right time. If the estimate is poor then it will cause delay, buffer overflows and loss of power on other devices which are trying to reach it. Tseng et al in [44] describes three different 802.11 based schemes depending upon mobility level.

4.4 Power Saving in 802.11

It is an established fact that power save mode or doze state is the most effective way to save power. It is thus desirable that the battery operated mobile devices stay in this state as long as possible without degradation in its functionality and quality of service. The time spent in doze state can be increased by minimizing the frequency of the wakeups and reducing the wake up period.

4.4.1 The 802.11 Power States

IEEE 802.11 has two power management modes i.e. the active mode and the PS mode [13]. In the active mode, a STA is fully powered and can send and receive frames. In the PS mode, STA can be in one of two states; the sleep state and the awake state. Most of the time, a STA in PS mode remains in sleep state, it only gets into awake state to listen to management frames called beacons transmitted by AP. In this mode, a STA consumes very low power [3] vis-à-vis the active mode. When a STA is in PS mode, the AP buffers all the frames that are directed to that STA.

4.4.2 Power Saving Mechanism

To enter the PS mode, a STA must first inform AP. A frame with a PS request is sent from STA to AP following the basic medium access procedure [1]. A reply should be sent by AP and received by STA before it can enter PS mode. Once the request reply exchange is successful, the STA goes in sleep state of PS mode and operates with very little power consumption. AP buffers all the frames addressed to this STA as shown in Figure 4.1. In case of unsuccessful exchange of request / reply

message, the STA will remain in active mode and retransmit the request to the AP.

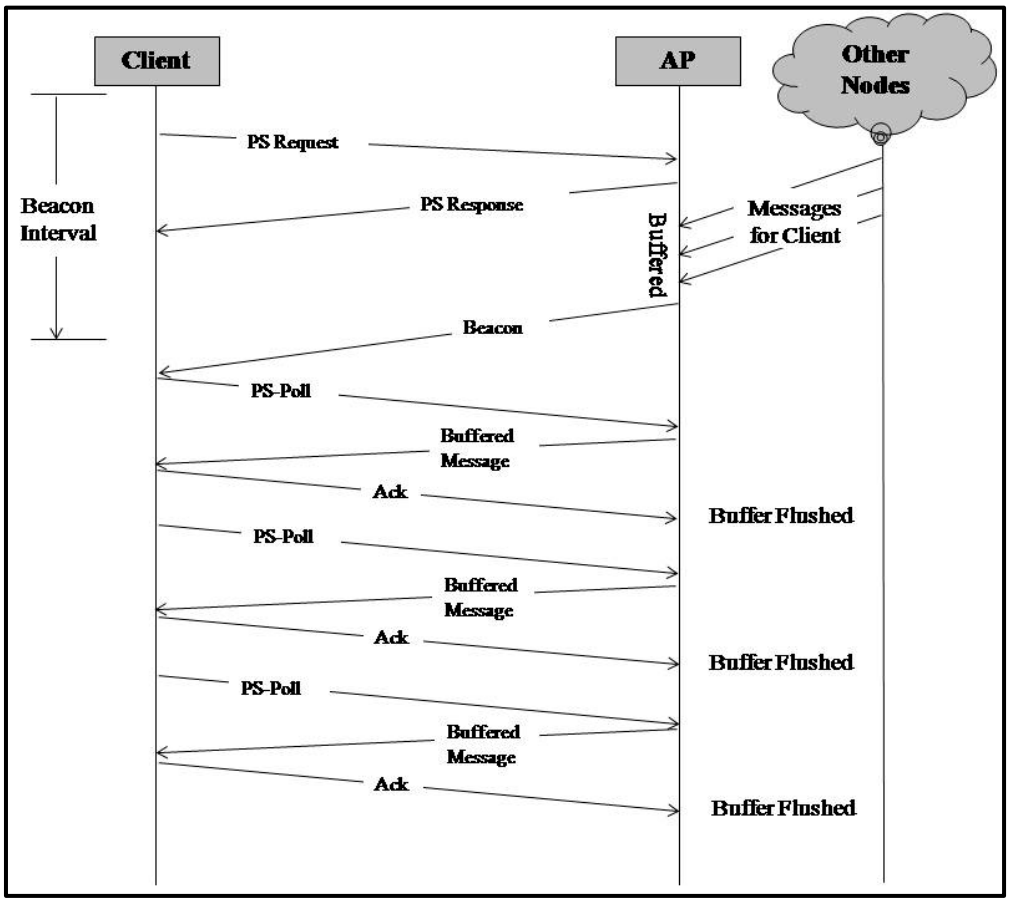
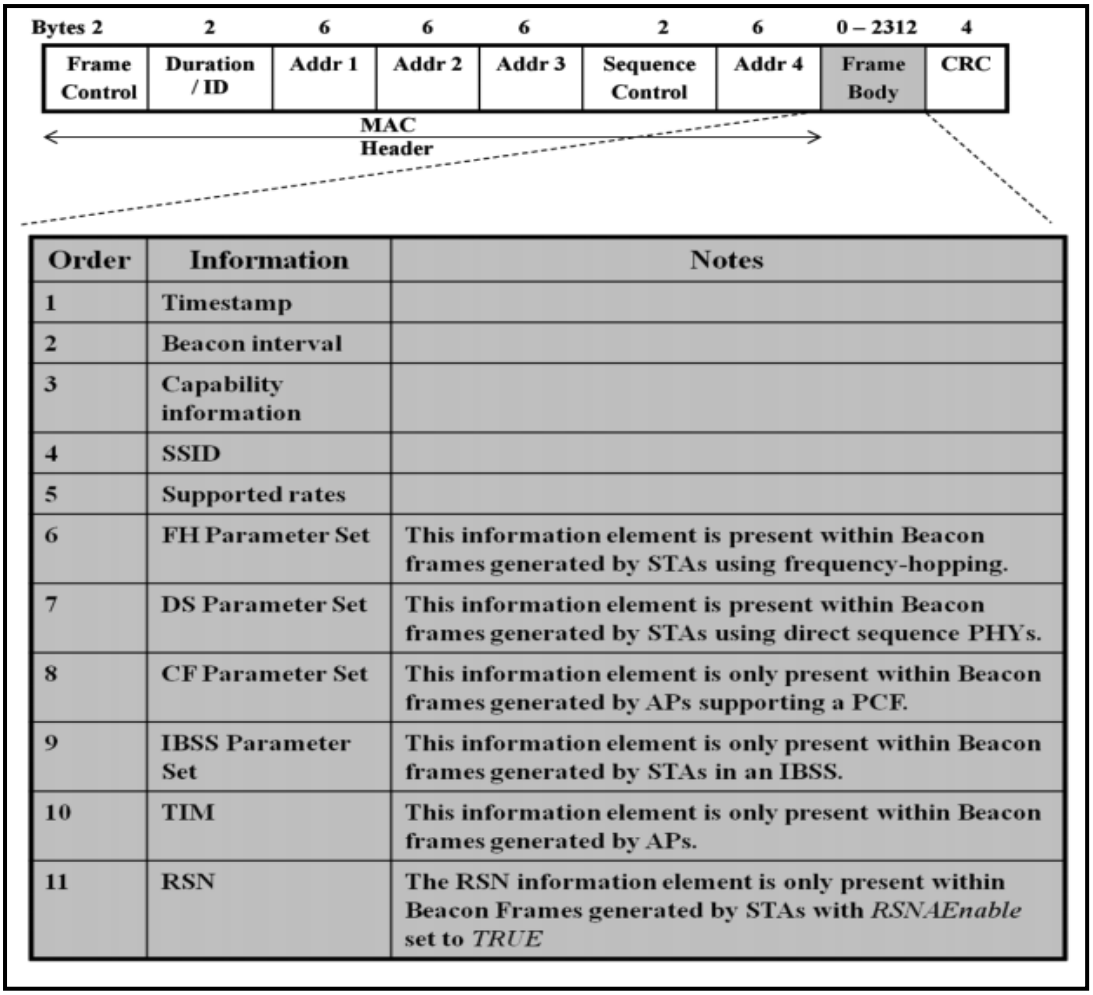


Figure 4.1: PS Mode

Multicasts and Broadcasts are also stored by the AP, and transmitted at a pre-known time (each DTIM), where all Power Saving STAs who wish to receive this kind of frames should be awake. To broadcast information required for synchronized operation of WLAN, the AP transmits beacon frames, as shown in Figure 4.2. To read this information STAs periodically change their state to awake on predefined intervals specified in "Beacon Interval" field of a beacon. Another piece of information contained in beacon is the Traffic Indication Map (TIM). TIM is composed of 2,008 bits. Each bit corresponds to a particular AID, if set, it indicates whether any frames directed to the indicated STA are pending in the AP. To receive a beacon, STA awakes after pre-decided number of beacon intervals. If there is an indication of pending unicast frames, STA can choose to receive those frames at its convenience.



Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	This information element is present within Beacon frames generated by STAs using frequency-hopping.
7	DS Parameter Set	This information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	This information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	This information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	This information element is only present within Beacon frames generated by APs.
11	RSN	The RSN information element is only present within Beacon Frames generated by STAs with *RSNAEnable* set to *TRUE*

Figure 4.2: Management Frame (Beacon)

To receive a unicast frame, the STA sends out a PS-Poll to the AP, this signals that the STA is ready to receive a frame. After the reception of PS-Poll, the AP forwards a pending frame to the STA. The “More Data” field can be set in the data frame to indicate further pending frames buffered at AP. Broadcast / multicast frames are sent without any PS-Poll message so STAs in PS mode cannot choose when to receive them, but can choose to ignore these frames. After successful reception of data frames, the STA can either go back to sleep state or choose to receive more frames by sending out another PS-Poll. If no more frames are buffered in the AP, then the STA will go back to the sleep state.

If a mobile STA switches to the active mode from a sleeping state, frames

can be transmitted without waiting for a PS-Poll. PS-Poll frames indicate that a STA in PS mode has temporarily switched to an active mode and is ready to receive buffered frames, even without receiving explicit notification.

4.5 MAC Header of PS-Poll Message

The format of the PS-Poll frame is shown in Figure 4.3. The Frame Control field and Frame Check Sequence (FCS) field have standard settings, as defined in [1].The MAC header comprising of four fields is explained in the list below.

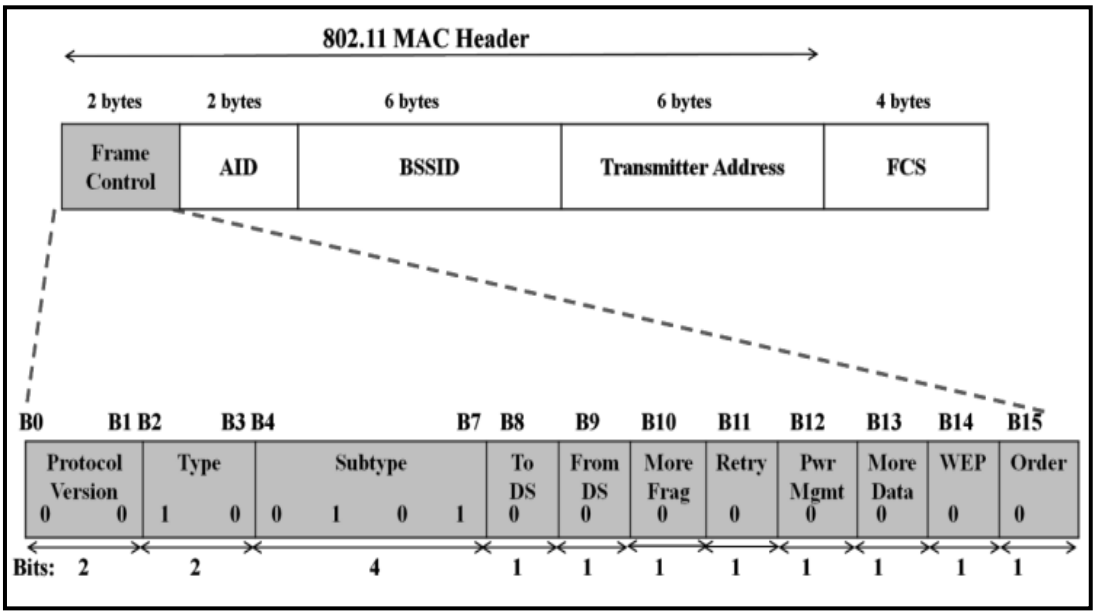


Figure 4.3: PS-Poll frame

4.5.1 Frame Control

This field has the standard settings of a control type frame as explained in Chapter 3. The frame type is set to “01” to indicate a control frame and the subtype is set to “1010” to indicate a PS-Poll frame. Rest all the bits are set to “0”.

4.5.2 Association ID – AID

Instead of a Duration field, PS-Poll frame uses the third and fourth bytes in the MAC header for the Association ID. This is a 16 bit numeric value (from the range 1-2,007) assigned by the AP to identify the association. Including this ID in the frame allows AP to find any frames buffered for the now awakened slumbering STA.

4.5.3 BSSID and Transmitter Address

This field contains the BSSID of the BSS created by the AP that the sender is currently associated with and the transmitter address is the address of the sender of PS-Poll frame.

4.6 AID Field in PS-Poll Frame

AID field as in Figure 4.4 represents the 16 bit ID of a STA allotted at the time of association. Its value is in the range 1–2007 (values from 2,008-16,383 are reserved and not used), placed in the 14 Least Significant Bits (LSB) of the AID field. Each of the two Most Significant Bit (MSB) is always set to “1”. The remaining 14 bit number in LSB is a sequential counter, incremented by one for each AID generated for every associating STA.

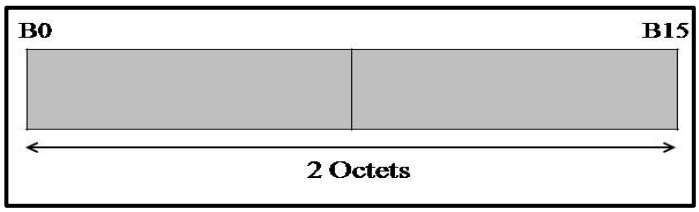


Figure 4.4: AID Field

4.7 Conclusion

Best power conservation strategy for a battery operated mobile device is to switch it off. However, to keep communicating and conserve power, different operating states have been defined in wireless environment. IEEE 802.11 defines a complete mechanism to conserve battery power without compromising availability. This chapter highlights the importance of PS mode of IEEE 802.11 standard by showing how communicating mobile devices save their scarcest resource. As such devices operate in power saving mode for most of their time so the need to secure this mode from identity vulnerabilities is highlighted. It builds the necessary background for subsequent chapter explaining the vulnerabilities presented by PS mode of 802.11.

Chapter 5

DOS ATTACKS AND PRIOR WORK

5.1 Introduction

A thorough analysis of vulnerabilities existing in the security specifications of evolving IEEE standards presented in chapter 3 paved the way to discuss the attacks on the persisting identity vulnerabilities. This chapter starts with an overview of various attacks / activities performed on WLANs with malicious intent. Various DoS attacks exploiting the identity vulnerabilities in WLANs are discussed. DoS attacks in PS mode being the focal point of this research are covered in detail with prime focus on PS-Poll based DoS attack. The chapter ends with a detailed survey / analysis of prior work on different solutions proposed for identity vulnerabilities.

5.2 Hacking Techniques

The mushroom growth of 802.11 networks invited the attention of people, who enjoy the intellectual challenge of creatively overcoming or circumventing limitations called *hackers* [51]. Programming enthusiasts started exploring the use of techniques, methods, analyses and uses in ways unintended by the designers of IEEE 802.11. The problem arose when certain hackers, called *attackers,* started using these techniques with malicious intentions.

5.2.1 Wireless Network Sniffing

Using the common cryptographic naming conventions; *Sniffing* is the act by Eve of making copies of a network packet sent by Alice intended to be received by Bob. Ironically it also is the underlying technique used in tools that monitor the health of a network.

5.2.1.1 Passive Scanning

Scanning is the act of sniffing by tuning to various radio channels. A passive

network scanner has a wireless card which permits reading of all raw 802.11 frames being transmitted without revealing the presence of the scanner. A station in monitor mode can capture packets without associating with an AP.

5.2.1.2 Detection of SSID by Sniffing

The management frames travel unprotected on the network. The attacker can discover the SSID of a network usually by passive scanning because the SSID is included in management frames like Beacons, Probes and Association which are neither encrypted nor authenticated.

5.2.1.3 Collecting the MAC Addresses

With packet-sniffers for wireless networks available for free, coupled with the fact that MAC addresses are sent in clear, it takes little effort from an adventurous attacker to sniff out legitimate MAC addresses. As the source and destination MAC addresses are always in the clear in all 802.11 frames so the attacker gathers legitimate MAC addresses for later use in constructing spoofed frames.

5.2.1.4 Collecting the Data Frames

The attacker sniffs a large number of frames from a single BSS. Although the frames are encrypted but given a sufficient number of mathematically weak frames, the systematic computation can expose useful information out of encrypted frames.

5.2.2 Wireless Spoofing

There are well-known attack techniques known as spoofing in both wired and wireless networks. After collecting information through sniffing, the attacker can construct frames by filling selected fields that contain addresses or identifiers with legitimate looking but non-existent values, or with values that belong to others. This activity is called spoofing.

5.2.2.1 MAC Address Spoofing

The attacker generally desires to be hidden. Therefore, the attacker fills the sender MAC Address field of the injected frames with a sniffed value so that his equipment is not identified. Many MAC spoofing tools and techniques such as *SpoofMAC* [52] and *SMAC* [53] are available which assist attackers in this activity. Changing the MAC address of a wireless card is also a very trivial task that can be performed even by novice attackers, using softwares such as *Technitium MAC Address Changer* [54] and *MAC-Changer* [55]. With spoofed MAC address a malicious user could exploit the network and launch DoS attacks.

5.2.2.2 Frame Spoofing

The attacker can inject frames that conform to 802.11 specifications, but whose content is carefully spoofed as described above. Frames themselves are not authenticated in 802.11 networks. So when a frame has a source address, spoofed to match a valid address it cannot be detected. If the frame to be spoofed is a management or control frame, then there is even no encryption to deal with.

5.2.3 Wireless Network Probing

Even though the attacker gathers considerable amount of information regarding a wireless network through sniffing without revealing his wireless presence at all, there are pieces that may still be missing. The attacker then sends artificially constructed packets to a target that trigger useful responses. This activity is known as probing or active scanning.

