Islamic University of Gaza
Deanery of Higher Studies
Faculty of Engineering
Computer Engineering Department

IEEE 802.11i Security and Vulnerabilities

Studying and Enhancing WIDS Performance

By:

Ramzi Mohammed Abed

120072398

Supervised by:

Dr. Aiman Abu Samra

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master in Computer Engineering

1431H (2010)

المنارة للاستشارات
www.manaraa.com

بسم الله الرحمن الرحيم

الجامعة الإسلامية – غزة
The Islamic University - Gaza

عمادة الدراسات العليا هاتف داخلي: 1150

ج س غ/35/
الرقم..... Ref 2010/09/27

التاريخ..... Date

نتيجة الحكم على أطروحة ماجستير

بناءً على موافقة عمادة الدراسات العليا بالجامعة الإسلامية بغزة على تشكيل لجنة الحكم على أطروحة الباحث/ رمزي محمد عبد العزيز عابد، لنيل درجة الماجستير في كلية الهندسة قسم هندسة الحاسوب وموضوعها:

IEEE 802.11i Security and Vulnerabilities Enhancing WIDS Performance

وبعد المناقشة التي تمت اليوم الأربعاء 20 شوال 1431هـ، الموافق 2010/09/29م الساعة العاشرة صباحاً، اجتمعت لجنة الحكم على الأطروحة والمكونة من:

د. أيمن أحمد أبو سمرة	مشرفاً ورئيساً	.....
أ.د. محمد أمين مكّي	مناقشاً داخلياً	.....
د. توفيق سليمان برهوم	مناقشاً داخلياً	.....

وبعد المداولة أوصت اللجنة بمنح الباحث درجة الماجستير في كلية الهندسة/ قسم هندسة الحاسوب.

واللجنة إذ تمنحه هذه الدرجة فإنها توصيه بتقوى الله ولزوم طاعته وأن يسخر علمه في خدمة دينه ووطنه.

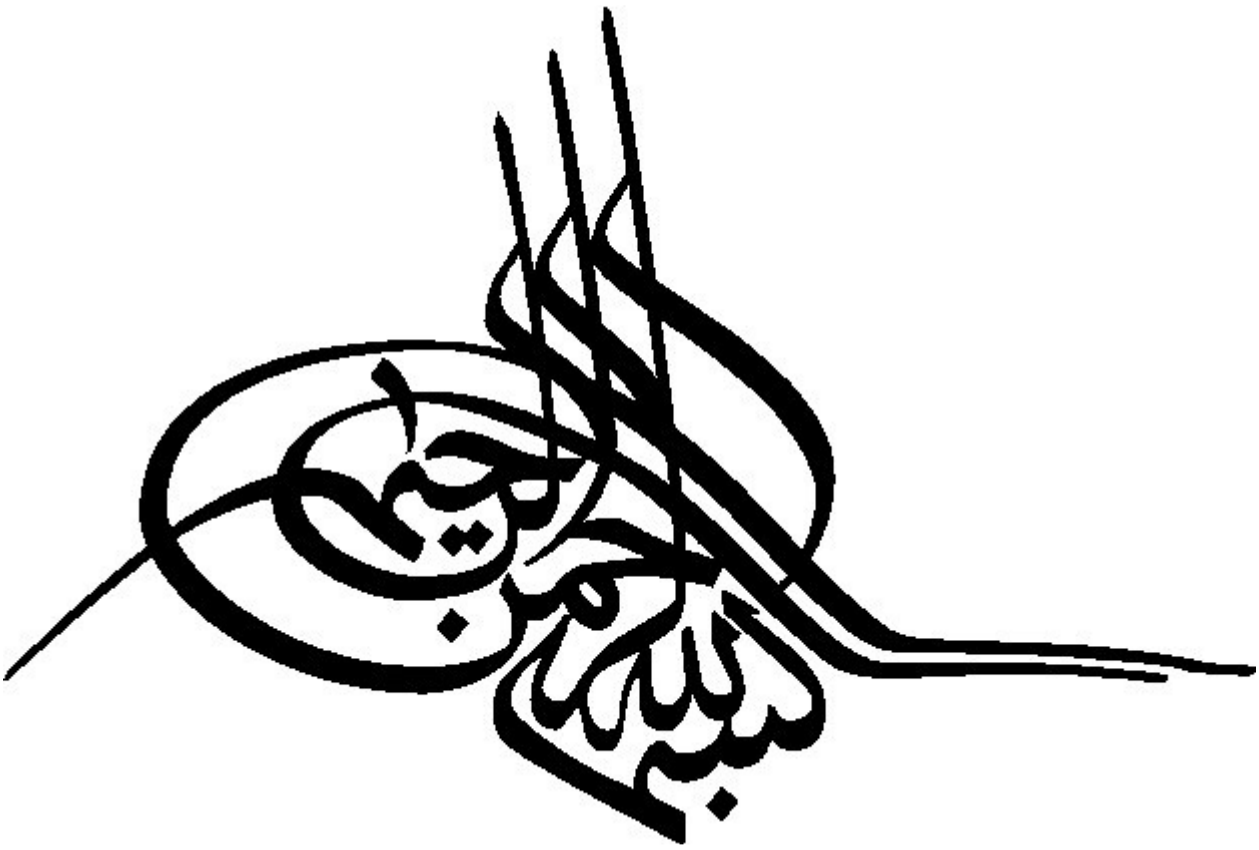
والله ولي التوفيق،،،

عميد الدراسات العليا

د. زياد إبراهيم مقداد

P.O. Box 108, Rimal, Gaza, Palestine fax: +970 (8) 286 0800 فاكس Tel: +970 (8) 286 0700 ص.ب. 108 الرمال، غزة، فلسطين هاتف
public@iugaza.edu.ps www.iugaza.edu.ps

المنارة للاستشارات
www.manaraa.com



المنارة للاستشارات
www.manaraa.com

Abstract

Despite using a variety of comprehensive preventive security measures, the Robust Secure Networks (RSNs) remain vulnerable to a number of attacks. Failure of preventive measures to address all RSN vulnerabilities dictates the need for enhancing the performance of Wireless Intrusion Detection Systems (WIDSs) to detect all attacks on RSNs with less false positive and false negative rates.

This research performs an analytical study for wireless intrusion detection techniques (WIDTs) for detecting attacks on IEEE 802.11i RSNs.

The research also verifies the effectiveness of two WIDTs in detecting MAC spoofing Denial of Service (DoS) attacks. These WIDTs are Received Signal Strength Detection Technique (RSSDT) and Round Trip Time Detection Technique (RTTDT) which can run in passive mode, do not require protocol or hardware modifications, and they are computationally inexpensive. We do our verification by applying three new different DoS attacks: TKIP DoS attack, Channel Switch DoS attack, and Quite DoS attack; and study the performance of these WIDTs. Moreover, we study the correlation of the generated alarms from these WIDTs for greater reliability and robustness. Finally, we propose an algorithm to enhance the performance of the correlation of these WIDTs by optimizing the value of the detection threshold; the proposed algorithm lowers the false positive rate.

Keywords: Wireless Intrusion Detection Technique, Wireless Intrusion Detection System, Robust Security Network, IEEE 802.11, Wireless LAN, Received Signal Strength, Round Trip Time

www.manaraa.com

عنوان البحث:

شبكات IEEE802.11i اللاسلكية أمنها وثغراتها الأمنية
تحسين اداء انظمة اكتشاف اختراق الشبكات اللاسلكية

ملخص البحث:

على الرغم من أن معايير الأمن التي تمت اضافتها للشبكات قوية الامن (RSN) من النموذج (IEEE802.11i) للشبكات اللاسلكية إلا أنها لا تزال عرضة للعديد من الثغرات الأمنية. فشل معايير (RSN) في حماية الشبكات اللاسلكية زاد من أهمية تحسين أداء أنظمة اكتشاف محاولات اختراق الشبكات اللاسلكية لتصبح قادرة على اكتشاف جميع محاولات اختراق شبكات (RSN) بنسبة قليلة من الأخطاء.

قمنا في هذا البحث بدراسة تحليلية لطرق اكتشاف محاولات اختراق الشبكات اللاسلكية والمخصصة لاكتشاف محاولات اختراق شبكات (IEEE802.11i) اللاسلكية.

يقوم هذا البحث أيضا بالتحقق من كفاءة تقنيتين لاكتشاف محاولات اختراق الشبكات اللاسلكية، واللتان تمتازان بأنها يمكن أن تعمل باستقلالية عن أجهزة الارسال والاستقبال المتصلة بالشبكة، ولا تحتاجان لتعديل على البروتوكولات أو على الأجهزة المستخدمة، كما تمتاز هاتان التقنيتان بانها لا تتطلب الكثير من عمليات المعالجة على الأجهزة التي تشغلها. هاتان التقنيتان هما: تقنية قوة الإشارة المستقبلة لاكتشاف محاولات الاختراق (RSSDT) وتقنية قياس زمن الارسال ثم التلقي لاكتشاف محاولات الاختراق (RTTDT)، حيث يقوم البحث بالتحقق من كفاءة هذه التقنتين في اكتشاف محاولات الاختراق التي تعتمد على تزوير العنوان الفيزيائي للأجهزة المتصلة بالشبكة والتي تقوم بتعطيل خدمات الشبكة، وذلك بتطبيق ثلاث طرق جديدة للهجوم ومن ثم دراسة كفاءة هاتين التقنيتين. كما يقوم البحث بدراسة فعالية الربط بين مخرجات هاتين الطريقتين للحصول على نتائج أكثر دقة واعتمادية في اكتشاف محاولات الاختراق للشبكات اللاسلكية.

أخيرا قمنا في هذا البحث بتقديم خوارزمية جديدة لتحسين كفاءة تقنية الربط بين التقنيتين السابقتين لاكتشاف محاولات الاختراق من خلال اختيار أفضل قيمة للنقطة الحرجة لمقياس الاكتشاف، بحيث تقوم هذه الخوارزمية بتقليل نسبة الاخطاء في عملية اكتشاف محاولات الاختراق.

المنارة للاستشارات
www.manaraa.com

Acknowledgment

First of all I would like to thank Allah who affords the accomplishment of this work.

Then I am grateful to my supervisor Dr. Aiman Abu Samra for his enormous support, valuable advice, encouragement and professional assistance throughout the work of this research.

I also would like to thank Mr. Motaz Saad for his valuable comments and advice.

www.manaraa.com

Contents

www.manaraa.com

www.manaraa.com

List of Tables

www.manaraa.com

List of Figures

www.manaraa.com

List of Abbreviations

ACK	Acknowledgement
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
AS	Authentication Server
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CCMP	Counter-mode with cipher block Chaining Message authentication code Protocol
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear To Send
DCF	Distributed Coordination Function
DIFS	DCF Inter-frame Space
DR	Detection Rate
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPoL	EAP Over LAN
ESS	Extended Service Set
FCS	Frame Check Sequence
FN	False Negative

www.manaraa.com

FP	False Positive
GTK	Group Transient Key
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
ID	Identifier
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IFS	Inter-frame Space
IP	Internet Protocol
ISM	Industrial Scientific Medical
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
Masq	Masquerading
MIC	Message Integrity Code
MITM	Man In The Middle
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
PHY	Physical Layer
PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent
PMK	Pairwise Master Key
PSK	Pre-shared Key

المنارة للاستشارات
www.manaraa.com

PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency
RFC	Request For Comment
RFF	Radio Frequency Fingerprinting
RFMON	Radio Frequency Monitoring
RSN	Robust Security Network
RSNA	Robust Security Network Association
RSN IE	RSN Information Element
RSS	Received Signal Strength
RSSDT	Received Signal Strength Based Intrusion Detection Technique
RSSI	Received Signal Strength Indication
RTS	Request To Send
RTT	Round Trip Time
RTTDT	Round Trip Time Based Intrusion Detection Technique
SA	Security Association
SIFS	Short Inter-frame Space
SNRA	Sequence Number Rate Analysis
SOE	Standard Operating Environment
SSFA	Signal Strength Fourier Analysis
SSID	Service Set Identifier
STA	Wireless Station
TKIP	Temporal Key Integrity Protocol
TP	True Positive
TSC	TKIP Sequence Counter

www.manaraa.com

TSN	Transitional Security Network
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIDT	Wireless Intrusion Detection Technique
WLAN	Wireless Local Area Network
WM	Wireless Medium
WPA	Wi-Fi Protected Access

www.manaraa.com

Chapter 1 Introduction

A wide variety of radio communication technologies are prevalent in today's rapid networking world. The most popular standard is the IEEE 802.11 family of wireless local area networks (WLANs). Beside home and small office usage, WLANs are also become a standard part of the enterprise networks.

Gartner points out the top three reasons for deploying WLANs in an enterprise which are [6]:

1. To improve productivity through mobility.
2. To provide access to places where wiring is impossible or too expensive to install.
3. To improve efficiency in specific business processes or operations.

Due to the vast interest in WLAN technologies, these wireless networks have matured a lot since ratification of the first 802.11 standard in 1997 [49]. Since then, several amendments have been made to the base standard[1], out of which most have been to the physical (PHY) layer to increase the operating speeds and throughput of WLANs. However, one amendment -IEEE 802.11i was ratified in 2004 to address the threats to confidentiality, integrity and access control in WLANs.

The security mechanisms provided by the base 802.11 standards suffered from a number of fundamental flaws and could easily be attacked. Until ratification of 802.11i, Layer 3 security mechanisms such as *Virtual Private Networks (VPNs)* were used to secure WLAN access. IEEE 802.11i introduces *Robust Secure Networks (RSNs)* and offers enhanced link layer security where confidentiality and integrity of WLAN traffic is protected using strong cryptographic algorithms and protocols, in addition, access control is implemented using 802.1X framework. *Extensible Authentication Protocol* (EAP) framework is used for authenticating peers. With the ratification of IEEE 802.11i, and the subsequent availability of implementations of the standard in current hardware, many of the security concerns surrounding the original wireless standards would seem to have been

[1] http://standards.ieee.org/getieee802/802.11.html

www.manaraa.com

addressed.

Despite enhanced 802.11i WLAN security, unfortunately security vulnerabilities still persist and RSNs remain vulnerable to a number of attacks. Failure of preventative measures to address all WLAN vulnerabilities suggests that it is a must to constantly monitor WLANs for security breaches, attacks, and intrusions to have any confidence in its security and operations. However, there is a lack of wireless intrusion detection techniques (WIDTs) that can reliably and accurately detect all possible attacks on IEEE 802.11i RSN WLANs.

1.1 Research Motivation

Unfortunately, despite ratification of the IEEE 802.11i, 802.11 WLANs still suffer from a number of security vulnerabilities. These vulnerabilities are caused by the existence of a number of unprotected frames in IEEE 802.11i RSNs such as Management, Control, and EAP frames. These unprotected frames can easily be forged and used to launch attacks on the RSNs. This problem is further exacerbated by the fact that almost all WLAN hardware permits the user to change its MAC address; hence permitting the user to spoof any MAC address. In addition, the 802.11i EAP authentication framework does not specify or provide guidance on which EAP method to use for authenticating peers. Unfortunately not all EAP methods are suitable to be used in WLANs [88,91], and use of an insecure EAP method due to a misconfiguration or lack of knowledge can defeat RSN security all together. The impact of misconfigurations on WLAN security is underlined by this statement from Gartner:

"...Even with the newest standards in place, WLANs and individual systems can become vulnerable to attack through misconfigurations, and unexpected and unwanted connections. Through 2010, 90% of WLAN security incidents will be the result of misconfigured systems (0.8 probability)..." [40]

Failure of preventative measures to address all RSN vulnerabilities makes it imperative to augment these measures with a monitoring framework which not only detects attacks and intrusions, but also

www.manaraa.com

provides security policy compliance checking. Monitoring of security policy compliance is of particular importance to high assurance and high security environments such as control systems and government facilities [88].

Such a monitoring system can be implemented using a Wireless Intrusion Detection System (WIDS) that monitors the airwaves constantly. Unfortunately, the currently available WIDTs are not very robust and reliable and are not able to detect all attacks on RSNs. The motivation for this work was to enhance the performance of WIDTs that can not only reliably detect RSN attacks and intrusions; but are also capable of security policy compliance monitoring.

1.2 Scope

All work in this dissertation is based on the IEEE 802.11 infrastructure WLANs[2] (see Section 2.2). The research is focused specifically on vulnerabilities, attacks and WIDTs for IEEE 802.11i RSNs. Pre-RSN vulnerabilities and attacks are not addressed in this work. No intrusion response techniques or mechanisms have been reviewed or discussed as part of this work. The sole focus of this dissertation is wireless intrusion detection for IEEE 802.11i RSNs. The work in this dissertation is also not based on statistical or mathematical modeling.

1.3 Research Aims

The aim of this research is to enhance the performance of wireless intrusion detection techniques that are capable of detecting all attacks on RSNs and can also detect violations of the site security policy. In summary, this dissertation aims to:

- Review security vulnerabilities that still exist in WLANs secured using IEEE 802.11i (specifically RSNs).
- Identify drawbacks and limitations of currently available wireless intrusion detection techniques and investigate if they are capable of reliably detecting attacks that exploit various outstanding RSN vulnerabilities.

[2]This includes all ratified amendments to the base standard

www.manaraa.com

- Enhance the performance of wireless intrusion detection techniques that address the gap left by current detection techniques in reliably detecting all attacks on RSNs.

1.4 Research Outcomes

The outcomes of this research have made contributions to each of the aims described above. These outcomes specifically are:

- A comprehensive review of the outstanding vulnerabilities and attacks in IEEE 802.11i RSNs.
- A comprehensive review of the wireless intrusion detection techniques currently available for detecting attacks on RSNs.
- Identifying the drawbacks and limitations of the currently available wireless intrusion detection techniques in detecting attacks on RSNs.
- Enhancing the performance of wireless intrusion detection techniques those detect RSN attacks.

1.5 Thesis Structure

This dissertation has been divided into five major chapters, which are structured around the aims of the research (as detailed in Section 1.3).

Chapter 2 provides background material regarding IEEE 802.11 WLANs, their operation and security. It discusses the security threats for WLANs and provides a discussion on weaknesses of Pre-RSN WLAN security measures. It also provides detailed background in IEEE 802.11i security and provides a comprehensive review of the attacks and vulnerabilities still relevant to RSNs.

Chapter 3 studies the relationship between these RSN vulnerabilities and analyses the current WIDTs in light of these relationships and dependencies. This chapter then provides insight into differences between wired and wireless intrusion detection. It then reviews the current WIDTs and identifies drawbacks and limitations of these in context of detecting attacks on RSNs. This chapter then identifies the requirements of an ideal WIDS which is used in Chapter 4.

Chapter 4 studies two anomaly based WIDTs to detect MAC spoofing activity -the *Received Signal*

www.manaraa.com

Strength Based Intrusion Detection Technique (RSSDT) and the *Round Trip Time Based Intrusion Detection Technique* (RTTDT). The usability and reliability of these techniques is tested using experimentation. This chapter also studies a correlation engine to correlate the detection results of the RTTDT and the RSSDT and hence enhance their reliability. Empirical evidence is then discussed to test the usability of the correlation engine. Finally the enhancement of the performance of these WIDTs is presented via a threshold optimization algorithm.

Finally conclusions and directions for future research are discussed in Chapter 5.

www.manaraa.com

Chapter 2 Security of 802.11 WLANs

The inherently broadcast nature of the wireless medium makes WLAN security significantly different from the security of the wired networks. Access to the physical medium is restricted by cables and buildings; however no such restrictions apply to the wireless medium. The broadcast nature of the medium exposes WLANs to passive eavesdropping and traffic analysis.

The WLAN standards acknowledge the security threats to WLANs and provide link layer security mechanisms to address these. However, early attempts at such mechanisms failed to address the security threats effectively and the WLAN security mechanisms have had to go through a number of revisions to get to their current robust and reliable state. Unfortunately, they still suffer from a number of vulnerabilities that can potentially be exploited to launch a number of attacks against WLANs.

This chapter provides a background in WLAN operations and reviews the evolution of WLAN security. It also reviews all outstanding security issues and attacks that can be used against WLANs protected using the latest WLAN security mechanisms. This chapter also identifies the common traits that can be used to detect such attacks using a wireless intrusion detection system.

2.1 History of 802.11 standards

In 1985, the Federal Communications Commission in USA opened several bands of the wireless spectrum for use without a government license. WLAN technologies started originating in 1990 when products operating in 900 megahertz (MHz) frequency band started appearing in the market. These products were proprietary, non-standard based and offered throughput of just 1 megabit per second (Mbps). In 1990, IEEE set up a new committee called 802.11 to investigate the development of a WLAN standard. The 802.11 WLAN standard was ratified in 1997 offering a maximum raw data rate of 2 Mbps [49].

IEEE 802.11 standard is a member of the IEEE 802 family, which specifies standards for local area networks (LANs). All 802 standards focus on the two lowest layers of the OSI model -Physical and Data link. All 802 networks implement a *Media Access Control* (MAC) component and a Physical

www.manaraa.com

(PHY) component; where PHY specifies details of the actual transmission and reception and MAC specifies how to access the medium and send data on it. The 802.2 standard specifies a common link layer that can be used by other lower layer 802 LAN networks -the Logical Link Control (LLC). IEEE802.11 is one such network that uses 802.2/LLC encapsulation. The 802.11 standard contains specification for the 802.11 MAC and PHY. The PHY is further subdivided into two sub layers -the *Physical Layer Convergence Procedure (PLCP)* and the *Physical Medium Dependent (PMD)*. The PLCP maps the MAC frames to the wireless medium and the PMD transmits these frames.

The 802.11 WLAN standard, ratified in 1997, supports three physical layers (PHY), where data can be transmitted via infrared (IR) signals or by either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) in the Industrial Scientific Medical (ISM) frequency band at 2.4 GHz. IEEE ratified two amendments to the 802.11 standard, namely 802.11a and 802.11b in 1999. These were changes to the802.11 PHY. IEEE 802.11b offers a theoretical raw data rate of 11 Mbps and operates in the 2.4 GHz ISM band using Direct Sequence Spread Spectrum (DSSS) Complementary Code Keying (CCK) modulation. Although 802.11b divides the 2.4 GHz spectrum into 14 overlapping channels whose center frequencies are 5 megahertz (MHz) apart, only 3 non-overlapping channels can be used at any one time. On the other hand, 802.11a operates in the 5GHz Unlicensed National Information Infrastructure (UNII) frequency band and uses a 52-subcarrier orthogonal frequency-division multiplexing (OFDM) with a maximum raw data rate of 54 Mbps. IEEE 802.11a offers 12 non-overlapping channels, 8 of which are dedicated to indoor and 4 to point to point. Due to differences in physical layer techniques, 802.11a is not interoperable with 802.11b.

IEEE confirmed another PHY amendment in June 2003 -802.11g. This standard operates in 2.4 GHz frequency spectrum and uses a mixture of OFDM and DSSS modulations to provide a raw data rate of up to 54 Mbps. IEEE 802.11g is backwards compatible with 802.11b, however it is not compatible with 802.11a. IEEE 802.11g's division of the 2.4 GHz frequency spectrum into channels is exactly the same as 802.11b.

المنارة للاستشارات
www.manaraa.com

The 802.11a, 802.11b and 802.11g amendments differ from the original 802.11 standard only in the physical layer (PHY) design. Apart from the PHY, these amendments introduce no other changes and specify the same Media Access Control (MAC) protocol as the original standard.

2.2 WLAN Network Topologies

Each 802.11 WLAN comprises of multiple network components which can be arranged in few different network topologies. The IEEE 802.11 WLANs consist of four fundamental architectural components namely:

- **Wireless Medium (WM)** -The medium used to transfer 802.11 WLAN frames between WLAN nodes[3].
- **Distribution System (DS)** -The logical component used to forward frames to their destination. It is usually implemented as a wired network, such as an Ethernet backbone.
- **Wireless Station (STA)** -Any device that accesses the wireless medium is essentially an STA. Usually this term is used to refer to endpoint devices such as laptops, desktops, mobile phones and other consumer electronics with 802.11 capabilities.
- **Access Point (AP)** -An AP is a specialized STA that provides connectivity between the various STAs and between the STAs and the distribution system (DS), which is usually a wired network.

For simplicity, throughout the dissertation, the term STA is used to refer to a non-AP device. The term *WLAN node* is used whenever referring to both APs and pure STAs.

Topologically, the basic building block of an 802.11 WLAN is the *Basic Service Set* (BSS). A BSS simply represents a group of STAs that can communicate with each other over the wireless medium and its coverage area is defined by the propagation characteristics of the wireless medium. If a station moves out of its BSS, it can no longer communicate with other members of the BSS. Each BSS is assigned a BSSID, which is a 48 bit binary identifier that distinguishes it from other BSSs. BSSs also

[3]The term *WLAN node* is used throughout this dissertation to refer to any WLAN entity that is capable of communicating using 802.11.

www.manaraa.com

have a 32 byte alphanumeric identifier called the *Service Set Identity (SSID)*. SSID allows another way of assigning identity to a BSS. BSSs can be divided into two structural configurations or designs, as follows:

- **Infrastructure BSS**: use APs to relay all information between the BSS STAs and the DS and between the STAs themselves. All communication in an infrastructure BSS occurs via an AP. All the STAs are required to be within the radio range of the AP; however no restriction is placed on the distance between the STAs themselves. Hence, an infrastructure BSS is defined by the distance from the AP. All STAs must establish *association* with the AP to obtain network access. In an infrastructure BSS, all STAs may associate with only one AP, however there is no limit on the number of STAs an AP may serve. In an infrastructure BSS, the BSSID is the MAC address of the wireless interface of the AP.
- **Ad-Hoc or Independent BSS**: has no central control entity such as an AP, but comprises of STAs in direct communication with each other over the wireless medium. STAs in an IBSS communicate directly with each other and hence must be within direct radio communication range. BSSID of IBSS WLANs is generated using random 46 bits.

While ad-hoc BSSs are typically used for creating short lived networks to support meetings or file transfers etc.; infrastructure BSSs are used as replacements or extensions of the conventional wired LAN segments and hence have become integral part of the information infrastructure. IEEE 802.11 also allows for creating networks of arbitrarily large size by chaining a number of individual Infrastructure BSSs together with a backbone network. Such a network is called an Extended Service Set (ESS). The SSID is same for all BSSs in an ESS.

This thesis focuses entirely on Infrastructure BSSs. Hereafter; all references to WLANs refer to Infrastructure BSSs.

2.3 WLAN Operations

In a WLAN, all nodes (STAs and APs) are identified by their 48 bit IEEE 802 MAC address and

www.manaraa.com

the frames are delivered based on the MAC address. This section discusses how access to the wireless medium is managed in WLANs and how WLAN nodes establish an association with the AP for data communication.

2.3.1 Media Access Control

802.11 uses a Carrier Sense Multiple Access (CSMA) scheme to control access to the wireless transmission medium. However, collisions in the wireless medium are expensive as they waste valuable transmission capacity, so rather than Collision Detection (CSMA/CD), 802.11 uses the Collision Avoidance technique (CSMA/CA).

Radio transmissions in unlicensed radio frequency bands are vulnerable to a high level of interference and noise due to radiations from a number of devices operating in that spectrum such as microwave ovens, cordless phones etc. In addition, multipath fading may also lead to frames not being received at the receiver node because it moved into a dead spot. Hence, 802.11 require a positive acknowledgment (ACK) for every transmitted frame. Every frame transmission from the sender node to the receiver and the receipt of its corresponding ACK from the receiver to the sender is an *atomic* operation. This means that a transmission is only considered successful if after transmitting a frame, the sender receives an ACK back from the receiver acknowledging the receipt of the frame. No other transmissions are permitted during this transaction. If either the frame or its ACK is lost, the sender has to retransmit the frame as it is considered lost.

Both the sender and the receiver WLAN nodes have to ensure that a third party node does not gain control of the network medium during the transaction as it would interfere with the operation's atomicity. Hence, besides physical carrier sensing, 802.11 also implements *virtual carrier sensing*. Physical carrier sense mechanism is provided by the PHY layer, whereas virtual carrier sense is provided by the MAC layer. If either of the mechanisms detects the medium to be busy, it is considered busy. To implement virtual carrier sense, every WLAN node has a *Network Allocation Vector* (NAV), which maintains a prediction of future traffic on the medium. It is a timer that represents the amount of

www.manaraa.com

time the medium will be reserved, in microseconds. The WLAN nodes reserve the medium by setting the *duration* field (see Section 2.3.2) in the frame MAC header to a value representing the expected time it would take for the frame's transmission and the receipt of its ACK (or any other necessary frame transmissions) to complete. All nodes that detect a unicast frame on the medium set their NAV values equal to the duration field of the detected frame. The virtual carrier sense mechanism considers the medium to be busy if the NAV has a non-zero value. A non-zero NAV is decremented every microsecond and only when NAV value reaches zero does the virtual carrier sense mechanism consider the medium idle. Hence, in this manner all other nodes besides the communicating nodes refrain from using the medium for the time period of the transmission.

Besides using the *duration* field of unicast frames to update NAV, 802.11 also allows for a special handshake to reserve the medium before the transmission commences. This mechanism is called the *RTS-CTS handshake*. Once a node has gained access to the medium, it uses the *Request-to-Send* (RTS) and *Clear-to-Send* (CTS) frames to reserve access to the medium for the duration of its transmission. The sender sends a RTS frame to the receiver node and the receiver responds with a CTS frame after a SIFS. The *duration* field in the MAC headers of both RTS and CTS frames contains the proposed duration of the transmission and other nodes which overhear either RTS, CTS or both, update their NAVs accordingly and defer access to the medium for this duration. Hence after the RTS-CTS handshake, the sender and the receiver can communicate without any interference from the other WLAN nodes for the duration of the transmission. The RTS-CTS handshake in itself is also an atomic operation.