5.2.3.1 Detection of SSID by Probing

Detection of SSID is often possible by simply sniffing Beacon frames as describe in a previous section. If the attacker does not want to wait for a Beacon, he can assemble a Probe Request frame counterfeited with a spoofed source MAC

address. The AP, thinking it to be a request from a legitimate node sends the Probe Response frame which contains, in the clear, the SSID. The attacker can then sniff these Probe Responses and extracts the SSIDs. Incase the attacker does not want to take a chance with the AP; he will find out a STA associated with the AP, and send the STA a forged Disassociation frame where the source MAC address is set to that of the AP. The station will then send a Re-association Request that exposes the SSID.

5.2.3.2 Detection of APs and STAs

Every AP is a station, so SSIDs and MAC addresses are gathered as described above. Certain bits in the frames identify that the frame is from an AP so on identifying the source of information, intelligent probing can enable attackers to gather valuable information from all the entities in a network.

5.3 Identity Vulnerabilities in 802.11

A study of persisting flaws in 802.11 security enhancements in chapter 3 and a brief look on the hacking tools and techniques in the preceding section revel that a WLAN, even conforming to the highest level of IEEE security specifications is still susceptible to various attacks. Sniffing and subsequently spoofing the identity of a legitimate node enables an attacker to impersonate himself as a legitimate user.

As IEEE 802.11 networks place an implicit trust in a speaker's source address so, for most management and control messages, the 802.11 networks do not include any mechanism for verifying the correctness of the self-reported identity. Therefore after an identity theft, the attacker now is at liberty to act as a legitimate user and keep requesting MAC-layer services. Enthusiastic attackers go a step further and bring the whole network down by repeatedly sending spoofed messages to consume network resources thereby denying normal network activity to legitimate users. Thus the term Denial of Service was coined.

5.4 DoS Attacks

A denial of service occurs when a system is not providing services to authorized clients because of resource exhaustion by unauthorized clients. The relative formidability of various risks was given in a survey which yielded viruses and DoS as the top two contenders respectively [56], as shown in Figure 5.1.

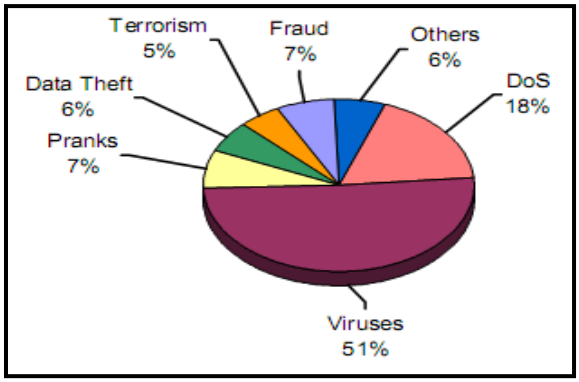


Figure 5.1: Probability of Digital Attacks (A Survey)

5.5 DoS Attacks in 802.11

While the security flaws in 802.11's basic confidentially mechanisms have been extensively publicized, the threats to network availability are far less widely appreciated. However, it has been suggested that 802.11 is highly susceptible to malicious DoS attacks targeting its management and media access protocols [57]. In wireless networks, DoS attacks are difficult to prevent, difficult to stop an on-going attack and the victim and its clients may not even detect the attacks.

5.5.1 De-authentication DoS Attack

After an 802.11 client has selected an AP, it must first authenticate itself before further communication may commence. Moreover, part of the authentication framework is a message that allows STAs and APs to explicitly request de-authentication from one another. This message itself is not authenticated using any keying material. Consequently the attacker may spoof it, either pretending to be the AP or the STA, and direct it to the other party. In response, the AP or STA will exit

the authenticated state and will refuse all further packets until authentication is reestablished. By repeating the attack persistently a STA may be kept from transmitting or receiving data indefinitely and an AP constantly busy in responding to authentication requests. DoS tool kits for example *Airjack* [58] are available which send spoofed de-authentication frames to an AP with inappropriate authentication algorithm and status codes. AP then drops connections with stations.

5.5.2 Disassociation DoS Attack

A very similar vulnerability may be found in the association protocol that follows authentication. Since a STA may be authenticated with multiple APs at once, the 802.11 standard provides a special association message to allow the STA and AP to agree which AP shall have responsibility for forwarding packets. As with authentication, association frames are unauthenticated, and 802.11 provides a disassociation message similar to the de-authentication message. Exploiting this vulnerability is functionally identical to the de-authentication attack. However, it is worth noting that the disassociation attack is slightly less efficient than the de-authentication attack. This is because de-authentication forces the victim node to do more work to return to the associated state than disassociation, ultimately requiring less work on the part of the attacker.

5.5.3 DoS Attacks in PS Mode

A detailed discussion on the power conservation functions of 802.11 was carried out in the preceding chapter. PS mode of 802.11 present several identity-based vulnerabilities discussed in the following section.

5.5.3.1 Faked Beacon Based DoS Attack (De-synchronization)

Using appropriate hacking tools as discussed above, an attacker could advertise as a legitimate AP by using the MAC address of an AP and could get STAs

to connect with it. Freely available toolkits like *HostAP* [59] and *Hotspotter* [60] can convert a wireless LAN user station to function as an AP.

The power conservation mechanism relies on time synchronization between the AP and its STAs. The synchronization information, such as the Beacon Interval and Timestamp broadcast by the AP in a Beacon Frame shown in Figure 4.2 are neither authenticated nor encrypted. By forging these management packets and by faking the Beacon message itself, an attacker can cause a STA to fall out of sync with the AP and fail to wake up at the appropriate intervals. These attacks are particularly easy with tools such as *changeM* [61], *FakeAP* [62] and *SchiffmanM* [63].

5.5.3.2 Spoofed TIM Based DoS Attack

It is potentially possible to trick the STA into thinking there are no buffered packets at the AP when in fact there are. The presence of buffered packets is indicated in a periodically broadcast packet in Beacon Frame called the traffic indication map, or TIM. If the TIM frame itself is spoofed, an attacker may convince a client that there is no pending data for it by setting the bits in TIM corresponding to AID and so the STA will immediately revert back to the sleep state. Many DoS attack tools such as *KisMAC* [64], *Void11* [65] can be used to launch these attacks.

5.5.3.3 PS-Poll Based DoS Attack

An attacker could initiate a DoS attack by sending spoofed PS-Poll messages to AP, pretending to be a legitimate client, operating in PS mode. The PS-Poll frame can easily be spoofed since it is neither encrypted nor authenticated. An attacker within range, running *NetStumbler* [66], *Airsnarf* [67], *dsniff* [68] or similar softwares, can passively sniff or actively probe to extract the AID and BSSID from within the management frames being sent in clear. The attacker can also monitor the transmission at the time of association and subsequently send counterfeited PS-Poll

frames thus forcing AP to transmit the buffered data which will be lost because the legitimate recipient is still asleep. The process is illustrated in Figure 5.2.

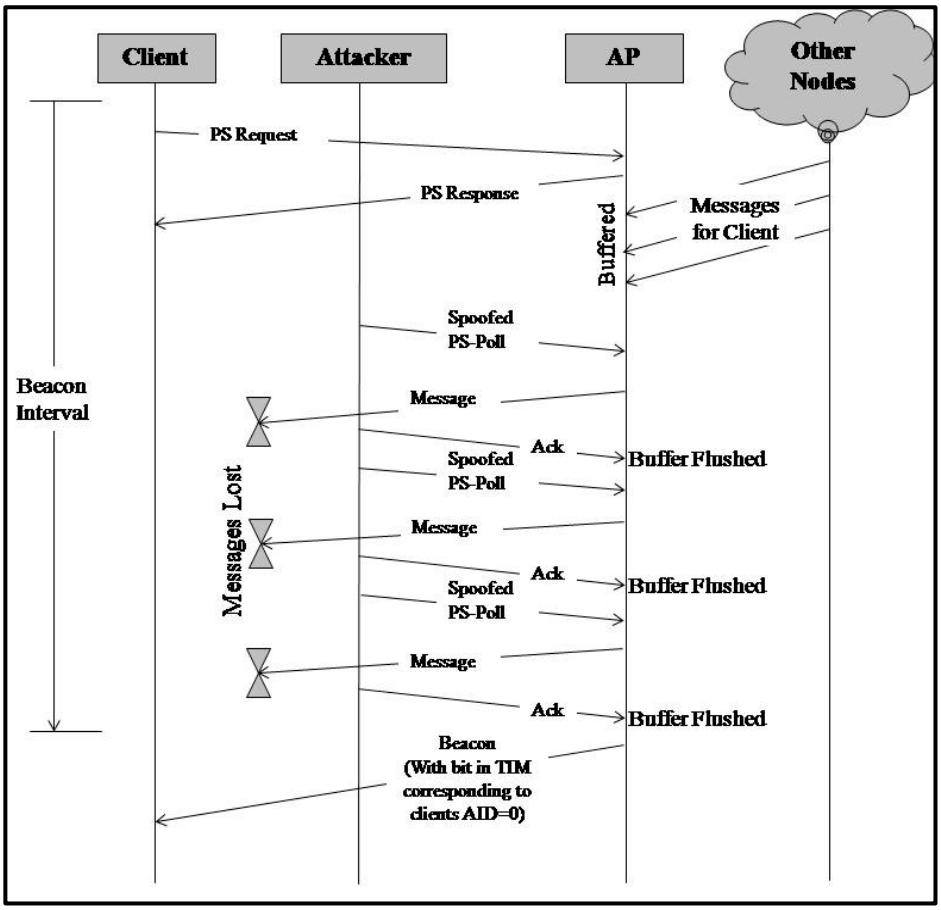


Figure 5.2: PS-Poll DoS Attack

5.6 Prior Work on Detection and Prevention of DoS Attack

Extensive research was carried out after the establishment of the fact that 802.11 despite a no of security enhancements is still vulnerable to malicious DoS attacks. The niche of DoS attacks in PS mode although recognized in most research on DoS attacks on 802.11 was not explored in due significance for possible solutions. The significance and high rate of success of these attacks in PS mode is mainly due to two reasons. Firstly, portable mobile devices recurrently operate in PS mode to conserve their scarcest recourse i.e. battery power and secondly, at the time when the attack is being perpetrated, the legitimate user is sleeping and thus oblivious of this malicious activity on the network.

5.6.1 Research Focused on Detection

Techniques to detect spoofing of MAC addresses have been presented in [69]. In the project, exploits of 802.11 were studied and tested. It was concluded that theses exploits can be used regardless of any wireless security added such as 802.11i. A list of possible exploits, not yet tested was also given. Authors of [70] studied usage patterns in university networks using information from packet capturing tools and syslog files. LaRoche et al. [71] proposed a genetic programming based network intrusion detection. There exists a relationship between a node and the traffic it generates, if spoofing is in progress then changing traffic statistics can be observed.

5.6.2 Various Preventive Solutions

E. D. Cardenas [72] uses Reverse Address Resolution Protocol (RARP) to detect spoofing. If MAC address is spoofed then two IP addresses would be found in response to RARP indicating multiple NICs with same MAC address.

Many researchers for e.g. F. Anjum et al. [73], F. Guo et al. [74], D. Dasgupta et al. [75], B. Aslam et al [76] and H. Xia et al. [77] have proposed sequence number based solutions to different DoS attacks. They proposed encryption of Sequence Number field present in de-authentication and disassociation frames.

Authors of [79] presented a solution to secure management frames by employing a modified Diffe-Hellman's algorithm for authentication and integrity checks. In that the disassociation and de-authentication frames are checked for authenticity before processing. Ying-Sung Lee et al. [80] proposed random bits placing into unused fields of management frames as an authentication mechanism. Authors of [57] also focused on fake de-authentication and disassociation attacks. Although they suggested that de-authentication vulnerability can be solved directly by explicitly authenticating management frames and dropping invalid requests but their

solution is based on queuing of such requests for 5-10 seconds so that AP has the opportunity to observe subsequent packets from the client.

Authors of [36] identified Robust Security Network Information Element (RSN IE) Poisoning attack in which the attacker modifies some insignificant bits in the frames so that the initial negotiation procedure fails. They also recognize a 4-Way Handshake Blocking attack in which the attacker spoofs the first message in a 4-way handshake to launch a memory DoS attack.

W. Gu, Z. Yang et al [81] primarily focus on Node Destroying and Node Penetrating attacks in wireless sensor networks; however, they have also recognized the practicality and effectiveness of DoS attacks in PS mode of 802.11 WLANs and tested it through simulations. They have identified the PS-Poll based DoS attack as the most effective attack on 802.11i compliant WLAN. They have proposed to delay the response of any frames which are suspected to be forged till the next beacon.

5.6.3 Commercial Softwares

Several commercial softwares and security solutions that identify security risks and attacks are available which provide intrusion detection in 802.11 WLANs. For example, *AirDefense Guard* by AirDefense, Inc [82] consists of distributed sensors and server appliances. It detects all rogue WLANs, secures a WLAN by recognizing and responding to intrusion and attacks, performs real-time network audits and tracks all WLAN activity.

Odyssey Server by Funk Software, Inc [83] is a WLAN access control solution based on 802.1x, providing strong security. It includes client and server softwares which secure the authentication and connection of WLAN users. Another software, *SnifferWireless* [84] by Network General Corporation spots security risks in real time, identifies network problems and helps to maximize network investments.

AirMagnet Enterprise [85] provides a scalable WLAN monitoring solution to proactively mitigate all types of wireless threats, enforce enterprise policies, prevent performance problems and audit the regulatory compliance of all their WiFi assets and users worldwide. It offers complete visibility and control over the wireless airspace. AirSnare [86] is another tool for Wireless Intrusion Detection. It generates alert on identification of unfriendly MAC addresses on the network.

5.7 Analysis of Prior Work

It has been established through review of previous work that limited research has been done in the area of developing practical or theoretical frameworks handling IEEE 802.11 availability issues. All the attacks analyzed above although different from the specific area identified in this research yet prove the point. DoS vulnerabilities in WLANs despite implementing the highest level of IEEE 802.11i security appear to be more severe for several reasons. First, with only moderate equipment, an adversary can launch an 802.11i attack very easily. Second, it is much more difficult for a network administrator to detect and locate these attacks.

Work focused on detection only [69, 70, 71] does identify the problem but a solution is neither proposed not tested for verification. Such detections require separate hardware monitoring devices and thus cannot be implemented easily at each node. RARP based solution [72] cannot detect attacks on PS mode because an RARP in a scenario where the victim node is asleep will fetch only one response that is from attacker node. Sequence Number based solutions [73, 74, 75, 76, 77] cannot be applied to the PS-Poll based DoS attack because of the absence of sequence number field in PS-Poll frame. Solution based on Diffe-Hellman algorithm [79] and the ones proposing frame bits modification [80] focus on de-authentication / disassociation attack only.

The feasibility and practicality of RSN-IE Poisoning and 4-Way Handshake Blocking attacks identified in [36] is low. In such attacks, a spoofed frame has to be inserted at a particular time. Sending fake frame too early or too late will be useless. Attacks with such restrictions are not very popular among attackers. Moreover their research does not focus on DoS attacks in PS mode.

The work specifically related to PS-Poll based DoS attacks [57, 81] rather practical has certain problems. The proposed defense mechanism is of a generalized nature. Instead of implementing a secure cryptographic defense to disallow an attacker to be able to forge the MAC frames, they have relied on mere identification of such frames by the AP. In their suggested *delayed processing* approach, it might not be logical to treat all the requests as forged, instead only the requests that do not pass the litmus test of cryptography should be distrusted and treated accordingly. The problem in such solutions is that it might significantly degrade the performance of a WLAN. In vague of spoofed requests; even the authentic requests get delayed and so the legitimate requests of STAs in PS mode (already short of battery power) get delayed unnecessarily.

The Delayed-Response solution [81], impose another restriction on STA to receive all buffered data frames with one null data frame. STAs have no choice to retrieve the frames later or one by one by sending different PS-Poll messages despite the fact that they might not be interested or may be gasping for battery power at that time. The commercial softwares listed above are WLAN intrusion detection systems. These systems consist of necessary hardware and software. These are very expensive to install and need special skills to manage.

Compared to the attacks reviewed above, this research identifies an attack [87] having two salient features. First, such attacks are hard to detect since the PS-Poll

frames are sent only when the victim node is sleeping and thus oblivious of this malicious activity and also because management and control frames are unencrypted and unauthenticated. Although currently de-authentication and disassociation frames are also unencrypted; however, the IEEE 802.11w working group [39] is planning to protect these management frames in the near future. However as yet, no plan has been carried out to protect PS-Poll frames. Second, PS-Poll based attacks are cost effective. Instead of constantly flooding frames, as in de-authentication and disassociation attacks, PS-Poll DoS attack only requires occasional insertion of fake frames.

It is an established fact that 802.11 despite a no of enhancements is still vulnerable to malicious DoS attacks. The niche of DoS attacks in PS mode although recognized in most research was not explored in due significance for possible solutions. All the solutions listed above do add a certain level of security and prevent some DoS attacks in their own specific domain. However, most of these solutions are either not practical, are inefficient or require special hardware.

5.8 Conclusion

The chapter makes an endeavor to identify the techniques used by attackers to extract useful information, subsequently used to exploit the identity vulnerabilities. DoS attacks possible due to the persisting identity vulnerabilities have been identified. As from here onwards, the focus of work narrows down to the identity vulnerabilities prevailing in PS mode of 802.11; therefore, DoS attacks possible in PS mode are explained in detail to highlight their significance. A survey of prior work in this domain is analyzed and then the attacks and solutions proposed have been reviewed. In the end a thorough comparison of this research with prior research has been done to justify the significance of the area identified. The remainder of thesis deals with PS-Poll based DoS attack; however it can be applied to other PS mode attacks as well.

Chapter 6

PROPOSED SOLUTION

6.1 Introduction

After establishing the practicality, significance and effectiveness of spoofed PS-Poll based DoS attack, a robust solution is presented. This chapter begins with an overview of 802.11i communication setup process which clarifies how and when the keys, later used in the protocol and in the proposed solution are established. Subsequently, an analysis of Pseudo Random Function (PRF) defined and used in a number of places in the security amendments of IEEE [11] and forming the basis of the proposed solution is given. This was important so that the basic assumptions of this solution are understood. Then a discussion on the solution is carried out. A thorough analysis of the proposed solution is also given at the end.

6.2 Overview of Communication Set-up Procedure

An overview of communication setup procedure is given, to understand the entities established during communication setup in a 802.11 WLAN having the highest level of 802.11i security standard. These pre-established entities form the basis of proposed solution; where without any additional computational burden on the already scarce resources of WLANs, a novel defense mechanism has been developed.