All nodes that detect a RTS or CTS or both on the medium defer access for the duration contained in these frames. This ensures that all WLAN nodes between the sender and the receiver are aware of the transmission and will not attempt to access the medium during the transmission. RTS-CTS handshakes are also useful in areas with multiple overlapping WLANs where a large number of WLAN nodes contest for access to the medium. Despite being on different networks, all nodes on the

www.manaraa.com

same physical channel would receive the NAV and hence defer access appropriately.

2.3.2 Framing Details

IEEE 802.11 frames consist of the following four fields: a Preamble, a Physical Layer Convergence Protocol (PLCP) Header, MAC Data, and a Cyclic Redundancy Code (CRC). The Preamble is PHY dependent and contains training bit sequence for the antenna, the start frame delimiter and other synchronization information. The PLCP header contains logical information that is used by PHY to decode the frame such as the number of bytes contained in the frame, the rate information and a header error check field. MAC Data field contains the transmitted data and the CRC field contains an error detection checksum for the frame.

MAC Data field of an 802.11 frame (simply referred to as the MAC frame) consists of the following basic components:

- **Frame Control**: Contains the frame type information and other control information.
- **Duration/connectionID**: When used as duration field, it contains the time in microseconds; the medium will be allocated for successful transmission of a WLAN MAC frame. This field is used to update the NAV of WLAN nodes. In certain Control frames, this field acts as a connection identifier.
- **Addresses**: The number of address fields and their meaning changes as per the context. Address field types are source, destination, transmitting station and receiving station.
- **Sequence Control**: Contains a 12 bit sequence number, which is used to number the frames transmitted between a given transmitter and receiver and a 4 bit fragment number, which is used for fragmentation and reassembly. This field is only present in frames of type Management and Data.
- **Frame Body**: The frame body is variable in length and specific to the frame.
- **Frame Check Sequence**: The frame check sequence (FCS) contains an IEEE 32bit cyclic redundancy check (CRC).

www.manaraa.com

MAC frames used in 802.11 can be divided into three categories (types) namely:

- **Control:** Control frames provide MAC-layer reliability functions and assist in delivery of data frames.
- **Management**: These frames implement various services in WLANs and manage communication between STAs and APs.
- **Data**: Data frames are used to encapsulate upper layer data to be exchanged between WLAN nodes.

The Control frame subtypes are as below:

- *Power save-poll (PS-Poll):* This frame requests the AP to transmit buffered frames for a STA that has just woken up from power-save mode.
- *Request to Send (RTS):* This frame is used in the RTS-CTS handshake mechanism by a node to alert the destination and all other nodes in range that it intends to transmit a frame to the destination.
- *Clear to Send (CTS):* This is the second frame in the RTS-CTS handshake mechanism. It is sent from the destination node to the sender, as an acknowledgment of the RTS frame and to grant permission to the sender for sending a data frame.
- *Acknowledgment (ACK):* This frame is sent from the destination to the sender and is used as an acknowledgment for receiving immediately preceding unicast data, Management or PS-Poll frame correctly.

The Management frame subtypes are:

- *Association Request:* This frame is sent from an STA to an AP for requesting association with the AP's BSS and it contains the STA's capability information.
- *Association Response:* This frame is sent from the AP to the STA in response to the *Association Request* frame, indicating whether it is accepting the STA's request.
- *Reassociation Request:* Sent to an AP by an STA when it moves from one BSS to another BSS

www.manaraa.com

so that the new AP knows to negotiate with the old AP for forwarding old/buffered data frames. It can also be used to change the association attributes while remaining connected to the same AP.

- *Reassociation Response:* This frame is returned to the STA by the AP in response to the Reassociation Request, indicating whether it is accepting the STA's request.
- *Probe Request:* This frame is sent from an STA to another AP to obtain information about it. It is usually used to locate a BSS.
- *Probe Response:* This frame is sent back to the STA from the AP, in response to a *Probe Request* and contains information about the AP.
- *Beacon:* A Beacon is transmitted periodically by an AP, advertising the presence of the BSS and detailing the AP's capabilities. It assists the STAs in locating the BSS.
- *Disassociation:* This frame is used to terminate the association between an STA and an AP. This frame can be sent from either WLAN node (STA or AP).
- *Authentication:* These frames are exchanged between an STA and an AP to authenticate each other during establishment of an association.
- *Deauthentication:* This frame is used to terminate the authentication (and hence the association) between an STA and an AP. This frame can be sent from either WLAN node (STA or AP).

The data frame subtypes are:

- *Data:* This is the frame that actually performs encapsulation of upper layer data.
- *Null Function:* This frame does not carry any user data and is used for power management.

2.3.3 Network Operation

Every WLAN node keeps two state variables for each node it communicates with over the WM, namely the *Authentication state* and the *Association state*. The values for the *Authentication state* variable are *unauthenticated* and *authenticated*. The values for the *Association state* variable are

www.manaraa.com

unassociated and associated. These variables create three states locally on a node for each remote node it communicates with over the WM:

- State 1: Initial start state, unauthenticated, unassociated.
- State 2: Authenticated, unassociated.
- State 3: Authenticated, associated.

The current state between a source and destination node determines what type of frames can be exchanged between them. For simplicity, these three states are referred to as the *802.11 states* throughout rest of the dissertation. The allowed frames are grouped into classes, which correspond to states (mentioned above). The frame classes are as below:

- *Class 1 frames:* Class 1 frames are permitted in State 1, State 2 and State 3. They provide basic operations used by 802.11 nodes. Class 1 frames allow STAs to find a WLAN and authenticate to it. All STAs start at State 1 and successful authentication transitions them to State 2. Frames that belong to Class 1 are RTS, CTS and ACK Control frames ; Probe Request, Probe Response, Beacon, Authentication and Deauthentication Management frames and data frames with ToDS and FromDS frame control bits set to 0 (i.e. IBSS frames).
- *Class 2 frames:* Class 2 frames are permitted in State 2 and State 3 only. These frames manage associations between STAs and APs and can only be transmitted after the STA has successfully authenticated to the network. Successful association or reassociation transitions the STA's state to State3. Frames that belong to Class 2 are Association Request/Response, Reassociation Request/Response and Disassociation Management frames. If an AP receives a Class 2 frame from a non-authenticated STA, it sends a Deauthentication frame to the STA, hence dropping it back to State 1.
- *Class 3 frames:* These frames are permitted only in State 3 i.e. when the STA has completed both authentication and association successfully with the AP. In State 3, the

www.manaraa.com

STA is permitted to exchange data frames with the DS and use power management features provided by AP. Frames that belong to Class 3 are PS-Poll Control frame; Deauthentication Management frame and any data frames. If an AP receives Class 3 frames from an STA that is not associated, it sends a Disassociation frame back to the STA, hence dropping it to State 2. If the STA is not authenticated, the AP sends a Deauthentication frame, hence dropping the STA to State 1.

Figure 2-1 shows the 802.11 state diagram where each WLAN node transitions from State 1 to State 3 using Management frames. Once in State 3, data exchange with the DS and other WLAN nodes can occur. The Deauthentication and Disassociation Management frames cause transitions to State 1 and State 2 respectively and hence are used to terminate STA-AP associations.

Having discussed WLAN operations, now an overview of the state of WLAN security is presented in Section 2.4 and Section 2.5 and Section 2.6.

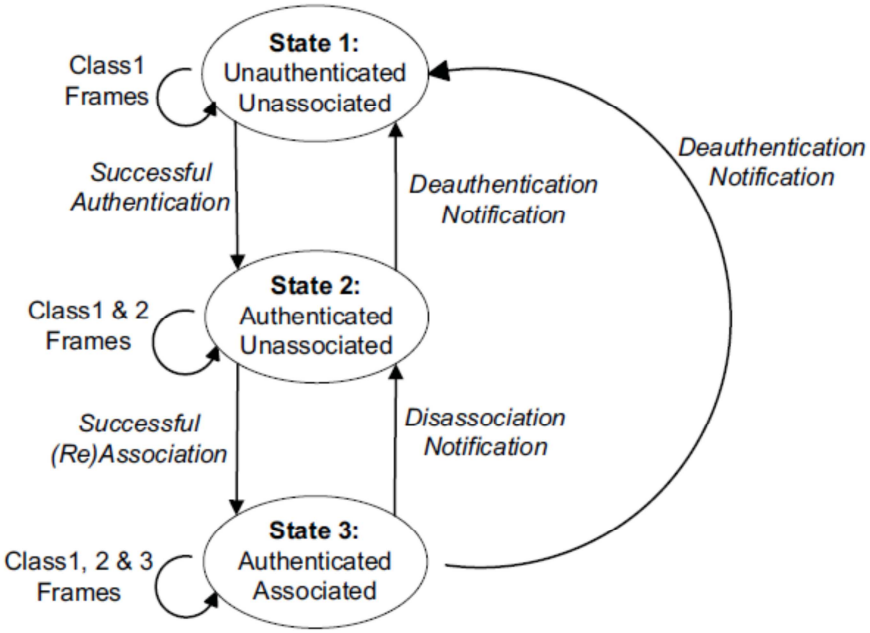


Figure 2-1: 802.11 State Diagram [48]

2.4 WLAN Security Objectives

Due to the shared nature of the wireless medium, WLAN security is uniquely different from wired network security. However, the security objectives for WLANs are similar to those of the wired LANs

www.manaraa.com

and other wireless networks. These are further discussed below [74]:

- **Confidentiality:** The WLAN must provide strong confidentiality protection of the data transmitted over it. No unauthorized parties should be able to read the communication between two legitimate WLAN nodes.
- **Integrity**: The WLAN must be able to detect any changes that happen to the data in transit, both intentional and unintentional. This also includes detecting retransmissions and replay protection.
- **Availability**: The WLAN and its resources should be accessible to all individuals and devices on demand. WLAN should prevent or at least mitigate against attacks on the usability of the network such as denial of service (DoS) attacks.
- **Access Control**: The WLAN should restrict the rights of the devices and individuals to access the network and its resources. The identities of WLAN nodes should be established and verified using strong authentication (mutual). Authorization and access control policies should be based on the results of such authentication.

However, the security challenges in WLANs are greater than those in wired networks due to the inherent characteristics of WLANs. Unlike wired networks, where the network access is provided via a network jack, the wireless medium is open to everybody within the transmission range of the network. Wired networks can secure their access by using physical security measures such as walls, doors, locks etc., whereas WLANS cannot control visibility of the network to devices within the transmission range. Interception of traffic in WLANs is as easy as running a WLAN compatible device in promiscuous mode. To launch an attack and inject traffic in a wired LAN, an attacker would have to either gain physical access to the network or compromise systems on it remotely. However, in WLANs the attacker simply needs to be within transmission range of the WLAN. To exacerbate the problem, an attacker can use high directional antennas to extend the range of the WLAN so that he/she is physically located miles away from the network and away from network administrator's or security guard's eyes.

www.manaraa.com

The mobility of the WLAN nodes also leads to more complex trust relationships between network components in WLANs as compared to wired networks.

Having discussed WLAN security objectives, the next section analyses the threats faced by WLANs due to their unique PHY and MAC protocol.

2.5 Threats

The threats to 802.11 WLANs can be divided into the following main categories [47, 74, 100]:

- **Threat 1. Traffic Analysis:** Traffic analysis refers to techniques used by an adversary to monitor the size and frequency of communications in a WLAN to collect information about the network communications. This threat is very real for WLANs as the adversary only requires a WLAN adapter in promiscuous mode to sniff all traffic on the WLAN. Assuming the WLAN traffic is encrypted, the adversary can still collect information such as number of nodes in the network, periods of high network activity, network topology and possibly network protocols used in the WLAN. Specialized radio equipment such as directional antennas make traffic analysis possible from a large distance from the WLAN. Unprotected Management frames such as *Beacon* and *Probe Response* also provide a lot of valuable information about the WLAN and assist in easy detection of the WLAN.
- **Threat 2. Passive Eavesdropping:** The broadcast nature of the wireless medium allows an adversary to passively collect all WLAN traffic, using a WLAN adapter in promiscuous mode, without ever associating with the WLAN or transmitting any traffic. The captured WLAN traffic can then be exposed to offline payload analysis, which can lead to information leakage or brute force key discovery attacks.
- **Threat 3. Message Modification, Deletion and Interception**: With ready access to the WLAN medium, an adversary can alter a legitimate message by deleting it, changing it, adding to it or reordering it. Message deletion can be achieved by interfering with the packet reception process on the receiver's antenna, for instance causing a CRC checksum error. Message

www.manaraa.com

interception refers to when the adversary captures a frame before the intended receiver can. This can be achieved by using two antennas simultaneously, one to cause CRC errors and collisions on the receiver and the other to capture frames.

- **Threat 4. Message Injection and Active Eavesdropping**: Unlike passive eavesdropping, active eavesdropping involves active traffic injection into the WLAN. The adversary not only monitors the WLAN traffic, but also injects traffic into the WLAN using message injection. Message injection refers to the traffic generation. Message injection can be easily achieved by using custom written software and normal off the shelf WLAN hardware. Message injection can be used for frame spoofing or inserting replayed frames into the WLAN. An adversary can send out frames with the spoofed source MAC address, BSSID and SSID of a legitimate AP and be able to lure unsuspecting STAs to associate with it. Using active eavesdropping, an adversary can also learn more about the WLAN by injecting custom frames and monitoring WLAN's reactions.
- **Threat 5. Unauthorized Access**: Wired networks require physical access to a network jack to obtain network association. However in WLANs, any adversary with a WLAN device can attempt to circumvent the access control and authentication mechanisms to obtain access to the WLAN. The threat of unauthorized access is further enhanced by the fact that most WLAN devices readily allow users to change their MAC addresses and hence change network identity. If access control checks are based merely on MAC address filtering, an adversary can easily obtain unauthorized access to the WLAN by simply eavesdropping WLAN traffic and creating a list of MAC addresses permitted to access the WLAN and then masquerading as those addresses.
- **Threat 6. Man-in-the-Middle**: The Management frames used in WLANs to manage associations between STAs and APs are not protected and no effort is made to authenticate the data origin or verify the integrity of these frames. Hence, an adversary can use spoofed

www.manaraa.com

Management frames to disconnect a legitimate STA from the network and then take over its connection with the AP by spoofing its MAC address. The adversary now receives all frames destined for the legitimate STA and sends out frames on its behalf. The adversary also starts up another AP with the same SSID as the legitimate AP on another channel. The legitimate STA establishes a connection with this fake AP and now the adversary can see all traffic between the legitimate STA and the legitimate AP. If the data encryption is weak or not implemented, then the adversary has full access to the payload of the traffic too. Unlike message interception, man-in-the-middle involves the adversary actively participating in the communication.

- **Threat 7. Session Hijacking**: Session hijacking is similar to man-in-the-middle, however after disconnecting the legitimate STA and taking over its connection with the AP, the adversary makes sure that the legitimate STA does not reassociate with the AP. Hence, the adversary uses the legitimate STA's session with the AP long after it has been forced off the network.
- **Threat 8. Message Replay**: If no replay protection is used, an adversary can monitor WLAN traffic passively and retransmit certain messages at a later stage, hence acting as a legitimate device/user. An example would be when an adversary captures the security association establishment between a STA and an AP and then later replays the messages from the STA to the AP, hence pretending to be the STA.
- **Threat 9. Denial of Service**: Denial of service (DoS) attacks in WLAN prohibit the normal use or management of the network and/or network devices. WLAN DoS attacks can be launched at both PHY and MAC layers. An adversary can use RF jamming devices to cause interference on communication channels or simply use Management frames of type Deauthentication or Disassociation to force legitimate WLAN STAs to terminate their network associations. MAC layer Management frames are not checked for authenticity of origin.

2.6 WLAN Security Evolution

Before ratification of IEEE 802.11i and its *Robust Security Network (RSN)* framework, IEEE

www.manaraa.com

802.11 suffered from a number of serious security weaknesses. This section explains Pre-RSN security shortcomings and how RSN addresses them.

2.6.1 Pre-RSN Security

To satisfy security objectives and threats identified in Section 2.5, the original IEEE802.11 specification uses a number of security mechanisms (Figure 2-2).

2.6.1.1 Data Confidentiality

The Wired Equivalent Privacy (WEP) protocol is used to protect confidentiality in the Pre-RSN 802.11 WLANS. WEP uses RC4 (Rivest Cipher 4) [85] stream cipher algorithm for encryption of data frames. The WEP standard specifies support for a 40-bit WEP key; however nonstandard extensions were introduced by vendors to offer keys of up to 128 and 256 bits. It also uses a 24 bit value as an initialization vector (IV) as seed to initialize the cryptographic key stream. Unfortunately, cryptographic technique used by WEP has known flaws. The 40 bit key is too short to prevent brute force attacks [16, 78]. Even use of a longer key does not prevent the high possibility of keystream reuse due to small size of the IV and a shared static key [99]. Concatenation of the IV and the shared WEP key has inherent weaknesses in generating per packet keys and an adversary can discover the key by eavesdropping 4,000,000 to 6,000,000 data frames [33, 92]. In 2004, it was shown that a 104 bit WEP key could be recovered from just 500,000 to 2,000,000 captured frames [77]. Later, in 2005, more correlations were discovered between the RC4 keystream and the WEP key which can be used to discover WEP keys[4]. Later, it was shown that it is possible to recover a 104 bit WEP key with a probability of 50% using just 40,000 captured packets and a success probability of 95% for 85,000 captured data frames [94].

WEP also provides no replay protection as it implements no incrementing counter, timestamp or other temporal data that could assist in detecting replayed data. Lack of replay protection in WEP assists in collecting the required traffic from a WEP protected network in a very short time [21].

[4]http://cage.ugent.be/klein/RC4/

www.manaraa.com

Hence, it has been proved beyond doubt that WEP confidentiality protection is flawed and should not be relied upon.

2.6.1. 2 Access Control and Authentication

Pre-RSN WLANs use two methods for authenticating the identities of WLAN devices *open system authentication*[5]and *shared key authentication*. The *open system authentication* is compulsory for IEEE 802.11 WLANs, whereas the *shared key authentication* is optional. *Open system authentication* is effectively a misnomer as it does not provide any identity verification. None of the communicating parties are actually authenticated. The *Shared key authentication* scheme is based on a unilateral challenge response mechanism and uses WEP encryption for response computation. Although it was supposed to be more robust than *open system authentication*, it actually is just as insecure. An adversary can trivially spoof the *shared key authentication* by simply eavesdropping the authentication session of a legitimate STA [10,16]. In fact using *open system authentication* can be more secure than *shared key authentication* as the latter can expose the keystream derived from the WEP key. During the *shared key authentication* WEP is used to encrypt the response by XORing the challenge with a pseudo-random keystream generated using a WEP key. An adversary can XOR the challenge and the response to reveal the keystream; which can later be used to authenticate [74]. *Shared key authentication* also does not implement mutual authentication (i.e. the AP is not authenticated) and it only authenticates devices and not users [30, p 91].

The access control mechanisms used in Pre-RSN WLANs are limited to the knowledge of the SSID and using MAC address filtering lists. Both of these are flawed and can easily be defeated as SSIDs are visible on the WLAN in clear text and majority of the WLAN hardware permits users to change their MAC addresses. An adversary can eavesdrop session from a legitimate STA and obtain the SSID and MAC address information. Now the adversary can obtain access to the WLAN by simply using the snooped MAC address and the SSID.

[5]A WLAN that requires only *open system authentication* for authenticating WLAN peers is referred to as *open WLAN* in this dissertation.

www.manaraa.com

2.6.1.3 Data Integrity

Pre-RSN WLANs use WEP to perform data integrity checking. WEP uses a 32 bit cyclic redundancy check (CRC-32) for protecting the integrity of each payload during transmission. The payload and the checksum are encrypted using RC4 before transmission. The encrypted CRC-32 checksum is called the *Integrity Check Value* (ICV). The receiver decrypts them, recomputes the checksum and compares against the transmitted checksum. Frame is dropped if checksums do not match. Unfortunately, ICV is subject to bit flipping attacks. This means that an adversary can arbitrarily modify a packet without detection or forge a frame with a valid ICV, without the knowledge of the key stream. Weak integrity protection also assists in plaintext recovery attacks such as inductive chosen plaintext attacks [9].

2.6.1.4 Availability

Pre-RSN WLANs implement no measures to protect the network against PHY and MAC layer DoS attacks. An adversary can use PHY layer *jamming* to render the frequencies unusable for the WLAN, hence causing a DoS. The *jamming* can also be caused unintentionally by other non WLANs devices operating in the same frequency band. At the MAC layer, the adversary can either inject a large number of spoofed frames in the WLAN (*flooding*); causing a DoS or use spoofed Management frames to degrade the security associations of WLAN nodes.

2.6.2 Interim Security Enhancement -WPA

Section 2.6.1 shows that WEP does not satisfy any of the security objectives identified in Section 2.4. Hence, IEEE commenced work on the IEEE 802.11i amendment. The WiFi Alliance[6] proposed *WiFi Protected Access (WPA)*to allow users to take advantage of their existing WEP compatible hardware and to provide an interim solution while 802.11i was getting ratified. WPA addresses all known WEP vulnerabilities without requiring new hardware.

Confidentiality protection is achieved in WPA using the *Temporal Key Integrity Protocol (TKIP)*,

[6]http://www.wi-fi.org/

www.manaraa.com

which still uses RC4; however unlike WEP it includes an extended IV space and a key mixing function to construct per packet keys. For integrity protection, WPA uses a weak keyed Message Integrity Code (MIC) computed using the *Michael* algorithm. The capabilities of the legacy hardware limited the choice of algorithms for WPA. WPA also implements replay protection by using per packet sequence numbers.

WPA provides two authentication mechanisms. In the first method, possession of a pre-shared key (PSK) is used to authenticate peers and a 128 bit encryption key, a 64 bit MIC key is also derived from the PSK for confidentiality and integrity protection. In the second method, IEEE 802.1X [50] and Extensible Authentication Protocol (EAP) [1] are used to provide strong authentication for the peers and fresh temporal keys are derived for confidentiality and integrity protection.

WPA however does suffer from some weaknesses, mainly due to limitations of the legacy hardware it was designed for. Although, the TKIP key mixing function is an improvement on WEP; it is possible to find the MIC given one per packet key [68]. This vulnerability discloses that parts of TKIP are weak on their own. To avoid negatively impacting performance on legacy hardware, Michael is designed to provide only 20 bits of security. This means that it is possible for an adversary to construct one successful forgery every 2^{19} packets. Thus countermeasures were implemented in Michael to limit the number of forgeries. However, these countermeasures may lead to DoS themselves [74]. Furthermore, 802.1X may be vulnerable to session hijacking and man-in-the-middle attacks [67] if mutual authentication and strong encryption is not used [93]. Hence, even TKIP is not suitable for high assurance environments and was always meant to be just an interim solution until everyone can upgrade to IEEE 802.11i Robust Security Networks (RSNs).

2.6.3 RSN Security

IEEE 802.11i was ratified in 2004 and is the sixth amendment to the baseline IEEE 802.11 standard and is designed to be the long term solution for WLAN security issues. The IEEE 802.11i specification introduces the concept of a *Robust Security Network (RSN).* A RSN is a WLAN security

www.manaraa.com

network that only permits the creation of *Robust Security Network Associations (RSNA)*. A RSNA is a logical connection between two IEEE 802.11 entities established using the IEEE 802.11i key management scheme called the *4-Way Handshake* (Figure 2-3). Moreover, RSNs achieves the following security objectives (Figure 2-2):

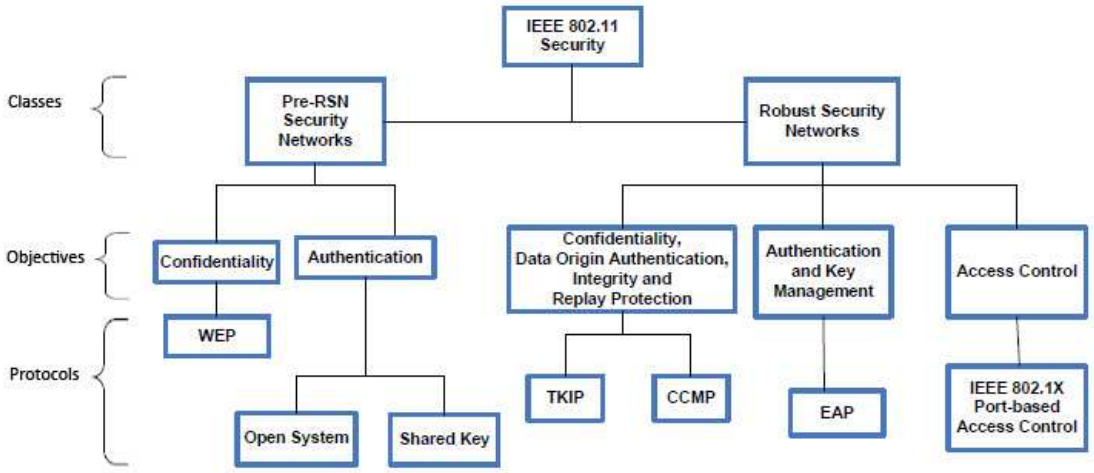


Figure 2-2: Taxonomy of 802.11 Security [74]

2.6.3.1 Data Confidentiality and Integrity

IEEE 802.11i defines two RSNA data confidentiality and integrity protocols -TKIP and Counter Mode with Cipher Block Chaining MAC Protocol (CCMP). TKIP has already been discussed in Section 2.6.2, so this section will concentrate on CCMP.

Unlike TKIP, which can be implemented on legacy WEP hardware via a software upgrade, CCMP requires new hardware. Support for CCMP is mandatory for any device claiming RSNA compliance, whereas TKIP support is optional. CCMP is based on the Advanced Encryption Standard (AES) [90] and uses its Counter with CBC-MAC operation mode with 128-bit block size [101]. CCMP uses the counter mode (CTR) for protecting data confidentiality and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for data integrity. CCMP protects the integrity of both the packet data and also portions of the802.11 header. It uses 128 bit session key to protect the duplex data channel. In addition, CCMP uses 48 bit packet number to construct a nonce to prevent replay attacks. This construction of the nonce allows for the key to be used for both integrity and confidentiality protection, without compromising either [57].

www.manaraa.com

2.6.3.2 Access Control and Authentication

IEEE 802.11i uses the IEEE 802.1X [50] standard to provide mutual authentication and exercise access control. IEEE 802.1X is an extensible framework for authenticating users. The actual authentication method is implemented using the Extensible Authentication Protocol (EAP) [1]. EAP provides a framework to use multiple methods for achieving authentication. The EAP framework is specified by the Internet Engineering Task Force (IETF) in RFC 3748; however the individual authentication protocols are not part of this RFC. In fact, the specific authentication protocols are specified in individual RFCs. For instance, RFC 2716 [2] specifies EAP authentication using transport layer security (EAPTLS). Numerous other EAP authentication methods exist such as EAP-SIM [45], EAPPOTP [76], and EAP-FAST [18], each specifying one separate method of achieving authentication over EAP.

However, not all EAP authentication methods are suitable for use in a WLAN environment. RFC 4017 [91] specifies the security requirements of EAP methods to be used for authenticating peers over a WLAN.

IEEE 802.1X authentication uses three main components: a *supplicant*, an *authenticator*, and an *authentication server (AS)*. In a WLAN, STAs are the *supplicant*, the AP is the *authenticator* and a RADIUS [83] server is usually used as the *authentication server*. Hereafter, these terms are used interchangeably. The authenticator merely passes authentication traffic between the supplicant and the AS. IEEE 802.1X uses port-based access control to control flow of data between DS and STAs. EAP authentication occurs via the *uncontrolled port* on the authenticator and non-EAP data frames pass through the IEEE 802.1X *controlled port*. The non EAP traffic is only permitted to pass through the *controlled port* once the supplicant has successfully completed IEEE 802.1X authentication with the AS.

Using this model, IEEE 802.1X blocks unauthorized access to the WLAN. The EAP over LAN (EAPoL) protocol is used to pass EAP messages between the supplicant and the authenticator over the

www.manaraa.com

WM and RADIUS [83] is the protocol most commonly used to exchange EAP messages between the AS and the authenticator. At the conclusion of a successful EAP authentication session, the AP's controlled port remains blocked. Even though the authentication is successful, the controlled port is only unblocked once the temporal keys have been negotiated and installed on the STA and the AP using the *4-Way Handshake*.

IEEE 802.11i also permits the use of a pre-shared key (PSK) for authentication. If PSK is being used the EAP authentication does not happen. However, *4-Way Handshake* is still used to negotiate temporal keys and unblock the AP's controlled port.

2.6.3.3 Availability

IEEE 802.11i does not introduce any measures to militate against the PHY and MAC based WLAN DoS attacks. The Management frames and Control frames still remain unprotected and hence can still be used to cause flooding and other spoofing based DoS attacks in WLANs. To exacerbate the problem even EAP and EAPoL frames remain unprotected and can be used to launch DoS attacks against the WLAN (see Section 2.7.5).

	Pre-RSN Security	**RSN Security**
Data Confidentiality and Integrity	1. WEP Protocol	2. TKIP protocol 3. CCMP
Access Control and Authentication	1. Open System 2. Pre Shared Key	1. IEEE 802.1X standard 2. Pre Shared Key
Availability	No protection against PHY and MAC layer DoS attacks	No protection against PHY and MAC layer DoS attacks

Table 1: Comparison between RSN and Pre-RSN

Table 1 summarizes the differences between RSN and Pre-RSN securities. We note that neither Pre-RSN nor RSN performs protection against PHY and MAC layer DoS attacks.

www.manaraa.com

2.6.3.4 RSN Key Management and Operations

This section discusses the RSNA establishment in detail. The RSNA establishment can be divided into five distinct phases (Figure 2-3):

- **Phase1: Discovery**: During this phase an AP advertises its capabilities and security policy using the RSN Information Element (RSN IE) in its Beacons and Probe Responses. The STA uses this information to select an AP to establish a security association with. During this phase the STA and the AP negotiate the confidentiality and integrity protocols for protecting unicast traffic, an authentication method for mutual authentication of the AP and AS, a cryptographic key management approach and pre-authentication capabilities.
- **Phase2: Authentication**: During this phase, the STA and the AS prove their identities to each other. For backward compatibility, the *open system authentication* step is still performed before IEEE 802.1X authentication occurs. During an EAP session, the authenticator (AP) does not participate in the authentication itself; it merely passes messages between the STA and the AS.
- **Phase3: Key Generation and Distribution**: During this phase, the AP and the STA perform several operations to generate and install cryptographic keys on the AP and the STA. During this phase, messages are passed only between the AP and the STA.
- **Phase4: Protected Data Transfer**: All data frames exchanged between the AP and the STA are cryptographically protected using cipher suites negotiated in the discovery phase. However, no end to end security is provided i.e. the frames are only protected between the AP and the STA.
- **Phase5: Connection Termination**: The security association between the WLAN and the STA is terminated.

www.manaraa.com

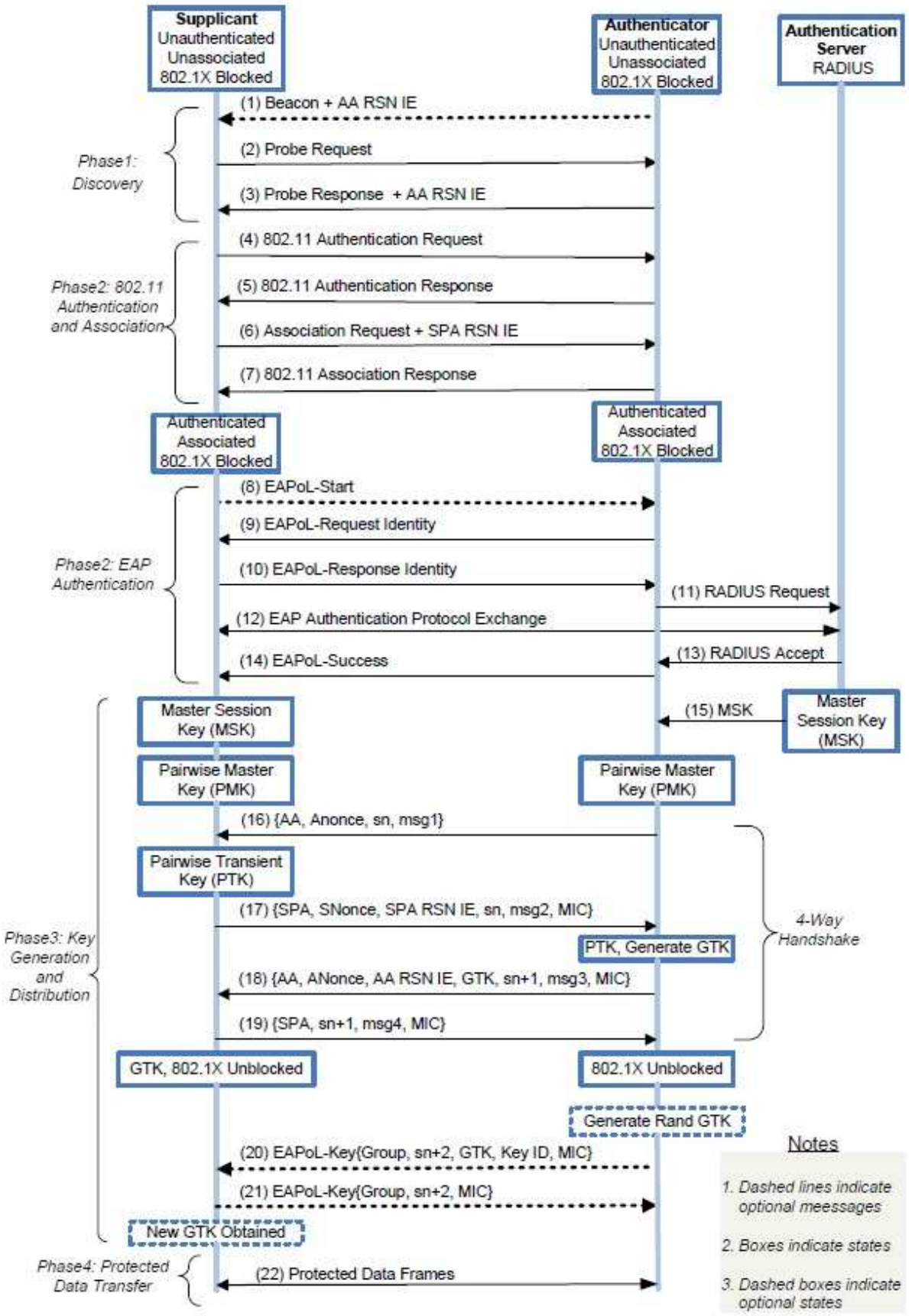


Figure 2-3: RSNA Establishment [46]

www.manaraa.com

2.6.4 Mixed Mode Networks

As shown in Section 2.6.1 and Section 2.6.3, IEEE 802.11i specifies two broad categories to classify security associations in WLANs: Robust Security Network Association (RSNA) and Pre-RSNA. Pre-RSNA comprises of associations based on WEP while RSNA is established using 802.1X authentication and *4-Way Handshake*. In a Robust Secure Network (RSN), APs do not allow associations from Pre-RSN STAs.

To facilitate migration of Pre-RSN networks to RSNs, IEEE 802.11i also allows for the creation of Pre-RSNAs and RSNAs in the same WLAN. Such a security network is called a *Transitional security network (TSN).* A TSN can be identified from the RSN IE in Beacons and Probe Responses as such a network uses WEP as its group cipher. APs in a TSN have to accept both Pre-RSNAs and RSNAs from STAs. TSNs are considered less secure than RSNs as they allow weaker security protocols to operate simultaneously with more secure protocols and algorithms. The Pre-RSNAs in a TSN can be attacked by an adversary and exploited to obtain access to the AP and/or other resources in the network (see Section 2.7.3).

2.7 Outstanding WLAN Security Issues

IEEE 802.11i has been designed to address all security issues – Except for Availability -related to Pre-RSN WLANs (see Section 2.6.1 and Section 2.6.2). As shown in Section 2.6.3, 802.11i RSNs fulfill all security objectives identified in Section 2.4.

For the sake of completeness, let's consider the threats identified in Section 2.5 in light of IEEE 802.11i RSNs. Traffic analysis is still a valid threat for RSNs as an adversary can still carry out analysis of traffic on the WLAN even if it is encrypted. However, only MAC layer information is available as the whole IP packet (including header) is encrypted. Such information leakage is considered less serious than IP layer traffic analysis. RSNs also only protect the data frames while the Management, Control and EAP frames still remain unprotected. However, use of CCMP in RSNs for confidentiality protection does address the threat of passive eavesdropping to some extent. RSNs do

www.manaraa.com

not protect the WLAN against eavesdropping; although the captured encrypted traffic is not vulnerable to offline brute force and key discovery attacks. Use of CCMP for integrity protection protects against the threat of message modification, while message deletion and message interception can still occur. The use of packet numbers for replay protection will assist the receiver in detecting these attacks. The threats of message injection and active eavesdropping are addressed in RSNs by the use of CCMP for confidentiality and integrity protection. An adversary will have to use the right keys to decrypt the frame and compute a valid MIC for the injected data traffic to be accepted by the AP. Message injection can still be carried out using unprotected Management, Control and EAP frames. The threats of unauthorized access, session hijacking and man-in-the-middle have been mitigated in RSN by using 802.1X based authentication that authenticates STAs and APs over EAP. The strength of the authentication depends directly on the EAP method chosen. A good EAP method should mutually authenticate both peers using cryptographic means. Not all EAP methods are suitable to be used in a WLAN environment [91]. The threat of message replay has been addressed by using packet numbers in RSNs; but there is no mitigation for DoS attacks based on PHY jamming or spoofed Management, Control or EAP frames.

Hence, stronger confidentiality and integrity protection combined with strong authentication in RSNs address most of the WLAN threats. However, the protection is only extended to data frames while the Management, Control and EAP frames still remain unprotected. No attempt is made to check the authenticity of the origin or content of such frames. Hence, DoS attacks based on injection of spoofed Management, Control and EAP frames are still a threat to RSNs. Such frames also assist in session hijacking and man-in-the-middle attacks if EAP methods with insufficient security are used [11]. Hence, it is still possible to perform traffic analysis, obtain information about the WLAN via passive eavesdropping, inject frames, spoof identity to gain unauthorized access and cause DoS using the unprotected Management, Control and EAP frames.

Hence, stronger confidentiality and integrity protection combined with strong authentication in

www.manaraa.com

RSNs address most of the WLAN threats. However, the protection is only extended to data frames while the Management, Control and EAP frames still remain unprotected. No attempt is made to check the authenticity of the origin or content of such frames. Hence, DoS attacks based on injection of spoofed Management, Control and EAP frames are still a threat to RSNs. Such frames also assist in session hijacking and man-in-the-middle attacks if EAP methods with insufficient security are used [11]. Hence, it is still possible to perform traffic analysis, obtain information about the WLAN via passive eavesdropping, inject frames, spoof identity to gain unauthorized access and cause DoS using the unprotected Management, Control and EAP frames.

Having discussed how the majority of the threats have been addressed in RSNs, the following sections discuss the attacks that can still be launched against RSNs[7].

2.7.1 Man-in-the-middle Attacks

RSN relies on EAP for authenticating the communicating peers effectively. As mentioned earlier, not all EAP methods are suitable to be used in WLANs as EAP was originally designed to provide authentication in wired point-to-point protocol (PPP) networks. IETF has produced RFC 4017 [91] to provide guidance on selecting EAP methods for WLANs.

Hence, to ensure security of the RSN, the EAP method should be carefully chosen to authenticate the peers. Most importantly, the authentication should be mutual and cryptographically sound. If the mutual authentication method is not implemented correctly [11], the RSN might be vulnerable to man-in-the-middle attacks. During the man-in-the-middle attack, the adversary disconnects the STA from the network using spoofed Management frames (usually Disassociation or Deauthentication) from the AP. Once the STA is disconnected from the network, the adversary can take over the STA's association with the AP by simply spoofing STA's MAC address and exploiting vulnerability in the EAP authentication method. Now the adversary starts up a fake AP with the same SSID as the legitimate AP on another channel. The legitimate STA, having been disconnected from the legitimate

[7]This discussion ignores *Traffic Analysis* and *Passive Eavesdropping* as real attacks as RSN protected data frames are considered secure and success of these attacks is subjective to what information adversary is looking for.

www.manaraa.com

AP, probes for the AP and finally associates with the fake AP. Now the adversary has access to the traffic to and from the legitimate STA [100]. Using such an attack, the adversary can learn the PMK[8].

2.7.2 Session Hijacking Attacks

Due to the existence of unprotected Management frames, session hijacking attacks are still possible in a RSN. Even if a strong authentication method is used for cryptographically authenticating the peers, an adversary can force a STA to terminate its security association with the AP by sending it a *Disassociation* Management frame with the spoofed source MAC address of the AP. Once the STA is disconnected from the network, the adversary can take over the STA's association with the AP by simply spoofing the STA's MAC address [67]. Now the adversary can receive all frames destined for the legitimate STA. However, to be able to decrypt this traffic and transmit traffic on behalf of the STA, the adversary still requires access to the relevant temporal keys. Hence, at no time is the confidentiality and integrity of the data compromised.

However, if the mutual authentication method is not implemented correctly this attack can lead to more serious information leakage. Now the adversary can successfully authenticate to the AP and can receive and decrypt all communication from the AP to the legitimate STA, while impersonating as the legitimate STA.

2.7.3 Security Level Rollback Attack

IEEE 802.11i does not permit Pre-RSNA algorithms when RSNA is being used. That is in a RSN, APs do not allow associations from Pre-RSN STAs. However, 802.11i does allow a *Transitional security network (TSN)* where Pre-RSNA and RSNA algorithms can co-exist. APs in a TSN have to accept both Pre-RSNAs and RSNAs from STAs. Unfortunately, when Pre-RSNA and RSNA algorithms are both permitted in a WLAN (TSN), an adversary can launch a *security level rollback* attack on WLAN nodes. Such an attack allows the adversary to avoid authentication and even lead to cryptographic keys being disclosed.

[8]As an aside, man-in-the-middle attacks in WLANs can also be launched using simple ARP poisoning [32]

www.manaraa.com

A security leve*l* rollbac*k* can be launched by an adversary by impersonating as the authenticator and sending forged Beacons and Probe Responses back to the supplicant indicating that only Pre-RSNA algorithms are supported. Alternatively, the adversary can forge the Association Request frames from the supplicant indicating that the supplicant only supports Pre-RSNA algorithms. Hence, the supplicant and the authenticator can be misleading into establishing a Pre-RSNA connection; despite them both being capable of RSNA algorithms. Since no cipher suite verification occurs in Pre-RSNA, this forgery goes undetected and the authenticator and the supplicant do not detect this attack. Now the adversary can attack the Pre-RSNA connection to reveal the cryptographic keys [47]. This attack requires timely injection of the forged Management frames as the authenticator or the supplicant.

2.7.4 Rogue AP

Although RSN requires STA and APs to authenticate each other using EAP, it is still possible for an adversary to start up a fake AP with the same SSID as a RSN AP and start transmitting Beacons and Probe Responses. Given that such Management frames are unprotected, it is possible for the adversary to easily forge such frames. Rather than a RSN, the fake AP implements an *open WLAN* which only requires *open system authentication*. This is done to avoid 802.1X/EAP mutual authentication, another scenario is that the adversary also implements a RSN, but uses a weak EAP method for authentication that does not perform mutual authentication and hence can easily be defeated. The STAs for which signal strength of the fake AP is stronger than that of the legitimate AP might migrate to the fake AP. Since the fake AP does not require 802.1X/EAP authentication, these STAs will associate with the fake AP without any authentication. Now the adversary can launch various upper layer attacks on the STAs associated to the fake AP and cause information leakage by convincing the STAs to reveal sensitive information such as passwords, encryption keys etc.

www.manaraa.com

2.7.5 Denial of Service Attacks

Availability is not treated as a primary objective in IEEE 802.11i; hence many DoS vulnerabilities still remain even if the strongest authentication, confidentiality and integrity protection is used. These DoS attacks can be launched at both the PHY and MAC layer and usually only require standard off the shelf WLAN hardware. The ease with which these attacks can be launched makes them a great threat to normal operations of WLANs. These attacks are discussed in detail now.

2.7.5.1 Algorithm and Protocol Based Attacks

A number of DoS vulnerabilities exist in RSNs due to flaws in RSN security protocols and algorithms. This section discusses attacks that exploit such flaws to their advantage.

Michael Algorithm Countermeasures: Due to restrictions of the legacy Pre-RSNA hardware, the Michael algorithm in TKIP only implements 20 bit security for data integrity protection. However, the designers of Michael realized that this was not enough security and a successful forgery can be constructed after just 2^{19} attempts. Hence, countermeasures were introduced to reduce the rate of successful forgeries for an adversary. All MIC failures are logged and if two MIC failures are detected within 60 seconds, all transmission and reception is ceased for 60 seconds, not allowing any new associations for STAs using TKIP. All temporal keys are erased and must be reinitialized and if 802.1X is being used and the control ports are blocked. These countermeasures effectively reduce the adversary's chances of learning more about the Michael key.

Unfortunately the countermeasures cause an obvious DoS condition where an adversary can construct two unsuccessful forgeries within 60 seconds and cause the connection to be reset and all communication to stop for 60 seconds. For addressing this DoS attack, the Frame Check Sequence (FCS), Integrity Check Value (ICV), TKIP Sequence Counter (TSC) and MIC are checked sequentially [47]. A MIC failure security event is only logged when FCS, ICV and TSC are correct but only MIC is invalid. This helps in detecting replayed packets and frame corruption caused by noise. If TSC is modified by the adversary, the frame will fail decryption and MIC failure will not be logged.

www.manaraa.com

Therefore, the DoS attack can be made more difficult by checking FCS, ICV, TSC and MIC in strict order. However, these measures still do not stop an adversary from launching a DoS using message interception, where the adversary intercepts a message for a recipient and forces the recipient to drop the same message (see Section 2.5), hence allowing the adversary to replay frames with valid TSC value. The adversary can forge a frame with valid TSC and an invalid MIC and adjust the FCS and ICV using weaknesses in the ICV algorithm. Now the adversary has a valid frame that will pass the FCS, ICV and TSC check but will fail the MIC check. The adversary can use these frames to cause a DoS [47].

RSN IE Poisoning: The RSN Information Element (RSN IE) contains information about the capabilities and the cipher suites used in the RSN. The RSN IE is used by an authenticator and a supplicant to negotiate security policy details such as authentication and key management protocols and cipher suites for data confidentiality and integrity protection. An authenticator inserts its supported RSN IE in the Beacons and Probe Response frames, while a supplicant inserts its chosen RSN IE in the Association/Reassociation Request frame. In particular, RSN IE contains authentication and pairwise key cipher suite selectors, an RSN Capabilities field, group key cipher suite selector, the Pairwise Master Key Identifier (PMKID) count and the PMKID list.

To protect the authenticator and the supplicants from security rollback attacks, where they are tricked into using weaker Pre-RSNA algorithms when both of them would otherwise use stronger RSNA security; the *4-Way Handshake* verifies the RSN IE selected by the supplicant and the authenticator. The supplicant is required to include the same RSN IE in Message 2 of the *4-Way Handshake* as was present in the Association/Reassociation Request frame. The authenticator bit-wise compares both these RSN IEs to confirm that they are the same. Similarly, the authenticator is required to send the same RSN IE in Message 3 of the *4-Way Handshake* as was included in the Beacon frame and the Probe Response Frame. The supplicant bit-wise compares these RSN IEs from the authenticator to check if they match exactly. If the RSN IE checks fail for the supplicant or the

www.manaraa.com

authenticator, the *4-Way Handshake* fails and both the authenticator and the supplicant deauthenticate each other and log a security event [20].

Unfortunately, in Message 3 of the *4-Way Handshake*, the RSN IE comparison is done before the MIC verification. Hence, an adversary can modify the RSN IE in Message 3 to cause the *4-Way Handshake* to fail. This causes a DoS condition, where a single modified message causes the authenticator and the supplicant to deauthenticate each other [47]. He and Mitchell [47] point out that even if this order was corrected and MIC was checked before the RSN IE, an adversary can still cause the *4-Way Handshake* to fail by injecting forged Beacons into the WLAN and poisoning the supplicant's record of the authenticator's RSN IE. These modified Beacon frames will be exactly the same as those of the legitimate authenticator; however some "insignificant" bits will be changed so that the 4-Way handshake commences but the bit-wise check fails when the supplicant compares the RSN IEs for the authenticator. This DoS attack is very easy to launch and requires minimum effort from the adversary while causing a lot of work for the victims.

4-Way Handshake Blocking: In a *4-Way Handshake*, the supplicant and the authenticator both generate nonces and send them to each other; which are used in combination with the MAC addresses of the peers and the PMK to generate the PTK. The supplicant's nonce is contained in Message 2, while Message 1 and Message 3 contain the nonce from the authenticator. Unlike other messages in the *4-Way Handshake*, Message 1 (from the authenticator) is unprotected and in clear text. Also the supplicant must accept all Message 1s generated by the authenticator to cater for frame loss and retransmissions. This allows an adversary to send a Message 1 to the supplicant with a random nonce value and hence corrupting the PTK calculations on the supplicant. This causes a DoS condition as the supplicant can no longer communicate with the authenticator as they do not share the same PTK [46, 47].

He and Mitchell [47] point out that this attack can be addressed if the supplicant stores all nonce values and their corresponding PTKs until Message 3 with a valid MIC is received, confirming which

www.manaraa.com

nonce (and hence PTK) to use. However, this exposes the supplicant to memory exhaustion DoS attacks as the adversary can send a very large number of forged Message 1s in a short interval. This attack is very easy to launch and requires very little work on the adversary's part.

2.7.5.2 EAP and EAPoL Based DoS Attacks

EAP is used in RSNs to provide authentication between the peers, however just like the Management and the Control frames, the EAP and EAPoL frames are transmitted in clear text and are not cryptographically protected. These frames can be used to cause a DoS by flooding the network with forged frames or negatively impact already established or in progress security associations between peers.

Security Association Deterioration Attacks: EAPoL-Star*t* frame is sent from the supplicant to the authenticator to commence authentication. An adversary can send a forged EAPoL-Star*t* frame to the authenticator on behalf of the supplicant. This frame will reset the 802.1X state machine for the supplicant and hence cause a DoS. Similarly, an EAP-Success frame is sent from the authenticator to the supplicant on successful completion of the authentication. An adversary can cause confusion and block the security establishment by sending forged EAP-Success frames to the supplicant while it is still undergoing EAP authentication for instance. EAPoL-Logof*f* frame is sent to the authenticator by the supplicant to indicate that the supplicant wishes to logoff from the network and the frame EAP-Failur*e* is sent from the authenticator to the supplicant on unsuccessful completion of authentication. Both EAPoL-Logof*f* and EAP-Failur*e* frames can be forged by an adversary to cause a supplicant to be disconnected from the network [47, 67].

EAP ID Exhaustion Attack: EAP frames use 8 bit field in their headers called the EAP ID as a session identifier. EAP ID assists in matching requests and responses in an EAP session. Given its small size, a flooding attack of forged EAP frames can exhaust the EAP ID space and hence prevent new EAP sessions from commencing [47].

- **Management Frame Based DoS Attacks**

www.manaraa.com

IEEE 802.11i makes no effort to protect the confidentiality or integrity of the 802.11 Management frames and nor does it attempt to authenticate the origin of such frames [47]. Recall from Section 2.3.3 that such frames are used by the 802.11 state machine and control the associations between STAs and APs. The Management frames are used to transition through the 802.11 state machine (from State 1 to State 3) and data exchanges can only happen in State 3. Deauthentication frames cause transition to State 1 from any state and Disassociation frames cause transition to State 2 if already authenticated (see Figure 2-1). This presents a very serious DoS vulnerability where forged Management frames (Deauthentication and Disassociation) can be used to negatively impact associations between STAs and APs [15]. To exacerbate the problem, these Management frames can also be sent to a broadcast destination MAC address. Hence a forged Deauthentication frame with spoofed source MAC address of the AP and destination MAC address set to broadcast will force all STAs in the BSS to terminate their associations and transition to State 1. This attack is particularly serious as it requires just one forged frame to cause a DoS condition in the whole BSS.

Besides using Management frames to cause state transitions, forged Management frames can also be used to cause DoS via flooding attacks where a very large number of frames are injected in the WLAN causing the AP to exhaust its resources. Management frames that can be used to launch such flooding attacks on the AP are *Authentication Request*, *Association Request* and *Reassociation Request*. DoS attacks based on forged Management frames with spoofed source MAC address of the STA or the AP can be launched using commercial off the shelf WLAN hardware and software.

- **Control Frame Based DoS Attacks**

Control frames are used for requesting and controlling access to the wireless medium and provide MAC-layer reliability functions. Like Management frames, 802.11 Control frames are also unprotected and can be easily forged by an adversary [47].

Before transmitting a frame, all nodes perform a clear channel assessment on the medium to check if it is busy. This check is performed by using both physical and virtual carrier sensing (NAV). An

www.manaraa.com

adversary can forge Control frames and set their *duration* field to an unusually high value so that virtual carrier sensing mechanism of all other nodes in the WLAN sense the medium to be busy for that period (see Section 2.3.1). By repeatedly injecting Control frames (such as RTS, CTS and ACK) with very high *duration field* values, an adversary can render the medium useless for all other WLAN nodes as it will always appear busy to them [15]. Such an attack is referred to as the *virtual jamming* attack as it uses the virtual carrier sensing mechanism for causing the DoS.

Another DoS attack can be launched by using the power-save mode of 802.11. IEEE802.11 permits a STA to enter a power saving (PS) mode to save battery life. During this mode, all the traffic destined to the dozing STA is buffered on the AP. The PS-Poll Control frame is used by the dozing STA when it wakes up from power-save mode to inform the AP to release its buffered frames. An adversary can also send a forged PS-Poll frame to the AP on behalf of the dozing STA and cause the AP to release all buffered frames for that STA before it has actually woken up. Hence, when the legitimate STA wakes up; it finds no frames buffered for it on the AP [15].

- **Carrier Sense Based DoS Attacks**

In 802.11, all nodes carry out carrier sensing before starting transmission to confirm that the medium is idle. This is achieved by using physical and virtual carrier sensing. However, the carrier sensing mechanism can be tricked using techniques at PHY and MAC layer by an adversary, to cause a DoS.

Radio Jamming Attacks: Radio jamming DoS attacks involve using radio equipment to transmit enough noise on the communication channel to render it useless for data transfer. Due to the level of noise on the medium, the physical carrier sensing would always conclude the medium to be busy. This is usually achieved by using specialized radio equipment that is capable of injecting noise in the same spectrum which the WLAN operates in. However, Wullems et al. [107] showed that radio jamming could be achieved by using commercial off the shelf WLAN equipment. They used a primitive of the physical layer management entity (PLME) that allowed 802.11b WLAN adapters to be placed in a test

www.manaraa.com

mode (PLME-DSSSTESTMODE) which made the WLAN adapters continuously transmit a specified bit pattern on a particular channel. These continuous transmissions rendered the medium useless for all other nodes in the BSS and caused a DoS.

NAV Based Attacks: As discussed in Section 2.7.5, an adversary can trick the virtual carrier sensing mechanism by injecting Control frames such as RTS, CTS and ACK with very high *duration field* values. All WLAN nodes that receive these frames update their NAVs and defer from accessing the medium accordingly. The same effect can be achieved by forging the duration field values of unicast data frames. This is referred to as *virtual jamming*.

Although the impact of this attack can be quite devastating, the real effects of this attack rely on how the WLAN nodes in their virtual carrier sensing mechanism are protocol compliant. Bellardo and Savage [15] reported that WLAN equipment they used in experiments completely ignored virtual carrier sensing and hence virtual jamming DoS had no effect on them.

2.7.6 Dictionary Attacks

IEEE 802.11i either uses 802.1X and EAP, or a simple Pre Shared Key (PSK) to negotiate the PMK between the authenticator and the supplicant. The PSK is 256 bits long and might be derived from a passphrase. A weak passphrase can expose the system to offline dictionary attacks on the passphrase, which in turn would result in disclosure of the PMK. IEEE 802.11i WLANs that operate in PSK mode should make sure that a good quality passphrase is always used or even better, a random 256 bit value is used as PSK. If an adversary obtains access to the PSK, he/she can compute the PMK and the PTKs for all data encrypted using that PSK in the past (given he/she also has access to the respective 4-Way Handshakes). Hence, unlike IEEE 802.1X/EAP authentication, PSK does not provide perfect forward secrecy. This makes choosing a good passphrase for the PSK even more important.

www.manaraa.com

2.7.7 Software Implementation Based Attacks

Besides factors such as protocol security flaws and oversights, vulnerabilities can also exist in WLANs as a result of insecure software implementations. Privileged software components such as WLAN device drivers are not usually written by security professionals, so their primary goal usually tends to be functionality and not security. Given that most drivers run as privileged processes in the operating system, any software vulnerabilities in them, if exploited, can potentially be catastrophic for the security of not only the WLAN node running the driver but also the whole WLAN. An adversary with privileged access to a WLAN node via vulnerability in its driver code can gain access to sensitive information such as the cryptographic keys and authentication credentials. Now the adversary cannot only masquerade as the victim node but also potentially use the system as a means to launch upper layer attacks on the WLAN infrastructure and other WLAN nodes. Such attacks on software implementations have been demonstrated to be quite realistic [66, 69] and in fact repositories have been established to catalog and address software based vulnerabilities in WLANs [108]. Given that techniques have been developed to determine the device driver of the WLAN node by simply monitoring its traffic [31, 34], the threat of vulnerable WLAN device drivers being used to compromise WLAN security becomes even more real.

Beside driver based vulnerabilities, vulnerabilities in complex software systems such as RADIUS servers can also be exploited using unprotected EAP/EAPoL frames. An adversary can inject forged EAP/EAPoL frames that contain a payload to exploit vulnerability in the RADIUS server software of the WLAN. This attack is particularly dangerous as once successful, the adversary has access to not only authentication credentials of all nodes on the WLAN, but he/she can use the RADIUS server to launch further attacks on the wired side of the network.

To further exacerbate the problem, in order to cut costs and simplify the hardware design, components of MAC implementations in WLAN hardware are being moved to software [80]. Where hardware usually hides the MAC implementations from prying eyes; software implementation exposes

www.manaraa.com

them to reverse engineering attacks, where an adversary can modify the MAC to cheat the 802.11 protocol and gain unfair advantage over other compliant WLAN nodes [82]. For instance, an adversary can modify the MAC implementation to ignore virtual carrier sensing and always choose the minimum value for the contention window in DCF. This can assist an adversary in modifying the MAC such that he/she can easily launch a number of attacks (such as DoS attacks) on other WLAN nodes; but at the same time protect himself/herself from similar attacks by being non-compliant to the protocol. For instance, an adversary can easily avoid being a victim of virtual jamming and Management frame based DoS attacks by simply ignoring such frames. Software modifications to the MAC can also be used by an adversary for stealth purposes and hiding his/her tracks [17].