6.2.1 Robust Security Network Association (RSNA) Establishment

RSNA security comprises of two data confidentiality algorithms CCMP and TKIP. Both use same key management i.e. 802.1x or PSK. It is mandatory for all IEEE 802.11i compliant devices to support RSNA. Three entities are involved in RSNA establishment i.e. wireless client (Supplicant), AP (Authenticator) and Authentication Server (AS). When PSK is used then only wireless client and AP are involved. RSNA establishment process takes place in a number of steps shown in

Figure 6.1, highlighting the establishment of various keys for secure communication.

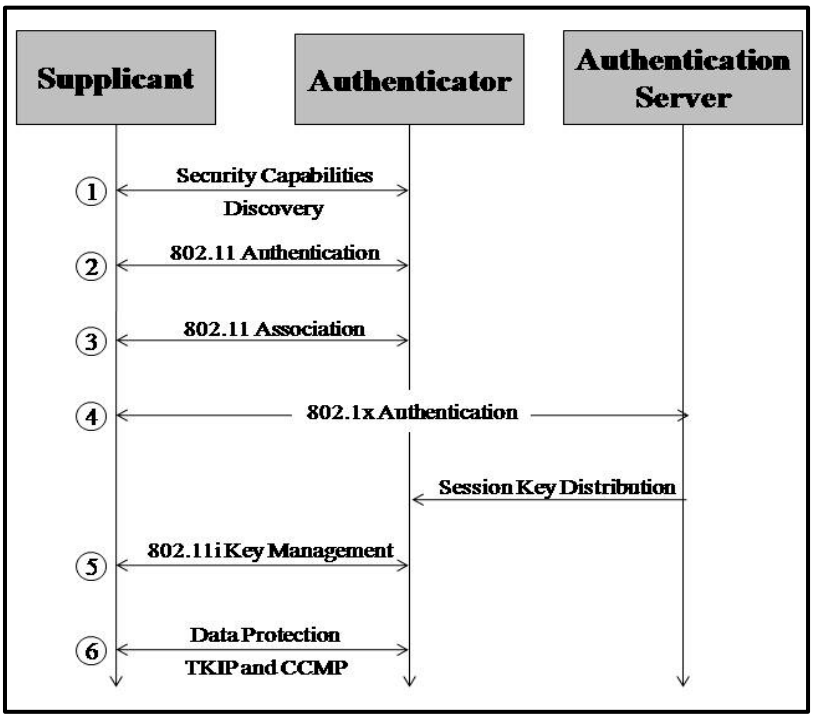


Figure 6.1: RSNA Establishment

Step 1: AP either broadcasts security capabilities or responds to clients probe request.

Step 2: Open System authentication takes place.

Step 3: Client associates with AP.

Step 4: 802.1x Authentication takes place. The client and AS authenticate each other and generate Master Session Key (MSK). MSK is transferred to AP. Both client and AP then generate Pair wise Master Key (PMK). This step may be skipped if Pre-Shared Key (PSK) is used as PMK.

Step 5: A 4-way handshake takes place between client and AP to generate Pair wise Transient Key (PTK). Group Key handshake may also take place, to generate Group Transient Key (GTK) and distributed by AP.

Step 6: Using PTK or GTK and selected data confidentiality algorithm secure data communication takes place.

6.2.2 802.11 / 802.1x States

The state machine shown in Figure 6.2 runs on both the AP and STA. State machine starts with state-1. On successful completion of authentication, both state machines transit to state 2. While in state-2, wireless client initiates association request and both transit to state-3 on successful association. Two messages are exchanged; one for authentication and one for association. No keys have been established between AP and client till now, so no encryption can be used while in state-3. While in state-3, 802.1x authentication is initiated. Depending on authentication mechanism, authentication messages will be exchanged. On successful completion of authentication, PMK will be established. 4-way handshake follows to generate PTK from PMK or PSK. PTK is now used for data encryption and integrity. The AP and client, being in state-4, can now initiate data encryption using PTK.

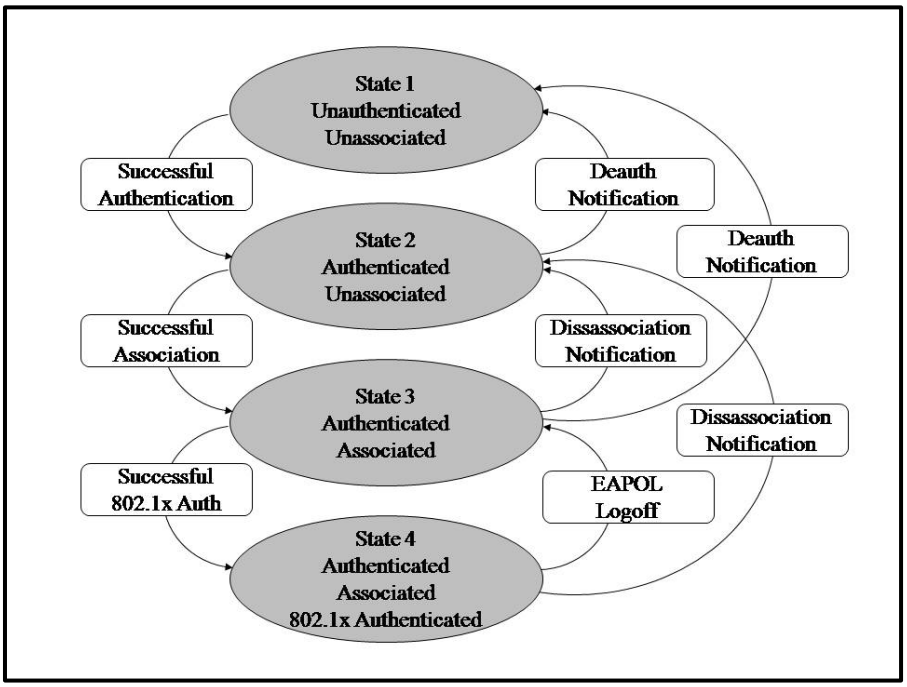


Figure 6.2: 802.11 / 802.1x State Machine

6.3 Analysis of Pseudo-Random Function – PRF

A PRF is a set of rules used to expand a short key into a key stream equal to the length of plaintext. It is a function defined and already implemented in the

security specifications of 802.11 / 802.11i devices. It hashes various inputs to derive a pseudo random value. Depending on its use, it may output various lengths of bits.

6.3.1 HMAC-SHA-1

PRF works on a Hash Message Authentication Code (HMAC) [89]; calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key. As with any HMAC, it may be used to simultaneously verify both the *data integrity* and the *authenticity* of a message. In PRF, Secure Hash Algorithm (SHA-1) [90] is the iterative cryptographic hash function used in the calculations; the resulting algorithm is termed HMAC-SHA-1. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, on the size and quality of the key and the size of the hash output length in bits. The HMAC is illustrated in Figure 6.3 and defined in Equation 6.1.

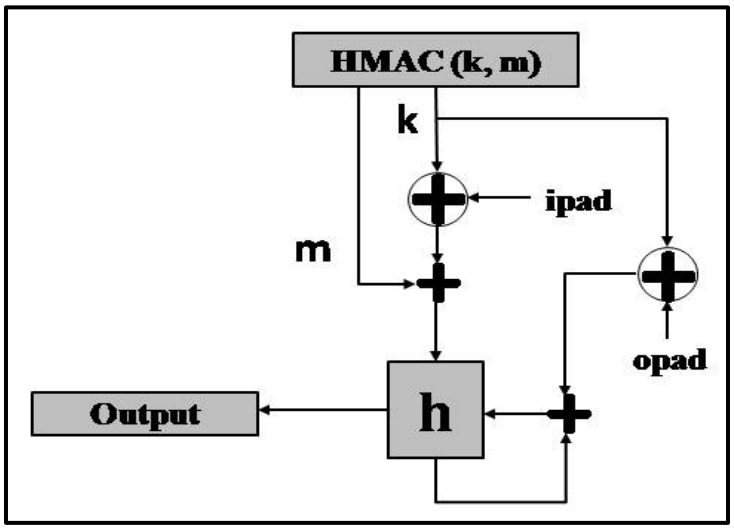


Figure 6.3: Illustration of HMAC

$$\boldsymbol{HMAC_k(m) = h\left((K \oplus opad) \parallel h\left((K \oplus ipad) \parallel m\right)\right)} \quad \text{(Equation 6.1)}$$

Where

$\boldsymbol{h}$: A cryptographic hash function (*SHA-1* in this case)

$\boldsymbol{K}$: A secret key padded to the right with extra zeros to the block size of the hash function

$\boldsymbol{m}$: The message to be authenticated

$\|$: *Concatenation* operation

$\oplus$: *Exclusive OR* (XOR) operation performed on two bit streams of equal length

$\boldsymbol{opad}$: The outer padding = *0x5c5c5c...5c5c* (one-block–long hexadecimal constant)

$\boldsymbol{ipad}$: The inner padding = *0x363636...3636* (one-block–long hexadecimal constant)

6.3.2 $\mathbf{PRF_{160}}$

The pseudo random number generator PRF_{160} is the function used in proposed solution. It takes inputs for HMAC generation using SHA-1 as the hash function, to produce an output of 160 bit pseudo randomized number. Even if a single bit in the input to the function is changed, it will produce an entirely different output thus cryptographically securing the output.

In the proposed solution, the inputs to the PRF are presented to HMAC-SHA-1 to get a 160 bit pseudo randomized output as represented in Equation 6.2 and 6.3.

$$\boldsymbol{PRF_{160}(K, A, B) = PRF(K, A, B, 160)} \quad \text{(Equation 6.2)}$$

$$\boldsymbol{H-SHA-1(K, A, B, X) \leftarrow HMAC-SHA-1(K,\ A\|Y\|B\|X)} \quad \text{(Equation 6.3)}$$

Where

$\boldsymbol{K}$: 512 bit PTK established after 802.1x *authentication* in state-4

$\boldsymbol{A}$: A unique label for each different purpose of the PRF, ***("Power Save Protection"*** in this case)

$\boldsymbol{Y}$: A single octet containing *"0s"*

$\boldsymbol{B}$: Block of data (*"MAC Address of AP"* in this case)

$\boldsymbol{X}$: A single octet containing the parameter, (*"MAC address of STA"* in this case)

$\|$: Denotes *concatenation* operation

6.4 Basic Assumptions

Basic assumptions in the proposed solution are that the state machines of AP and client are in state 4, so the STA is in possession of PTK jointly negotiated by STA and AP. Initiation of PS-Poll message by the client will be from state 4. A unique label "A" proposed is "Power Save Protection" to differentiate / identify the purpose for which PRF is being used.

6.5 Proposed Solution for PS-Poll DoS Attack

The basic idea of proposed solution is to encrypt AID field in PS-Poll frame. The encryption will be done by using a simple *Exclusive-OR* (XOR) operation between 16 bit of AID and 16 bits taken from a pseudo randomized Key Stream (KS). For generation of 160 bits KS, PRF_{160} defined in [11] and explained above can be used, as suggested in [76].

6.5.1 Key Stream Generation

A key stream is generated and stored initially on establishment of PTK in state 4 and then subsequently on expiry of 160 bit key stream after every ten PS-Poll messages. The counter maintained at both ends synchronizes selection of same bits at both ends for encryption and the corresponding decryption. Equation 6.4 is the function used to generate 160 bits pseudo randomized KS.

$$\boldsymbol{KS_{160}} \leftarrow \{\boldsymbol{PRF_{160}}(\boldsymbol{PTK}, \boldsymbol{Power\ Save\ Protection},\ \boldsymbol{APA}, \boldsymbol{SA})\} \quad \text{(Equation 6.4)}$$

Where

$\boldsymbol{KS_{160}}$: 160 bit Key stream, generated for encryption of AID

$\boldsymbol{PRF_{160}}$: Pseudorandom function producing 160 bits of output, (defined in 8.5.1.1 of [7])

$\boldsymbol{APA}$: MAC Address of AP

$\boldsymbol{SA}$: MAC Address of STA

Flow diagram given in Figure 6.4 illustrates the complete process of generation of 160 bits key stream.

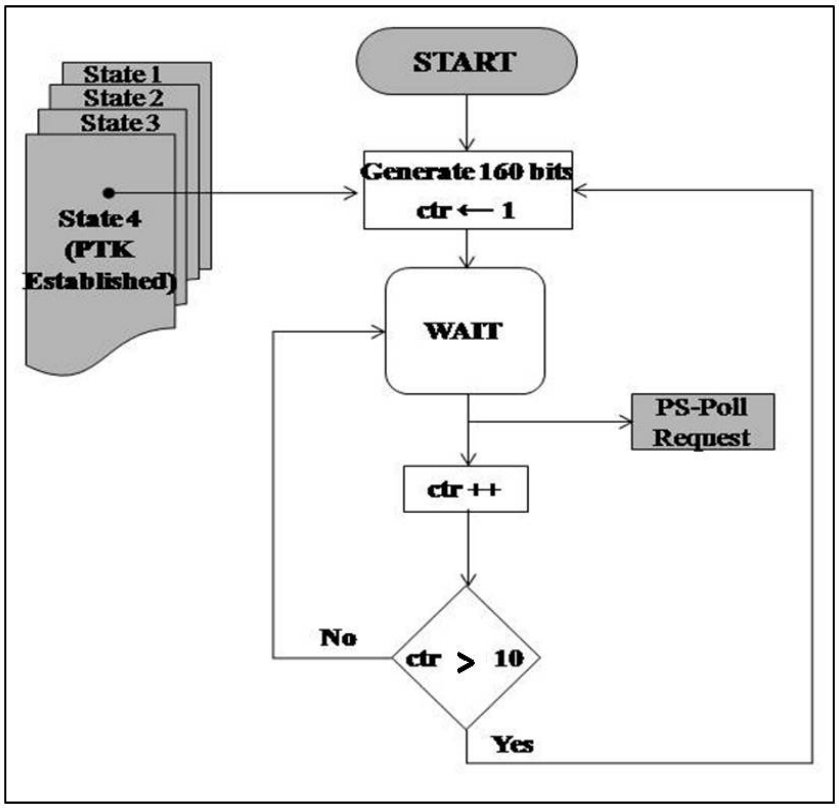


Figure 6.4: Flow Chart (Key Generation)

6.5.2 Encryption of AID by STA

The encryption in Equation 6.5 is a simple bitwise XOR between 16 bit AID assigned to STA at the time of association and 16 bits taken out of generated KS_{160}. For each PS-Poll, the STA will pickup bits from KS_{160}, starting from 0^{th} bit at LSB of KS_{160} to 15^{th} bit for first PS-Poll, 16^{th} bit to 31^{st} bit for the second and so on till all the 160 bits are used.

$$\boldsymbol{AID_E} \leftarrow \boldsymbol{AID_{16}} \oplus \boldsymbol{KS_L^M} \quad \text{(Equation 6.5)}$$

Where

$\boldsymbol{AID_E}$: Association ID after encryption

$\boldsymbol{KS_L^M}$: Partial key stream to encrypt AID_{16} , taken from KS_{160} , starting from LSB side bit L till MSB side bit M

$\boldsymbol{AID_{16}}$: 16 bit *AID* assigned to the STA by AP at the time of association

$\oplus$: *Exclusive OR* (XOR) operation performed on two bit streams of equal length

$\boldsymbol{ctr}$: A counter initialized at "1"; maintained both at AP and STA for synchronization of partial key stream bits taken from KS_{160}

$\boldsymbol{L}$: $\{(ctr - 1) * 16\}$

$\boldsymbol{M}$: $(ctr * 16) - 1$

6.5.3 Decryption Function at AP

Equation 6.6 shows the decryption at AP to authenticate the PS-Poll is again a simple bitwise XOR to verify the AID assigned to STA at the time of association.

$$\boldsymbol{AID_{16}} \leftarrow \boldsymbol{AID_E} \oplus \boldsymbol{KS_L^M} \quad \text{(Equation 6.6)}$$

6.6 Sequence of Events in Proposed Solution

After the process of Authentication and Association, a 4-way handshake is initiated to generate a 512 bit PTK. The STA and AP then transit to state-4. Parts of PTK are used for different purposes given in the security specifications [11]. The modified protocol just maintains two counters on the 512 bit PTK and the 160 bit KS_{160}. Partial Pair-wise Transient Key Counter (PPTK_ctr) is used to pick eight PPTKs of 64 bit length each from PTK. Key Stream Counter (KS_ctr) is maintained on both ends to keep the partial KS_{16} synchronized. Using this counter, 16 bit keys are picked from KS_{160} for encryption of AID in every PS-Poll message.

After every PS-Poll, the value of KS_ctr is incremented and when it exceeds the limit of One Hundred Sixty i.e. after every ten PS-Poll messages, next 64 bit PPTK is used to generate a new KS_{160} and the PPTK_ctr is incremented. This ensures that for every PS-Poll, a new key is used which is never repeated. The KS_ctr will iterate ten times to pick 16 bits from KS_{160} after which a new PPTK is picked to

generate another KS_{160} which will last for another ten messages. As the 512 bit PTK will render eight 64 bit PPTKs therefore, after a total of eighty PS-Poll messages the PPTK_ctr will reach its maximum value of eight. At this point i.e. after eighty successful PS-Polls, the STA will generate an EAPOL logoff message to transit from state-4 to state-3. In state-3, AP will again initiate a 4-way handshake to establish a fresh PTK.

For increased security, the 802.11i protocol periodically refreshes PTK. It may be after a certain amount of time or after an exchange of a fixed number of messages. In modified protocol if the condition set to refresh PTK is reached in normal processing of messages, all the counters are reset and the KS_{160} is regenerated after the establishment of fresh PTK though a 4-Way handshake.

6.6.1 Flow of Events in Modified STA

Complete flow of events showing the process of key generation, maintenance of counters, checking of conditions and the actions taken on the basis of these decisions at a STA working with the proposed protocol is illustrated in Figure 6.5. After establishing the keys and initializing the counters, STA enters in PS mode and periodically wakes up to listen to Beacon and read TIM info showing the presence of data at AP awaiting delivery on reception of authenticated PS-Poll frame. The same flow of events is subsequently followed in the coding for simulation.

The function of both counters, the exact instances of key generation / regeneration, the correlation of modified protocol with the actual 802.11i specifications in terms of state machines and key refreshing is depicted in the flow chart. The flow has been carefully designed to ensure that the modification does not conflict with the base protocol. Simulation by coding the flow in MATLAB confirms the accuracy of design.