2.7.8 RSN Vulnerabilities

Figure 2-4 shows taxonomy of all the RSN attacks discussed above. It shows how RSNs have improved the level of WLAN security over Pre-RSN networks. Unfortunately, as demonstrated by various attacks discussed in Section 2.7, RSNs still suffer from multiple vulnerabilities which negatively impact their security. Figure 2-4 also shows the vulnerabilities that allow various attacks to manifest in a RSN (labeled as Cause). These vulnerabilities are as below:

- **MAC Spoofing**

  It refers to the capability of the adversary to inject frames using the MAC address of another WLAN node. Almost all WLAN hardware permits the user to change the MAC address to any arbitrary value.

  In this dissertation, the term *spoofing* has been used to describe a scenario when an attacker injects frames in the WLAN with the source address of another node, and the term *masquerading* has been used as a specialization of the term *spoofing*. A masquerading attack is a spoofing attack, where the victim node is not active in the WLAN any longer. Hence, when an attacker *masquerades* as another node, it is the only node communicating with that identity (MAC address) in the WLAN. However, when an attacker *spoofs* as another node, there is no guarantee that the

www.manaraa.com

attacker is the only node using that identity in the WLAN.

- **Improper EAP Authentication**

It describes the scenario when the EAP method used for authenticating peers in a RSN is not robust enough.

- **Unprotected Management Frame**

It refers to the lack of confidentiality, integrity and replay protection for 802.11 Management frames. These frames are also not checked for authenticity of data origin.

- **Unprotected Control Frame**

It refers to the lack of confidentiality, integrity and replay protection for 802.11 Control frames.

- **Unprotected EAP/EAPoL Frames**

It refers to the lack of confidentiality, integrity and replay protection for EAP and EAPoL frames.

- **Software Vulnerabilities**

It describes vulnerabilities caused by software design and implementation.

- **Mutable and Unprotected Duration Field**

It describes how the *duration* field in the MAC frame header can be set to any arbitrary value by a WLAN node and negatively impacts the virtual carrier sensing in the WLAN.

- **Weak Passphrase**

It refers to selecting a weak passphrase for generating the PSK used for securing a RSN.

- **Michael MIC Weakness**

It refers to the weakness in Michael Algorithm where valid MICs can be forged.

- **Unprotected Message 1 of the 4-Way Handshake**

This vulnerability refers to the unprotected authenticator's nonce in Message 1 of the *4-Way Handshake*, which can be forged to cause the supplicant to calculate different PTK than the authenticator.

www.manaraa.com

- **Shared Nature of the Wireless Medium**

  This refers to the inherent broadcast nature of the wireless medium where the bandwidth is limited and has to be shared by all WLAN nodes operating. Excessive transmissions on the medium can consume most of the bandwidth and render it useless for other WLAN nodes.

Out of all the vulnerabilities mentioned above, *MAC Spoofing* is the most exploited one in all RSN attacks (see Figure 2-4). This vulnerability permits the adversary to inject forged frames (Management, Control, EAP) with the identity (MAC address) of any legitimate WLAN node. An adversary can easily forge frames that are unprotected in a WLAN. However, without MAC Spoofing, most of the unprotected frame vulnerabilities will be useless in terms of an exploit. A forged frame is only effective if it is injected using the MAC address of some other WLAN node (usually an AP). Also exploiting unprotected MAC frame *duration* field to cause a DoS is only possible in combination with *MAC Spoofing*. *Software Implementation Based Attacks* are also launched when an adversary injects forged frames into the WLAN using the MAC address of another WLAN node. These frames contain the payload to exploit the software vulnerability in the target system. Hence, *MAC Spoofing* in combination with unprotected frames (Management, Control, EAP/EAPoL) and unprotected MAC frame fields (duration) is responsible for majority of the attacks on RSNs. Even attacks that do not use *MAC Spoofing* directly would use it to launch further attacks on the WLAN. For instance, after an adversary has successfully obtained key material using the *dictionary attack*, it would use *MAC Spoofing* to authenticate to the WLAN using the key material and the MAC address of the victim node.

Another notable vulnerability is that of improper EA*P* authentication. The security of a RSN relies directly on the strength of the EAP authentication method implemented to authenticate communicating peers. Even though a wide variety of EAP methods are available, not all are suitable to be implemented in a WLAN [91]. If not implemented correctly, the seemingly secure EAP methods could become vulnerable to attacks such a Man-in-the-middle [11]. Hence, it is absolutely imperative to select the EAP method carefully to ensure security of a RSN.

www.manaraa.com

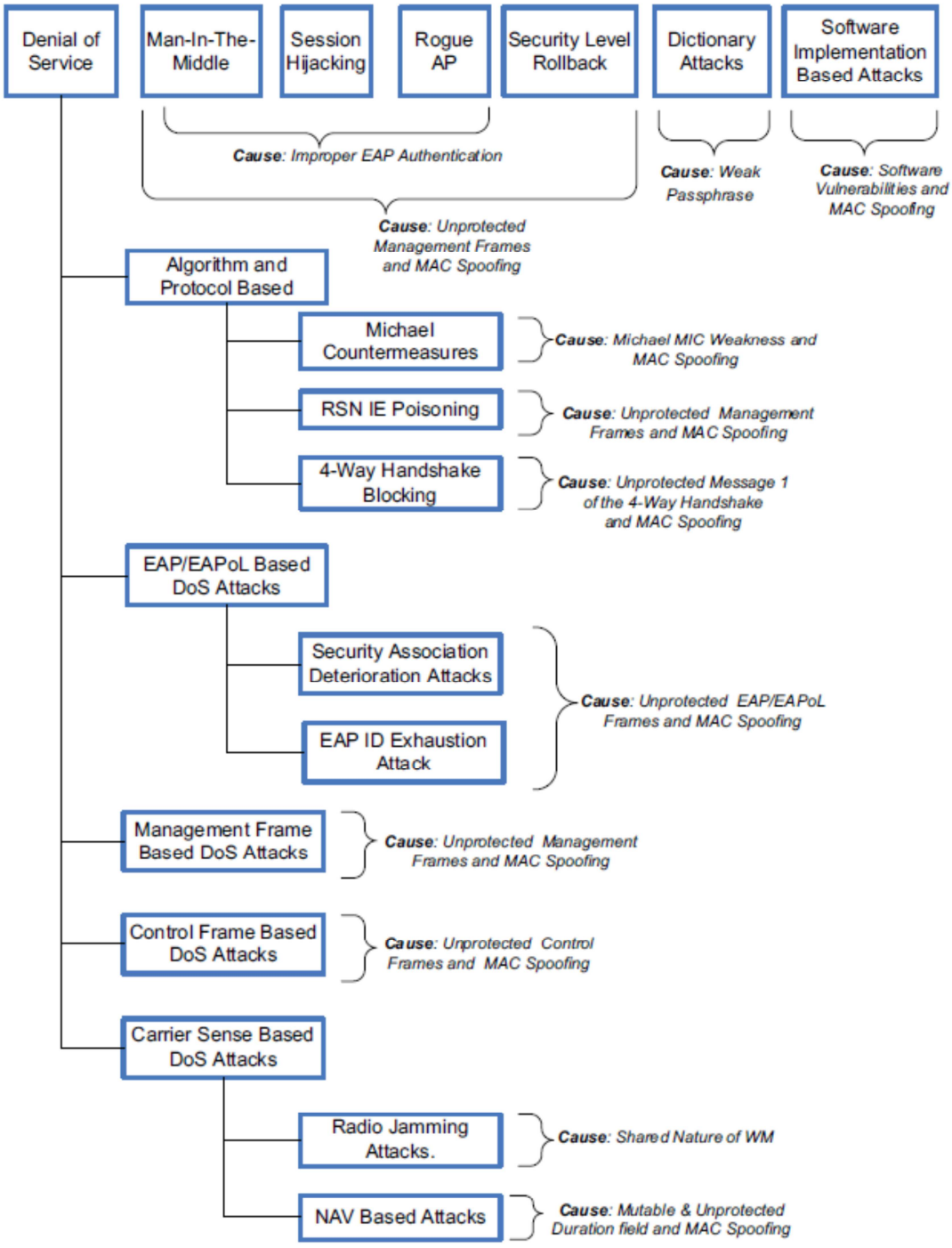


Figure 2-4: Taxonomy of RSN attacks

www.manaraa.com

Chapter 3 Existing Intrusion Detection Techniques for 802.11 WLANs

As discussed in Chapter 2, despite recent enhancements to their preventative security measures, WLANs still suffer from a number of security vulnerabilities and attacks. Hence, it has become vital to use wireless intrusion detection systems (WIDSs) to constantly monitor air waves for detecting attempts to exploit these vulnerabilities and acts of non-compliance to the WLAN security policy. Wireless intrusion detection systems act as second layer of defense to WLAN preventative security measures and help provide assurance that no malicious traffic or unauthorized activity is taking place on the network. Even sites with *no wireless* policy require WIDSs to monitor compliance to such a policy at all times.

This chapter provides a review of all the current wireless intrusion detection techniques (WIDTs) that have been academically published or have been used in open source WIDSs. This chapter then discusses the limitations of the current WIDTs in terms of their reliability and robustness. Finally this chapter identifies the need for new WIDTs to address the gap left by the current WIDTs and the requirements of an ideal WIDS.

The term *security policy* has been used throughout this dissertation to refer to the components of the security policy specific to WLAN deployment and usage such as WLAN authentication method(s), algorithms for cryptographic protection of confidentiality and integrity of WLAN data and key management algorithms.

3.1 Intrusion Detection

Computer systems and networks can be monitored by intrusion detection systems (IDSs) for security events. These security events can be well known attacks, abnormal activity or security policy violations. The reliability and robustness of IDSs is usually measured using the following three characteristics:

- **False Positive Rate:** The relative frequency of alerts incorrectly raised for benign and

www.manaraa.com

non-security related events.

- **True Positive Rate**: The relative frequency of alerts correctly raised for corresponding security events.
- **False Negative Rate**: The relative frequency at which the IDS fails to raise an alert for security events.

In this dissertation, the term *security event* is used to describe both attacks and security policy violations and an *intrusion* is defined to be a security event. The term *event of interest* is used throughout the dissertation to describe the events that an intrusion detection technique or system uses to detect security events. For the same security event, different intrusion detection techniques might have different event(s) of interest.

The IDSs can be divided into two categories based on the data source used for detecting intrusions:

- **Network Intrusion Detection Systems (NIDS)**: These analyze network events to detect intrusions.
- **Host-Based Intrusion Detection Systems (HIDS)**: These use events produced at the host computer(s) to detect intrusions.

The work presented in this dissertation is based around a NIDS.

The intrusion detection systems can be divided into two main categories depending on how their events of interest are established [12, 27, 38]:

- **Misuse-Based IDSs**: Require that patterns representing security events be explicitly defined. This pattern is usually referred to as a *signature*. The IDS monitors computer systems and networks looking for these signatures and raises an alert when it finds a match. The signatures are derived from known attacks or vulnerabilities and represent characteristics of the attack that must be present for the attack to succeed. These signatures can be provided to the IDS for detecting events of interest in two manners:
    - *Simple Signatures:* Events of interest for a misuse-based IDS can be defined as simple

www.manaraa.com

bit patterns [19] or regular expressions [79] associated with malicious code or exploit tool. These signatures are based on well-known unique characteristics of particular security events/attacks.

- *State Transition Models.* Events of interest for a misuse-based IDS can also be defined as state transition models that occur when a particular attack is carried out. The state transition model provides a sequence of events characteristic to a particular attack or security event. The modeling and analysis of state transitions as a technique for defining events of interest for misuse-based IDSs has been described by Ilgun *et al.* [52] and implemented as a tool called the *State Transition Analysis Tool (STAT).* STAT represents intrusions as signature actions, which are state transitions required for the intrusive activity to succeed. The misuse-based IDS uses these signature actions to detect security events.

A misuse-based IDS is able to detect only those intrusions and security events that it has been provided signatures for. It assumes that all other traffic and events are non-malicious. Hence, the major drawback of the misuse-based IDSs is that they require the system to have prior knowledge of characteristics of a particular attack or intrusive activity in the form of a signature. This limits the capabilities of misuse-based IDSs to the detection of only known attacks [27]. The *false negative* rate of the misuse-based IDS is inversely proportional to the comprehensiveness and completeness of the attack signatures provided to it.

As a result of signature based detection, misuse-based systems are highly accurate. Whenever an alert is raised by a misuse-based IDS, it is highly unlikely for it to be a *false positive* i.e. an alert raised incorrectly in response to non-malicious traffic. False positives in a misuse-based IDS only occur when the signatures used to describe the security events are not expressive enough to uniquely identify the attack. Misuse-based systems must be updated as new attacks or variants of existing attacks emerge, increasing the ongoing management complexity of misuse-based

www.manaraa.com

systems.

- **Anomaly-Based IDSs**: Anomaly-based IDSs on the other hand, do not require explicit signatures of security events. They use expected or non-malicious behavior and raise any deviations from this behavior as security events. Hence, events of interest to an anomaly-based IDS are deviations from the expected or normal behaviors of the monitored system, with intrusions defined as these deviations.

  The events of interest for anomaly-based IDSs can be defined in two ways:

  - *Statistical Models:* The statistical modeling approach is widely used to identify events of interest in anomaly-based systems. Variables and characteristics are measured over certain time scales by the IDS and statistically profiled to develop a baseline of normal or expected behavior of the monitored computer system or network. Divergence from this baseline exceeding a threshold will result in an alert being raised. This approach requires a certain training period for the IDS to develop an understanding of what is expected or normal behavior of the monitored entity. Presence of security events during this training phase can lead to the IDS treating even security events as normal behavior and hence increase the number of false negatives. Selecting the right variables and characteristics to profile is usually a daunting task and choosing the wrong attributes can lead to a high false positive rate.
  - *Specification-Based Models:* In recognition of the difficulty and room for error in training anomaly-based IDSs based on statistical models, another approach has been suggested called the *specification based model* [86, 97, 98, 38]. Specification based anomaly detection does not rely on a learning phase or collecting statistics representing the correct behavior of the monitored system or network. Instead the expected correct behavior is explicitly provided in a declarative manner. This is referred to as a *specification*. Deviations from this specification are treated by the IDS as security

www.manaraa.com

events. A specification can be based on state transitions that would occur during normal behavior and/or specify correct behavior based on the security policy in a declarative fashion. Sekar *et al.* [86] combine state machine protocol modeling with statistical techniques to develop an anomaly-based IDS.

The major strength of the anomaly-based IDSs is that they are capable of detecting both existing and novel attacks without having to be reconfigured or updated in any manner [27]. The statistical model based systems tend to suffer from a higher rate of false positives, which depends directly on the accuracy of the model, the characteristics profiled and the quality of the training phase. The *false negative* rate of an anomaly-based IDS is directly proportional to the comprehensiveness and completeness of the statistical models or the specification used.

	Misuse-based IDS	**Anomaly-based IDS**
Used method to identify Intrusions	Signatures	deviations from the expected behaviors of the monitored system
Detection models	Simple signatures – State transition models	Statistical models – Specification models
Rate of false positives	Very low	High
Rate of false negatives	Proportional to the completeness of attack signatures	Proportional to the completeness of training

Table 2: Comparison between IDS categories

Table 3-1 summarizes the main differences between the two IDS categories. Figure 3-1 presents a summary of the IDSs and the models they use for detecting intrusions and other security events. The intrusion detection techniques used by a misuse-based system are referred to as *misuse-based*

www.manaraa.com

techniques and those used in an anomaly-based system are called *anomaly-based techniques*. The anomaly based and misuse-based techniques are used by both wired and wireless intrusion detection systems for detecting intrusions and malicious activity. Wireless intrusion detection systems however do specialize in detecting WLAN specific security events. These differences between wired and wireless intrusion detection systems are discussed in the next section.

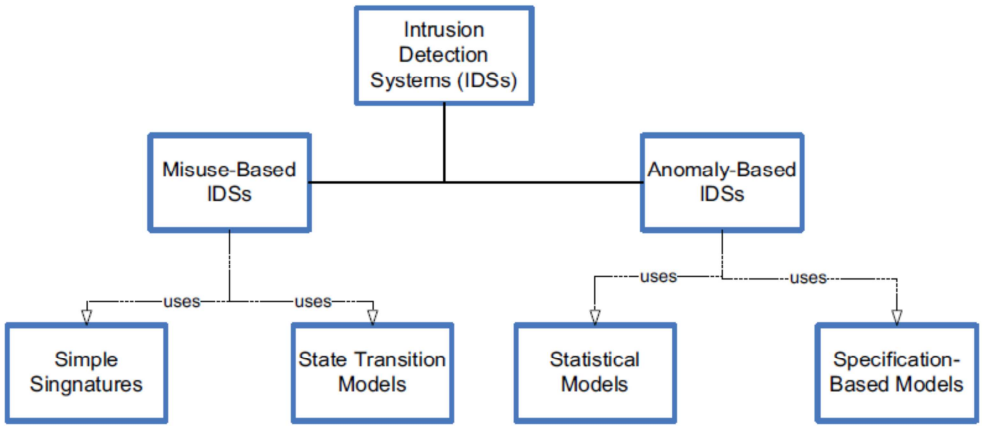


Figure 3-1: Intrusion Detection Systems (IDSs)

3.2 Wireless vs. Wired Intrusion Detection

Intrusion detection systems in wired networks are quite different from WIDSs. Although both of them are designed to detect security events of interest, they both operate at different OSI layers [26]. While wired IDSs mostly concentrate on OSI layers 3 (*Network*) and above; the WIDS specialize in detecting attacks exploiting protocols and mechanisms at the lower two layers (*Physical* and *Data Link*). The remainder of this section discusses other differences between wired and wireless intrusion detection systems. They are as below:

- Wired IDSs can be strategically placed at choke points in the network so that they have a complete view of the network. Given the nature of the wireless medium and radio communication, a WIDS sensor can only capture traffic in its radio range. Hence to obtain a complete picture of the WLAN, a WIDS has to use multiple sensors strategically placed through the WLAN. Within themselves, the sensors should be able to capture all WLAN traffic. To further explore the

www.manaraa.com

problem, different 802.11 PHY layers tend to operate at different frequencies and permit the existence of a number of radio communication channels for the WLAN nodes to communicate over. Hence to be able to capture all traffic on the WLAN, dedicated sensors have to be deployed for monitoring each channel and frequency throughout the WLAN or the sensors have to use some sort of sampling algorithm where the sensor periodically switches between different channels and frequencies. One technique is where each channel is observed for an equal, predetermined length of time. Another sampling strategy weights the time spent on each channel according to the number of frames observed on that channel [29]. Choosing the wrong channel sampling strategy for the WIDS sensors can lead to loss of traffic for the WIDS [110].

- Wired IDSs cannot see the Management and Control frames in a WLAN. They also do not see the EAP frames exchanged between the STAs and the APs. Hence a wired IDS cannot detect attacks based on these unprotected frames (see Section 2.7 and Figure 2.3). All data traffic within the WLAN (one STA to another) is also switched directly between the two communicating STAs via the AP. Hence, any malicious payload delivered via these data frames from one peer to another would go undetected by a wired IDS.
- Wired IDSs also cannot detect PHY and MAC layer based jamming attacks. Both radio and virtual jamming are DoS attacks against the shared wireless medium, which result in other WLAN nodes not being able to access the medium.

Unlike WIDSs, the wired IDSs cannot assist in identifying the physical location of an unauthorized node, rogue AP or an adversary within the WLAN [73]. WIDSs provide this feature by using the distributed nature of their sensors throughout the WLAN. Depending on which sensor raised the alert, the offending WLAN node can be placed somewhere near the physical location of that sensor. If multiple sensors raise the alert, triangulation of the received signal strengths can be performed to calculate more accurate location parameters of the offending node.

MAC spoofing is the root of all injection attacks in WLANs (see Section 2.7). A wired IDS does

www.manaraa.com

not have access to any information regarding the WLAN node to make a decision about whether a particular frame has come from the legitimate node or an adversary spoofing its MAC address.

Hence, WIDSs have a unique part to play in the security of WLANs. They can be used along with wired IDSs in a complementary manner, where WIDS detects intrusions at MAC and PHY layers and wired IDS monitors for upper layer intrusions. Table 3-2 summarizes the capabilities of Wired IDSs versus WIDSs.

Wired IDS	WIDS
Operates at OSI layer 3 (network) and above	Operates at OSI layer 1 (Physical) and layer 2 (Data Link)
Usually placed at choke points in the network for maximum network visibility	Uses multiple (dedicated) radio sensors for complete network coverage
Unable to detect attacks based on 802.11 unprotected frames	Capable of detecting attacks based on 802.11 unprotected frames
Cannot detect PHY and MAC layer based jamming attacks	Capable of detecting PHY and MAC layer based jamming attacks
Unable to assist in identifying the physical location of an unauthorized node, rouge AP, or an adversary within the WLAN	WIDSs provide this feature by using the distributed nature of their sensor throughout the WLAN
Unable to monitor the WLAN activity for securing policy compliance violations (EAP method, weak ciphers etc.)	Has complete visibility of such violations
Unable to determine if a WALN node is MAC spoofed	Capable of MAC spoof detection for WLAN nodes

Table 3: Wired IDS versus WIDS

www.manaraa.com

WIDS usually use a centralized-distributed design. In such a design, sensors are distributed throughout the WLAN, which silently capture all WLAN traffic and pass their captured traffic to the centralized components of the WIDS for intrusion detection. Some examples of the commercial WIDSs are AirDefense [53], AirMagnet [54] and AirTight Networks [71]. Some open source WIDS have also been developed such as Snort-Wireless [8] and WIDZ [64]. This dissertation does not discuss the commercial WIDSs and uses academic publications for its discussions. Even though a number of different WIDTs and WIDSs have been proposed in academic research, many of them have not actually been implemented in an open source system. The next section discusses all current WIDTs based on academic publications and open source systems.

3.3 Wireless Intrusion Detection -State of the Art

As discussed in Section 2.7.8, the IEEE 802.11i RSNs do not address all vulnerabilities that can be exploited in a WLAN to launch an attack. To be able to detect all possible attacks on a RSN, a WIDS should employ intrusion detection techniques that are aware of these vulnerabilities and are capable of recognizing when these vulnerabilities are being exploited in a WLAN.

Figure 3-2 shows the relationship between all the RSN vulnerabilities discussed in Section 2.7.8. The RSN vulnerabilities have been hierarchically arranged in Figure 3-2, which shows that almost all RSN vulnerabilities depend on the *MAC Spoofing* vulnerability to be exploited. This means that almost all attacks that exploit RSN vulnerabilities use MAC spoofing to carry out the exploit. Use of CCMP for confidentiality and integrity protection in RSNs has removed the threat of eavesdropping based passive attacks such as brute force and other key discovery attacks on the captured WLAN traffic. Hence, all attacks in RSNs (see Section 2.7) perform active injection of forged frames into the WLAN using spoofed identity (MAC address) of another WLAN node. Hence, almost all RSN vulnerabilities rely directly on the MAC Spoofing vulnerability to be exploited.

The vulnerabilities that depend on MAC spoofing to be exploited can be broken into two main categories: *Protocol Limitations*, and *Security Policy Violations*. These categories are based on the

www.manaraa.com

nature of the vulnerabilities themselves.

The *Protocol Limitations* category contains vulnerabilities which result from limitations, oversights and flaws in protocols and algorithms. The vulnerabilities categorized under *Protocol Limitations* are the ones concerning unprotected Management, Control and EAP/EAPoL frames. This category also includes the *Mutable and Unprotected Duration Field* vulnerability, the *Unprotected Message 1 of the 4-Way Handshake,* and the *Michael MIC Weakness* vulnerability.

On the other hand, the *Security Policy Violations* category includes the *Weak Passphrase* and the *Improper EAP Authentication* vulnerabilities. This is because they are clearly violations of a good RSN security policy which would always state to use a strong PSK passphrase and a robust EAP method for 802.1X authentication. Essentially, this category *includes* vulnerabilities whose exploits relate to ANY security policy non-compliance.

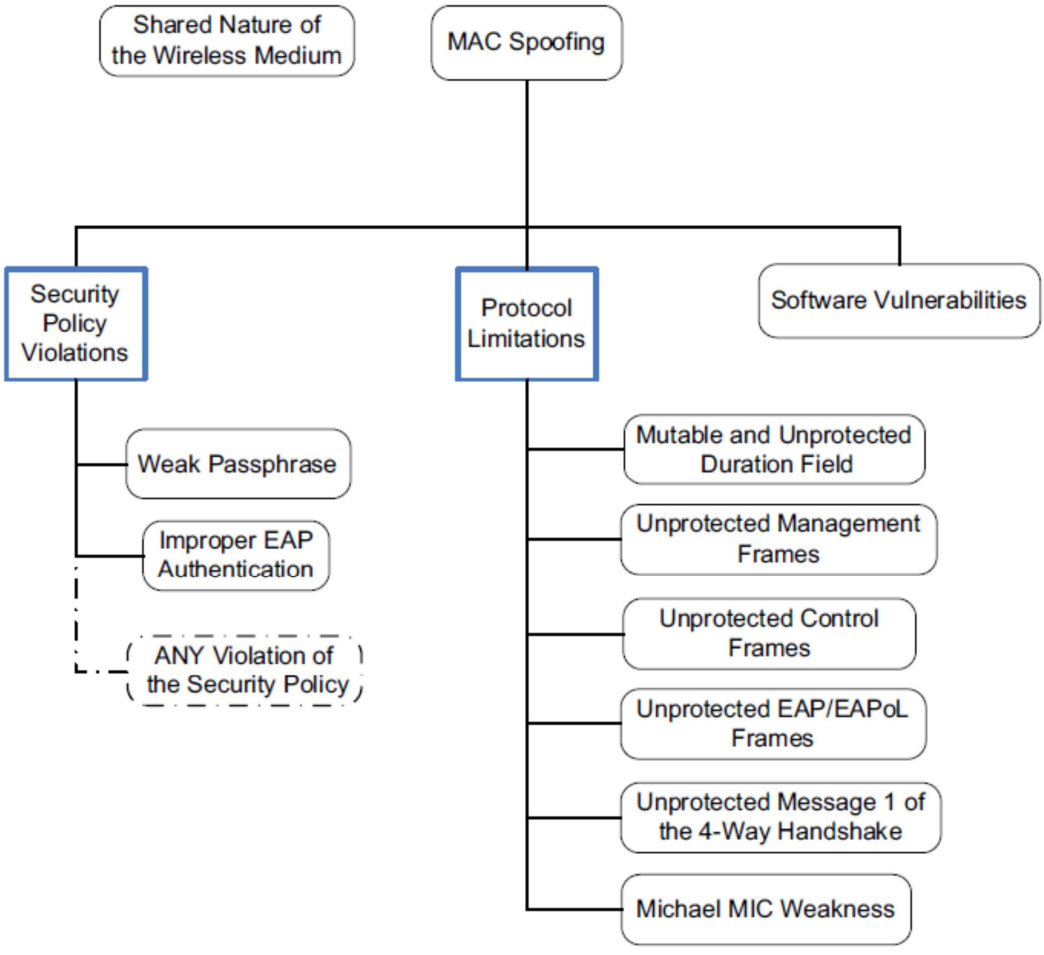


Figure 3-2: Categorization of RSN Vulnerabilities

www.manaraa.com

Although RSN attacks that exploit software vulnerabilities in protocol implementations, drivers and software sub systems, do not use MAC spoofing directly, the forged frames that carry the exploit code are injected in the WLAN using MAC spoofing. Hence, *Software Vulnerabilities* depend on the *MAC Spoofing* vulnerability too. It is not categorized under either of the other two categories as it is neither a security policy violation nor a protocol limitation.

The hierarchical distribution and categorization of the RSN vulnerabilities was performed to assist in the analysis of existing WIDTs. Since the vulnerabilities listed and categorized in Figure 3-2 represent all the RSN attacks currently known; WIDTs that address these vulnerabilities would certainly be able to detect all known RSN attacks and even the ones that are not currently known but somehow exploit the vulnerabilities discussed above.

A discussion of the existing WIDTs is now presented using the vulnerability hierarchy discussed in Figure 3-2.

3.3.1 Wireless Intrusion Detection Techniques for MAC Spoofing

As discussed in Section 2.7.8, the RSNs suffer from a number of security vulnerabilities; out of which the ability to spoof a WLAN node's MAC address is the most serious one. MAC spoofing allows an adversary to assume the MAC address of another WLAN node and launch attacks on the WLAN using the identity of the legitimate node. Without this vulnerability, an adversary will not be able to inject forged frames (Management, Control, EAP) into the WLAN and all attacks based on injection of such frames would be impossible. Some of these attacks are *Man-in-the-Middle*, *Session Hijacking*, *Rogue AP*, *Security Level Rollback*, *RSN IE Poisoning*, *EAP based DoS* attacks, *Management* and *Control* frame based DoS attacks (see Section 2.7 for details of these attacks). Even exploiting the unprotected MAC frame *Duration* field to cause a DoS (virtual jamming) is also only possible in combination with *MAC Spoofing*. *Software Implementation Based Attacks* are also launched when an adversary injects forged frames containing exploit code into the WLAN using the MAC address of another WLAN node. The *4-Way Handshake Blocking* and *Michael*

www.manaraa.com

Countermeasures DoS attacks are also launched using forged frames with spoofed MAC addresses.