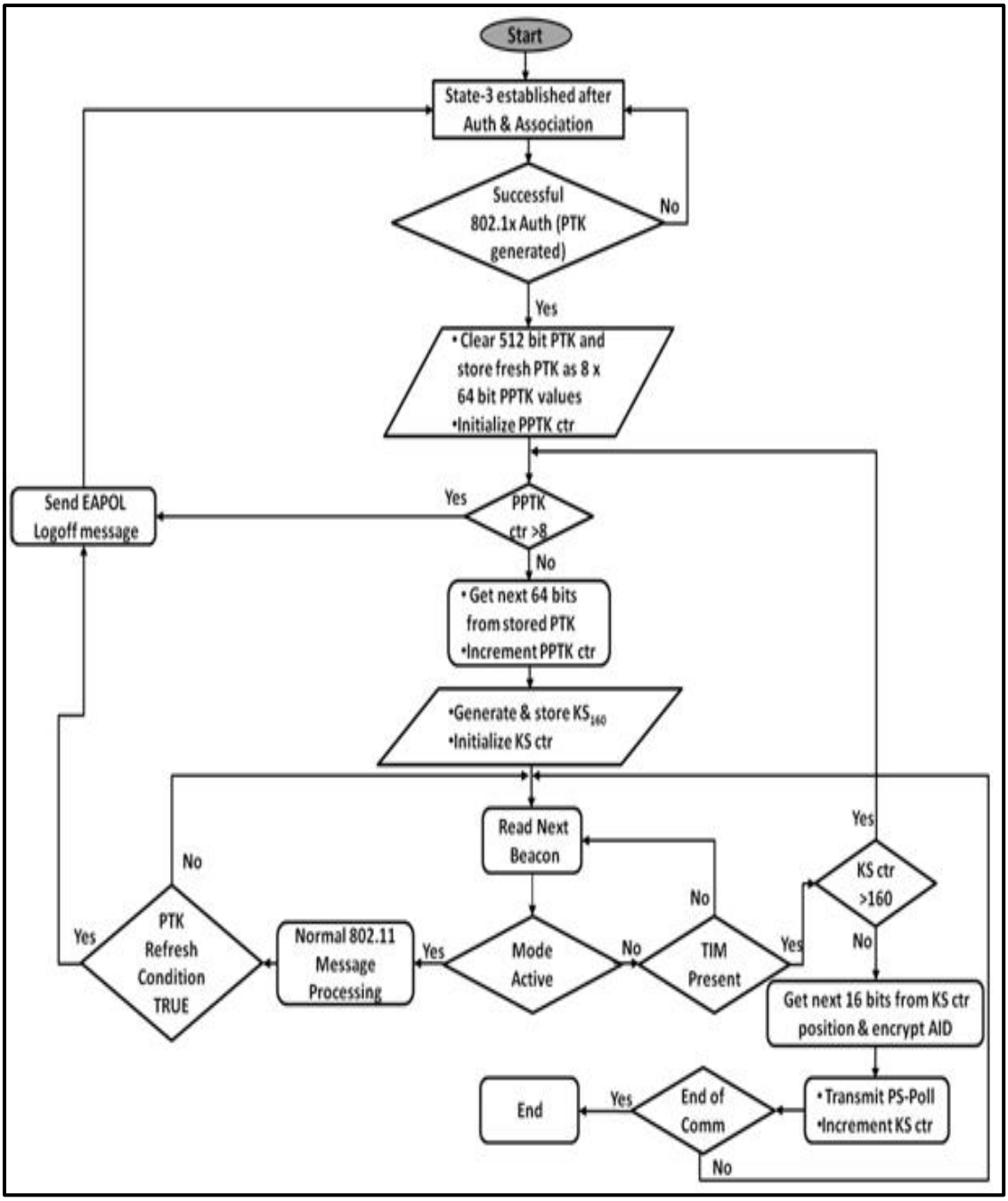


Figure 6.5: Flow of Events in Modified STA

6.6.2 Flow of Events in Modified AP

All the processes of an AP running the proposed protocol are illustrated in Figure 6.6. Same flow of events is subsequently followed in the code written to simulate the solution. Function of both the counters and the exact instances of key generation / regeneration clearly show the ease and accuracy with which a PS-Poll based DoS attack will be detected and prevented in the modified protocol. Exact

placement of processes, for e.g. incrementing the KS_ctr in the last process box ensures that the counter is only incremented after a legitimate PS-Poll. This ensures that DoS attack does not disturb the synchronization of counters at AP and STA. The flow has been carefully designed to ensure that the modification does not conflict with the base protocol. Simulation by coding the flow in MATLAB confirms the accuracy of design.

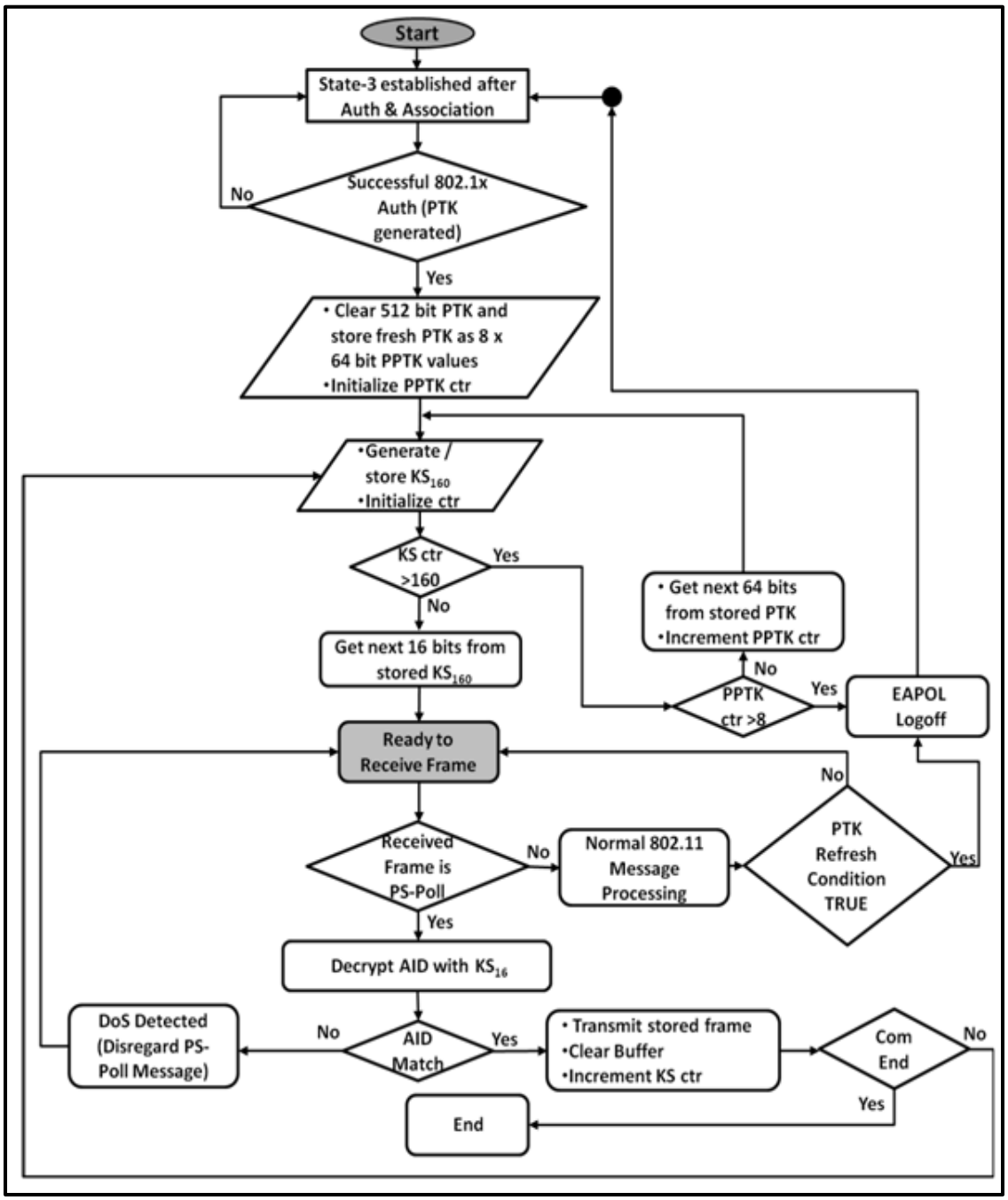


Figure 6.6: Flow of Events in Modified AP

6.7 Analysis of Proposed Solution

Strength of the proposed solution is its simplicity to avert processing overhead, its effectiveness to guarantee detection of attack, its robustness vis-à-vis key freshness / randomness, its efficacy to prevent the Spoofed PS-Poll based DoS attacks and its efficiency in terms of low storage overhead.

6.7.1 Processing Power Efficiency

To save the processing overhead during communication, KS_{160} is computed during communication setup phase and only an XOR operation is carried out when a STA in PS mode wants to retrieve frames buffered at AP by sending PS-Poll frame. As the XOR operation is carried out with lowest computing resources, so the processing overhead is very low. The only overhead imposed is the regeneration of KS_{160} after every ten successful PS-Poll messages which is not considerable, as confirmed through simulation.

The initial generation and subsequent refreshing of PTK is also an inbuilt function of 802.11i. The only processing overhead imposed after a forced state-4 to state-3 transition through EAPOL logoff is the 4-way handshake. This is enforced after every eighty successful PS-Poll messages for key freshness. However, the probability of occurrence of this event is low; as 802.11i itself ensures key freshness by periodically refreshing PTK through EAPOL logoff. This decision is based on certain conditions (specified time interval or number of processed frames) which are likely to occur more often than the condition enforced by modified protocol.

6.7.2 Key Freshness / Randomness

Each time a STA in PS mode has to send a PS-Poll frame, it picks up a fresh 16 bit partial key stream KS_{16} using the counter value maintained at the STA as well as at AP. This method ensures synchronization of key stream bits at both ends.

Moreover, after ten successful PS-Polls by a STA and its subsequent processing at AP, the used 160 bits of KS_{160} will be cleared from memory and new 160 bits KS will be generated, so we will have freshly generated KS after every ten PS-Poll frames. Similarly the refreshing of PTK through inbuilt condition of actual protocol or through the condition imposed by the modified protocol ensures key freshness.

6.7.3 Storage Requirement

At any given point in time, the storage requirement of a STA and that of an AP, with modified protocol is given by Equation 6.7 and Equation 6.8 respectively.

$$\boldsymbol{S_{MSTA} = S_{CSTA} + KS_{160} + PPTK\_ctr + KS\_ctr} \quad \text{(Equation 6.7)}$$

$$\boldsymbol{S_{MAP} = S_{CAP} + \sum_{1}^{N}(KS_{160} + PPTK\_ctr + KS\_ctr)} \quad \text{(Equation 6.8)}$$

Where

$\boldsymbol{S_{MSTA}}$	:	Storage required for a STA with proposed solution
$\boldsymbol{S_{MAP}}$	:	Storage required for an AP with proposed solution
$\boldsymbol{S_{CSTA}}$	:	Storage required for a Conventional STA with 802.11i
$\boldsymbol{S_{CAP}}$	:	Storage required for a Conventional AP with 802.11i
$\boldsymbol{KS_{160}}$	:	Key Stream of 160 bits generated to encrypt AID
$\boldsymbol{PPTK\_ctr}$	:	A 3 bit counter with stored values (1 to 8), indicating the number of Partial PTKs used
$\boldsymbol{KS\_ctr}$	:	A 4bit counter with stored values (1 to 10), indicating the number of 16 bit key streams used
$\boldsymbol{N}$	:	Number of nodes associated with AP

6.7.4 Cryptographic Strength

The cryptographic strength of the KS against a cryptanalysis attempt is that of a One-Time-Pad (OTP) symmetric cipher. The strength of PTK and that of KS_{160} is well established, as both are generated through PRF by using HMAC-SHA-1. Therefore the randomness of the seed to encrypt AID is guaranteed. The probability

of attacker node generating same encrypted AID is given by Equation 6.9.

$$P\{Spoofed\ AID = AID_E\} = {}^{1}/_{2^{16}} \quad \text{(Equation 6.9)}$$

Fresh bits are used each time to encrypt AID; therefore the probability of success of the attack is independent of the number of tries made. The probability of at least one success in 'N' tries is given by Equation 6.10.

$$P\{Atleast\ One\ Spoofed\ AID = AID_E\} = 1 - (1 - P\{Spoofed\ AID = AID_E\})^N \quad \text{(Equation 6.10)}$$

6.7.5 Additional Hardware Requirement

The proposed solution does not recommend any change in the base 802.11 protocol in terms of new functions. All the functions used in modified protocol already exist in 802.11 and are implemented in WPA2 compliant devices. Therefore, wireless clients (STA and AP) can use the proposed solution without the need of any special hardware. The solution can be implemented by just a firmware upgrade.

6.8 Conclusion

IEEE 802.11 standard suffers from basic security flaws; the remedies introduced via IEEE standard 802.11i addressed some of the concerns but failed to guarantee availability. The vulnerability is due to lack of authentication mechanisms for management and control frames which can be exploited by attackers to launch spoofed PS-Poll based DoS attacks. This attack can consume important information intended for wireless clients. A robust solution based on randomized AID field in PS-Poll frame is proposed. The solution is effective, efficient and low on computing and storage resources. All the operations in the proposed solution are performed through functions already existing in the conventional 802.11 protocol and implemented in WPA2 compliant devices; therefore it does not require any additional hardware and can be implemented in both wireless clients and AP via firmware / software upgrade.

Chapter 7

IMPLEMENTATION OF PROPOSED SOLUTION

7.1 Introduction

This chapter gives an insight on the simulator, developed and employed for verification of proposed solution. Different simulators considered and the reasons for choosing MATLAB are also discussed here. The simulated wireless networks along with its component modules are explained. In order to compare and verify the results, simulation of both conventional and modified wireless nodes has been carried out using MATLAB 6.1.

7.2 Simulators Considered

During the course of studies and research work, a no of simulators already available, were considered for implementing and simulating the proposed solution. The details of simulators are given below.

7.2.1 OPNET

OPNET is a network simulator with excellent graphical user interface. It has different versions such as Academic, Research, Complete etc. Only academic version is freely available but it has limited documentation and no support. The current academic version does not have detailed functions about wireless networks, especially infrastructure mode and further it is impossible to make modification / additions in academic version. It was therefore discarded for simulating the solution.

7.2.2 OMNET

A freely available Windows based network simulator. It has user list and a support forum. It has wireless modules but not very well developed. OMNET only supports ad hoc mode and has no functionality regarding authentication and association. Although modifications can be made to tailor the simulator according to

own requirements, yet sketchy documentation makes it very difficult. Furthermore 802.11i is not implemented in simulator so for simulating the solution there was a need to first implement 802.11i. This implementation is a full project in itself needing considerable time and effort, it was therefore also discarded.

7.2.3 NS2

NS2 is a freely available Linux based network simulator. It has an active user list to discuss the problems and issues relating to implementation of different solutions. The complete source code of the simulator along with decent documentation is also available. Some tutorials are available on the Internet that can serve as good starting point. NS2 uses both C++ and OTCL. C++ is used for source coding the modules and OTCL for simulation control. NS2 has good support for wireless networks and IEEE 802.11 protocol is also supported. However, the infrastructure mode is not supported and the detailed functioning of MAC is also not included. Control and management frames are simply discarded which is the main focus of this research. Due to its object oriented programming, any modification requires understanding of complete code of the simulator and specially the C++ and OTCL binding. It was therefore also discarded.

7.2.4 MATLAB

MATLAB® is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notations. It’s typical uses include algorithm development, modeling, simulation and prototyping, Data analysis, exploration, visualization, scientific / engineering graphics, application development and Graphical User Interface (GUI) building are the known strengths of MATLAB. It is available in student and professional versions

with a complete online help and support. A number of forums, easy to use simulation tool boxes and a well developed help system make it the best choice for students and researchers. MATLAB 6.1 release 12.1 was therefore selected for development of a simulator to implement the proposed solution and thereby verify the results.

7.3 Simulation Scenario

The simulation scenario comprise of two infrastructure mode wireless networks having one AP and two wireless STAs each. One of the wireless networks having a set of one AP and two wireless nodes has a modified protocol incorporating the proposed solution while second wireless network having a set of AP and two wireless nodes has been implemented with simple 802.11 protocol. Both simple and modified wireless networks are then presented with the same data to be transmitted. Two attacker nodes have also been implemented which are responsible for PS-Poll based DoS attacks on their associated APs. The simulation scenario is illustrated in Figure 7.1.

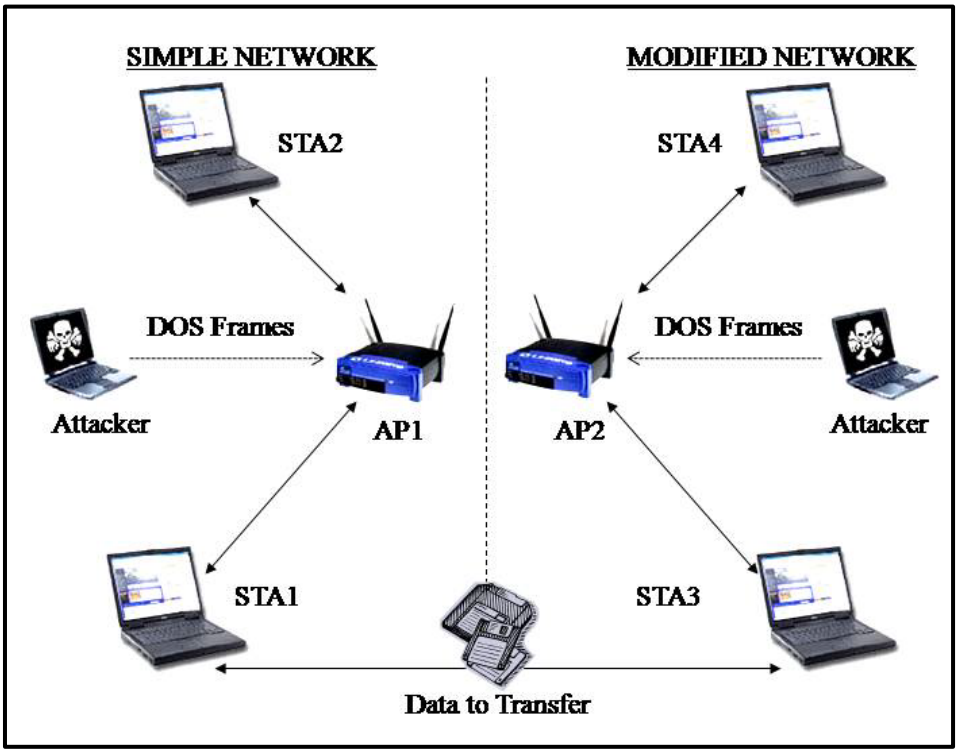


Figure 7.1: Simulation Scenario

7.4 Basic Assumptions

To simulate the WLAN and develop a simulator focusing on the functionality required for verification of proposed solution, certain assumptions / benchmarks were made. First, All wireless nodes have already been associated and authenticated and state machines of all network entities are in State-4. There is no disassociation or de authentication done during the transfer of data. Second, all frames and packets are received intact, there are no CRC errors and all messages are acknowledged so there is no retransfer of any frame. Third, a free media in the simulation indicates that back off has already been catered for. Fourth, an attacker node has already sniffed the Association IDs of victim node, the MAC addresses of AP and Victim node, and the BSSID of the Network. Fifth, all the Wireless Nodes and APs are standard 802.11 compliant so only the part of the protocol required to verify and implement the proposed solution for PS-Poll based DOS attack is simulated.