The use of CCMP for confidentiality and integrity protection in RSNs has removed the threat of eavesdropping based passive attacks such as brute force and other key discovery attacks on the captured WLAN traffic. Hence, most attacks in RSNs are performed using active injection of forged frames into the WLAN using spoofed identity (MAC address) of other WLAN nodes. Even attacks that do not use *MAC Spoofing* directly exploit it in post attack activity. For instance, after an adversary has successfully discovered key material using the *Dictionary Attack*, it would use *MAC Spoofing* to authenticate to the WLAN using the key material and the MAC address of the victim node.

Hence, *MAC Spoofing* is responsible for majority of the attacks on RSNs. Refer to Figure 3-2 to understand how almost all RSN vulnerabilities depend on MAC spoofing for them to be exploited. Spoofing based attacks in WLANS are possible as the existing WLAN standards fail to address the lack of authentication of unprotected WLAN frames and network card addresses. To further exacerbate the problem, almost all WLAN hardware provides a mechanism to change its MAC address; hence trivializing changing identities.

MAC Spoofing is the root cause of all injection based attacks on RSNs. A number of different techniques have been suggested to detect MAC spoofing activity in a WLAN. These are discussed below:

Sequence Number Monitoring: One approach for detecting MAC spoofing is based on using the Sequence Control field in the 802.11 MAC frames (see Section 2.3.2). This 2 byte long field contains a 12 bit sequence number, which is used to number the frames transmitted between a given transmitter and receiver and a 4 bit fragment number, which is used for fragmentation and reassembly (see Figure 3-3). The 802.11 protocol requires all WLAN nodes to monotonically increment the 12 bit sequence number field in the MAC header for each transmitted Management and Data frame[9]. Abrupt changes in sequence numbers for a particular MAC address are used as an

[9]Control frames do not have sequence numbers

www.manaraa.com

indicator of MAC spoofing. The assumption is that both the legitimate node and the adversary would be at different sequence numbers at any point in time and the frames transmitted by the adversary, using the MAC address of the legitimate node, will not contain the sequence number expected next for the legitimate node. When the adversary's frames and the legitimate node's frames interleave, a large gap in the sequence numbers is registered; which clearly indicated MAC spoofing.

This approach was first suggested by Wright [102] and was later used by Godber and Dasgupta [43] for detecting rogue APs. Kasarekar and Ramamurthy [58] have suggested using a combination of sequence number checks along with ICMP augmentation for detecting MAC spoofing. The idea is that an adversary spoofing the MAC address of a legitimate node will be assigned the same IP address as the legitimate node by the DHCP server of the WLAN. Hence, an ICMP ping to that IP address will return two replies; clearly identifying existence of MAC spoofing.

Guo and Chiueh [43] extended sequence number based MAC spoofing detection by monitoring patterns of sequence number changes. Rather than raising an alarm if a single sequence number gap is detected for a MAC address, the MAC address is transitioned to a verification mode and the subsequent sequence numbers of that MAC address are monitored for any anomalous gaps. In this manner, false positives raised due to lost and out of order frames are avoided. Their system also caches the last few frames for each MAC address to verify retransmissions and out of order frames. Their solution also uses regular ARP requests to all STAs to synchronize with their sequence numbers based on ARP responses. This is done to defeat an adversary successfully injecting frames with correct sequence numbers somehow and detect the spoofing even if the legitimate node is no longer transmitting.

Madory [65] suggests a technique called *Sequence Number Rate Analysis* (SNRA) to detect MAC spoofing using sequence numbers. This technique calculates a transmission rate for a MAC

www.manaraa.com

address by using the difference (modulo 4096)[10] between the sequence numbers of consecutive frames from that MAC address and dividing it by their inter arrival time. If the calculated transmission rate is greater than the theoretical transmission limit for PHY of the WLAN it is considered to be an indication of a MAC spoof.

Fingerprinting: The second approach for MAC spoofing detection is fingerprinting MAC addresses based on their unique characteristics. The combination of device driver, radio chipset and firmware provides each WLAN node a unique fingerprint of its 802.11 implementation. Ellch [31] suggests using CTS frame responses and 802.11 Authentication and Association frames to fingerprint 802.11 implementations of WLAN nodes. He also suggests using the *Duration* field (see Section 2.3.2) values in 802.11 frames to fingerprint WLAN nodes in a particular WLAN. Such fingerprints can be used to detect MAC spoofing activity as the fingerprint for the adversary would be different from the legitimate node. Franklin et al. [34] also suggest similar fingerprinting of 802.11 device drivers. Their technique exploits the fact that most 802.11 drivers implement the active scanning algorithm differently. They suggest that each MAC address could be mapped to a single device driver fingerprint and hence could be used for detecting MAC spoofing.

Fingerprinting of WLAN nodes can also be performed at the PHY layer. Hall et al. [44] suggest using Radio Frequency Fingerprinting (RFF) for MAC spoof detection where the RFF uniquely identifies a transceiver based on the transceiverprint of the signal it generates. By using the transceiverprint of a MAC address (WLAN node), any attempts to spoof that MAC address can be detected. Some watermarking techniques have also been suggested to uniquely identify the signal from a particular node [59]. Such PHY layer watermarking can assist in distinguishing adversaries from legitimate clients.

Location Determination: Location of the WLAN nodes can also be used to detect MAC spoofing.

[10]The sequence numbers only range from 0 to 4096.

www.manaraa.com

Location of a particular node is usually determined using its signal strength values as a location dependent metric. Once the location of a MAC address is known, any changes in its location can be used as an indication of MAC spoofing activity. Bahl and Padmanabhan [13] record the received signal strength (RSS) values of each node on each AP and then compare these against a pre-calculated database that maps these RSS values to physical locations. Smailagic and Kogan [87] improve on this system and use a combination of triangulating WLAN nodes' RSS values from multiple APs and lookups in a database that maps RSS values to physical locations. Many other systems have also been proposed that establish location of a WLAN node using its RSS values and hence can be used for detecting MAC spoofing in a WLAN [4, 6, 35, 56, 95].

Signal Strength Fourier Analysis: Madory [65] also suggests a statistical technique called the *Signal Strength Fourier Analysis* (SSFA) to detect MAC spoofing using received signal strength (RSS) values of a WLAN node. It performs Discrete Fourier Transform on a sliding window of RSSs and uses the statistical variance of the high-frequencies which result from the interference between the attacker and the victim to detect MAC spoofing.

Some of the techniques for detecting spoofing based attacks have been implemented in some open source WIDSs such as *Snort-Wireless* [8]. Snort-Wireless claims to be capable of detecting MAC spoofing by monitoring for inconsistencies in MAC frame sequence numbers.

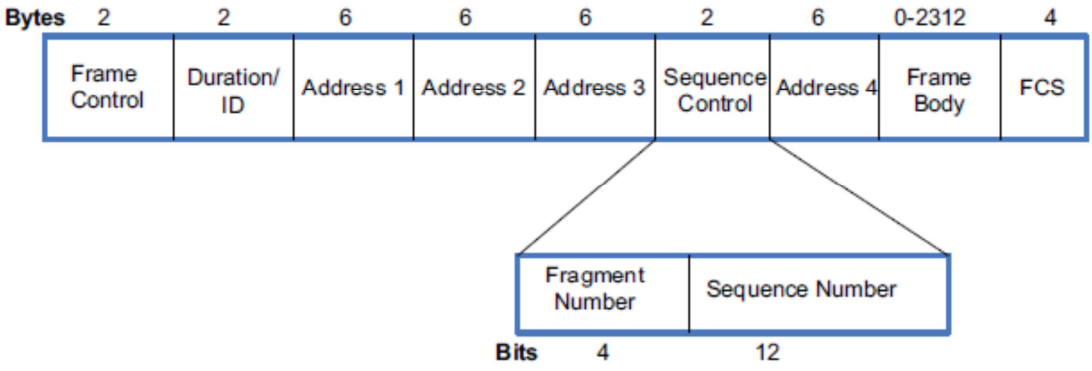


Figure 3-3: 802.11 MAC Header Containing the Sequence Control Field

www.manaraa.com

3.3.2 Wireless Intrusion Detection Techniques for Protocol Limitations

Unfortunately no existing WIDTs specifically detect the 4-Way Handshake blocking caused by unprotected Message 1 of the handshake and DoS caused by MIC countermeasures (see Section 2.7.5). However, a discussion of the WIDTs that detect injection of unprotected frames and virtual jamming is presented below:

Detecting Forged Management/Control/EAP/EAPoL Frames:

Although Wardriving[11] is not an attack, however a number of systems have been proposed that use signatures to detect wardriving tools such as *Netstumbler* [63]. Some of such systems are presented at [48, 58, 62, 102, 103].

One simple approach used for detecting unauthorized WLAN nodes that inject forged Management/Control/EAP/EAPoL frames is to use lists of authorized MAC addresses. Frames detected to and from MAC addresses that do not exist in the authorized MAC list are considered malicious frames. In this manner, attacks such as rogue APs can be detected as they inject forged Beacons (Management frame) into the WLAN. Many systems have been proposed to use MAC filters to identify unauthorized nodes and traffic [1, 23, 48, 72]. Adya et al. [3] also use MAC filtering to detect rogue APs, however they augment this check with channel information. The alarm is only raised if the AP is using a MAC address not in the authorized list and is on a different channel than expected.

Spoofed Management frames can also be identified using abrupt changes in the *Sequence Control* field in the MAC header (see Section 3.3.1 for more details). Schmoyer et al. [84] proposed using the sequence numbers to detect spoofing of Deauthentication and Disassociation frames.

Snort-Wireless [8] and Neumerkel et al. [72] use the rate of Management frame injection for DoS detection. Neumerkel et al. also use the total number of unique source MAC addresses to

[11]Commonly used term used to describe searching for WLANs by sending out null Probe Request frames.

www.manaraa.com

identify a *Authentication Flood* DoS attack. In such an attack, a flood of *Authentication Request* Management frames are sent to the AP with different source MAC addresses.

Unfortunately, no WIDTs exists that specifically detect attacks that exploit unprotected Control frames and EAP/EAPoL frames.

Virtual Jamming Detection

Virtual jamming refers to when malicious node(s)[12] set the *Duration* field to abnormally high values in their frames in order to trick the virtual carrier sensing of other WLAN nodes, such that the medium always appears busy to them (see Section 2.7.5). Kyasanur and Vaidya [61] proposed a system to detect such MAC layer misbehavior. However, it was not very practical as it required changes to the 802.11 MAC protocol itself. Later Raya and Aad [82] proposed an improved approach that was based on pure passive traffic monitoring and did not require any modifications to 802.11. Their approach used throughput and backoff statistics to detect misbehaving nodes. They checked the NAV against actual transmission times of frames to detect nodes that intentionally set NAV high. Their technique can be implemented on an AP which can identify malicious nodes by simply observing their traffic. Work has also been done to build theoretical frameworks for studying the structure of MAC layer misbehavior problems such as virtual jamming [81].

Techniques have also been suggested for the detection of PHY jamming [109]. Such techniques use anomalies in statistics of characteristics such as signal strength distribution, carrier sensing time distribution and successful packet delivery ratio.

3.3.3 Wireless Intrusion Detection Techniques for Security Policy Violation

A review of the existing WIDTs showed that currently no techniques exist for detecting security policy violations in a WLAN. Security policy violations include not only activity by malicious nodes and adversaries; but also refer to the activity of misconfigured or non-compliant nodes. As shown in

[12]This can be an adversary or a misbehaving node.

www.manaraa.com

Figure 3-2, the *Security Policy Violation* category refers not just to use of weak passphrase and unauthorized EAP method; it refers to ANY violation of the security policy. This could be use of WEP instead of CCMP for confidentiality protection or advertising WLAN capabilities in the Beacons that violate the WLAN security policy. All security policy violations should be treated as intrusions and should be alarmed for action immediately and with high priority, once detected.

The security policy refers to the components of the security policy specific to WLAN deployment and usage such as WLAN authentication method(s), algorithms for cryptographic protection of confidentiality and integrity of WLAN data and key management algorithms.

3.3.4 Wireless Intrusion Detection Techniques for Attacks Exploiting Software Vulnerabilities

Unfortunately no WIDTs currently exist that specifically detect exploitation of software vulnerabilities in a WLAN. These attacks exploit software vulnerabilities in drivers, protocol implementations and software sub systems by injecting frames that carry payload to exploit software vulnerabilities on the target system. These attacks might get detected indirectly if they use Management frames to deliver the payload and trigger off the alerts for WIDTs used for detecting Management frame based attacks (see Section 3.3.2).

3.4 Room for Improvement

The current WIDTs, as discussed in Section 3.3, are a combination of signature based and anomaly based techniques. Unfortunately, they are not very robust and reliable and suffer from a number of drawbacks and weaknesses. This section discusses the limitations of the current WIDTs.

The current techniques for detecting unprotected Management frames rely on MAC filtering; in which an adversary can easily defeat by simply changing the MAC address of the WLAN card to a MAC address that he/she eavesdropped as belonging to a legitimate WLAN node. Augmenting the MAC address filters with attributes such as channel information cannot assist in rogue AP detection but it is not an unspoofable attribute as an adversary can observe the channel information by simply eavesdropping the WLAN traffic. Now the adversary can change his/her WLAN card's MAC address

www.manaraa.com

and the channel to inject Beacons as the legitimate AP. Using injection rate of forged Management frames to detect DoS can also be defeated if the adversary maintains the injection rate below the detection threshold.

It is possible to cause a DoS without using a very high rate of frame injection. This is especially true of Deauthentication and Disassociation Management frames as such frames can be sent to a broadcast destination address and hence using a single frame, all STAs in a BSS can be disconnected.

Using abrupt changes in sequence numbers for detecting spoofed Management frames or MAC spoofing is also not foolproof as the sequence numbers range only from 0 to 4096 and are reset every time the node restarts or resets. Frame loss and out of order frames also cause false positives in sequence number checking. Additionally sequence numbers cannot be used to detect forged Control frames as these frames do not contain a *Sequence Control* field (see Section 2.3.2). Sequence numbers are used in intrusion detection as they were considered immutable as they were controlled and set in the firmware. Hence, malicious users could not set the sequence number in a MAC frame to arbitrary values. However, this is changing as more and more MAC features are moving out of the firmware (see Section 2.7.7) and tools are becoming available to assist an adversary in setting the *Sequence Control* field to arbitrary values [105]. An adversary can eavesdrop the sequence numbers used by a legitimate node and then start injecting frames using the MAC address and the expected sequence numbers for that node. ICMP augmentation to sequence number checking for detecting MAC spoofing is also not reliable as the adversary does not need to obtain an IP address to launch WLAN attacks based on MAC spoofing.

Although Guo and Chiueh [43] improved the sequence number based MAC spoofing detection, their scheme relies on the adversary and the legitimate WLAN node to be injecting frames at the same time. Hence, attacks such as session hijacking would go undetected, where the legitimate node is no longer transmitting after the adversary has taken over its session. Guo and Chiueh [43] attempt to address this problem by using regular ARP requests to all STAs to synchronize with their sequence

www.manaraa.com

numbers based on ARP responses. However, ARP requests and responses are unprotected themselves and can easily be forged by an adversary to defeat this scheme. Madory [65] uses *Sequence Number Rate Analysis* (SNRA) to detect MAC spoofing using sequence numbers; however SNRA requires the adversary's and the legitimate node's frames to interleave within a threshold time frame. This might not be true for all attacks (for instance session hijacking). SNRA also does not seem to address false positives caused by retransmissions and out of order frames. Madory [65] also suggests using *Signal Strength Fourier Analysis* (SSFA) to detect MAC spoofing using received signal strength (RSS) values of a WLAN node. Unfortunately, SSFA requires the WLAN node to be stationary to be able to detect any MAC spoofing attacks against it. This can be quite a limiting pre-condition, given the high mobility of WLAN handheld devices.

Using MAC layer and PHY fingerprinting is a promising new area for detecting MAC spoofing. However it is not clear how reliably each fingerprint can be matched to a MAC address. It would be particularly easy to avoid such fingerprints if the adversary is an insider and is using a standard operating environment (SOE) WLAN hardware and software to launch an attack against the WLAN. Given the same combination of device driver, radio chipset and firmware for SOE devices from same WLAN, an adversary using an SOE device could easily go undetected. The PHY fingerprinting seems more promising as it relies on the finer transceiver fingerprint. However, it is not clear how effectively such fingerprinting can be used for intrusion detection.

Using location determination of a WLAN node for intrusion detection purposes also seems unreliable and prone to false positives and false negatives. The unpredictable nature of the environmental effects on signal propagation and a lack of signal strength stability due to calibration drift in low-quality wireless networking cards present significant challenges for using location calculation derived from the RSS based physical location maps for reliable intrusion detection. These techniques also seem to have a processing intensive pre-requisite of developing a reference database that maps a physical location to RSS values. Maintaining such a reference database would be quite

www.manaraa.com

challenging in itself too.

Although current WIDTs used for detecting MAC layer misbehavior (virtual jamming) seem effective, analysis of the current WIDTs shows that there are no available techniques to detect attacks that exploit security policy violations such as using an insecure EAP method for authentication and using an insecure PSK. Similarly, no detection is available for protocol limitation attacks that exploit the unprotected Message 1 of the 4-Way Handshake. Also there are no WIDTs those specifically detect attacks that target the unprotected Control and EAP/EAPoL frames. Specific detection of the attacks that exploit Michael algorithm's MIC weakness and those that exploit software vulnerabilities in WLAN nodes is not exist too.

Approach	Requires Protocol or HW modifications	Relies on spoofable parameters
MAC Filtering	NO	Yes
Sequence Number Monitoring	NO	Yes
Monitoring Sequence Number with ARP Request-Response	NO	Yes
SNRA	No	Yes
SSFA	No	Yes
Fingerprinting	No	No
Location Determination	No	No
Virtual Jamming Detection	Yes	No

Table 4: Summery of Available WIDTs

Table 3-3 lists the available WIDTs, and weather each technique requires protocol or HW modifications, and does the technique rely on spoofable parameter.

3.5 Requirements of a Wireless Intrusion Detection System

This section discusses a number of requirements or desirable characteristics for wireless intrusion detection systems with respect to the WIDTs it implements. These requirements are based on addressing the deficiencies in current approaches and considerations for integrating wireless and existing wired intrusion detection systems and easing the ongoing management of the wireless intrusion detection systems.

- **Passive:** The techniques used for wireless intrusion detection should not require the modification of access points (APs), stations (STAs) or the protocols in any manner.

www.manaraa.com

Monitors or sensors used by the WIDS, should operate in receive only mode so as not to announce their presence or affect the performance of the network [75].

- **Capable of detecting all RSN vulnerabilities:** The wireless intrusion detection system should be comprehensive and should be capable of detecting all attacks that target vulnerabilities described in Figure 3-3 (*MAC Spoofing*, *Security Policy Violations* and *Protocol Limitations)*. Given, it is very difficult to design a WIDT that detects attacks targeting all RSN vulnerabilities; this requirement can be fulfilled by the WIDS using a combination of WIDTs.
- **Robust:** The WIDTs employed by the WIDS must not be easily avoided by adversaries and intruders.
- **Accurate and sensitive:** The WIDS should be accurate enough so that alerts are only raised as a result of an attack or non-compliant transmissions (minimal false positives) and sensitive enough to ensure that all attacks are detected (minimal false negatives).
- **Maintainable:** The WIDS, once deployed, should not require extensive reconfiguration as new attacks emerge. Additionally, the system should be flexible and extensible enough to accommodate changes in the site security policy, or the addition of new link layer cryptographic algorithms and new authentication methods.
- **Flexible:** The WIDS should be capable of operating in both online and offline modes, interoperate with existing wired intrusion detection correlation systems, and be deployable in an autonomous distributed fashion or support centralized analysis of alerts.
- **Attack resistant:** The WIDS and its detection techniques should be designed to resist attacks that target their own resources, providing assurance that the monitoring capability is not easily disabled.

While developing new WIDTs to address the gaps in existing detection capabilities and techniques, the above mentioned WIDS requirements should be kept in mind. This is because WIDTs are hardly

www.manaraa.com

ever used in isolation and should be designed from the very beginning to work as part of a bigger system. The WIDTs should be complementary in nature so that when used together in a WIDS, the capabilities and strengths of all techniques together can help the WIDS detect all RSN attacks in a reliable manner. The complementary nature of the WIDTs can also assist the WIDS to correlate alarms across different WIDTs to further enhance its robustness and reliability.

www.manaraa.com

Chapter 4 Intrusion Detection in WLANs through Profiles Based on PHY and MAC Layer Attributes

Due to the failure of the WLAN standards to address the lack of authentication of 802.11 Management frames and network card addresses, it is possible for adversaries to spoof the identity of legitimate WLAN nodes and take over their associations. Such attacks, where the attacker assumes the identity of another WLAN node, are referred to as MAC spoofing or simply spoofing based attacks. Such attacks are of grave concern as they can lead to unauthorized access and leakage of sensitive information. As discussed in Chapter 2, MAC spoofing is the root of almost all RSN attacks. Without the ability to inject forged frames using a spoofed MAC address, none of the RSN attacks can be launched.

Unfortunately, not many intrusion detection techniques are available for reliably and accurately detecting MAC spoofing. The few that exist are not very robust and reliable (see Section 3.4). Given the enormous impact MAC spoofing has on WLAN security, wireless intrusion detection techniques are required to reliably and accurately detect MAC spoofing activity in WLANs.

R. Gill et al. [39] address this issue by proposing wireless intrusion detection techniques (WIDTs) that are capable of not only reliably detecting the spoofing based attacks, but also operate in a totally passive and undetectable manner. These techniques also do not require modification of any kind to the existing hardware, software or protocols.

R. Gill et al. [37, 39] examined the effectiveness of their proposed techniques in detecting session hijacking attacks; they performed their experiments using a simulated attack by manually bringing down STA's wireless interface and associating the attacker with the AP using masqueraded MAC address of the STA.

In this chapter we verify the effectiveness of the detection techniques proposed in [39] in detecting MAC spoofing DoS attacks by executing real attacks against a STA that is associated to an AP. We also enhance the performance of these techniques by lowering the false positives rate, and hence we

www.manaraa.com

enhance the performance of the WIDS by preferring these enhanced techniques.

4.1 Need for Enhanced WIDTs for Detecting Spoofing

The current techniques for detecting spoofing based attacks are not only limited in number but also ineffective as they are based on spoofable and predictable parameters such as sequence numbers. A reliable WLAN intrusion detection technique should utilize unspoofable characteristics from the MAC and the PHY layer to enhance confidence in the detection results. These characteristics should be computationally inexpensive to calculate; allowing them to be determined in a fast and efficient manner. These techniques should be able to operate in real time, in a passive fashion, and do not require modification to the communication protocols, software drivers, or the operating system software. The detection technique should also operate without causing any interference to the live traffic or network performance. It should be accurate and sensitive, while maintaining a minimum level of false positives and false negatives (see Section 3.5). In a real world WIDS, an approach based on co-operating detection techniques can also increase confidence in the validity of raised alerts.

4.2 Passive Detection of Spoofing Based Attacks

This section introduces two intrusion detection techniques that can be used by a WIDS to passively detect spoofing based attacks. The techniques described meet many of the desirable characteristics as they: are based on unspoofable characteristics of the PHY and MAC layers of the IEEE 802.11 standard; are passive and do not require modifications to the standard, wireless card drivers, operating system or client software; are computationally inexpensive; and do not interfere with live traffic or network performance.

4.2.1 Monitoring Received Signal Strength (RSS)

Received signal strength (RSS) is a measure of the energy observed by the physical layer at the antenna of a receiver. In IEEE 802.11 networks the RSS indication (RSSI) value is used when performing medium access control clear channel assessments and in roaming operations. The radio

www.manaraa.com

frequency (RF) signal strength can be measured in either an absolute (decibel milliwatts -dBm), or relative (RSSI) manner.

Strength of the RF signals undergoes some attenuation during transmission after leaving the sender's radio and this signal strength deterioration is governed by a variety of factors such as RF interferences, distance between the sender and the receiver, obstacles etc. The distance between the sender and the receiver has the biggest impact on signal fading. However, RF signal strength does not fade in a linear manner; rather it attenuates roughly inversely as the square of the distance between the sender and the receiver [14]. Along with distance, the RSS for a particular node, as observed by the receiver, also depends on various other factors such as the WLAN equipment used by both the sender and the receiver nodes, the physical obstacles in between and their surrounding environment. The mathematical path loss model for IEEE 802.11 RF waves used by Wullems et al. [106] also suggests a direct relationship between the RSS and the distance between the sender and the receiver along with numerous other factors, including: frequency used; antenna gain; and an environmental coefficient.

This means that it is not possible for an adversary to accurately guess the RSS for a sender as perceived by a receiver. The adversary will need to be at exactly the same location as the receiver, use exactly the same radio equipment, and receive the radio signal with same level of interference, reflections and refractions to know the exact RSS value as perceived by the receiver. Even if the sender is stationary, the RSS values tend to slightly fluctuate and hence prove almost impossible to guess. This prohibits the adversary from using radio equipment (such as a high gain directional antenna) to spoof the RSS as perceived by the receiver.

4.2.1.1 Discussion

From an intrusion detection perspective, the observed RSS for a particular node is valuable, as it is unspoofable and computationally inexpensive to measure. The observed RSS is relative to the measuring entity and is calculated at the receiver; hence secure from eavesdropping and very difficult to predict.

www.manaraa.com

By periodically monitoring the RSS values for a particular WLAN node from a passive monitor (usually a passive sensor); a dynamic RSS profile can be developed for that node. Any abrupt or unusual changes in the RSS profile for a node are indicative of a spoofing attack targeting that node. This RSS profile is dynamic as it is constantly updated with the latest RSS values for the node, as observed by the monitor. Every new RSS value observed for a node is being compared against the last observed value and the absolute difference is measured (*RSSdiff*). If the *RSSdiff* is abnormally high (greater than a pre-determined threshold), an alarm is raised for that node. This intrusion technique is referred to as the *Received Signal Strength Based Intrusion Detection Technique* (RSSDT) hereafter.

The RSSDT is capable of detecting spoofing based attacks against both AP nodes and normal STAs. For instance, if a legitimate STA has an active session with an AP, the passive monitor will build a dynamic RSS profile for both the AP and the STA, based on their observed RSS values at the monitor. If an attacker node hijacks STA's session by forcing it off the network and spoofing its MAC address; the monitor will pick up the sudden change in the RSS profile of the STA (due to an unusually high *RSSdiff* value) and raise an alert. The RSS values for the STA will change as they will now correspond to the attacker's actual location, radio equipment and surrounding environment. Similarly, if the attacker node tries to spoof as the AP, it will also get detected as the dynamic RSS profile for the AP will undergo abrupt fluctuations. The RSSDT is potentially capable of detecting all spoofing based attacks as any spoofing activity will cause changes in the RSS profile of the victim node. The RSSDT, however, does require the victim and the attacker to be present at the same time.

Since APs are generally stationary, any abrupt changes in their RSS dynamic profile can be flagged as suspicious activity with a higher confidence level. A mobile STA's RSS values change more rapidly as observed by a passive monitor; however despite the motion, the absolute difference between consecutive RSS measurements for that node (i.e. *RSSdiff*) still remain predictable and small. The RSSDT raises an alarm only when the *RSSdiff* is abnormally high (i.e. it exceeds the *RSSdiff threshold*). Computation of the RSS does not require any extra processing, as it is usually performed

www.manaraa.com

by the RF hardware automatically for its normal WLAN operations. As we are only interested in the absolute difference between consecutive RSS measurements (i.e. *RSSdiff*) and not their absolute values, the RSS measurements can be made either using dBm or RSSI units.

The RSSDT uses uncertainty of the wireless medium in favor of the intrusion detection as the adversary has no means of knowing what RSS values to spoof. Hence, the RSSDT proves effective against both insider and outsider spoofing attacks and requires no additional bandwidth consumption.

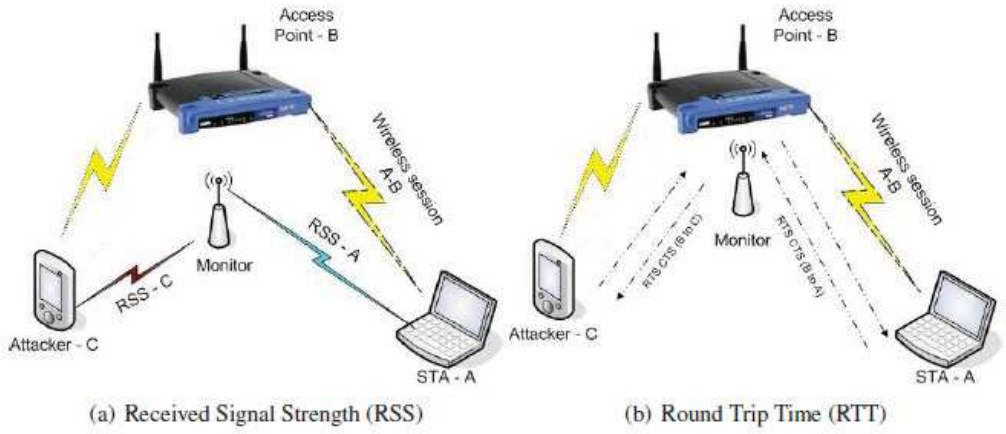


Figure 4-1: Passive Monitoring of RSS and RTT for Intrusion Detection [39]

4.2.1.2 Experiments

To put the RSSDT to the test, preliminary experiments were carried out in a lab environment using the experimental setup described in Figure 4-1(a). These experiments were designed to verify if RSSDT could detect MAC spoofing activity in a WLAN, and to choose the best *RSSdiff* threshold to be used in the detection process. These were simple preliminary tests and more comprehensive experimentation is discussed in Section 4.3.

A Netgear DG834G Wireless Access Point was used as an AP (B). A Windows laptop with Intel WiFi Link 5100AGN WLAN card was used as STA (A) and a Linux laptop with Intel PRO/Wireless 3945ABG WLAN card was used as the attacker (C). A PC with Netgear WG111 wireless adapter

www.manaraa.com

running *Wireshark*[13] tool under Linux was used in Radio Frequency Monitoring (RFMON) mode as the Monitor to passively observe the RSS values for (A). RFMON mode allows the wireless card to passively monitor all WLAN traffic without any active participation in the network. The monitored RSS values for each wireless node are in dBms. These values were used to maintain the RSS profiles by the Monitor.

Although the RSSDT can be used to monitor intrusions against both AP and STA nodes; these experiments concentrated on attacks on the STA alone. Four different scenarios were studied to observe the effectiveness of RSS monitoring as an intrusion detection technique for the spoofing based attacks. In all scenarios, the AP B and the Monitor were stationary and the Monitor was placed in very close proximity of the AP:

- Scenario I - STA A was placed close to the AP B (in the same room separated by a distance of about 3 meters).
- Scenario II - STA A was placed far away from the AP B (in another room, separated by a distance of about 10 meters)
- Scenario III - STA A performed a round trip (at walking pace, goes away and drawn near)
- Scenario IV - STA A was stationary and attacker C was stationary; Attacker launches a TKIP DoS attack against A. The attack was performed using *tkiptun-ng* [96] tool.

For each scenario, 400 RSS readings were taken for STA A by the Monitor, and the results have been represented in graphs shown in Figure 4-2. In *Scenario I*, as STA A was in very close proximity of the AP B, the absolute difference between consecutive RSS readings (i.e. *RSSdiff*) for A were very small i.e. an average difference of 1.508dBm with an average absolute RSS reading of -42.43dBm. In *Scenario II*, even though the individual absolute RSS readings were quite different from those in *Scenario I* (average absolute value of -83.75dBm); the *RSSdiff* across the readings remained very low (i.e. 0.75dBm). In *Scenario III*, the fluctuations between consecutive RSS readings became more

[13]http://www.wireshark.org/

www.manaraa.com

apparent. The average *RSSdiff* was however still a low 3.56dBm, with average absolute RSS reading of -62.97dBm. In Scenario IV, a large fluctuation between consecutive RSS readings was recorded at about reading number 333. This was caused by the MAC spoofing of A by the attacker C. The *RSSdiff* between the observed RSS for C and the last observed RSS for A was much larger (7.28dBm) than the values noticed during *Scenario I*, *Scenario II*, *Scenario III* and the non-attack part of *Scenario IV*. Table 4-1 summarizes these obtained results. Hence, the RSSDT correctly detected the intrusion and also demonstrated a low false positive rate; as shown by the low average *RSSdiff* for all non-attack traffic throughout the scenarios.

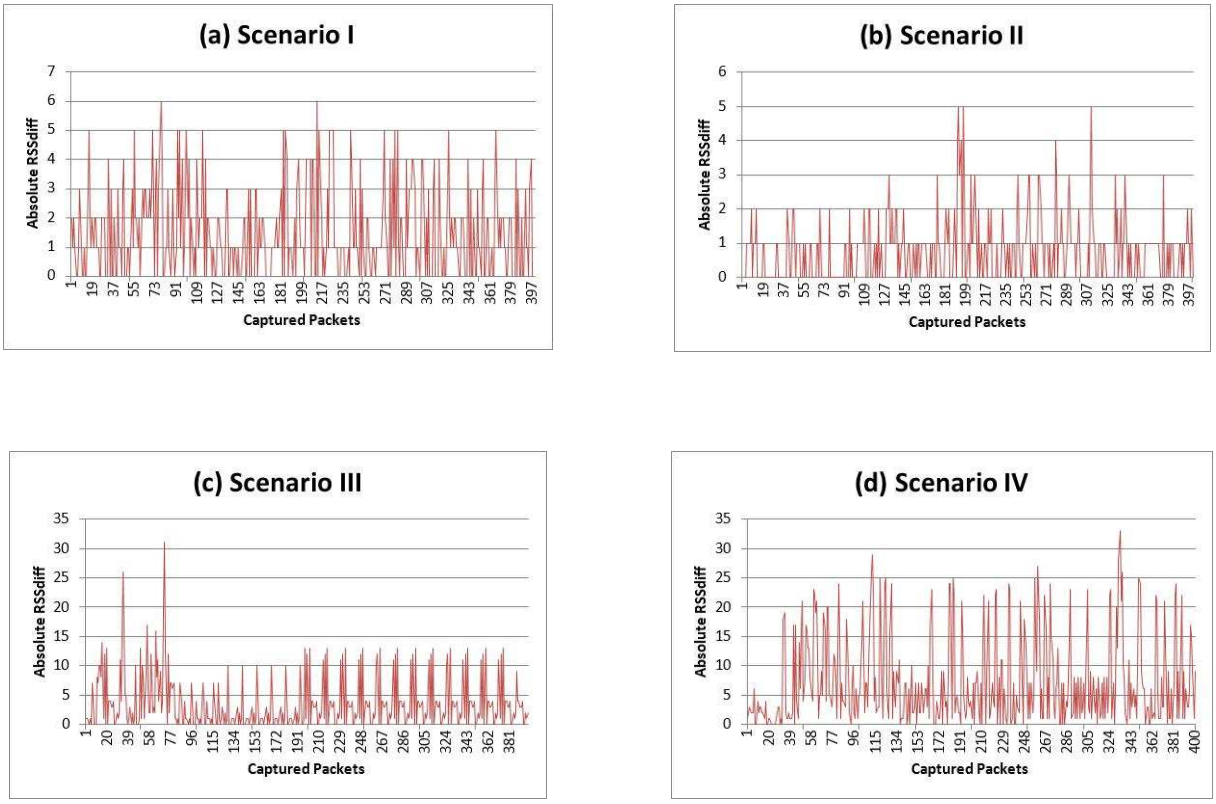


Figure 4-2: Monitoring RSS measurements

4.2.2 Monitoring Round Trip Times of RTS-CTS Handshake

IEEE 802.11 uses both virtual and physical carrier sensing to monitor the state of the medium. Every unicast frame uses its *duration* field to update the *Network Allocation Vector* (NAV) of every node in range that receives the frame (wireless medium is broadcast). A node can only transmit data when its NAV is zero. The NAV value reflects the predicted time (in microseconds) it will take to

www.manaraa.com

transmit the frame from the sender to the receiver and the corresponding acknowledgment (ACK) frame to return from the receiver to the sender. However, another virtual carrier sensing mechanism is used to mitigate collisions from hidden terminals that are not in direct range of the sender or the receiver and might start transmitting after incorrectly sensing the medium free. Before starting transmission, the sender requests positive control over the medium by sending a *Request to Send* (RTS) frame to the receiver. On receipt of the RTS frame, the receiver sends a *Clear to Send* (CTS) frame as an acknowledgment back to the receiver. The duration field in a RTS frame is large enough for the RTS-CTS handshake, the data frame and its associated ACK frame. The duration field of CTS frame contains an updated duration value which takes in account the time elapsed during the RTS-CTS handshake. All wireless nodes that receive either the RTS or CTS frame update their NAVs and defer access to the medium.

Scenario	Average RSSdiff (dBm)	Average RSS Reading (dBm)
Scenario I	1.508	-42.43
Scenario II	0.75	-83.75
Scenario III	3.56	-62.97
Scenario IV	7.28	-45.75

Table 5: RSSDT Preliminary experiments results

Virtual carrier sensing ensures that the transmission of a data frame and receipt of its ACK from the receiver is an atomic event, free from collisions.

This concept can also be extended to the RTS-CTS handshake scenario. Similar to the data-ACK exchange between two nodes, the RTS-CTS handshake is also protected by virtual carrier sensing. In fact RTS-CTS is used to establish the virtual carrier sensing for making the transmission of data frames possible without collisions. The successful receipt of the CTS frame from the receiver indicates that the receiver successfully received the sender's RTS frame and is ready for receiving data. The sender can monitor the time taken for completion of the RTS-CTS handshake between itself and the receiver i.e. $Time_s^{rtt}$. This is the total time taken for the RTS frame to travel from the sender to the receiver and the CTS frame to be sent back as an acknowledgment. This includes the processing time on the

www.manaraa.com

receiver and the mandatory wait of SIFS time period before the receiver can transmit a CTS.

The RTS-CTS handshake is atomic and free from collisions with other wireless nodes. Hence the only factors that affect the value of $Time_s^{rtt}$ between two communicating nodes include 1) the distance between the sender and the receiver, 2) the local environment around the nodes i.e. the number of physical obstacles between the nodes and the number of reflections, refractions and multipaths suffered by radio waves while travelling from sender to receiver and back, and 3) the nature of radio equipment used by both the sender and the receiver. The size of the RTS and the CTS frames is fixed and does not affect $Time_s^{rtt}$ values for a fixed transmission rate.

This makes $Time_s^{rtt}$ between two nodes an unspoofable parameter which cannot be easily guessed by an adversary passively monitoring the airwaves. It is also protected from eavesdropping as it is a property that is calculated by the sender of the RTS-CTS handshake. It is a measurement relative to the entity measuring it and hence the adversary will have to be at exactly the same location as the sender, using exactly the same radio equipment with same attenuation and antenna gain and receiving the radio waves after the same number of reflections and refractions as the sender to exactly predict the values of $Time_s^{rtt}$ between the sender and the receiver, as measured by the sender. It can also be calculated without any significant computational overhead or waste of bandwidth.

4.2.2.1 Discussion

From intrusion detection perspective, rapid and abrupt changes in $Time_s^{rtt}$ between two nodes can be used as a mechanism to detect spoofing based attacks. Interestingly this property still remains usable if rather than monitoring $Time_s^{rtt}$ values on the sender a passive wireless monitor is used for these time measurements. However, the monitor cannot calculate $Time_s^{rtt}$ completely as it is a property relative to the sender.

www.manaraa.com

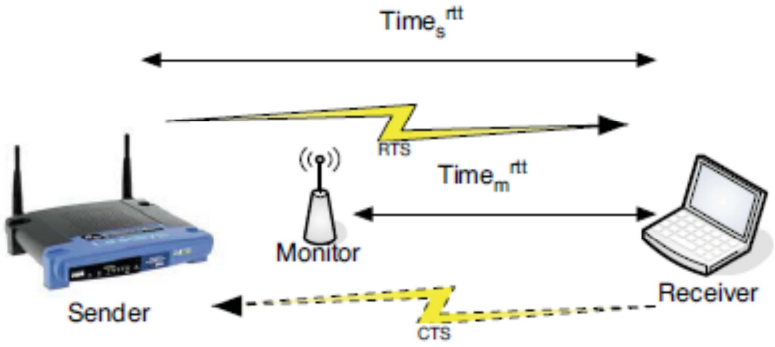


Figure 4-3: RTS-CTS Round Trip Time (RTT) [37]

The Monitor can only measure the elapsed time between when it first detected a RTS frame from the sender to the receiver and when it detected a return CTS from the receiver back to the sender i.e. $Time_m^{rtt}$ (see Figure 4-3). This time can be roughly represented as:

$$Time_m^{rtt} = Time_M^{rtt} - Time_{s-r}^{rtt} - Time_{m-s}^{rtt}$$

Where $Time_{s-r}^{rtt}$ is the time it takes for a RTS frame to cover distance between the sender and the monitor, $Time_{m-s}^{rtt}$ is the time it takes for a CTS frame to cover distance between the monitor and the receiver and $Time_M^{rtt}$ is the actual time it takes for the RTS-CTS handshake to complete between a sender and the receiver as observed by the monitor (assuming somehow the monitor could measure it). In reality, the monitor has no way of knowing actual values of $Time_M^{rtt}$, $Time_{s-r}^{rtt}$, or $Time_{m-s}^{rtt}$. Monitoring observed $Time_m^{rtt}$ values - at the monitor - presents a reliable passive detection mechanism for spoofing based attacks as it is an unspoofable parameter relative to its measuring entity, which cannot be guessed as its exact value depends on 1) the position of the receiver and the monitor, 2) the distance between the monitor and the receiver and 3) the environment around the receiver and the monitor. This is a property that cannot be measured or spoofed by an attacker passively monitoring network traffic or using specialized radio equipment.

It is proposed that, for a WLAN association, the absolute difference between consecutive $Time_m^{rtt}$ values for the two communicating nodes (*RTTdiff*) can be monitored by a passive monitor and any abrupt fluctuations can be flagged as suspicious. This will help in detecting an adversary who attempts

www.manaraa.com

to take over either of the communicating node's session (STA or AP) by forcing it off the network and spoofing its MAC address. This intrusion detection technique is hereafter referred to as the *Round Trip Time Based Intrusion Detection Technique* (RTTDT). Unlike the RSSDT, which maintains RSS profiles for each WLAN node (including APs); the RTTDT maintains RTT profiles for each WLAN association (i.e. a node-AP pair). If any of the two parties in an association change, the RTTDT would detect a change in the RTT profile for that association. Hence, just like the RSSDT, the RTTDT is capable of detecting spoofing attacks against both the APs and the STAs. Just like RSSDT, the RTTDT is also capable of detecting all spoofing based attacks, given that RTS-CTS handshakes are exchanged between the attacker and a legitimate WLAN node; where the same WLAN node was exchanging RTS-CTS handshakes with the victim node before the attack. Just like the RSSDT, the RTTDT also requires the victim and the attacker to be active in the WLAN at the same time.

For instance, if a legitimate STA has an established session with an AP, the passive monitor calculates $Time_m^{rtt}$ for every RTS-CTS handshake between them and maintains it in a dynamic profile that gets constantly updated. This profile is only valid for the duration of the association. If an attacker takes over the STA's session with the AP by spoofing STA's MAC address, the monitor will notice change in $Time_m^{rtt}$ for the STA-AP association and will raise an alert. Similarly, if the attacker spoofs the AP's MAC address to communicate with the STA, it will get detected too as a result of fluctuation in the RTT profile of the STA-AP association. However, to be able to detect MAC spoofing for both the APs and the STAs, the $Time_m^{rtt}$ profile for a STA-AP association should be maintained using RTS-CTS handshakes in both directions between the AP and the STA.

4.2.2.2 Experiments

To verify the ability of the RTTDT for MAC spoofing detection, and to choose the best *RTTdiff* threshold; preliminary experiments were carried out in a lab environment using the experimental setup described in Figure 4-1(b). These were simple preliminary tests and more comprehensive experimentation is discussed in Section 4.3.

www.manaraa.com

A Netgear DG834G Wireless Access Point was used as an AP (B). A Windows laptop with Intel WiFi Link 5100AGN WLAN card was used as STA (A) and a Linux laptop with Intel PRO/Wireless 3945ABG WLAN card was used as the attacker (C). A PC with Netgear WG111 wireless adapter running *Wireshark* tool under Linux was used in Radio Frequency Monitoring (RFMON) mode as the Monitor. The DG834G router's *RTSThreshold* option was set to 1 (always on). This option controls when a RTS-CTS handshake is initiated in a WLAN. Before transmitting a frame, the sender checks if the size of the Data frame is greater than the *RTSThreshold* value. If so, a RTSCTS handshake is initiated. Setting the *RTSThreshold* to 1 enabled RTS-CTS handshakes for all data traffic from AP to STA. The speed and accuracy of the RTTDT relies on the frequency of the RTS-CTS handshakes as more RTS-CTS events mean that the RTT profiles can be updated more frequently.

The RTTDT is capable of detecting spoofing attacks against both the APs and the STAs. However, for the purposes of these experiments, only attacks against STAs were addressed. Hence only RTS-CTS handshakes originating from the AP were used for maintaining the RTT profiles. Also for simplicity, only one type of spoofing based attack was used in the experiments i.e. the TKIP DoS Attack. All scenarios, as described in Section 4.2.1, were repeated to observe the effectiveness of the RTTDT as an intrusion detection technique. In all scenarios, the AP B and the Monitor were stationary and the Monitor was placed in close proximity to the AP. The RTT values were calculated using *Wireshark* timestamps of WLAN traffic captured by the Monitor.

For each scenario, 400 RTS-CTS handshake events were captured and the results have been represented in graphs shown in Figure 4-4. In *Scenario I*, the observed *RTTdiff* were small (maximum of 0.298 mSec with average of 0.0738 mSec). In *Scenario II*, the observed RTT values increased as distance was increased, while *RTTdiff* values were still small (maximum of 0.177 mSec with average of 0.00715 mSec). In Scenario III, the average *RTTdiff* remained small (maximum of 3.035 mSec with average of 0.5594 mSec), while the observed RTT measurements fluctuates due to the movement of the STA. In Scenario IV, a large *RTTdiff* fluctuation was registered at the reading number 44. This was

www.manaraa.com

caused by MAC spoofing of STA A. The *RTTdiff* between the observed RTT value for C and the last observed RTT value for A was much larger (18.867 mSec) than any values noticed during Scenarios I, Scenario II, Scenario III and the non-attack part of *Scenario IV*. Hence, the RTTDT correctly detected the intrusion, and also demonstrated a low false positive rate; as shown by the low average *RTTdiff* for all non-attack traffic throughout the scenarios. Table 4-3 summarizes these observations.

4.3 Correlating Across Profile Anomalies

In the previous section, two intrusion detection techniques (the RSSDT and the RTTDT) were introduced to detect spoofing based attacks and some preliminary experiments were conducted to provide confidence in these techniques. This section addresses these outstanding issues and demonstrates the accuracy and utility of the intrusion detection techniques presented in Section 4.2 through empirical data and use of correlation techniques. The RSSDT and the RTTDT, both use threshold values, namely the RSSdiff threshold and the RTTdiff threshold respectively. The RTTdiff and RSSdiff values greater than these thresholds are considered anomalous.

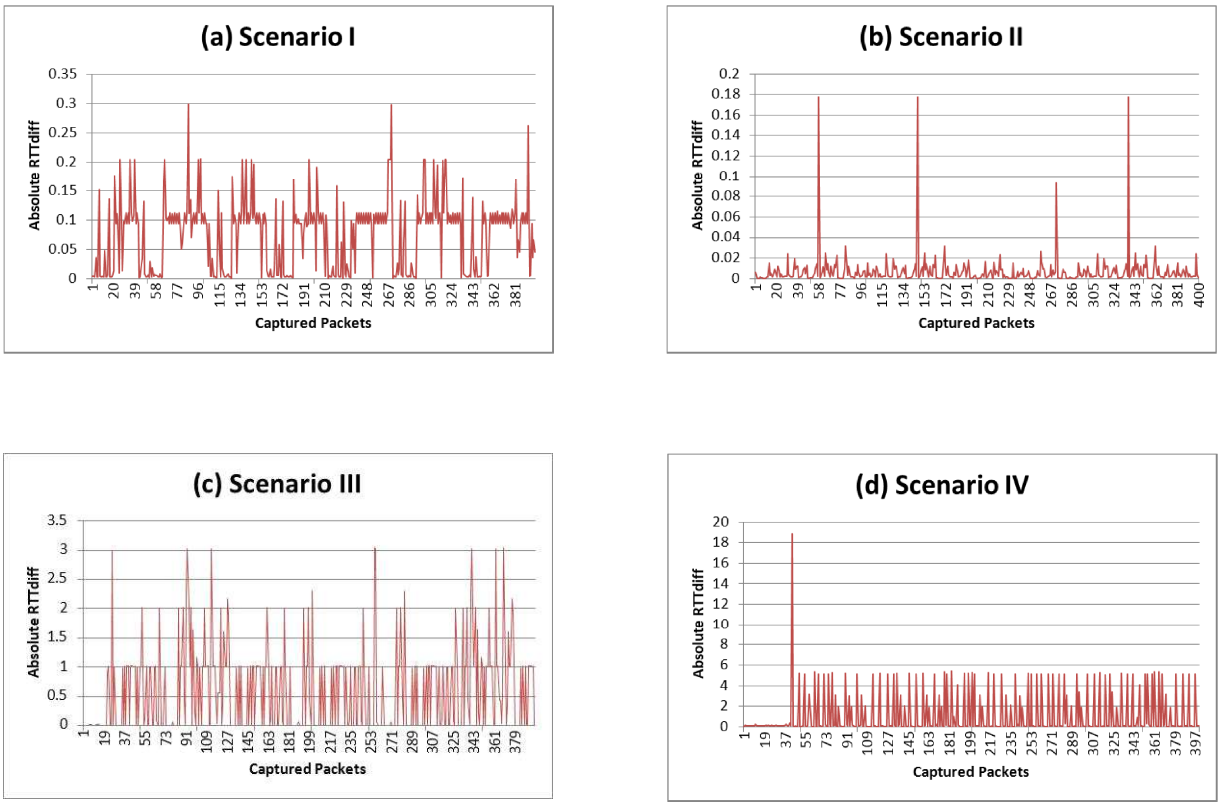


Figure 4-4: Monitoring RTT Measurements

www.manaraa.com

Scenario	Average RTTdiff (mSec)	Maximum RTTdiff (mSec)
Scenario I	0.0738	0.298
Scenario II	0.00715	0.177
Scenario III	0.559	3.035
Scenario IV	1.036	18.867

Table 6: RTT preliminary experiments results

To assist empirical analysis, eight experiment scenarios per attack were designed to study the effectiveness of the RSSDT and the RTTDT in the presence of an attacker, who launches three different new attacks against a legitimate STA; TKIP Cryptographic DoS attack [41], Channel Switch DoS attack [60], and Quite DoS attack [60]

The motivation for the scenarios was derived from an everyday corporate office environment where fixed and mobile wireless stations coexist. To provide a reasonable degree of realism, these experiments were carried out using real WLAN equipment, with real network drivers and software.

These experiments are discussed now in detail.

4.3.1 Equipment and Preparation

The experiments were carried out in a lab environment. The same networking hardware/software was used in all experiment scenarios. The following four parties took part in the scenarios: a legitimate client (STA), an access point (AP), a passive Intrusion Detection System (IDS) sensor, and an attacker. The AP and the IDS sensor were always stationary in these experiments. However depending on the mobility of the STA, the experiments were divided into two distinct sets: *Set1* and *Set2*. In *Set1*, all parties were stationary and in *Set2* the STA was in motion. When in motion, the STA traveled at walking speed, moving across walls, doors and other physical obstacles. Based on the results of the preliminary experiments presented in section 4.2, the *RSSdiff threshold* and the *RTTdiff threshold* was set to the value of 5 in all these experiment sets. Threshold optimization was later explored in Section 4.4 to minimize the number of false positives. Although the RSSDT and the RSSDT can be used to detect all spoofing based attacks against both the APs and the STAs; for simplicity these experiments involved only attacks on the STAs.

www.manaraa.com

4.3.2 Correlation Engine

Results from both the RTTDT and the RSSDT were correlated to provide more confidence in the generated alarms. The correlation engine used was event based i.e. if one of the detection techniques detected an anomaly (an alert), the correlation engine activated and waited until it obtained the detection results from the other technique, before making a decision on whether or not to raise an alarm[14]. If both the detection techniques detected the anomaly, then an alarm will be raised (See Figure 4-5 for correlation engine state machine). For instance, if the RSSDT registered an abrupt spike in the RSS values for a particular MAC address, the correlation engine would register an alert and check the results of the RTTDT. If both techniques registered an alert for that MAC address, then an alarm would be raised. All the RSS events, that occurred while the correlation engine was waiting for the RTTDT's results, had no effect on the output. An alarm was only raised if both techniques registered an alert. Similarly, if the RTTDT detected that the RTT taken by the RTS-CTS frames for a particular MAC address had suffered a rapid surge; the correlation engine waited for the next RSS event and only raised an alarm if the RSSDT also registered a spike in the RSS value for that MAC address. The RTS-CTS events for that MAC address, while the correlation engine was waiting for an RSS event, were ignored for the purposes of intrusion detection. For the purposes of this dissertation, the passive IDS sensor was only used to create traffic capture dumps. The implementing the RSSDT, the RTTDT and the correlation engine, was then executed over the offline traffic captures to detect spoofing based attacks. Alerts generated by the RSSDT and the RTTDT were passed on to the correlation engine code for raising alarms if any.

4.3.3 Hardware Configuration

A Netgear DG834G Wireless Access Point was used as an AP (B). A Windows laptop with Intel WiFi Link 5100AGN WLAN card was used as STA (A) and a Linux laptop with Intel PRO/Wireless

[14]In this chapter, the detection results of the RTTDT and the RSSDT are referred to as alerts and the output of the correlation engine is called an alarm.

www.manaraa.com

3945ABG WLAN card was used as the attacker (C). A PC with Netgear WG111 wireless adapter running Wireshark tool under Linux was used in Radio Frequency Monitoring (RFMON) mode as the Monitor. The DG834G router's RTSThreshold option was set to 1 (always on). This enabled RTS-CTS handshake for traffic from AP to STA. No external antennas were used to enhance the reception and no attempt was made to modify the transmission power of any of the wireless equipment.

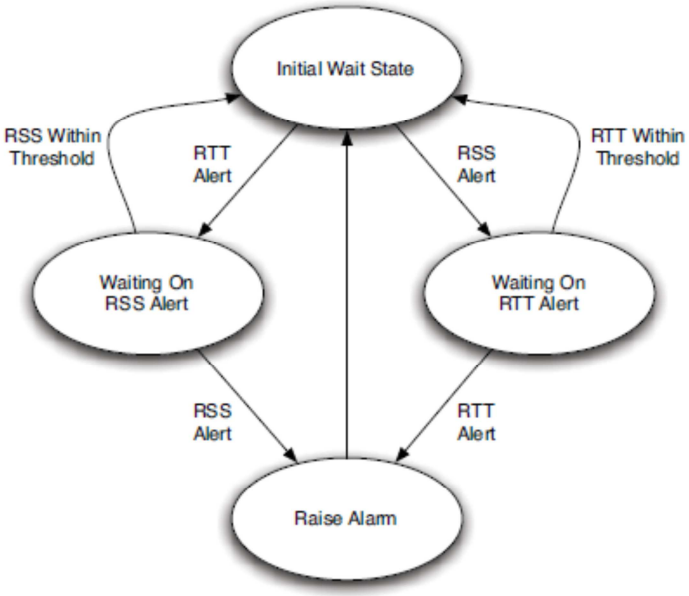


Figure 4-5: Correlation Engine State Machine [37]

4.3.4 Experimentation -Set1

In *Set1* of the experiments, robustness and reliability of the RTTDT and the RSSDT were tested when none of the participants were in motion. The AP, the IDS sensor, the STA and the attacker were all stationary in this set. In all scenarios, the AP was placed in close proximity to the IDS sensor. In Figure 4-6, points A, B and C represent location of the STA, the AP and the IDS sensor respectively. Points X,Y and Z in Figure 4-7 represent location of the attacker in Scenarios Two, Three and Four respectively.

4.3.4.1 Scenario One

In *Scenario One*, there was no attacker present and the AP and the STA were placed in close

www.manaraa.com

proximity to each other at points B and A respectively (see Figure 4-6). Network traffic was generated from the STA to the AP. The IDS sniffer was used to capture this WLAN traffic between the STA and the AP. After examination of 1000 captured frames, the *correlation engine* did not raise any alarms. As there was no attacker present, both the detection techniques and the correlation engine correctly did not generate any false positives.

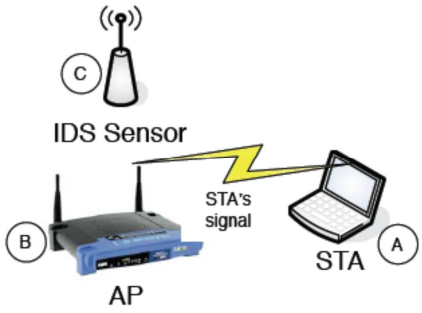


Figure 4-6: Correlation Experiments Scenario One

4.3.4.2 Scenario Two

In *Scenario Two*, the AP and the STA were placed in close proximity to each other at points B and A respectively. The attacker was placed in line of sight of the STA at point X (see Figure 4-7). Then network traffic was generated between the STA and the AP. The attacker then launched the attack on the STA.

In this scenario three different experiments were carried out; in the first one, the attacker launched a TKIP DoS Attack [41], in the second experiment he launched a Channel Switch DoS attack [60], while in the third experiment the attacker launched a Quite DoS attack [60]. For each experiment, traffic was captured using *Wireshark*, after that the captured traffic was examined using the IDS Sensor which is based on the *correlation engine*, which resulted in two alarms.

4.3.4.3 Scenario Three

In *Scenario Three*, the AP and the STA were placed in close proximity to each other (at points B and A respectively in Figure 4-7). The attacker was placed away from of the STA, in a different room, with no line of sight to the STA (at point Y in Figure 4-7). Then the remainder of the experiments was

www.manaraa.com

conducted in exactly same manner as *Scenario Two.* After running the IDS Sensor over the captured frames, three alarms were generated.