7.5 Simulator Design

To simulate WLAN, eight major functions performed by wireless LAN entities i.e. AP, Wireless Node and an attacker have been programmed and integrated using MATLAB 6.1. The major modules are AP Modules, STA modules, Attacker Modules and Test Bench Modules. The AP Modules act as an AP. The STA Modules act as WLAN nodes while Attacker Module acts as an attacker in the simulated environment. The methods of Carrier sense, Reception, Transmission and log generation have been programmed as an integral part of each major function. To create a simulation scenario two Test Bench functions have been programmed which are responsible for GUI creation and simulation control. The main control window is as shown in Figure 7.2. It shows the pixel by pixel transfer of data in both WLANs.

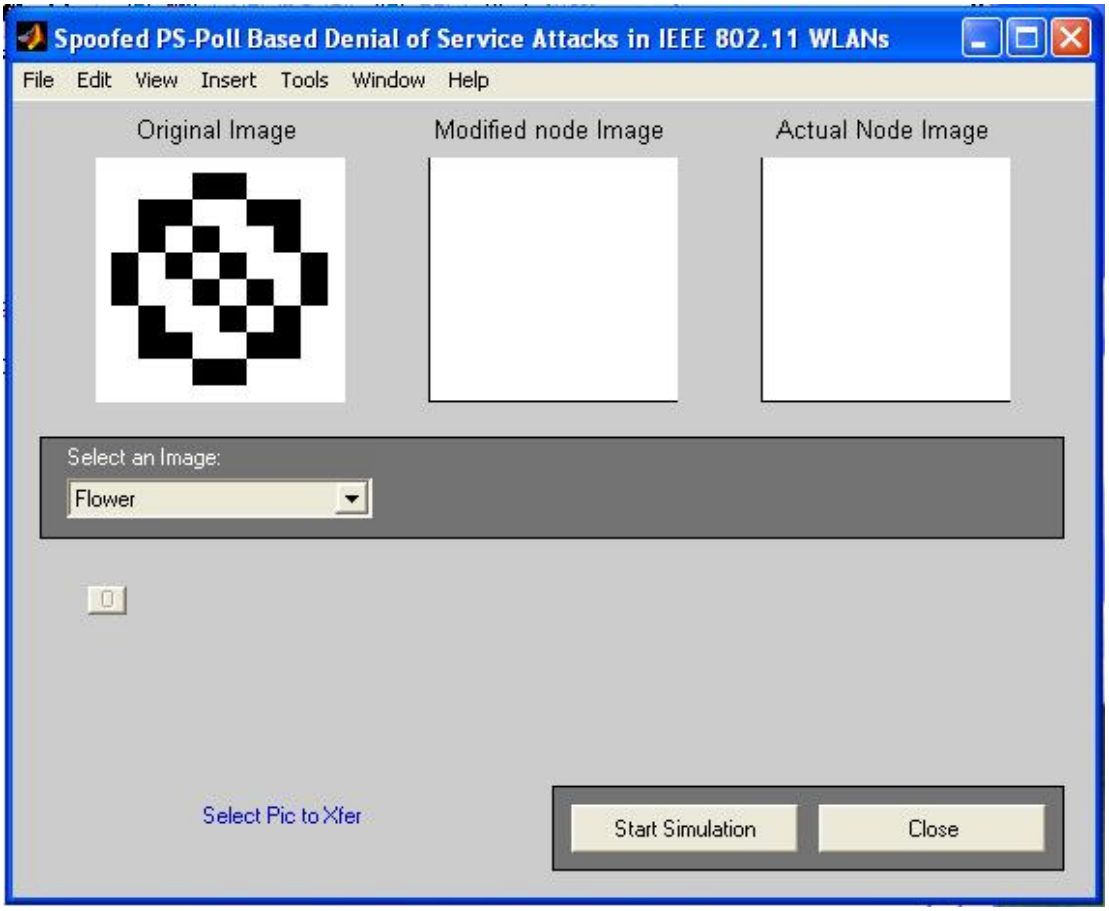


Figure 7.2: GUI for Simulation Control

The relationship between different functions is shown in Figure 7.3. Test bench functions initialize the simulator scenario, set up the data to transfer and create two independent standard WLANs consisting of an AP, two workstations and an attacker each.

Media has been simulated with a memory space where each WLAN entity writes / reads its data. A flag is used for media write operations which indicates whether the media is busy or free. The details of the simulator are explained in next sections. The complete log of all the activities carried out by each entity of wireless network along with the media status is recorded in a Microsoft Access Data base.

Apart from the main functions shown in Figure 7.3, a number of supporting functions simulating other actions performed in WLANs have also been programmed, for example generate_beacon, decrypt_beacon, generate_data_frame etc.

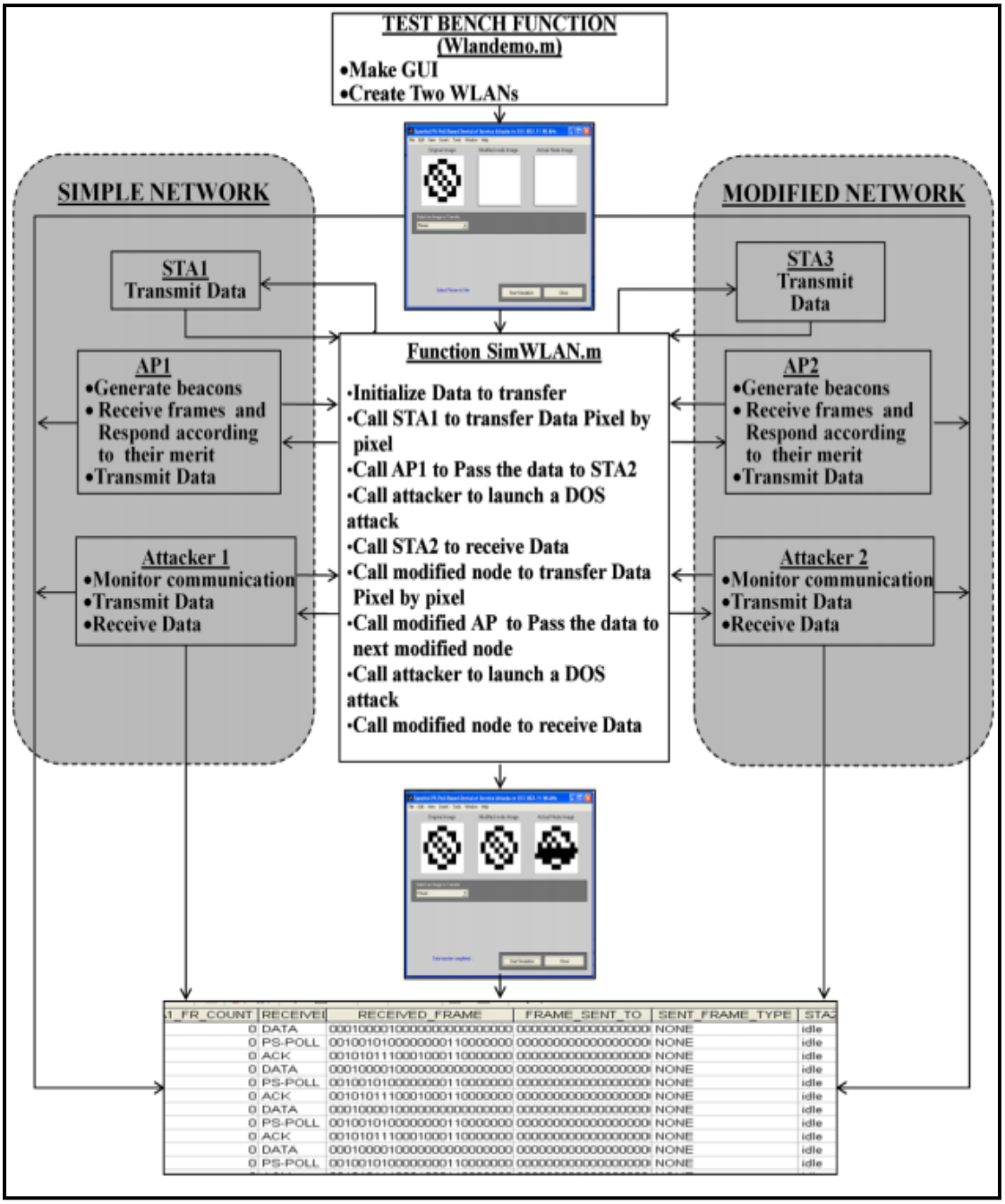


Figure 7.3: Simulator Design

7.5.1 Wireless Media Simulation

The test bench Module (wlandemo.m) during the environment setup process defines a memory named “wdm”. This memory space acts as a wireless media during simulation. It is a shared memory space used for writing the sent data. For clarity and ease of simulation each node and AP has its own memory space inside this shared memory space. The “busy” or “idle” status of each node or AP inside this memory

space defines the overall media status at any particular time. When a node or AP needs to send a frame it checks the status of target node (to whom the frame is addressed) or AP inside the shared memory space. If the status of target is found “idle” then media is considered to be free and data is written in the space allocated for that particular node or AP. To read the data all nodes check their allocated space only when their status is set busy indicating some data in memory space which has not been read yet. Figure 7.4 shows some pending data in wireless media which has not been read by STA4. At this instance of time no AP or node is allowed to write any data addressed to STA4.

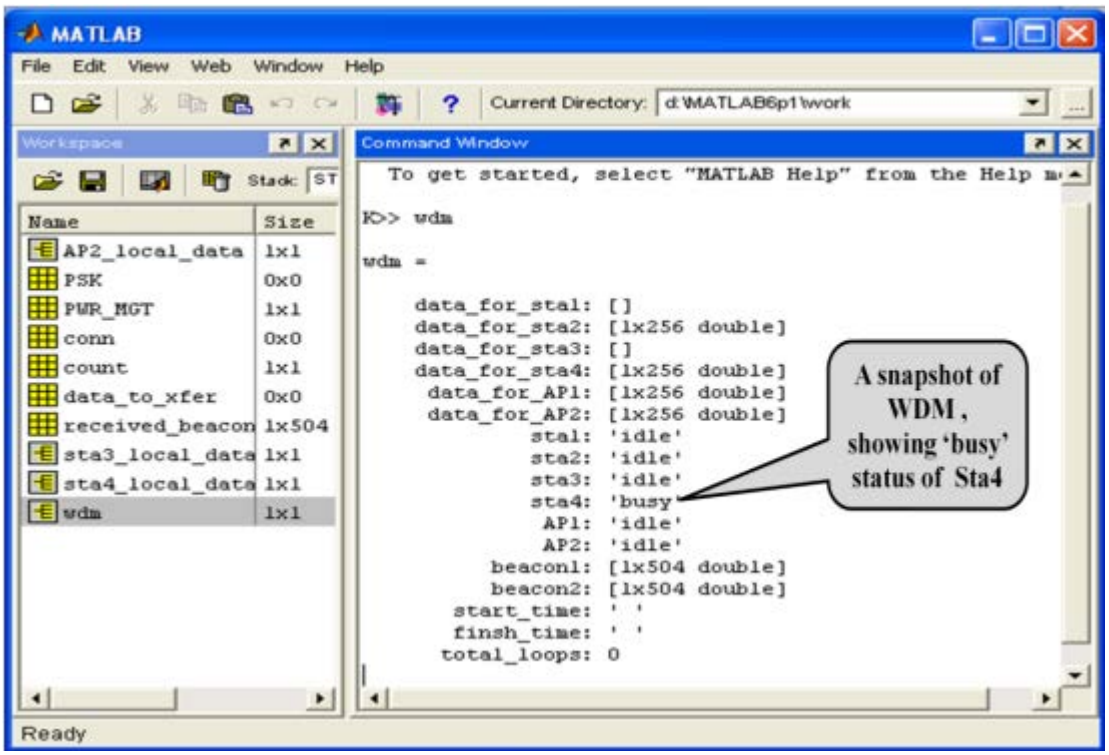


Figure 7.4: Snapshot of Wireless Media Simulation

7.5.2 Simulation of Carrier Sense Mechanism

All nodes and APs avoid collision of transmitted data by monitoring the status of media. Any node that has a frame to send monitors the status of target node or AP in the media, when found “idle” media is considered free and data is written in shared memory space. If the media is found “busy” then execution control is

transferred to other functions and the transmission of frame is pended till the media becomes free. Figure 7.5 shows how CSMA / CA is catered for in the simulator. The status of STA2 is checked in the media before writing any data addressed for the target node.

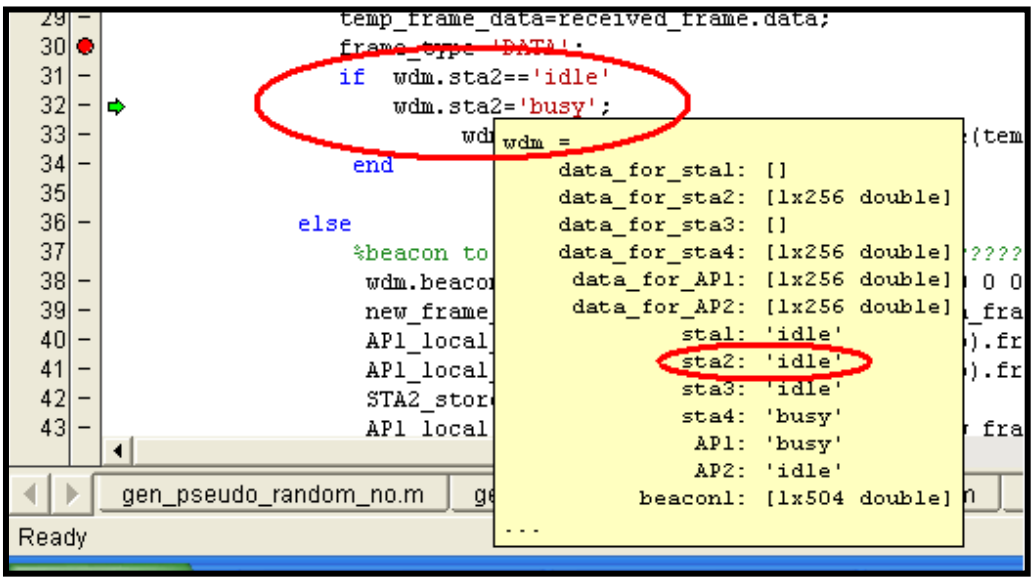


Figure 7.5: Carrier Sense Simulation

7.5.3 Access Point-1 Function (AP1.m)

This function simulates a standard AP. The function takes an argument which is used to trigger the log generation ON or OFF as required by the user. The function generates beacons on execution before checking the memory of any pending data. If the data is received then the received frames are decoded and appropriate functions are called to process the received frame. The major task of this function in the simulator is to maintain the Power Status of STA2 and transfer the data received from STA1 to STA2. The complete log of all the actions taken by the function is written on AP1 table in a MS Access database. These actions include reception of frames and checking of their MAC addresses and types. On determining the type, a frame is accordingly processed for transfer of data in case of a data frame or further processing in case of a PS-Poll frame type For each frame, an acknowledge message

is also processed. Figure 7.6 shows actions taken by AP on reception of a frame.

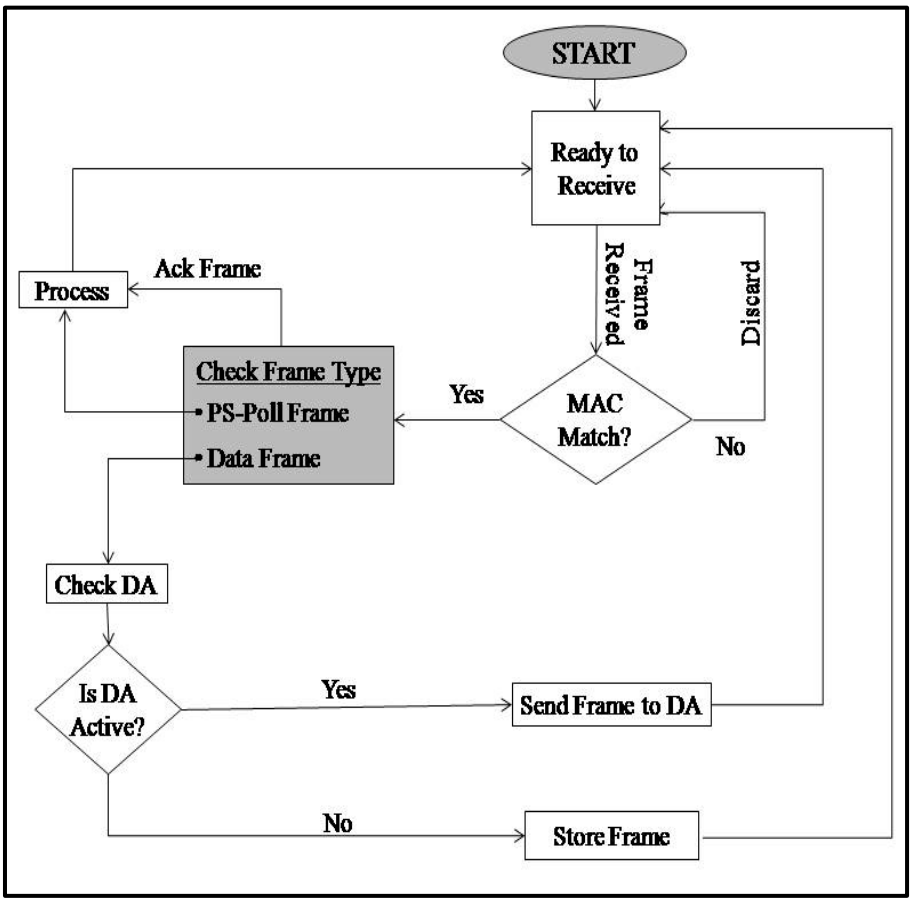


Figure 7.6: Frame Processing by AP1

7.5.4 STA1 function

This function gets the data to transfer from Test Bench module and converts the data to appropriate frames and sends all frames one by one to STA2 through AP1. The function also generates the log for all activities done.