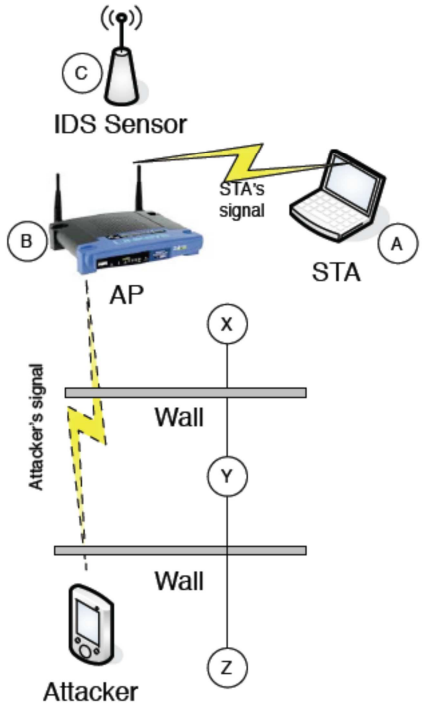


Figure 4-7: Correlation Experiments Scenario 2 (X), 3(Y), and 4(Z)

4.3.4.4 Scenario Four

In *Scenario Four*, the AP and the STA were placed in close proximity to each other (at points B and A respectively in Figure 4-7). The attacker was placed very far away from the STA (close to the RF range limit of the AP), with no line of sight to the STA (at point Z in Figure 4-7). The remainder of the experiment was conducted in similar fashion to Scenario Two. . After running the IDS Sensor over the captured frames, two alarms were generated.

4.3.5 Experimentation -Set2

In *Set2* of the experiments, the robustness and reliability of the RTTDT and the RSSDT were tested with the attacker stationary and the STA in motion between a point closer to the AP and another point far away from it. The AP, the IDS sensor, and the attacker were all stationary at locations B, C and D (see Figure 4-8 and Figure 4-9). In all scenarios, the IDS sensor was placed in close proximity to

www.manaraa.com

the AP. The equipment setup was exactly as described in Section 4.3.1.

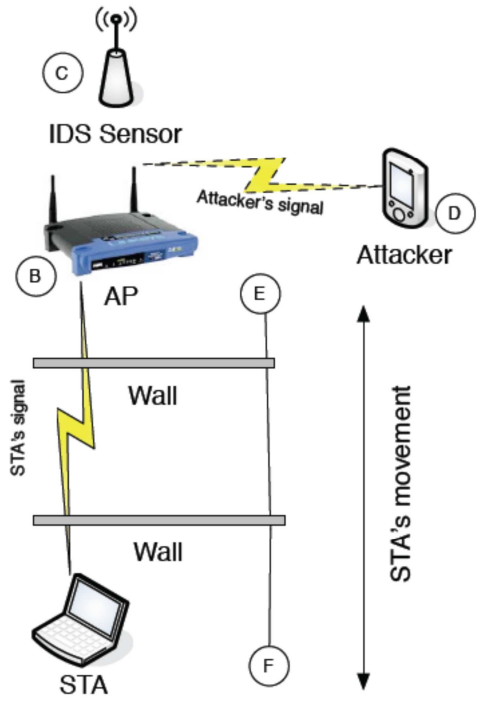


Figure 4-8: Correlation Experiments Scenario 5, and 6

4.3.5.1 Scenario Five

In *Scenario Five*, the AP and the attacker were stationary and were placed in close proximity to each other (in line of sight at points B and D in Figure 4-8). Network traffic was then generated from the STA to the AP. The STA then started traveling (at walking pace) from a point close to the AP to a point far away from it (i.e. from point E to F in Figure 4-8). Towards the end of the STA's journey, the attacker then launched three different attacks on the STA as described in Scenario Tow. After capturing the traffic; executing IDS Sensor over the captured traffic resulted in two alarms.

4.3.5.2 Scenario Six

In *Scenario Six*, the AP and the attacker were stationary and were placed in close proximity to each other (in line of sight at points B and D in Figure 4-8). Network traffic was then generated from the STA to the AP. The STA then started traveling (at walking pace) from a point far away from the AP to a point close to it (i.e. from point F to E in Figure 4-8). Towards the end of the STA's journey, the

www.manaraa.com

attacker then launched the attacks on the STA. The launched attacks were in exactly the same fashion as described in Scenario Tow. Executing IDS Sensor over the edited traffic capture two alarms were raised.

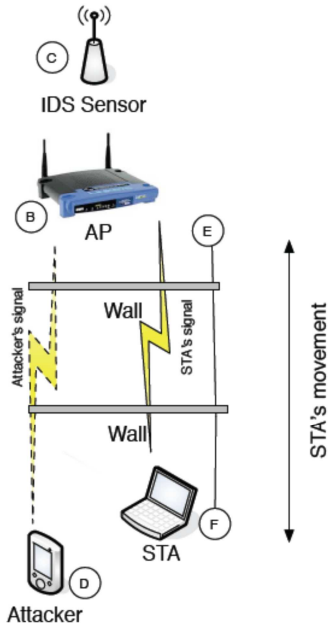


Figure 4-9: Correlation Experiments Scenario 7, and 8

4.3.5.3 Scenario Seven

In *Scenario Seven*, the AP and the attacker were stationary and were placed far away from each other (not in line of sight, at points B and D in Figure 4-9). Network traffic was then generated from the STA to the AP. The STA then started traveling (at walking pace) from a point at close proximity to the AP to a point far away from it (i.e. from point E to F in Figure 4-9). Towards the end of the STA's journey, the attacker then launched the attacks on the STA, which are the same as in Scenario Tow. After capturing the traffic and running IDS Sensor over it, three alarms were raised.

4.3.5.4 Scenario Eight

In *Scenario Eight*, the AP and the attacker were stationary and were placed far away from each other (not in line of sight, at points B and D in Figure 4-9). Network traffic was then generated from the STA to the AP. The STA then started traveling (at walking pace) from a point far away from the AP to

www.manaraa.com

a point close to it (i.e. from point F to E in Figure 4-9). Towards the end of the STA's journey, the attacker then launched the attacks on the STA, which are the same as in Scenario Tow. Executing IDS Sensor over the captured traffic three alarms were generated.

4.3.6 Analysis

4.3.6.1 True Positives and False Positives

A true positive is the alarm raised when an IDS correctly identifies an abnormal event as an attack, while a false positive is the alarm raised when an IDS misclassifies a normal event as an attack. A false negative is just the opposite of a true positive where the IDS fails to identify the attack and does not raise an alarm. In our experiments, no false negatives were registered i.e. all the attacks were successfully and accurately detected. However, some false positives were raised by the correlation engine.

Tables 4-3, 4-4, and 4-5 summarize the true positives raised by the correlation engine when applying TKIP DoS attack, Channel Switch DoS attack, and Quite DoS attack respectively in all eight scenarios. The first column is the scenario number, the second column is *RSSdiff* value that raises the alert, the third column represents the frame number (in the captured traffic dumps per scenario) where the RSS anomaly occurred, the fourth column is *RTTdiff* value that triggers the alert, and the fifth column represents the frame number (in the captured traffic dumps per scenario) where the RTT anomaly occurred. For instance, the entry for *Scenario Two* in Table 4-3 shows that when applying the first attack, the true alarm was raised by the correlation engine at frame 499. This alarm was caused by a RSS fluctuation (*RSSdiff* =19dBm) at frame 499 and a RTT spike at frame 510 (*RTTdiff* =29.651 mSec) for the STA. Frame 510 was the very next RTS-CTS handshake event for the STA after frame 499. Hence, both the RSSDT and the RTTDT sensors reported the anomaly and the TKIP DoS attack was identified correctly and accurately. Also, the entry for *Scenario Two* in Table 4-4 shows that when applying the second attack, the true alarm was raised by the correlation engine at frame 520. This alarm was caused by a RSS fluctuation (*RSSdiff* =16dBm) at frame 520 and a RTT spike at frame 543

www.manaraa.com

(*RTTdiff* =25.556 mSec) for the STA. Frame 543 was the very next RTS-CTS handshake event for the STA after frame 520. Hence, both the RSSDT and the RTTDT sensors reported the anomaly and the Channel Switch DoS attack was identified correctly and accurately. Moreover, the entry for *Scenario Two* in Table 4-5 shows that when applying the third attack, the true alarm was raised by the correlation engine at frame 602. This alarm was caused by a RSS fluctuation (*RSSdiff* =16dBm) at frame 602 and a RTT spike at frame 620 (*RTTdiff* =26.447 mSec) for the STA. Frame 620 was the very next RTS-CTS handshake event for the STA after frame 602. Hence, both the RSSDT and the RTTDT sensors reported the anomaly and the Quite DoS attack was identified correctly and accurately.

Scenario	RSSdiff (dBm)	Frame number	RTTdiff (mSec)	Frame number
One	NA	NA	NA	NA
Two	19	499	29.651	510
Three	34	550	39.204	585
Four	47	606	51.014	657
Five	32	554	43.751	590
Six	23	622	31.098	634
Seven	27	530	38.773	549
Eight	30	583	40.007	603

Table 7: True Positives for TKIP DoS Attack experiments

Scenario	RSSdiff (dBm)	Frame number	RTTdiff (mSec)	Frame number
One	NA	NA	NA	NA
Two	16	520	25.556	543
Three	37	603	40.002	630
Four	42	583	49.099	599
Five	27	532	40.071	545
Six	26	601	37.655	628
Seven	27	530	38.773	549
Eight	30	583	40.007	603

Table 8: True Positives for Channel Switch DoS Attack experiments

In all scenarios, the first alert raised was the RSS alert followed by the RTT alert. This can be explained by the fact that the number of RSS events in a traffic capture is higher than the RTS-CTS events and the attacker never starts the any one of the above attacks with a RTS-CTS handshake. The attacker sends a spoofed frame to the AP, leading to a RSS event first. The response transmission from

www.manaraa.com

the AP initiates a RTS-CTS handshake, enabling the passive monitor to take the RTT reading for the attacker. Hence, the RSSDT always detects the attack before the RTTDT.

Scenario	RSSdiff (dBm)	Frame number	RTTdiff (mSec)	Frame number
One	NA	NA	NA	NA
Two	16	602	26.447	620
Three	34	603	39.077	626
Four	38	593	47.014	639
Five	30	495	38.977	512
Six	28	598	36.007	620
Seven	22	617	31.055	633
Eight	26	589	32.411	603

Table 9: True Positives for Quite DoS Attack experiments

Scenario	RSSdiff (dBm)	Frame number	RTTdiff (mSec)	Frame number
One	NA	NA	NA	NA
Two	14	730	19.011	744
Three	24 27	698 811	31.112 33.009	718 840
Four	23	800	34.093	832
Five	13	389	24.225	411
Six	12	370	18.999	393
Seven	15 9	278 396	21.112 14.001	307 420
Eight	29 22	290 340	34.112 29.901	312 366

Table 10: False Positives for TKIP DoS Attack experiments

Scenario	RSSdiff (dBm)	Frame number	RTTdiff (mSec)	Frame number
One	NA	NA	NA	NA
Two	13	698	20.332	709
Three	30 32	721 826	33.878 35.552	754 865
Four	19	748	28.221	773
Five	11	335	21.222	378
Six	9	293	16.988	316
Seven	13 11	271 377	18.909 12.727	300 399
Eight	21	389	27.101	409

Table 11: False Positives for Channel Switch DoS Attack experiments

www.manaraa.com

Scenario	RSSdiff (dBm)	Frame number	RTTdiff (mSec)	Frame number
One	NA	NA	NA	NA
Two	11	765	19.991	789
Three	29 32	777 870	33.117 35.550	808 897
Four	26	781	38.887	800
Five	10	278	27.002	301
Six	15	390	25.333	409
Seven	22	410	33.011	437
Eight	12 14	300 378	17.112 15.553	329 404

Table 12: False Positives for Quite DoS Attack experiments

An interesting observation was made that in *Scenarios Two*, *Scenario Three* and *Scenario Four*, where all parties were stationary, all the false positives were detected in frames generated after the attack had commenced (Tables 4-3 : 4-8). This meant that all the false positives were caused by abnormal fluctuations in observed RSS and RTT values for the attacker. This observation was most likely the result of increasing distance between the attacker and the passive IDS monitor from *Scenario Two* to *Scenario Four*. Lack of line of sight connectivity and presence of various obstacles (walls, doors etc.) most likely acted as contributing factors to random fluctuations in observed RSS and RTT values for the attacker. Being positioned in close proximity of the sensor in all these scenarios, the STA did not suffer such random fluctuations and hence did not generate any false positives before the attack was launched.

However, in *Scenario five* to *Scenario Eight*, just the opposite was observed. The false positives were detected in frames generated before the attack had commenced, which meant that the source of these abnormalities was the STA and not the attacker. In these scenarios, the attacker was always stationary and the STA was in motion. These false positives can be attributed to the fluctuations in observed RSS and RTT values for the STA as a result of it being in motion.

The correlation technique successfully managed to keep the number of these false positives fairly low. The RSSDT and the RTTDT both successfully detected the performed attacks.

In *Scenario One*, *Scenario Two*, *Scenario Three* and *Scenario Four*, as expected, the *RSSdiff* and

www.manaraa.com

RTTdiff values increased as the attacker was placed further away from the STA. In *Scenario Five* and *Scenario Six*, the AP, the IDS sensor and the attacker were located in close proximity of each other and as expected, the *RSSdiff* and *RTTdiff* values increased as the STA moved away from them and decreased as the STA moved closer. In *Scenario Seven* and *Scenario Eight*, the attacker was located further away from the IDS sensor and the AP. The observed *RTTdiff* and *RSSdiff* values increased as the STA moved away from the attacker, and decreased as it moved closer to the attacker (see Tables 4-3, 4-4, and 4-5).

4.3.6.2 Single Anomalies

Analysis of the *Correlation Engine* debug logs indicated that there were instances when the RSSDT and the RTTDT disagreed with each other. In this dissertation, we refer to these disagreements as *single anomalies*. A single anomaly would occur if a RSS alert was registered by the RSSDT, while the RTTDT did not register an anomaly in the next RTS-CTS event for that MAC address. Another example would be if a RTT alert was raised by the RTTDT but the next RSS reading for that MAC address was below the threshold. The RSSDT and the RTTDT only raise an alert if the difference between the last observed and current characteristic is above a threshold. In these experiments, both these thresholds *RSSdiff threshold* and the *RTTdiff threshold* were set to the value of 5. Single anomalies were ignored by the correlation engine and an alarm was only raised if both the detection techniques register an alert.

Scenario	TKIP Dos Attack		Channel Switch DoS Attack		Quite DoS Attack	
	Number of RSS Single Anomalies	Number of RTT Single Anomalies	Number of RSS Single Anomalies	Number of RTT Single Anomalies	Number of RSS Single Anomalies	Number of RTT Single Anomalies
One	None	None	None	None	None	None
Two	1	1	1	1	1	1
Three	3	1	3	1	3	1
Four	1	0	1	0	1	0
Five	5	2	5	2	5	2
Six	3	3	3	3	3	3
Seven	4	2	4	2	4	2
Eight	4	4	4	4	4	4

Table 13: Number of Single Anomalies

www.manaraa.com

Table 4-9 shows the number of the observed single anomalies in each scenario and demonstrates the number of potential false positives per scenario that were successfully avoided by the correlation technique. The number of single anomalies is a direct function of the threshold values chosen for each detection technique. As expected, both the RSS and RTT single anomalies increased in number in the last four scenarios, due to the mobility of the STA.

Figure 4-10 shows the distribution of single anomalies registered by the RSSDT and the RTTDT when running the TKIP DoS Attack experiment, where the correlation engine did not raise an alarm, even though an anomaly was detected by at least one of the detection techniques.

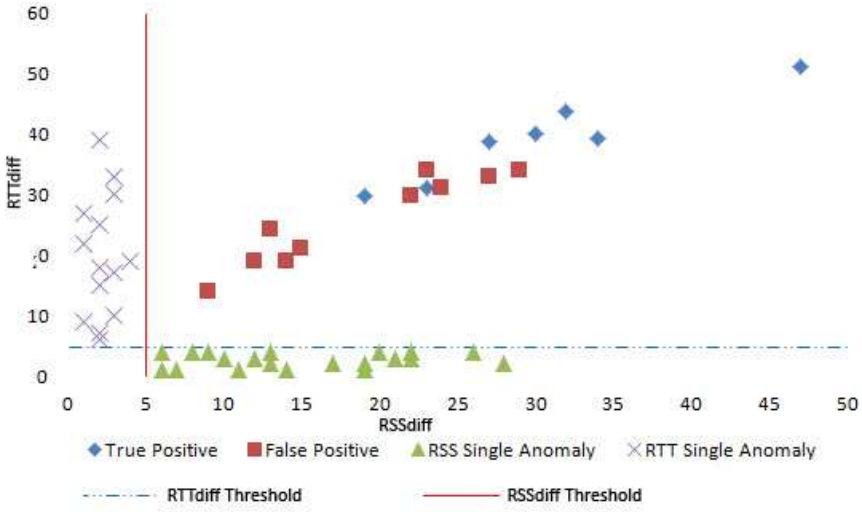


Figure 4-10: Alarms and Single Anomalies for TKIP Dos Attack Experiment

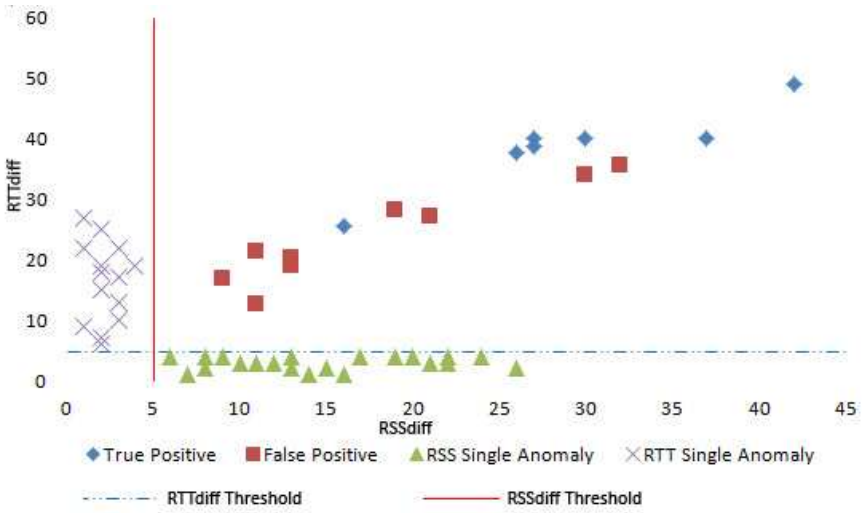


Figure 4-11: Alarms and Single Anomalies for Channel Switch DoS Attack Experiment

www.manaraa.com

Figure 4-11 shows the distribution of single anomalies registered by the RSSDT and the RTTDT when running the Channel Switch DoS Attack experiment, where the correlation engine did not raise an alarm, even though an anomaly was detected by at least one of the detection techniques.

Figure 4-12 shows the distribution of single anomalies registered by the RSSDT and the RTTDT when running the Quite DoS Attack experiment, where the correlation engine did not raise an alarm, even though an anomaly was detected by at least one of the detection techniques.

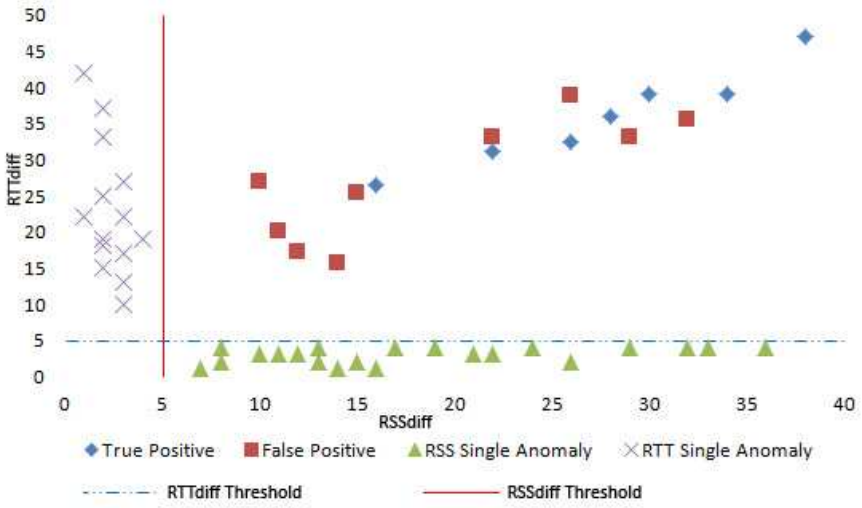


Figure 4-12: Alarms and Single Anomalies for Quite DoS Attack Experiment

4.4 Threshold Optimization

In all these experiments discussed in sections 4.3.4 and 4.3.5, the *RSSdiff threshold* and the *RTTdiff threshold* were set to a value of 5; this value was suggested according to the results of the preliminary experiments presented in sections 4.2.1 and 4.2.2. This means a RSS anomaly was only registered if the *RSSdiff* was greater than 5 and a RTT anomaly was only acknowledged if the *RTTdiff* value was greater than 5. An alarm was raised by the correlation engine only when both the *RSSdiff threshold* and the *RTTdiff threshold* were exceeded. The threshold value 5 was thought to be just low enough to avoid a high number of false negatives and just high enough to avoid a large volume of false positives. Since ideally both the techniques should exhibit the same level of accuracy, the same threshold value was used for both. In these experiments (in sections 4.3.4 and 4.3.5), both the

www.manaraa.com

thresholds were set to the same value, while there is no need for the *RTTdiff threshold* and the *RSSdiff threshold* to be with the same value.

1. *Read the captured packets from the dump file*
2. *Filter the points according to their class (true positive, false positive…)*
3. *Let F_{min}=($RSSdiff_{min}$, $RTTdiff_{min}$) be the frame of class "true positive" such that it has the least RSSdiff and RTTdiff values*
4. *If $RSSdiff_{min} \in \mathbb{N}$*

   Set the optimized RSSdiff threshold = $RSSdiff_{min} - 1$

   Else If $RSSdiff_{min} \in \mathbb{R}$

   Set the optimized RSSdiff threshold = $\lfloor RSSdiff_{min} \rfloor$
5. *If $RTTdiff_{min} \in \mathbb{N}$*

   Set the optimized RTTdiff threshold = $RTTdiff_{min} - 1$

   Else If $RSSdiff_{min} \in \mathbb{R}$

   Set the optimized RTTdiff threshold = $\lfloor RTTdiff_{min} \rfloor$

Where $\mathbb{N}$ is the set of all natural numbers, and $\mathbb{R}$ is the set of all real numbers

Figure 4-13: RSSdiff threshold and RTTdiff threshold optimization algorithm

In the real world, we need to optimize these threshold values to ensure the lowest possible number of false positives and false negatives.

Experiment	New *RSSdiff* threshold	New *RTTdiff* threshold
TKIP DoS Attack	18	29
Channel Switch DoS Attack	15	**25**
Quite DoS Attack	**15**	26

Table 14: Optimized RSSdiff and RTTdiff thresholds

Choosing the best threshold value for each detection technique can be performed using the algorithm presented in Figure 4-13.

www.manaraa.com

Table 4-10 represents the optimized thresholds after applying the algorithm in Figure 4-13 on the results of section 4.3.4 and 4.3.5 experiments.

Referring to Table 4-10 we found that the optimized thresholds are very close for the three attacks experiments. In our opinion, from a general intrusion detection perspective, it is far more critical for an IDS to minimize the false negative rate than to maintain a low false positive rate. The cost of missing an attack is much higher than the cost of raising a false alarm. Therefore, we choose the minimum threshold to avoid the false negatives i.e. 15 for *RSSdiff* threshold and 25 for *RTTdiff* threshold.

Figures 4-10, 4-11, and 4-12 represent the true positives, false positives and single anomalies registered by the IDS when using the initial threshold settings. In Figures 4-10, 4-11, and 4-12; *RSSdiff Threshold* and *RTTdiff Threshold* refer to initial values used for thresholds (i.e. 5 for all scenarios). Figures 4-14, 4-15, and 4-16 represent the true positives, false positives and single anomalies registered by the IDS when using the optimum threshold settings. In Figure 4-14, 4-15, and 4-16, *RSSdiff Threshold* and *RTTdiff Threshold* refer to the optimized values of *RSSdiff* and *RTTdiff* thresholds respectively. These values were generated by applying the Algorithm in Figure 4-13 to minimize the number of false positives and false negatives.

Table 4-13 demonstrates that RSSdi*ff* thresho*ld* of 15 and RTTdi*ff* threshold of 25 which are the optimum choice for the thresholds of the detection techniques. Figures 4-14, 4-15, and 4-16 show how the single anomalies, false positives and true positives are affected by the new optimum threshold values. As a result of the new thresholds, some false positives became RSS single anomalies or RTT single anomalies. The new thresholds did not introduce any false negatives since there are no true positives became false negatives. Moreover, no single anomaly was converted into a false positive as a result of the new threshold. However, some of the single anomalies (both RSS and RTT single anomalies) became normal events. Hence with 100% true positive detection, *RSSdiff* Optimized Threshold of 5 and *RTTdiff* Optimized Threshold of 25 prove to be the optimum threshold values for the test scenarios presented in this chapter.

www.manaraa.com

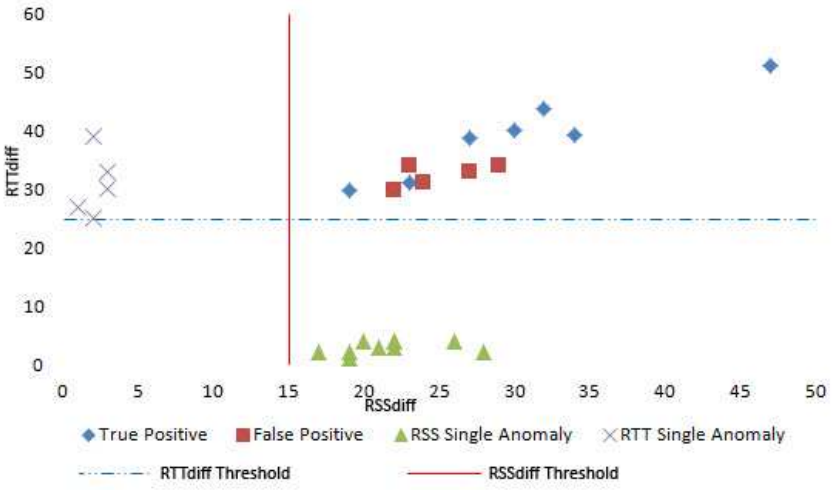


Figure 4-14: Alarms and Single Anomalies for TKIP DoS Experiment when applying the optimized threshold

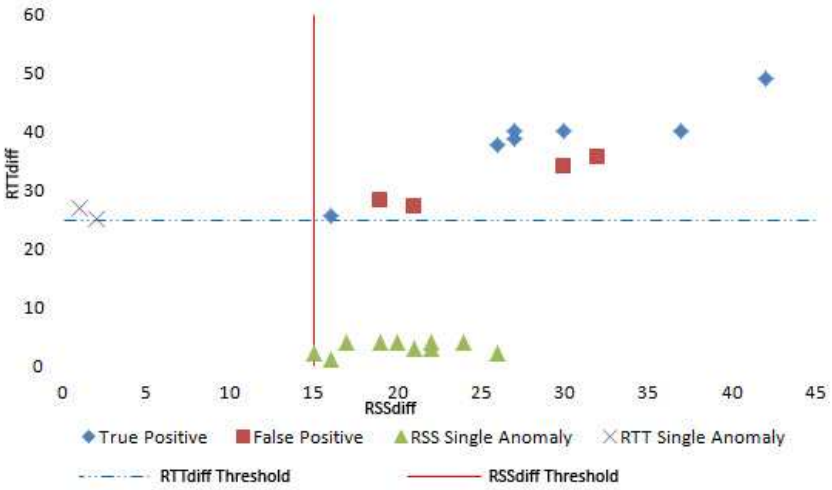


Figure 4-15: Alarms and Single Anomalies for Channel Switch DoS Experiment when applying the optimized threshold

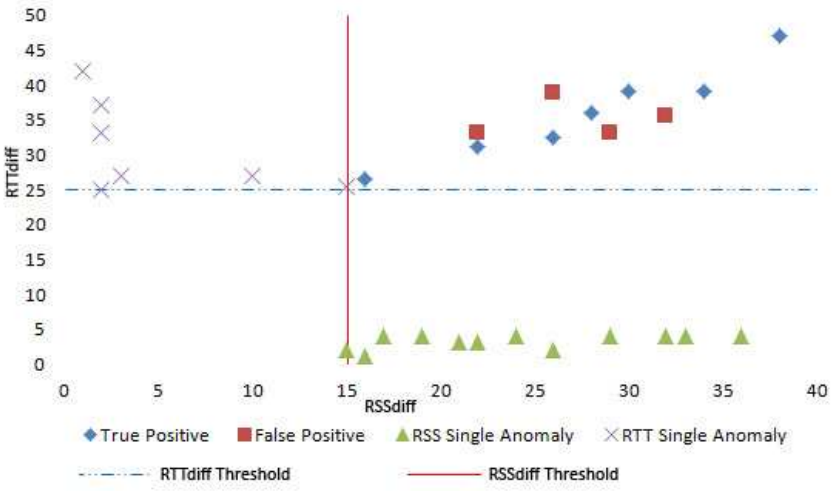


Figure 4-16: Alarms and Single Anomalies for Quite DoS Experiment when applying the optimized threshold

www.manaraa.com

Accuracy and efficiency of the RSSDT and the RTTDT depends on the choice of suitable threshold values and hence places a large expectation on these threshold values to be optimally calculated. This increases the importance of our developed algorithm (Figure 4-13).

Thresholds are unique to each WLAN environment and can also change frequently. Hence, the thresholds should be regularly calculated to optimum values. Using a distributed approach and deploying multiple distributed co-operating IDS sensors can decrease this expectation on the accuracy of the threshold values. Rather than relying on the alarms generated by a single IDS sensor, the intrusion detection process can be enhanced by correlating detection results across multiple sensors. This also makes it a much harder job for the attacker to launch a successful spoofing attack as they will have to guess and spoof the RSS and the RTT values for the legitimate nodes, as observed by each IDS sensor. This will require the attacker to be at multiple locations at the same time, hence making it very hard for the attacker to launch an undetected attack.

4.5 Correlating Across IDS Sensors

In the previous sections we examine the performance of correlating RSSDT and RTTDT results across single IDS monitor, this monitor is supposed to be close to the AP. All the performed experiments were conducted to include all home or office computers' states, including being stationary or mobile at walking pace. Correlation results yields the increased detection performance by reducing false positives.

If we suppose implementing a WIDS in a multi AP WLAN, then we intend to use several IDS sensors distributed across the WLAN in the same manner as the APs distribution; the distributed nature of the WIDS will produce highly reliable detection results. This is achieved by correlating the alarms raised for a node across the sensors. Then these cross sensor correlated alarms are further correlated across the detection techniques (as in section 4.3.2) to provide a method to automatically detect attack scenarios and assign a response priority to them. Hence, cross sensor and cross detection technique correlation is used to detect a large number of WLAN attack scenarios reliably and automatically.

www.manaraa.com

Chapter 5 Conclusions and Future Research Directions

Achieving security objectives solely with preventative techniques is not always possible. Preventative approaches can fail to ensure security either owing to flaws in the design, implementation or configuration of the preventative control measures. Accepting that control measures may be imperfect, the need to supplement them with monitoring techniques capable of detecting intrusions and to confirm that the measures are operating as expected is readily apparent.

The notion of monitoring computer systems and networks for malicious activity is long-standing [7]. Nowhere is the requirement for preventative approaches to security to be supplemented by a monitoring and detection capability more crucial than in wireless local area networks (WLANs). The broadcast nature of the physical (PHY) layer in wireless networks makes gaining access to the medium a trivial undertaking. Flawed legacy encryption schemes such as wired equivalence privacy (WEP), the forgeabilty of management frames and the spoofability of MAC addresses and other frame contents combine to make attacks like eavesdropping, session hijacking and denial of service a real threat for WLANs.

While recent enhancements to the IEEE 802.11 standard [51] undoubtedly improve the level of security that preventative techniques can bring to bear on wireless network deployments, security vulnerabilities still persist. To augment preventative measures, a comprehensive monitoring capability seems imperative in WLANs.

The aim of this research was to:

- Review security vulnerabilities that still exist in WLANs secured using IEEE 802.11i (specifically RSNs).
- Identify drawbacks and limitations of currently available wireless intrusion detection techniques and investigate if they are capable of reliably detecting attacks that exploit various outstanding RSN vulnerabilities.

www.manaraa.com

- Enhance the performance of intrusion detection techniques that address the gap left by current detection techniques in reliably detecting all attacks on RSNs.

5.1 WLAN Security

Chapter 2 reviewed the security of WLANS in light of IEEE 802.11i RSNs. It found that use of well proven and robust security measures in RSNs has reliably addressed the threats of traffic analysis, passive eavesdropping, message injection/modification/replay and unauthorized access in WLANs.

Unfortunately, the preventative measures employed in IEEE 802.11i RSNs fail to address a number of security issues and hence there still exist a number of vulnerabilities in RSNs that can be exploited to launch an attack against 802.11i protected WLANs (discussed in detail in Section 2.7.8).

In summary, the 802.11i security measures are only designed to work for protection of the Data frames, while the Management and the Control frames still remain unprotected and hence vulnerable to abuse and forgery. Although 802.11i uses EAP for authentication, the standard does not have any requirements or guidance on which EAP methods are suitable to use in RSNs. As pointed out in Section 2.7, not all EAP authentication methods are suitable for use in WLANs [88, 91]. Hence despite using the strongest confidentiality and integrity protection, if a RSN does not use an appropriately strong EAP method, it is still vulnerable to unauthorized access based attacks. The EAP frames themselves are also unprotected and hence can be easily forged by an adversary.

IEEE 802.11i does not address any attacks on availability of WLANs using virtual or radio jamming.

5.2 Wireless Intrusion Detection

In light of the vulnerabilities that still infect RSNs, it is imperative to augment preventative security measures with a comprehensive monitoring capability which not only detects attacks and intrusions but also monitors compliance to the security policy. Security policy compliance monitoring would not

www.manaraa.com

only help detect adversaries, but it will also assist in detecting misconfigured and misbehaving nodes. Any deviations from the security policy such as using the wrong cryptographic algorithms or unsafe EAP methods can introduce serious vulnerabilities in a WLAN.

Chapter 3 reviewed the hierarchical relationship between all the RSN vulnerabilities discussed in Section 2.7.8 to facilitate the analysis of the current WIDTs. This analysis also laid the foundation for the focus of work presented in Chapter 4. The hierarchical analysis of the RSN vulnerabilities showed that almost all RSN vulnerabilities depend on the MAC spoofing vulnerability to be exploited. Hence a good WIDS should use WIDTs that can reliably detect MAC spoofing activity, as this is the basic component of all RSN attacks. The rest of the vulnerabilities were divided into two main categories -*Security Policy Violations* and *Protocol Limitations* (see Figure 3.2). The *Protocol Limitations* category comprises of vulnerabilities such as unprotected frames, Michael algorithm's weakness, unprotected duration field etc. The *Security Policy Violations* category contains all vulnerabilities caused by violations of site security policy. Hence a comprehensive WIDS should be capable of detecting MAC spoofing and attacks that exploit vulnerabilities caused by security policy violations and various protocol flaws and limitations in RSNs.

Chapter 3 analyzed the currently available WIDTs for each RSN vulnerability. It found that current WIDTs are not capable of detecting all attacks that exploit various RSN vulnerabilities and suffer from a number of flaws and cannot be relied upon from an intrusion detection perspective. There is a need to enhance the performance of WIDTs that are more robust in detecting attacks on RSNs and are complementary in nature so that when used together in a WIDS, they can assist each other in detecting the attacks in a more reliable and robust manner.

5.3 MAC Spoofing Detection using Anomaly-Based WIDTs

The hierarchical analysis of RSN vulnerabilities in Chapter 3 demonstrated that MAC spoofing is the common component in all attacks on RSNs. Hence, Chapter 4 studied two anomaly-based WIDTs to reliably detect MAC spoofing activity. These WIDTs were the *Received Signal Strength*

www.manaraa.com

Based Intrusion Detection Technique (RSSDT) and the *Round Trip Time Based Intrusion Detection Technique* (RTTDT). These techniques monitor anomalous fluctuations in the received signal strength (RSS) and the RTS-CTS handshake round trip time (RTT) profiles to detect MAC spoofing activity. Monitoring the RSS and RTT profiles is reliable from an intrusion detection perspective as these profiles are based on unspoofable attributes of the PHY and MAC layers and hence cannot be spoofed or guessed by an adversary.

Accuracy of both these techniques relies on selection of appropriate thresholds. Hence, Chapter 4 also presented a novel algorithm that calculates the optimum thresholds.

As both the RSSDT and the RTTDT are capable of detecting MAC spoofing activity, Chapter 4 also verified that correlating the detection results of both the detection techniques using an event based correlation engine provides even more reliable and robust detection of MAC spoofing.

5.4 Limitations

The RSSDT and the RTTDT are specialized in detecting MAC spoofing activity. Each detection technique however suffers from its own limitations and drawbacks. The limitation of the RSSDT and the RTTDT is that they require the victim and the attacker to be present at the same time in the WLAN. The RSSDT's rate of detection is directly proportional to the frame injection rate of the victim and that of the attacker. On the other hand, the RTTDT's rate of detection is directly proportional to the frequency of RTS-CTS handshakes in the WLAN.

5.5 Future Directions

An avenue for future research is enhancing the RTTDT to use handshake events that are more frequent than RTS-CTS handshakes. One potential candidate is using the atomic DATA-ACK exchanges to measure the RTT between an AP and an STA. This is possible because every Data frame is positively acknowledged using a return ACK frame from the receiver and just like the RTS-CTS handshake, a DATA-ACK exchange is guaranteed to be an atomic operation using virtual carrier

www.manaraa.com

sensing. It is envisaged that using DATA-ACK exchanges will assist the RTTDT in detecting MAC spoofing more readily than having to wait for RTS-CTS events.

Further research is also required for developing methods to correlate alarms not only across wireless intrusion detection techniques within a WIDS, but also across the WIDSs themselves. Correlation across wired IDSs and WIDSs also requires further research.

The hypotheses discussed in this dissertation to inform cross sensor correlation algorithms should also be tested further using more comprehensive empirical data and statistical techniques. The lack of existence of a standard test data set for WLAN attacks also needs to be addressed to provide statistical significance to detection results of various WIDTS.

It was also noted that the wireless intrusion response techniques available currently are quite inadequate and exploit the same vulnerabilities that the adversaries use to launch an attack against the WLANs [23, 48, 104]. Some of these flawed techniques include sending forged Deauthentication or Disassociation frames to the adversary to disconnect it from the WLAN. It should be noted that active responses over the wireless medium expose the WIDS to fingerprinting [104]. Intrusion response actions can also be taken over the wired network with the assistance of the APs. Hence, wireless intrusion response techniques and their delivery mechanisms remain candidates for further research.

5.6 Concluding Remarks

Despite using a number of preventative security measures, IEEE 802.11i RSNs still suffer from multiple vulnerabilities that can be exploited by an adversary to launch attacks against them. This underlines the need for using a monitoring framework as a second layer of defense for WLANs. Such a monitoring capability can be implemented using a wireless intrusion detection system. Unfortunately, the currently available wireless intrusion detection techniques are not very reliable and robust and also do not detect all the attacks on RSNs.

This research addresses this gap in the current body of knowledge by studying and enhancing the performance of two wireless intrusion detection techniques that address majority of RSN attacks. This

www.manaraa.com

research also demonstrates that the detection results can be correlated across the WIDS sensors and also the detection techniques themselves to provide greater assurance in the reliability of the alarms and enable automatic attack scenario recognition.

www.manaraa.com

References

[1] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). *The Internet Engineering Task Force-Request for Comments*, RFC 3748, 2004.

[2] B. Aboba and D. Simon. PPP EAP TLS Authentication Protocol, 1999.

[3] F. Adelstein, P. Alla, R. Joyce, and G. Richard III. Physically locating wireless intruders. *International Conference on Information Technology: Coding and Computing (ITCC'04)*, 1, 2004.

[4] A. Adya, P. Bahl, R. Chandra, and L. Qiu. Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks. *Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 30– 44, 2004.

[5] A. Agiwal, P. Khandpur, and H. Saran. LOCATOR: location estimation system For wireless LANs. *Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, pages 102–109, 2004.

[6] R. Ahlawat and K. Dulaney. Magic Quadrant for Wireless LAN Infrastructure, 2006. *Gartner Research*, 2006.

[7] J. Anderson. Computer Security Threat Monitoring and Surveillance. Report 79F296400, James P. Anderson Co., 1980.

[8] L. Andrew. Snort-Wireless. [Online] Available: http://www.snort.org/ [Accessed: November 2009], 2005.

[9] W. Arbaugh. An inductive chosen plaintext attack against WEP/WEP2. *IEEE Document*, 802(01):230, 2001.

[10] W. Arbaugh, N. Shankar, and Y. Wan. Your 80211 wireless network has no clothes. *Wireless Communications, IEEE*, 9(6):44–51, 2002.

[11] N. Asokan, V. Niemi, and K. Nyberg. Man-in-the-Middle in Tunnelled Authentication Protocols. *11th Security Protocols Workshop*, pages 28–41, 2003.

www.manaraa.com

[12] R. Bace and P. Mell. NIST Special Publication on Intrusion Detection Systems. *National Institute of Standards and Technology, draft document, February*, 2001.

[13] P. Bahl and V. Padmanabhan. RADAR: an in-building RF-based user location and tracking system. *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 2, 2000.

[14] J. Bardwell. Converting Signal Strength Percentage to dBm Values. [Online] Available: http://www.wildpackets.com/elements/ whitepaper/Converting_Signal_Strength.pdf [Accessed: August 2010], 2002.

[15] J. Bellardo and S. Savage. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In *Proceedings of the USENIX Security Symposium. Washington D.C., USA*, 2003.

[16] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11. *Proceedings of the 7th annual international conference on Mobile computing and networking*, pages 180–189, 2001.

[17] L. Butti and F. Veysset. Wi-Fi Advanced Stealth, BlackHat 2006 Briefing, [Online] Available: http://2006.hack.lu/images/4/4f/ HackLU06-ButtiVeysset-WiFiAdvancedStealth-slides-3.pdf [Accessed: May 2010], 2006.

[18] N. Cam-Winget, D. McGrew, J. Salowey, and H. Zhou. EAP Flexible Authentication via Secure Tunneling (EAP-FAST). *draft-cam-winget-eap-fast-00, February*, 2003.

[19] B. Caswell, J. Foster, R. Russell, J. Beale, and J. Posluns. *Snort 2.0 Intrusion Detection*. Syngress Publishing, 2003.

[20] J. Chen, M. Jiang, and Y. Liu. Wireless LAN security and IEEE 802.11i. *Wireless Communications, IEEE*, 12(1):27–36, 2005.

[21] H. Cheung. FBI Teaches Lesson in how to break into Wi-Fi networks. *Information Week Network Pipeline*, 2005.

[22] C. Chin-Yang Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A

www.manaraa.com

specification-based intrusion detection system for AODV. In *SASN*, pages 125–134, 2003.

[23] M. Chirumamilla and B. Ramamurthy. Agent based intrusion detection and response system for wireless LANs. In *IEEE ICC '03. Volume: 1 , 11-15 May*, pages 492–496, 2003.

[24] D. Dai Zovi and S. Macaulay. Attacking automatic wireless network selection. *Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. Proceedings from the Sixth Annual IEEE*, pages 365–372, 2005.

[25] DARPA. DARPA Intrusion Detection Evaluation Data Sets. Lincoln Laboratory, Massachusetts Institute of Technology, [Online] Available: http://www. ll.mit.edu/IST/ideval/data/data_index.html [Accessed: March 2010], 2005.

[26] J. Day and H. Zimmermann. The OSI reference model. *Proceedings of the IEEE*, 71(12):1334–1340, 1983.

[27] H. Debar and J. Viinikka. Intrusion detection: Introduction to intrusion detection and security information management. *FOSAD*, 2005:2005, 2004.

[28] H. Debar and J. Viinikka. Intrusion Detection: Introduction to Intrusion Detection and Security Information Management. In *FOSAD 2004/2005*, 2005.

[29] U. Deshpande, T. Henderson, and D. Kotz. Channel Sampling Strategies for Monitoring Wireless Networks. *Proceedings of the Second International Workshop On Wireless Network Measurement (WiNMee)*, pages 1–7, 2006.

[30] J. Edney and W. Arbaugh. *Real 802.11 Security: Wi-Fi Protected Access and 802.11 i*. Addison-Wesley, 2004.

[31] J. Ellch. *Fingerprinting 802.11 Devices*. PhD thesis, Naval Postgraduate School; Available from National Technical Information Service, 2006.

[32] B. Fleck and J. Dimov. Wireless Access Points and ARP Poisoning. *Available from* http://www.eecs.umich.edu/˜aprakash/eecs588/handouts/arppoison.pdf, 2003.

[33] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4.

www.manaraa.com

Eighth Annual Workshop on Selected Areas in Cryptography, 2001.

[34] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Van Randwyk, and D. Sicker. Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. *Proceedings of the 15th Usenix Security Symposium*, 2006.

[35] S. Ganu, A. Krishnakumar, and P. Krishnan. Infrastructure-based location estimation in WLAN networks. *IEEE Wireless Communications and Networking Conference (WCNC 2004)*, 1:465–470, 2004.

[36] M. Gast and M. Loukides. *802.11 Wireless Networks: The Definitive Guide*. ISBN0596001835. O'Reilly & Associates, Inc., 2002.

[37] R. Gill, J. Smith, and A. Clark. Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks. In R. Safavi-Naini, C. Steketee, and W. Susilo, editors, *Fourth Australasian Information Security Workshop (Network Security) (AISW 2006)*, volume 54 of *CRPIT*, pages 221–230, Hobart, Australia, 2006. ACS.

[38] R. Gill, J. Smith, and A. Clark. Specification-Based Intrusion Detection in WLANs. In *Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06)*, pages 141–152. IEEE Computer Society, 2006.

[39] R. Gill, J. Smith, M. Looi, and A. Clark. Passive Techniques for Detecting Session Hijacking Attacks in IEEE 802.11 Wireless Networks. In *Proceedings of AusCERT Asia Pacific Information Technology Security Conference (AusCert 2005): Refereed R&D Stream*, pages 26 – 38, 2005.

[40] J. Girard and J. Pescatore. Wi-Fi Security Best Practices for Company Offices. *Gartner Research*, 2006.

[41] S. Glass and V. Muthukkumarasamy. A Study of the TKIP Cryptographic DoS Attack. 15th IEEE International Conference on Networks, 2007.

[42] A. Godber and P. Dasgupta. Countering rogues in wireless networks. *International Conference on*

www.manaraa.com

Parallel Processing Workshops, pages 425–431, 2003.

[43] F. Guo and T. Chiueh. Sequence Number-Based MAC Address Spoof Detection. In *8th International Symposium on Recent Advances in Intrusion Detection*, pages 309 – 329, 2005.

[44] J. Hall, M. Barbeau, and E. Kranakis. Radio frequency fingerprinting for intrusion detection in wirless networks. *IEEE Transactions on Defendable and Secure Computing*, 2005.

[45] H. Haverinen and J. Salowey. EAP SIM Authentication. *Work in Progress, April*, 2004.

[46] C. He and J. Mitchell. Analysis of the 802.11i 4-way handshake. In *WiSe '04: Proceedings of the 2004 ACM workshop on Wireless security*, pages 43–50. ACM Press, 2004.

[47] C. He and J. Mitchell. Security Analysis and Improvements for IEEE 802.11i. In *Proceedings of the 12th Annual Network and Distributed System Security Symposium*, Feb 2005.

[48] W. Hsieh, C. Lo, J. Lee, and L. Huang. The implementation of a proactive wireless intrusion detection system. In *The Fourth International Conference on Computer and Information Technology. CIT '04. 14-16 Sept*, pages 581–586, 2004.

[49] IEEE. IEEE Standard 802.11-1997. 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, 1999. Institute of Electrical and Electronics Engineers.

[50] IEEE. IEEE Standard 802.1X-2001. IEEE Standard for Local and metropolitan area networks -Port-Based Network Access Control, June 2001. Institute of Electrical and Electronics Engineers.

[51] IEEE. 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, 2004. Institute of Electrical and Electronics Engineers.

www.manaraa.com

[52] K. Ilgun, R. Kemmerer, and P. Porras. State Transition Analysis: A Rule-Based Intrusion Detection Approach. *IEEE Trans. Software Eng.*, 21(3):181–199, 1995.

[53] AirDefense Inc. Airdefence, [Online] Available: http://www. airdefense.net/ [Accessed: June 2010], 2007.

[54] AirMagnet Inc. AirMagnet, [Online] Available: http://www.airmagnet. com/ [Accessed: June 2010], 2007.

[55] Malinen J. Hostap, [Online] Available: http://hostap.epitest.fi/ [Accessed: July 2010], 2007.

[56] R. Jan and Y. Lee. An indoor geolocation system for wireless LANs. *32nd International Conference on Parallel Processing Workshops*, pages 29–34, 2003.

[57] J. Jonsson. On the Security of CTR+ CBC-MAC. *Selected Areas in Cryptography, 9th Annual Workshop (SAC 2002)*, 2595:76–93, 2002.

[58] V. Kasarekar and B. Ramamurthy. Distributed hybrid agent based intrusion detection and real time response system. *First International Conference on Broadband Networks (BroadNets 2004)*, pages 739–741, 2004.

[59] J. Kleider, S. Gifford, S. Chuprun, and B. Fette. Radio frequency watermarking for OFDM wireless networks. *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'04)*, 5, 2004.

[60] B. Konings, F. Schaub, F. Kargl, and S. Dietzel. Channel switch and quiet attack: New DoS attacks exploiting the 802.11 standard. IEEE 4th Conference on Local Computer Networks, 2009.

[61] P. Kyasanur and N. Vaidya. Detection and handling of MAC layer misbehavior in wireless networks. *International Conference on Dependable Systems and Networks*, pages 173–182, 2003.

[62] Y. Lim, T. Yer, J. Levine, and H. Owen. Wireless intrusion detection and response. In *Information Assurance Workshop. IEEE Systems, Man and Cybernetics Society, 18-20 June*, pages 68–75, 2003.

www.manaraa.com

[63] Milner M. Netstumbler, [Online] Available: http://www.stumbler.net/ [Accessed: February 2010], 2005.

[64] Osborne M. WIDZ, [Online] Available: http://www.loud-fat-bloke.co.uk/w80211.html [Accessed: December 2009], 2007.

[65] D. Madory. *New Methods of Spoof Detection in 802.11 b Wireless Networking*. PhD thesis, Dartmouth College, 2006.

[66] D. Maynor and J. Cache. Device Drivers, BlackHat 2006 Briefing, 2006.

[67] A. Mishra and W. Arbaugh. An Initial Security Analysis of the IEEE 802.1X Standard. Technical report, [Online] Available: http://citeseer.ist. psu.edu/566520.html [Accessed: June 2010], 2003.

[68] V. Moen, H. Raddum, and K. Hole. Weaknesses in the temporal key hash of WPA. *ACM SIGMOBILE Mobile Computing and Communications Review*, 8(2):76–83, 2004.

[69] H. Moore. Apple Airport 802.11 Probe Response Kernel Memory Corruption, 2006. [Online] Available: http://www.securiteam.com/securitynews/ 6M0010AHFW.html [Accessed: April 2010], 2006.

[70] J. Morrison. IEEE 802.11 wireless local area network security through location authentication, 2002. Masters Thesis. Naval Postgraduate School Monterey, California.

[71] AirTight Networks. AirTight, [Online] Available: http://www.airtightnetworks.net/ [Accessed: January 2010], 2007.

[72] R. Neumerkel and S. Grob. A Sophisticated Solution for Revealing Attacks on Wireless LAN. *Proceedings of the 3rd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus 06)*, pages 162–171, 2006.

[73] NIST. Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, Nov 2002. National Institute of Standards and Technology. Special Publication 800

48. [Online] Available: http://csrc.nist.gov/publications/nistpubs/ 800-48/NIST_SP_800-48.pdf

[74] NIST. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, Feb 2007.

www.manaraa.com

National Institute of Standards and Technology. Special Publication 800-97. [Online] Available: http://csrc.nist.gov/publications/ nistpubs/800-97/SP800-97.pdf

[75] NSA. Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS), National Security Agency. Network Hardware Analysis and Evaluation Division. [Online] Available: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/wireless/I332-005R-2005.pdf [Accessed: January 2010], 2005.

[76] M. Nystroem. The Protected One-Time Password Protocol (EAP-POTP). *Network Working Group Internet Draft, June*, 2005.

[77] M. Ossmann. WEP: Dead Again, [Online] Available: http://www.securityfocus.com/infocus/1814 [Accessed: March 2010], 2007.

[78] J. Park and D. Dicoi. WLAN security: current and future. *Internet Computing, IEEE*, 7(5):60–65, 2003.

[79] V. Paxson. Bro: A system for detecting network intruders in real-time. *COMPUT. NETWORKS*, 31(23):2435–2463, 1999.

[80] Prism54. Prism54 softmac linux driver, [Online] Available: http://jbnote.free.fr/prism54usb/ [Accessed: June 2010], 2007.

[81] S. Radosavac, J. Baras, and I. Koutsopoulos. A framework for MAC protocol misbehavior detection in wireless networks. *Proceedings of the 4th ACM workshop on Wireless security*, pages 33–42, 2005.

[82] M. Raya and I. Aad. DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots. *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, pages 84–97, 2004.

[83] S. Rigney and A. Willens. Remote Authentication Dial In User Service (RADIUS). *IETF RFC 2865*, 2000.

www.manaraa.com

[84] T. Schmoyer, L. Yu-Xi, and H. Owen. Wireless intrusion detection and response: a classic study using man-in-the-middle attack. In *WCNC. IEEE , Volume: 2 , 21-25 March*, pages 883–888, 2004.

[85] B. Schneider. *Applied Cryptography:: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, 1996.

[86] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H Yang, and Zhou S. Specification-based anomaly detection: a new approach for detecting network intrusions. In *ACM CCCS*, pages 265 – 274, 2002.

[87] A. Smailagic and D. Kogan. Location sensing and privacy in a context-aware computing environment. *Wireless Communications, IEEE Personal Communications*, 9(5):10–17, 2002.

[88] J. Smith, R. Gill, and A. Clark. On Securing Wireless LAN Access to Government Information Systems. In P. Mendis, J. Lai, and E. Dawson, editors, *Proceeedings of 2006 RNSA Security Technology Conference -Recent advances in security technology*, page 440 453, 2006.

[89] T. Song, C. Ko, H. Tseng, P. Balasubramayan, A. Chaudhary, and K. Levitt. Formal Reasoning About a Specification-Based Intrusion Detection for Dynamic Auto-configuration Protocols in Ad Hoc Networks. In *Formal Aspects in Security and Trust*, pages 16–33, 2005.

[90] A.E. Standard. FIPS 197. *National Institute of Standards and Technology, November*, 2001.

[91] D. Stanley, J. Walker, and B. Aboba. Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs. Technical report, IETF, 2005. RFC 4017.

[92] A. Stubblefield, J. Ioannidis, and A. Rubin. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. *Proceedings of the 2002 Network and Distributed Systems Security Symposium*, 1722, 2002.

[93] Cisco Systems. Cisco Aironet response to University of Maryland's paper, An initial security analysis of the IEEE 802.1X standard, 2002.

[94] Erik T., Ralf-Philipp W., and Andrei P. Breaking 104 bit wep in less than 60 seconds. Cryptology

www.manaraa.com

ePrint Archive, Report 2007/120, [Online] Available: http://eprint.iacr.org/ [Accessed: January 2010], 2007.

[95] A. Taheri, A. Singh, and A. Emmanuel. Location fingerprinting on infrastructure 802.11 wireless local area networks (WLANs) using Locus. *29th Annual IEEE International Conference on Local Computer Networks*, pages 676–683, 2004.

[96] *Tkiptun-ng*, [Online] Available: http://www.aircrack-ng.org [Accessed: June 2010], 2010.

[97] C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specification-based intrusion detection system for AODV. *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 125–134, 2003.

[98] P. Uppuluri and R. Sekar. Experiences with Specification-Based Intrusion Detection. In *Recent Advances in Intrusion Detection*, pages 172–189, 2001.

[99] J. Walker. Unsafe at any key size; an analysis of the WEP encapsulation. *IEEE Document*, pages 802–11, 2000.

[100] D. Welch and S. Lanthrop. Wireless Security Threat Taxonomy. In *Proceedings of the 2003 IEEE Workshop on Information Assurance*, pages 76 – 83, West Point, NY, USA, June 2003. IEEE.

[101] D. Whiting, R. Housley, and N. Ferguson. Counter with CBC-MAC (CCM). *Available from* http://csrc.nist.gov/encryption/modes/proposedmodes/ccm/ccm.pdf.

[102] J. Wright. Detecting Wireless LAN MAC Address Spoofing, 2003. White paper. [Online] Available: http://www.polarcove.com/whitepapers/detectwireless.pdf

[103] J. Wright. Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection. 2003. White paper. [Online] Available: http://www.polarcove.com/ whitepapers/layer2.pdf [Accessed: March 2010], 2003.

[104] J. Wright. Weaknesses in Wireless LAN Session Containment. White paper. [Online] Available: http://i.cmpnet.com/nc/1612/graphics/ SessionContainment_file.pdf [Accessed: February

www.manaraa.com

2010], 2005.

[105] J. Wright and M. Kershaw. LORCON (Loss Of Radio CONnectivity), 2007. [Online] Available: http://802.11ninja.net/lorcon/

[106] C. Wullems, K. Tham, and M. Looi. Proximity-Based Network Packet Filtering For IEEE 802.11 Wireless Devices. In *International Association for Development of the Information Society, Applied Computing International Conference*, 2004.

[107] C. Wullems, K. Tham, J. Smith, and M. Looi. A trivial denial of service attack on IEEE 802.11 direct sequence spread spectrum wireless LANs. *Wireless Telecommunications Symposium, 2004*, pages 129–136, 2004.

[108] WVE. Wireless vulnerabilities & exploits, 2007. [Online] Available: http://www.wve.org/

[109] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. *Proceedings of the 6th ACM inter national symposium on Mobile ad hoc networking and computing*, pages 46–57, 2005.

[110] J. Yeo, S. Banerjee, and A. Agrawala. Measuring traffic on the wireless medium: Experience and pitfalls. *Department of Computer Science University of Maryland. December*, 2002.

[111] J. Yeo, S. Banerjee, and A. Agrawala. Measuring traffic on the wireless medium: Experience and pitfalls. Technical report, December 2002. CS-TR 4421, Department of Computer Science, University of Maryland. Available at http:// citeseer.ist.psu.edu/yeo02measuring.html.

www.manaraa.com