7.5.5 STA2 Function

This function receives the frames from AP1 and extracts information from these frames. The processed information is then passed to GUI for visual painting of received data in the simulator window. The function also switches to “SLEEP” mode and also sends PS-Poll frames to receive any stored data in AP1.

7.5.6 Attacker Functions

The attacker functions monitor beacons generated by APs and launch a PS-

Poll based DOS attack whenever there is a pending stored data of any victim node.

7.5.7 Test Bench Simulation

There are two Test bench functions namely “wlandemo.m” and “sim_wlan.m” programmed for the conducted simulation. These are the main / top-level functions of simulator. They instantiate and interconnect different devices in simulation such as AP, media, wireless nodes etc. The test data to be transferred is selected and presented to both WLAN from these functions. Simulation control is also achieved through these functions. The output results are collected and displayed by these functions. Test bench functions also serve as application layer providing data to nodes for transmission. All nodes are controlled and sequenced by these functions. On screen outputs are also controlled and displayed by these functions.

7.5.8 Log Generation

Log module defines the logs that are generated by each wireless node and AP. Every device makes an entry to log file whenever it performs some action. On termination of simulation the log gives detailed account of the sequence of events performed by various devices. The log can be observed to check the behavior of any device.

7.6 Simulation Conducted

To monitor the results of a PS-Poll based DOS attack on a simple and modified node two distinct WLAN were created using the simulator developed. For ease of understanding the effects of a PS-Poll based DOS attack, a graphical image was selected to be the test data. This test data was presented simultaneously to both simple and modified WLAN. The results of the simulation are instantly displayed by the simulator. The simple WLAN transferred complete data but responded to fake PS-Poll messages by the attacker as expected, thereby flushing the buffered data when

actual station was “ASLEEP” .The modified node not only detected but also prevented the PS-Poll based DOS attack by successfully employing the proposed solution. The simulation was repeated for different Test Data and results were confirmed through log and on screen displays.

7.7 Results

The results were verified and confirmed both through visual analysis of the transferred image in the wlandemo module and through inspection of generated log. In the visual representation of wireless transmission shown in Figure 7.7, the mottled image received through AP-1 at Station-2 clearly indicates the success of DoS attack in a conventional 802.11 compliant network. Whereas, reception of unaltered crisp image received at a modified node (Station-4) through modified access point (AP-2) verifies the successful detection and prevention of DoS attack through use of the proposed solution.

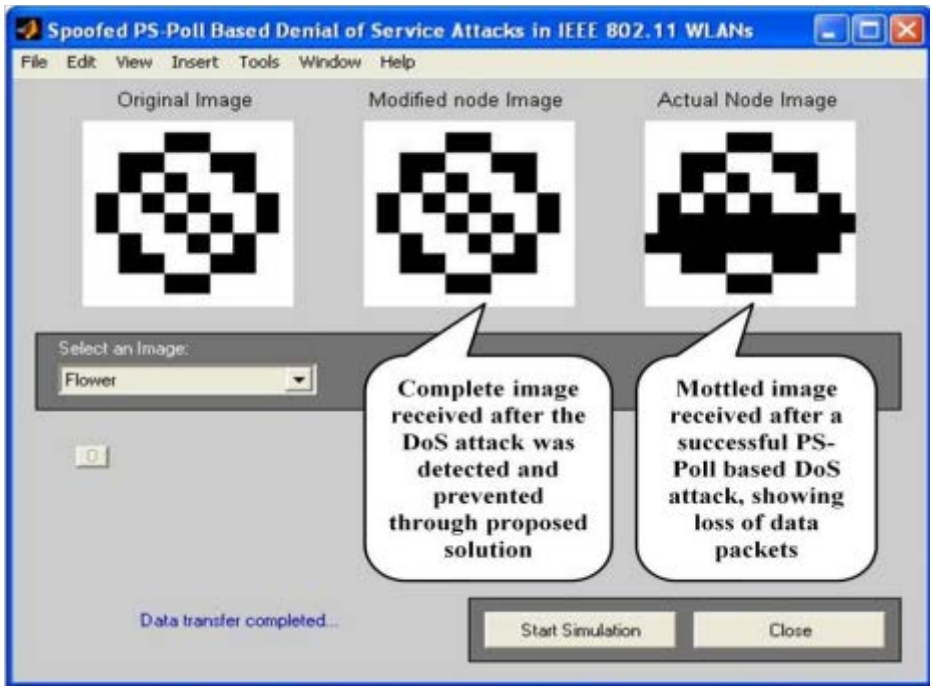


Figure 7.7: Visual Analysis of Conventional and Modified Protocol

The log provides the exhaustive list of actions performed at various devices along with time and other important data. The results show that the AP with

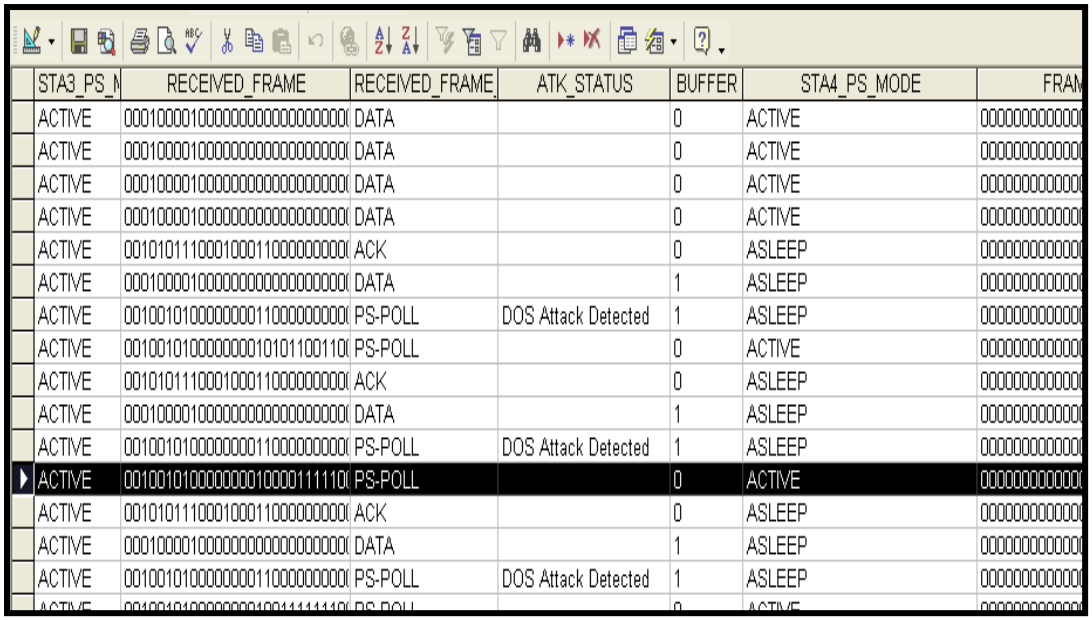
conventional 802.11 protocol (AP1) fails to detect the attack and thus the buffer to store the frames for STA2 is flushed even when the actual node is "ASLEEP" as indicated in Figure 7.8. The modified wireless network with the implementation of proposed solution not only detects but even prevents the PS-Poll based DoS attack as shown in Figure 7.9. The legitimate PS-Poll frame as shown in Figure 7.10 is processed as per the protocol. Complete log of all activities is given in Appendixes.

STA1	RECEIVED_FRAME	FRAME_SENT_TO	RECEIVED_FRAI	BUFFER	STA2_PS_MODE	SENT_FRAI
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ACTIVE	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ACTIVE	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ACTIVE	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ACTIVE	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ACTIVE	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ACTIVE	DATA
0	001010111000100011000000	000000000000000000000001000000000000000000000010	ACK	0	ASLEEP	NONE
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	1	ASLEEP	NONE
0	001001010000000011000000	000000000000000000000001000000000000000000000010	PS-POLL	0	ASLEEP	NONE
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ASLEEP	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ASLEEP	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ASLEEP	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ASLEEP	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ASLEEP	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ASLEEP	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ASLEEP	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ASLEEP	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ASLEEP	DATA
0	000100001000000000000000	000000000000000000000001000000000000000000000010	DATA	0	ASLEEP	DATA

Figure 7.8: Failure of Attack Detection by Simple Node

RECEIVED_FRAME_TYPE	RECEIVED_FRAME	STA4_PS_MODE	BUFFER	ATK_STATUS	FR
DATA	000100001000000000000000	ACTIVE	0		0000000000000000000000100
DATA	000100001000000000000000	ACTIVE	0		0000000000000000000000100
DATA	000100001000000000000000	ACTIVE	0		0000000000000000000000100
ACK	001010111000100011000000	ASLEEP	0		0000000000000000000000100
DATA	000100001000000000000000	ASLEEP	1		0000000000000000000000100
PS-POLL	001001010000000011000000	ASLEEP	1	DOS Attack Detected	0000000000000000000000100
PS-POLL	001001010000000010101100	ACTIVE	0		0000000000000000000000100
ACK	001010111000100011000000	ASLEEP	0		0000000000000000000000100
DATA	000100001000000000000000	ASLEEP	1		0000000000000000000000100
PS-POLL	001001010000000011000000	ASLEEP	1	DOS Attack Detected	0000000000000000000000100
PS-POLL	001001010000000010000111	ACTIVE	0		0000000000000000000000100
ACK	001010111000100011000000	ASLEEP	0		0000000000000000000000100
DATA	000100001000000000000000	ASLEEP	1		0000000000000000000000100
PS-POLL	001001010000000011000000	ASLEEP	1	DOS Attack Detected	0000000000000000000000100
PS-POLL	001001010000000010011111	ACTIVE	0		0000000000000000000000100

Figure 7.9: Successful Attack Detection by Modified Node



STA3_PS_M	RECEIVED_FRAME	RECEIVED_FRAME_	ATK_STATUS	BUFFER	STA4_PS_MODE	FRAM
ACTIVE	0001000010000000000000000000(	DATA		0	ACTIVE	0000000000000
ACTIVE	0001000010000000000000000000(	DATA		0	ACTIVE	0000000000000
ACTIVE	0001000010000000000000000000(	DATA		0	ACTIVE	0000000000000
ACTIVE	0001000010000000000000000000(	DATA		0	ACTIVE	0000000000000
ACTIVE	0010101110001000110000000000(	ACK		0	ASLEEP	0000000000000
ACTIVE	0001000010000000000000000000(	DATA		1	ASLEEP	0000000000000
ACTIVE	0010010100000000110000000000(	PS-POLL	DOS Attack Detected	1	ASLEEP	0000000000000
ACTIVE	0010010100000000010101100110(	PS-POLL		0	ACTIVE	0000000000000
ACTIVE	0010101110001000110000000000(	ACK		0	ASLEEP	0000000000000
ACTIVE	0001000010000000000000000000(	DATA		1	ASLEEP	0000000000000
ACTIVE	0010010100000000110000000000(	PS-POLL	DOS Attack Detected	1	ASLEEP	0000000000000
ACTIVE	0010010100000000010000111110(	PS-POLL		0	ACTIVE	0000000000000
ACTIVE	0010101110001000110000000000(	ACK		0	ASLEEP	0000000000000
ACTIVE	0001000010000000000000000000(	DATA		1	ASLEEP	0000000000000
ACTIVE	0010010100000000110000000000(	PS-POLL	DOS Attack Detected	1	ASLEEP	0000000000000

Figure 7.10: Processing of Legitimate PS-Poll Frame by Modified AP

7.8 Conclusion

The simulator design and its different modules have been discussed in the chapter. The proposed solution was verified using different test data. The PS-Poll based DoS attack has been successful against simple node whereas the modified node has successfully detected and prevented the DoS attack. The processing of legitimate PS-Poll frame by the modified node has also been successful. The results clearly indicate that the proposed solution effectively detects and prevents the PS-Poll based DoS attack whereas it allows the legitimate PS-Poll frames to be processed by the modified node.

Chapter 8

CONCLUSION

8.1 Overview

IEEE 802.11 standard suffers from basic security flaws. The enhancements in the final IEEE released security standard 802.11i did tackle a number of security concerns in WLANs, but failed to address the vulnerabilities exposing network to DoS attacks. These vulnerabilities linger because of unauthenticated and unencrypted management and control frames. This vulnerability is much pronounced in PS mode due to the fact that clients are inactive in order to conserve battery power and thus oblivious to the attack being perpetrated. This weakness is exploited by attackers to launch spoofed PS-Poll based DoS attacks.

A robust solution based on encryption of AID field in PS-Poll message using pre established PTK is proposed. The strength of the solution lies in the use of a new key for encryption of each message and the fact that the solution can be implemented in STAs and APs via firmware upgrade and does not require any additional hardware.

This research differs from the work done previously in the following ways. First, instead of just studying and evaluating the vulnerabilities in WLANs; a novel defense mechanism has also been developed. Second, the solution proposed is robust and practical. Third, the implementation of the solution through simulation of all the required functions using MATLAB, confirms its effectiveness.

8.2 Achievements

The research objectives set forth during the initial phases have been achieved. An understanding of the standards with causes of DoS attacks has been achieved. A detailed survey of existing solutions has been carried out that can serve as a starting point for finding more solutions to the problem. A defense for the persisting

problem of PS-Poll based DoS attack has been found and verified for its effectiveness.

The main concern while developing the solution was to keep it efficient which was successfully catered by using the entities already established during communication setup process. The only computation required during operation is a simple bitwise XOR operation which is known to be extremely low on memory and computing resources.

The proposed solution has been analyzed for its practicability and security. The effectiveness of the solution has also been verified through simulation in MATLAB. Proposed solution can be implemented in APs and STAs. The solution is effective against advanced attackers. The solution is fast and does not require heavy computation / storage. This property makes it robust against DoS attacks caused by repeated spoofed PS-Poll notifications that consume AP's resources.

8.3 Limitations

Verification through simulation is an important step during research and development, which has been achieved. But there is no substitute to live testing that can only be carried out in actual APs and wireless STAs. The solution proposes modifications in the part of protocol that is implemented in firmware; therefore actual testing cannot be done without vendor support.

8.4 Future Work

This work is mainly aimed at wireless networks in infrastructure mode in which all the traffic is directed through AP. Future research can be aimed at studying the DoS attacks in ad hoc networks and studying the effectiveness of proposed or a modified version of proposed solution in these networks. Another possible future research is to confirm the effectiveness of proposed solution by implementing it on actual hardware and make any modification in existing solution if necessary.

APPENDIX-A – SAMPLE SIMULATION LOG (STA1)

FR NO	TIME	STATUS	MODE OF STA1	TYPE OF FRAME SENT	REMARKS
33	04:22:17	idle	ACTIVE	data	STA1 Transmitting Data Frames to AP1 for STA2
34	04:22:19	idle	ACTIVE	data	Normal Data Transfer
35	04:22:21	idle	ACTIVE	data	"
36	04:22:23	idle	ACTIVE	data	"
37	04:22:26	idle	ACTIVE	data	"
38	04:22:28	idle	ACTIVE	data	"
39	04:22:31	idle	ACTIVE	data	"
40	04:22:33	idle	ACTIVE	data	"
41	04:22:36	idle	ACTIVE	data	"
43	04:22:39	idle	ACTIVE	data	"
46	04:22:45	idle	ACTIVE	data	"
49	04:22:51	idle	ACTIVE	data	"
52	04:22:56	idle	ACTIVE	data	"
55	04:23:02	idle	ACTIVE	data	"
58	04:23:08	idle	ACTIVE	data	"
61	04:23:13	idle	ACTIVE	data	"
63	04:23:18	idle	ACTIVE	data	"
64	04:23:20	idle	ACTIVE	data	"
65	04:23:21	idle	ACTIVE	data	"
66	04:23:24	idle	ACTIVE	data	"
67	04:23:26	idle	ACTIVE	data	"
68	04:23:28	idle	ACTIVE	data	"
69	04:23:30	idle	ACTIVE	data	"
70	04:23:32	idle	ACTIVE	data	"
71	04:23:34	idle	ACTIVE	data	"
72	04:23:36	idle	ACTIVE	data	"
73	04:23:38	idle	ACTIVE	data	"
74	04:23:41	idle	ACTIVE	data	"
75	04:23:43	idle	ACTIVE	data	"
76	04:23:45	idle	ACTIVE	data	"
77	04:23:46	idle	ACTIVE	data	"
78	04:23:48	idle	ACTIVE	data	"
79	04:23:51	idle	ACTIVE	data	"
80	04:23:53	idle	ACTIVE	data	"
81	04:23:54	idle	ACTIVE	data	"
82	04:23:57	idle	ACTIVE	data	"
83	04:23:59	idle	ACTIVE	data	"
84	04:24:02	idle	ACTIVE	data	"
85	04:24:04	idle	ACTIVE	data	"
86	04:24:06	idle	ACTIVE	data	"
87	04:24:09	idle	ACTIVE	data	"
88	04:24:11	idle	ACTIVE	data	"
89	04:24:14	idle	ACTIVE	data	"
90	04:24:16	idle	ACTIVE	data	"
91	04:24:19	idle	ACTIVE	data	"
92	04:24:21	idle	ACTIVE	data	"
93	04:24:24	idle	ACTIVE	data	"
94	04:24:26	idle	ACTIVE	data	"
95	04:24:28	idle	ACTIVE	data	"
96	04:24:31	idle	ACTIVE	data	"
97	04:24:33	idle	ACTIVE	data	"

APPENDIX-B – SAMPLE SIMULATION LOG (AP1)

FR NO	TIME	TYPE OF FRAME RECEIVED FROM STA1	TYPE OF FRAME SENT TO STA2	MODE OF STA2	FRAME BUFFER	REMARKS
33	04:22:18	DATA	DATA	ACTIVE	0	STA2 Active-Normal data transfer
34	04:22:20	DATA	DATA	ACTIVE	0	"
35	04:22:21	DATA	DATA	ACTIVE	0	"
36	04:22:24	DATA	DATA	ACTIVE	0	"
37	04:22:26	DATA	DATA	ACTIVE	0	"
38	04:22:29	DATA	DATA	ACTIVE	0	"
39	04:22:31	DATA	DATA	ACTIVE	0	"
40	04:22:34	DATA	DATA	ACTIVE	0	"
41	04:22:36	DATA	DATA	ACTIVE	0	"
42	04:22:38	ACK	NONE	ASLEEP	0	Sta2 Entering PS Mode
43	04:22:40	DATA	NONE	ASLEEP	1	Frame from STA1 for STA2; stored
44	04:22:42	PS-POLL	NONE	ACTIVE	0	Data Sent to STA2 & Buffer Cleared
45	04:22:44	ACK	NONE	ASLEEP	0	Sta2 Entering PS Mode
46	04:22:46	DATA	NONE	ASLEEP	1	Frame from STA1 for STA2; stored
47	04:22:48	PS-POLL	NONE	ACTIVE	0	Data Sent to STA2 & Buffer Cleared
48	04:22:50	ACK	NONE	ASLEEP	0	"
49	04:22:51	DATA	NONE	ASLEEP	1	"
50	04:22:53	PS-POLL	NONE	ACTIVE	0	"
51	04:22:55	ACK	NONE	ASLEEP	0	"
52	04:22:57	DATA	NONE	ASLEEP	1	"
53	04:22:59	PS-POLL	NONE	ACTIVE	0	"
54	04:23:01	ACK	NONE	ASLEEP	0	"
55	04:23:03	DATA	NONE	ASLEEP	1	"
56	04:23:05	PS-POLL	NONE	ACTIVE	0	"
57	04:23:06	ACK	NONE	ASLEEP	0	"
58	04:23:08	DATA	NONE	ASLEEP	1	"
59	04:23:10	PS-POLL	NONE	ACTIVE	0	"
60	04:23:12	ACK	NONE	ASLEEP	0	STA2 Entering PS Mode
61	04:23:14	DATA	NONE	ASLEEP	1	Frame stored
62	04:23:16	PS-POLL	NONE	ASLEEP	0	**Spoofed PS Poll DoS Attack-Data Lost**
63	04:23:18	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
64	04:23:20	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
65	04:23:22	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
66	04:23:24	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
67	04:23:26	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
74	04:23:41	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
75	04:23:43	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
76	04:23:45	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
77	04:23:47	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
78	04:23:49	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
79	04:23:51	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
80	04:23:53	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
81	04:23:55	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
82	04:23:57	DATA	DATA	ASLEEP	0	STA2 ASLEEP-Data sent by STA1 **lost**
83	04:24:00	DATA	DATA	ACTIVE	0	STA2 status reverted to Active
84	04:24:02	DATA	DATA	ACTIVE	0	STA2 Active-Normal data transfer
85	04:24:04	DATA	DATA	ACTIVE	0	"
86	04:24:07	DATA	DATA	ACTIVE	0	"
87	04:24:09	DATA	DATA	ACTIVE	0	"

APPENDIX-C – SAMPLE SIMULATION LOG (STA2)

FR NO	TIME	PS MODE	RECEIVED FRAME TYPE	SENT FRAME TYPE	TIM INFO	REMARKS
39	4:22:32	ACTIVE	DATA	none	0000000000000000	Normal data transfer
40	4:22:34	ACTIVE	DATA	none	0000000000000000	
41	4:22:37	ASLEEP	DATA	ACK	0000000000000000	STA2 going to SLEEP ACK sent - PS bit set
42	4:22:38	ASLEEP		none	0000000000000000	
43	4:22:40	ACTIVE		PS-POLL	0000000000000010	PS-POLL sent on reading TIM info
44	4:22:42	ASLEEP	DATA	ACK	0000000000000000	Data frame received in response to PS-POLL, ACK sent - PS bit set
45	4:22:44	ASLEEP		none	0000000000000000	
46	4:22:46	ACTIVE		PS-POLL	0000000000000010	PS-POLL sent on reading TIM info
47	4:22:48	ASLEEP	DATA	ACK	0000000000000000	Data frame received in response to PS-POLL, ACK sent - PS bit set
48	4:22:50	ASLEEP		none	0000000000000000	
49	4:22:51	ACTIVE		PS-POLL	0000000000000010	
50	4:22:53	ASLEEP	DATA	ACK	0000000000000000	
51	4:22:55	ASLEEP		none	0000000000000000	
52	4:22:57	ACTIVE		PS-POLL	0000000000000010	
53	4:22:59	ASLEEP	DATA	ACK	0000000000000000	
54	4:23:01	ASLEEP		none	0000000000000000	
55	4:23:03	ACTIVE		PS-POLL	0000000000000010	
56	4:23:05	ASLEEP	DATA	ACK	0000000000000000	
57	4:23:07	ASLEEP		none	0000000000000000	
58	4:23:09	ACTIVE		PS-POLL	0000000000000010	
59	4:23:11	ASLEEP	DATA	ACK	0000000000000000	
60	4:23:12	ASLEEP		none	0000000000000000	No TIM info, **Successful DoS Attack**
61	4:23:14	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
62	4:23:16	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
69	4:23:31	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
70	4:23:33	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
71	4:23:35	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
72	4:23:37	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
73	4:23:39	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
74	4:23:41	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
75	4:23:43	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
76	4:23:45	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
77	4:23:47	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
78	4:23:49	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
79	4:23:51	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
80	4:23:53	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
81	4:23:55	ASLEEP		none	0000000000000000	**DoS Attack – Data Lost**
82	4:23:58	ACTIVE	DATA	none	0000000000000000	Back to Active Mode
83	4:24:00	ACTIVE	DATA	none	0000000000000000	Normal data transfer
84	4:24:02	ACTIVE	DATA	none	0000000000000000	Normal data transfer
85	4:24:05	ACTIVE	DATA	none	0000000000000000	Normal data transfer

APPENDIX-D – SAMPLE SIMULATION LOG (STA3)

FR NO	TIME	STATUS	PS MODE	SENT FRAME TYPE	REMARKS
33	04:22:18	idle	ACTIVE	data	STA3 Transmitting Data Frames to AP2 for STA4
34	04:22:20	idle	ACTIVE	data	Normal Data Transfer
35	04:22:22	idle	ACTIVE	data	“
36	04:22:25	idle	ACTIVE	data	“
37	04:22:27	idle	ACTIVE	data	“
38	04:22:30	idle	ACTIVE	data	“
39	04:22:32	idle	ACTIVE	data	“
40	04:22:35	idle	ACTIVE	data	“
41	04:22:37	idle	ACTIVE	data	“
43	04:22:41	idle	ACTIVE	data	“
46	04:22:46	idle	ACTIVE	data	“
49	04:22:52	idle	ACTIVE	data	“
52	04:22:58	idle	ACTIVE	data	“
55	04:23:03	idle	ACTIVE	data	“
58	04:23:09	idle	ACTIVE	data	“
61	04:23:14	idle	ACTIVE	data	“
65	04:23:22	idle	ACTIVE	data	“
69	04:23:31	idle	ACTIVE	data	“
73	04:23:39	idle	ACTIVE	data	“
77	04:23:47	idle	ACTIVE	data	“
81	04:23:55	idle	ACTIVE	data	“
83	04:24:00	idle	ACTIVE	data	“
84	04:24:03	idle	ACTIVE	data	“
85	04:24:05	idle	ACTIVE	data	“
86	04:24:08	idle	ACTIVE	data	“
87	04:24:10	idle	ACTIVE	data	“
88	04:24:12	idle	ACTIVE	data	“
89	04:24:15	idle	ACTIVE	data	“
90	04:24:17	idle	ACTIVE	data	“
91	04:24:20	idle	ACTIVE	data	“
92	04:24:22	idle	ACTIVE	data	“
93	04:24:25	idle	ACTIVE	data	“
94	04:24:27	idle	ACTIVE	data	“
95	04:24:30	idle	ACTIVE	data	“
96	04:24:32	idle	ACTIVE	data	“
97	04:24:34	idle	ACTIVE	data	“
98	04:24:37	idle	ACTIVE	data	“
99	04:24:39	idle	ACTIVE	data	“
100	04:24:42	idle	ACTIVE	data	“
101	04:24:44	idle	ACTIVE	data	“
102	04:24:47	idle	ACTIVE	data	“
103	04:24:49	idle	ACTIVE	data	“
104	04:24:52	idle	ACTIVE	data	“
105	04:24:54	idle	ACTIVE	data	“
106	04:24:56	idle	ACTIVE	data	“
107	04:24:59	idle	ACTIVE	data	“
108	04:25:01	idle	ACTIVE	data	“
109	04:25:04	idle	ACTIVE	data	“

APPENDIX-E – SAMPLE SIMULATION LOG (AP2)

FR NO	TIME	RECEIVED FRAME TYPE	ATTACK STATUS	STA4 PS MODE	STA4 Buffer	SIXTEEN BITS	CTR	REMARKS
40	04:22:35	DATA		ACTIVE	0	Not gen yet	0	Normal Data Transfer
41	04:22:37	DATA		ACTIVE	0	Not gen yet	0	"
42	04:22:39	ACK		ASLEEP	0	Not gen yet	0	STA4 enters PS Mode
43	04:22:41	DATA		ASLEEP	1	Not gen yet	0	Data for STA4 stored
44	04:22:43	PS-POLL		ACTIVE	0	0100011111001000	17	PS Poll received, 160bits KS generated, Successful decryption of AID with first 16bits, ctr set to 17
45	04:22:44	ACK		ASLEEP	0	0100011111001000	17	STA4 ACK & enters PS Mode again
46	04:22:47	DATA		ASLEEP	1	0100011111001000	17	Data for STA4 stored
47	04:22:49	PS-POLL		ACTIVE	0	0101111111000101	33	PS Poll received, Successful decryption of AID with next 16bits, ctr set to 33
48	04:22:50	ACK		ASLEEP	0	0101111111000101	33	STA4 ACK & enters PS Mode again
49	04:22:52	DATA		ASLEEP	1	0101111111000101	33	Data for STA4 stored
50	04:22:54	PS-POLL		ACTIVE	0	1010100100100111	49	KS used, ctr set to 49
51	04:22:56	ACK		ASLEEP	0	1010100100100111	49	
52	04:22:58	DATA		ASLEEP	1	1010100100100111	49	Data for STA4 stored
53	04:23:00	PS-POLL		ACTIVE	0	1100010111101110	65	KS used, ctr set to 65
54	04:23:01	ACK		ASLEEP	0	1100010111101110	65	
55	04:23:04	DATA		ASLEEP	1	1100010111101110	65	Data for STA4 stored
56	04:23:06	PS-POLL		ACTIVE	0	1110111011101111	81	KS used, ctr set to 81
57	04:23:07	ACK		ASLEEP	0	1110111011101111	81	
58	04:23:10	DATA		ASLEEP	1	1110111011101111	81	Data for STA4 stored
59	04:23:11	PS-POLL		ACTIVE	0	1111011011100010	97	KS used, ctr set to 97
60	04:23:13	ACK		ASLEEP	0	1111011011100010	97	
61	04:23:15	DATA		ASLEEP	1	1111011011100010	97	Data for STA4 stored
62	04:23:17	PS-POLL	**DOS Attack Detected**	ASLEEP	1	1111011011100010	97	PS Poll received, AID Decrypted with next 16bits **(Failure)**, ctr maintained at 97
63	04:23:19	PS-POLL		ACTIVE	0	0000000000111100	113	PS Poll received, Successful decryption of AID with next 16bits, ctr set to 113
64	04:23:21	ACK		ASLEEP	0	0000000000111100	113	STA4 ACK & enters PS Mode again
65	04:23:23	DATA		ASLEEP	1	0000000000111100	113	Data for STA4 stored
66	04:23:25	PS-POLL	**DOS Attack Detected**	ASLEEP	1	0000000000111100	113	PS Poll received, AID Decrypted with next 16bits **(Failure)**, ctr maintained at 113
67	04:23:27	PS-POLL		ACTIVE	0	1010100100100111	129	PS Poll received, Successful decryption of AID with next 16bits, ctr set to 129
68	04:23:29	ACK		ASLEEP	0	1010100100100111	129	STA4 ACK & enters PS Mode again
69	04:23:31	DATA		ASLEEP	1	1010100100100111	129	Data for STA4 stored

FR NO	TIME	RECEIVED FRAME TYPE	ATTACK STATUS	STA4 PS MODE	STA4 Buffer	SIXTEEN BITS	CTR	REMARKS
70	04:23:33	PS-POLL	**DOS Attack Detected**	ASLEEP	1	1010100100100111	129	PS Poll received, AID Decrypted with next 16bits **(Failure)**, ctr maintained at 129
71	04:23:36	PS-POLL		ACTIVE	0	1010100100100111	145	PS Poll received, Successful decryption of AID with next 16bits, ctr set to 145
72	04:23:38	ACK		ASLEEP	0	1010100100100111	145	STA4 ACK & enters PS Mode again
73	04:23:40	DATA		ASLEEP	1	1010100100100111	145	Data for STA4 stored
74	04:23:42	PS-POLL	DOS Attack Detected	ASLEEP	1	1010100100100111	145	PS Poll received, AID Decrypted with next 16bits **(Failure)**, ctr maintained at 145
75	04:23:44	PS-POLL		ACTIVE	0	regenerated	161	PS Poll received, Successful decryption of AID with next 16bits, ctr set to 161; New 160bits KS generated (ctr at bit-1 of new KS)
76	04:23:46	ACK		ASLEEP	0	regenerated	161	STA4 ACK & enters PS Mode again
77	04:23:48	DATA		ASLEEP	1	regenerated	161	Data for STA4 stored
78	04:23:50	PS-POLL	DOS Attack Detected	ASLEEP	1	0000001100110101	1	PS Poll received, AID Decrypted with first 16bits of new KS **(Failure)**, ctr maintained at 1
79	04:23:52	PS-POLL		ACTIVE	0	0001101000100110	17	PS Poll received, Successful decryption of AID with first 16bits, ctr set to 17 of new KS
80	04:23:54	ACK		ASLEEP	0	0001101000100110	17	STA4 ACK & enters PS Mode again
81	04:23:56	DATA		ASLEEP	1	0001101000100110	17	Data for STA4 stored
82	04:23:58	PS-POLL		ACTIVE	0	1110110011011110	33	PS Poll received, Successful decryption of AID with next 16bits, ctr set to 33 of new KS
83	04:24:01	DATA		ACTIVE	0	1110110011011110	33	STA4 awake
84	04:24:03	DATA		ACTIVE	0	1110110011011110	33	Normal data transmission resumes
85	04:24:06	DATA		ACTIVE	0	1110110011011110	33	"
86	04:24:08	DATA		ACTIVE	0	1110110011011110	33	"

APPENDIX-F – SAMPLE SIMULATION LOG (STA4)

FR NO	TIME	PS MODE	SENT FRAME TYPE	Sixteen bits	AID ctr	REMARKS
39	04:22:33	ACTIVE	none	Not gen yet	0	Normal reception of data
40	04:22:35	ACTIVE	none	Not gen yet	0	"
41	04:22:38	ASLEEP	ACK	Not gen yet	0	Entering PS Mode by setting PS bit in ACK
42	04:22:39	ASLEEP	none	Not gen yet	0	
43	04:22:41	ACTIVE	PS-POLL	0100011111001000	17	TIM info read in Beacon, 160bits KS generated, AID encrypted with 1st 16 bits & PS-Poll sent, ctr set to 17
44	04:22:43	ASLEEP	ACK	0100011111001000	17	Data received ACK & PS bit set
45	04:22:45	ASLEEP	none	0100011111001000	17	
46	04:22:47	ACTIVE	PS-POLL	0101111111000101	33	TIM info read in Beacon, AID encrypted with next 16 bits & PS-Poll sent, ctr set to 33
47	04:22:49	ASLEEP	ACK	0101111111000101	33	Data received ACK & PS bit set
48	04:22:50	ASLEEP	none	0101111111000101	33	
49	04:22:53	ACTIVE	PS-POLL	1010100100100111	49	PS-Poll sent, ctr set to 49
50	04:22:54	ASLEEP	ACK	1010100100100111	49	
51	04:22:56	ASLEEP	none	1010100100100111	49	
52	04:22:59	ACTIVE	PS-POLL	1100010111101110	65	PS-Poll sent, ctr set to 65
53	04:23:00	ASLEEP	ACK	1100010111101110	65	
54	04:23:02	ASLEEP	none	1100010111101110	65	
55	04:23:04	ACTIVE	PS-POLL	1110111011101111	81	PS-Poll sent, ctr set to 81
56	04:23:06	ASLEEP	ACK	1110111011101111	81	
57	04:23:07	ASLEEP	none	1110111011101111	81	
58	04:23:10	ACTIVE	PS-POLL	1111011011100010	97	PS-Poll sent, ctr set to 97
59	04:23:12	ASLEEP	ACK	1111011011100010	97	
60	04:23:13	ASLEEP	none	1111011011100010	97	DoS Attack on AP
61	04:23:16	ASLEEP	none	1111011011100010	97	Attack blocked by AP
62	04:23:17	ACTIVE	PS-POLL	0000000000111100	113	Encrypted PS-Poll sent, ctr set to 113
62	04:23:17	ACTIVE	none	0000000000111100	113	Waiting for frame while AP decrypts AID with bits from 97 to 112
63	04:23:19	ASLEEP	ACK	0000000000111100	113	ACK of data sent by AP in response to encrypted PS Poll, PS bit set again
64	04:23:21	ASLEEP	none	0000000000111100	113	DoS Attack on AP
65	04:23:24	ASLEEP	none	0000000000111100	113	Attack blocked by AP
66	04:23:25	ACTIVE	PS-POLL	1010100100100111	129	Encrypted PS-Poll sent, ctr set to 129
66	04:23:26	ACTIVE	none	1010100100100111	129	Waiting for frame while AP decrypts AID with bits from 113 to 129
67	04:23:28	ASLEEP	ACK	1010100100100111	129	ACK of data sent by AP in response to encrypted PS Poll, PS bit set again
68	04:23:29	ASLEEP	none	1010100100100111	129	DoS Attack on AP
69	04:23:32	ASLEEP	none	1010100100100111	129	Attack blocked by AP
70	04:23:34	ACTIVE	PS-POLL	1010100100100111	145	Encrypted PS-Poll sent, ctr set to 145

FR NO	TIME	PS MODE	SENT FRAME TYPE	Sixteen bits	AID ctr	REMARKS
70	04:23:34	ACTIVE	none	1010100100100111	145	Waiting for frame while AP decrypts AID with bits from 113 to 145
71	04:23:36	ASLEEP	ACK	1010100100100111	145	ACK of data sent by AP in response to encrypted PS Poll, PS bit set again
72	04:23:38	ASLEEP	none	1010100100100111	145	DoS Attack on AP
73	04:23:40	ASLEEP	none	1010100100100111	145	Attack blocked by AP
74	04:23:42	ACTIVE	PS-POLL	regenerated	161	Encrypted PS-Poll sent, ctr set to 161 – New 160bits KS generated (ctr on bit 1 of new KS)
74	04:23:42	ACTIVE	none	regenerated	161	Waiting for frame while AP decrypts AID with bits from 145 to 161
75	04:23:44	ASLEEP	ACK	regenerated	161	ACK of data sent by AP in response to encrypted PS Poll, PS bit set again
76	04:23:46	ASLEEP	none	regenerated	161	DoS Attack on AP
77	04:23:48	ASLEEP	none	regenerated	161	Attack blocked by AP
78	04:23:50	ACTIVE	PS-POLL	0001101000100110	17	TIM info read in Beacon, AID encrypted with 1st 16 bits of new KS & PS-Poll sent, ctr set to 17
78	04:23:50	ACTIVE	none	0001101000100110	17	Waiting for frame while AP decrypts AID with bits from 1 to 16
79	04:23:52	ASLEEP	ACK	0001101000100110	17	ACK of data sent by AP in response to encrypted PS Poll, PS bit set again
80	04:23:54	ASLEEP	none	0001101000100110	17	
81	04:23:56	ACTIVE	PS-POLL	1110110011011110	33	TIM info read in Beacon, AID encrypted with next 16 bits of new KS & PS-Poll sent, ctr set to 33
82	04:23:59	ACTIVE	none	1110110011011110	33	Turning to Active mode
83	04:24:01	ACTIVE	none	1110110011011110	33	Normal reception of data
84	04:24:04	ACTIVE	none	1110110011011110	33	“
85	04:24:06	ACTIVE	none	1110110011011110	33	“
86	04:24:08	ACTIVE	none	1110110011011110	33	“

BIBLIOGRAPHY

[1] *IEEE Standard Information technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Standard 802.11, 1999 (Reaffirmed 2003).

[2] J. M. Rulnick and N. Bambos, "Mobile Power Management for Maximum Battery Life in Wireless Communication Networks," *Fifteenth Annual Joint Conference of the IEEE Computer Societies. Networking the Next Generation. INFOCOM apos; 96. Proceedings IEEE*, vol. 2, pp. 443–450, Mar. 1996.

[3] Mark Stemm and Randy H. Katz, "Measuring and Reducing Energy Consumption of Network Interfaces in Handheld Devices". *IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Science*, pp. 1125–1131, Aug. 1997.

[4] R. Kravets and P. Krishnan, "Power Management Techniques for Mobile Communication," presented at *MobiCom'98: The 4th International Conference on Mobile Computing and Networking*, Dallas, Texas, USA, Oct. 1998.

[5] Rong-Jaye Chen, Ting-Yu Lin, and Yi-Bing Lin, "Reducing Power Consumption for Mobile Multimedia Handsets," *Tamkang Journal of Science and Engineering*, vol. 2, no. 3, pp. 133–141, 1999.

[6] Eugene Shih, Paramvir Bahl and Michael J. Sinclair, "Wake on Wireless: An Event Driven Energy Saving Strategy for Battery Operated Devices," presented at *MobiCom'02: The 8th Annual International Conference on Mobile Computing and Networking, Session: Energy Efficient Systems,* Atlanta, Georgia, USA, Sep. 2002.

[7] W. E Arbaugh, N. Shankar, J. Wang, and K. Zhang. "Your 802.11 Network has no Clothes," presented at the *First IEEE International Conference on Wireless LANs and Home Networks*, Suntec City, Singapore, Dec. 2001.

[8] T. Karygiannis and L. Owens (2002, Nov.), "Wireless Network Security — 802.11, Bluetooth and Handheld Devices," *NIST Special Publication 800-48*. Available: http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

[9] N. Cam-Winget, R. Housley, D. Wagner and J. Walker, "Security Flaws in 802.11 Data Link Protocols," *SPECIAL ISSUE: Wireless Networking Security — Communications of the ACM*, vol. 46, no. 5, pp. 35–39, May 2003.

[10] *IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control*, IEEE Standard 802.1x-2004 (Revision of IEEE Standard 802.1x-2001), 2004.

[11] *IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications — Amendment 6: Medium Access Control (MAC) Security Enhancements*, IEEE Standard 802.11i-2004, 2004.

[12] A. Mishra, W. A. Arbaugh, "*An Initial Security Analysis of the IEEE 802.1x Standard, University of Maryland*," Tech. Rep. CS-TR-4328, UMIACS-TR-2002-10, 2002.

[13] Matthew S. Gast, *802.11 Wireless Networks: The Definitive Guide*. O'Reilly Publishing, 0-596-00183-5, Apr. 2002.

[14] J. Geier, *Wireless LANs, Second Edition*, SAMS Publishing, Indiana, USA, Jul. 2001.

[15] R. L. Rivest, "*The RC4 Encryption Algorithm*," RSA Data Security Inc, Mar. 1992. (Proprietary).

[16] J. Walker, "*Unsafe at Any Key Size: An Analysis of the WEP Encapsulation*," Tech. Rep. 03628E, IEEE 802.11 Committee, Mar. 2000.

[17] N. Borisov, L. Goldberg, D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," presented at *Mobicom'01: The 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Rome, Italy, Jul. 2001.

[18] Scott Fluhrer, Itsik Mantin, and Adi Shamir, "Weaknesses in the Key Scheduling Algorithm of RC — Lecture Notes in Computer Science," revised paper from the *8th Annual International Workshop on Selected Areas in Cryptography*, pp. 1–24, 2001.

[19] A. Stubblefield, J. Ioannidis and A. Rubin, "*Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*," AT&T Labs, Tech. Rep. TD-4ZCPZZ, 2001.

[20] Airsnort. Available: http://www.airsnort.shmoo.com

[21] Aircrack. Available: http://www.cr0.net:8040/code/network/

[22] WepLab. Available: http://www.weplab.sourceforge.net/

[23] R. Jueneman, S. Matyas, and C. Meyer. Message authentication. *IEEE Communications Magazine*," vol. 23, no. 9, pp. 29–40, Sep. 1985.

[24] S. G. Stubblebine and V. D. Gligor, "On Message Integrity in Cryptographic Protocols," presented at the *IEEE Symposium on Research in Security and Privacy*, pp. 85–105, 1992.

[25] Core SDI. "*CRC32 — Compensation Attack Against ssh-1.5*," Jul. 1998. Available: http://www.coresdi.com/soft/ssh/attack.txt

[26] "Airjack". Available: http://www.sourceforge.net/projects/airjack/

[27] "KisMAC". Available: http://www.binaervarianz.de/projekte/programmieren/kismac/

[28] "Void11". Available: http://www.wlsec.net/void11

[29] R. Housley, D. Whiting and N. Ferguson, "*Alternate Temporal Key Hash: IEEE doc. 802.11-02/282r2*," IEEE Press, Apr. 2002.

[30] N. Ferguson, "*Michael: An improved MIC for 802.11 WEP*. *IEEE doc. 802.11=2/020r0*," IEEE Press, Jan. 2002.

[31] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, "*Extensible authentication protocol (EAP), RFC 3748*," Networking Group, The Internet Society, Jun. 2004.

[32] M. Akhlaq, B. Aslam, Muzammil A. Khan and M. N. Jaffri, "Comparative Analysis of IEEE 802.1x Authentication Methods," presented at *ICCOM'07: The 11th WSEAS International Conference on Communications*, Crete Island, Greece, Jul. 2007.

[33] "coWPAtty". Available: http://www.new.remote-exploit.org/index.php/Codes_main

[34] Vebjorn Moen, Havard Raddum , Kjell J. Hole, "Weaknesses in the Temporal Key Hash of WPA," *ACM SIGMOBILE: Mobile Computing and Communications Review*, vol. 8, no. 2, Apr. 2004.

[35] *National Institute of Standards and Technology Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication (FIPS) 197, Nov. 2001. Available: http://csrc.nist.gov/publications/fips/

[36] C. He and J. C. Mitchell, "Security Analysis and Improvements for IEEE 802.11i," presented at *NDSS: The 12th Annual Network and Distributed System Security Symposium*, San Diego, California, USA, Feb. 2005.

[37] T. A. Dismukes. (2002, Jul.) Wireless Security Blackpaper. *Ars Technica* [Online]. Available: http://arstechnica.com/articles/paedia/security.ars

[38] AusCERT. Denial of Service Vulnerability in IEEE 802.11 Wireless Devices. AA-2004.02 (2004, May.) *AusCERT: Australian Computer Emergency Response Team* [Online]. Available: http://www.auscert.org.au/render.html?it=4091

[39] *IEEE Standards for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications — Protected Management Frames*, IEEE Standard 802.11w, IEEE Computer Society LAN MAN Standards Committee.

[40] Christian Rhl, Hagen Woesner and Adam Wolisz, "A Short Look on Power Saving Mechanisms in the Wireless LAN Standard Draft IEEE 802.11," presented at the *6th WINLAB Workshop on Third Generation Wireless Systems*, New Brunswick, NJ, USA, 1997.

[41] J. Zhu, C. Qiao and X. Wang, "A Comprehensive Minimum Energy Routing Scheme for Wireless Ad hoc Networks," presented at *IEEE INFOCOM'04: The 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*, Hong Kong, China, Mar. 2004.

[42] M. L. Sichitiu, "Cross Layer Scheduling for Power Efficiency in Wireless Sensor Networks," presented at *IEEE INFOCOM'04: The 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*, Hong Kong, China, Mar. 2004.

[43] J. C. Chen, K. M. Sivalingam, P. Agrawal and S. Kishore, "A Comparison of MAC Protocols for Wireless Local Networks Based on Battery Power Consumption," presented at *IEEE INFOCOM'98: The 17th Annual Joint Conference of the IEEE Computer and Communications Societies*, San Francisco, CA, USA, Apr. 1998.

[44] Y. C. Tseng, C. S. Hsu, T. Y. Hsieh. "Power-Saving Protocols for IEEE 802.11 Based Multi-Hop Ad hoc Networks," *IEEE Computer Networks*, vol. 43, no. 3, pp. 317—337, 2002.

[45] L. Alonso and R. Agusti, "Automatic Rate Adaptation and Energy Saving Mechanisms based on Cross-Layer Information for Packet Switched Data Networks", IEEE Communication Magazine, March 2004.

[46] J. Gomez and A.T. Campbell, "A Case for Variable Range Transmission Power Control in Wireless Multihop Networks," presented at *IEEE INFOCOM'04: The 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*, Hong Kong, China, Mar. 2004.

[47] W. Z. Song, Yu Wang, X. Y. Li and O. Frieder, "Localized Algorithms for Energy Efficient Topology in Wireless Ad hoc Networks," presented at *MobiHoc'04: The 5th ACM International Symposium on Mobile Ad hoc Networking and Computing*, Tokyo, Japan, May. 2004.

[48] R. Kravets and P. Krishnan, "Application-driven Power Management for Mobile Communication," *ACM Wireless Networks (2000)*, vol. 6, no. 4, pp. 263—277, 2000.

[49] C. K. Toh, V. Vassiliou, G. Guichal, and C. H. Shih, "Fast MARCH: A Medium Access Control Protocol for Multihop Wireless Ad hoc Networks," *IEEE MILCOM*, vol. 1, pp. 512–16, 2000.

[50] E. Jung and N.H. Vaidya, “An Energy Efficient MAC Protocol for Wireless LANs,” presented at *IEEE INFOCOM’02: The 21st Annual Joint Conference of the IEEE Computer and Communications Societies*, New York, USA, Jun. 2002.

[51] Chris Hurley, Michael Puchol, Russ Rogers and Frank Thornton, *WarDriving: Drive, Detect, Defend — A Guide to Wireless Security*. ISBN: 1931836035, Syngress, 2004.

[52] “SpoofMAC”. Available: http://www.klcconsulting.net/smac/

[53] “SMAC for Windows VISTA, 2003, XP, and 2000 Systems”. Available: http://www.klcconsulting.net/smac/

[54] “Technitium—MAC Address Changer”. Available: www.technitium.com/tmac/index.html

[55] “MAC Changer”. Available: http://www.alobbs.com/

[56] The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions, RSA Security Inc., “An RSA Security Survey,” 2003. Available: www.rsa.com/solutions/topics/whitepapers/CSOP_WP_1003.pdf

[57] John Bellardo and Stefan Savage “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” presented at *USENIX- Security’03: The 12th USENIX Security Symposium, Washington DC, USA,* Aug. 2003. Available: http://www.cs.ucsd.edu/users/savage/papers/UsenixSec03.pdf

[58] “Airjack - Advanced 802.11 Attack Tools”. Available: http://sourceforge.net/projects/airjack/

[59] “HostAP”. Available: http://hostap.epitest.fi

[60] “Hotspotter”. Available: http://www.remote-exploit.org/codes.htm

[61] “ChangerM — A GNU/Linux Utility for Viewing/Manipulating the MAC Address of Network Interfaces”. Available: http://www.alobbs.com

[62] “FakeAP — Black Alchemy Weapons Lab”. Available: http://www.blackalchemy.to/project/fakeap/

[63] “SchiffmanM — Radiate 802.11b Frame Handling”. Available: http://www.packetfactory.net/projects/radiate/

[64] “KisMAC”. Available: http://binaervarianz.de/projekte/

[65] “Void11”. Available: http://www.wlsec.net/void11/

[66] “Netstumbler”. Available: http://www.netstumbler.com

[67] “Airsnarf”. Available: http://airsnarf.shmoo.com/

[68] “Dsniff — Collection of Tools for Network Penetration”. Available: http://packages.debian.org/stable/net/dsniff/

[69] J. Wright. (2002, Jan.) “Detecting Wireless LAN MAC Address Spoofing,” Johnson & Wales University. Available: http://www.linuxsecurity.com/articles/documentation_article-6585.html

[70] D. Kotz, K. Essien, “Analysis of a Campus-Wide Wireless Network,” presented at *MobiCom’02: The 8th Annual International Conference on Mobile Computing and Networking*, Atlanta, Georgia, USA, Sep. 2002.

[71] P. LaRoche, A. N. Zincir-Heywood, “802.11 Network Intrusion Detection using Genetic Programming,” presented at the *2005 Workshops on Genetic and Evolutionary Computation,* Washington, D.C, USA, 2005.

[72] E. D. Cardenas (2003, Aug.) “MAC Spoofing - An Introduction,” SANS Institute, As part of GIAC Practical Repository. Available: http://www.giac.org/practical/GSEC/

[73] F. Anjum, S. Das, P. Gopalakrishnan, L. Kant, K. Byungsuk, “Security in an Insecure WLAN Network,” presented at *IEEE Wirelesscom’05: The International Conference on Wireless Networks, Communications and Mobile Computing*, Hawaii, USA, Jul. 2005.

[74] F. Guo and T. Chiueh, “Sequence Number-Based MAC Address Spoof Detection,” presented at *RAID 2005: The 8th International Symposium on Recent Advances in Intrusion Detection*, Seattle, WA, USA, Sep. 2005.

[75] D. Dasgupta, F. Gonzalez, K. Yallapu and M. Kaniganti, “Multilevel Monitoring and Detection Systems (MMDS),” presented at the *15th Annual Computer Security Incident Handling Conference (FIRST)*, Canada, Jun. 2003.

[76] B. Aslam, M. H. Islam, S. A. Khan, “Pseudo randomized Sequence Number Based Solution to 802.11 Disassociation DoS Attack,” presented at *MCWC’06: The 1st International Conference on Mobile Computing and Wireless Communications*, Amman, Jordan, Sep. 2006.

[77] H. Xia and J. Brustoloni. “Detecting and Blocking Unauthorized Access in Wi-Fi Networks,” presented at the *IFIP Networking'2004 Conference*, Athens, Greece, *Lecture Notes in Computer Science*, 3042:795-806, Springer-Verlag, May 2004.

[78] W. Diffie and M. E. Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[79] Fahad Samad, Waqar Mahmood, Arshad Ali Umar Kaleem. “Improved Security in IEEE802.11 Wireless LANs,” presented at *DNCOCO’06: The 5th WSEAS International Conference on Data Networks, Communications and Computers,* Bucharest, Romania, Oct. 2006.

[80] Ying-Sung Lee, Hsien-Te Chien, Wen-Nung Tsai. “Using Random Bit Authentication to Defend IEEE 802.11 DoS Attacks,” presented at *DNCOCO’06: The 5th WSEAS International Conference on Data Networks, Communications and Computers,* Bucharest, Romania, Oct. 2006.

[81] W. Gu, Z. Yang, C. Que, D. Xuan, and W. Jia, “On Security Vulnerabilities of Null Data Frames in IEEE 802.11 based WLANs,” presented at the *ICDCS 2008: The 28th International Conference on Distributed Computing Systems*, Beijing, China, Jun. 2008.

[82] “AirDefense Guard” by AirDefense, Inc. Available: http://www.airdefence.net

[83] “Odyssey Client/Server” by Funk Software, Inc. Available: http://www.juniper.net/

[84] “Sniffer Wireless” by Network General Corporation. Available: http://www.networkgeneral.com/default.aspx

[85] “AirMagnet Enterprise”. Available: http://www.airmagnet.com/products/enterprise/

[86] “AirSnare”. Available: http://home.comcast.net/~jay.deboer/airsnare/index.html

[87] Zaffar I. Qureshi, Baber Aslam, Athar Mohsin, Yonus Javed, “A Solution to Spoofed PS-Poll Based Denial of Service Attacks in IEEE 802.11 WLANs,” presented at *ICCOM'07: The 11th WSEAS International Conference on Communications*, Vol. 11, Agios Nikolaos, Crete Island, Greece, pp. 7 –11, Jul. 2007.

[88] *Federal Information Processing Standard FIPS PUB 198 — The Keyed-Hash Message Authentication Code*, NIST Standard, Feb. 1997. Available: http://csrc.nist.goc/publications/fips/fips198/fips-198a.pdf

[89] *Federal Information Processing Standard FIPS PUB 180-1 — Secure Hash Standard*, NIST Standard, Apr. 1995. Available: http://www.itl.nist.gov/fipspubs/fip180-1.htm