Islamic University of Gaza

Deanery of Higher Studies

Faculty of Information Technology

Department of Computer Science

Wireless Intrusion Detection Enhancement using Backpropagate Neural Network

By:

Eyad Husni Elshami

120091353

Supervised by:

Dr. Tawfiq S. Barhoom

A Thesis Submitted as Partial Fulfillment of the Requirements for the Degree of Master in Information Technology

1432H (2011)

بسم الله الرحمن الرحيم

الجامعة الإسلامية – غزة
The Islamic University - Gaza

عمادة الدراسات العليا		هاتف داخلي: 1150

الرقم Ref ج س غ/35/
التاريخ Date 2011/07/03

نتيجة الحكم على أطروحة ماجستير

بناءً على موافقة عمادة الدراسات العليا بالجامعة الإسلامية بغزة على تشكيل لجنة الحكم على أطروحة الباحث/ **إياد حسني محمد الشامي** لنيل درجة الماجستير في **كلية *تكنولوجيا المعلومات*** **برنامج تكنولوجيا المعلومات** وموضوعها:

Wireless Intrusion Detection Enhancement using Back–propagate neural Network

وبعد المناقشة التي تمت اليوم الأحد 01 شعبان 1432هـ، الموافق 2011/07/03م الساعة الواحدة ظهراً، اجتمعت لجنة الحكم على الأطروحة والمكونة من:

د. توفيق سليمان برهوم	**مشرفاً ورئيساً**	....
أ.د. نبيل محمود حويحي	**مناقشاً داخلياً**	....
د. علاء مصطفى الهليس	**مناقشاً داخلياً**	....

وبعد المداولة أوصت اللجنة بمنح الباحث درجة الماجستير في **كلية *تكنولوجيا المعلومات*/ برنامج تكنولوجيا المعلومات**.

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

بسم الله الرحمن الرحيم

Abstract:

IEEE 802.11 wireless networks (WLANs) through its evolution stages are vulnerable for service availability security issues, Denial-of-Service (DoS) attacks are the most danger for the availability of the WLANs. Many of the existing wireless Intrusion detection Systems (WIDSs) have been studied to find a way to enhance the WIDS' performance. The MAC frame, as a part of the 802.11 wireless frames, contains useful features in detecting the DoS attacks.

In this dissertation a traffic has been generated on Infrastructure WLAN by using four different DoS attacks (Airflood, Channel Switch, Quiet and TKIP Cryptographic) to create a suitable data set with two different classes (Normal and Attack) for the Backpropagate Neural Network (BNN) which will be used as a model for anomaly-based WIDS. Four different goals experiments have been done to: measure the performance of the BNN's model; ranking the data set features by using three different ranking algorithms to find the optimal features set; finding the best BNN's architecture for both BNN's models, the one with all features and with optimal features sets; and finally the results of the experiments will be confirmed by using another tool. The main used tool is RapidMiner while the confirmation tool is MATLAB. The experimental results show that the accuracy of the BNN's models is too closed to 100% and the False Negative/False Positive rates are too small.

Keywords: Wireless Networks, MAC Frame, Intrusion Detection, Denial-of-Service, Backpropagation Neural Network, Information Gain, Information Gain Ratio, Support Vector Machine.

عنوان البحث:

تعزيز وسائل كشف التسلل الى الشبكات اللاسلكية باستخدام الشبكات العُصَيبِية

ملخص:

الشبكات اللاسلكية IEEE 802.11 وعبر مراحل تطورها المتعددة الا انها لازالت ضعيفة امام الاختراقات التي تهدد وجود خدمة هذه الشبكات. وتعتبر هجمات حجب الخدمة DoS attacks من اخطر الهجمات التي تهدد الشبكات اللاسلكية. في هذا البحث تم دارسة العديد من وسائل اكتشاف الهجمات على الشبكات اللاسلكية WIDS بهدف تحسين اداء هذه الوسائل فتبين ان MAC Frame يحتوي على صفات مميزة يمكن ان تفيد في الكشف عن هجمات حجب الخدمة. ولذلك في هذا البحث تم بناء قاعدة بيانات data set بالاعتماد على اربع هجمات (Airflood, Channel Switch, Quiet and TKIP Cryptographic) مختلفة لحجب الخدمة وذلك لبناء شبكة عُصَبِيية Neural Network لاكتشاف هجمات حجب الخدمة بناءاً على الشذوذ في صفات الـ MAC Frame, تم اعداد اربع انواع مختلفة الهدف من التجارب لـ: قياس دقة نموذج الشبكة العُصَيبِية في اكتشاف الهجمات؛ تحديد افضل مجموعة من صفات (بالاعتماد على ثلاث خوارزميات لتحدد اوزان الصفات في عملية اكتشاف الهجمات) لتكون هي الاساس في بناء الشبكة العُصَيبِية وبذلك نحصل على افضل اداء باقل فترة زمنية لازمة لتعليم الشبكة العُصَيبِية؛ تحديد افضل هيكلية للشبكة العُصَيبِية بناءا على مجموعة الصفات المستخدمة في عملية الاكتشاف؛ استخدام اداة اخرى للتأكد من نتائج التجارب السابقة. نتائج التجارب العملية في هذا البحث توضح ان نسبة الخطأ في اكتشاف هجمات حجب الخدمة تكاد ان تصل الي الصفر.

Table of Contents

List of Tables:

List of Figures:

List of Abbreviations:

ACK	Acknowledgment
AP	Access Point
ARP	Address Resolution Protocol
BNN	Backpropagate Neural Network
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CRC	Cyclic Redundancy Code
CSMA	Carrier Sense Multiple Access
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CTS	Clear-to-Send
DARPA	Defense Advanced Research Projects Agency
DoS	Deinal of Services
DS	Distributuion System
EAP	Extensible Authentication Protocol
EAPoL	EAP Over LAN
ESS	Extended Service Set
FCS	Frame Check Sequence
HIDS	Host-based IDS
ICV	Integrity Check Value
ID	Identifier
IDS	Intrusion Detection System

IEEE	Institute of Electrical and Electronic Engineers
IG	Information Gain
IGR	Information Gain Ratio
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
NAV	Network Allocation Vector
NN	Neural Network
OSI	Open System Interconnection
PHY	Physical Layer
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependent
PS	Power Saving
PS-Poll	Power Save-Poll
RF	Reply Frame
RFF	Radio Frequency Fingerprinting
RSN	Robust Secure Networks
RSNA	Robust Security Network Associations
RSS	Received Signal Strength
RTS	Request-to-Send
RTT	Round Trip Time
SSID	Service Set Identity
STA	Wireless Station

SVM	Support Vector Machine
TKIP	Temporal Key Integrity Protocol
VPN	Virtual Private Networks
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Network
WM	Wireless Medium
WPA	Wi-Fi Protected Access

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)[21][58]. Beside home and small office usage, WLANs are also become a standard part of the enterprise networks.

Gartner [44] points out the top three reasons for deploying WLANs in an enterprise which are:

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 [21]. 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.

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. With the ratification of IEEE 802.11i, it still vulnerable for availability security issues. Failure of preventative measures to address all

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

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 systems (WIDSs) that can reliably and accurately detect all possible Denial of Service (DoS) attacks on IEEE 802.11i RSN WLANs.

1.1 Research Motivation

Unfortunately, despite ratification of the 802.11 WLANs still suffer from a number of availability security vulnerabilities. Also the Intrusion Detection System (IDS) is one of the important defense lines in networking world, and it is very difficult to apply intrusion detection techniques which have been developed for one environment “Wired Networks” to another “Wireless Network”. That problem can be concluded from the following:

- The wireless network does not have a fixed infrastructure, and today’s network-based IDSs rely on real-time traffic analysis, which may no longer function well in the new environment.
- Furthermore, there may a vague separation between normalcy and anomaly in mobile environment, so intrusion detection may find it difficult to distinguish false alarms from real intrusions.

Neural Networks (NN) are good participant in IDS for the wired networks, and it achieves high accuracy in detecting the anomaly intrusion [61]. The motivation for this dissertation was to enhance the performance of WIDTs by using the IEEE 802.11 MAC frame to build NN anomaly detection system.

1.2 Scope and Limitation:

All work in this dissertation is based on the IEEE 802.11 WLANs infrastructure mode in side organization. The research is focused specifically on availability security issues, especially detecting the Airflood, Channel Switch, Quiet and TKIP Cryptographic DoS attacks based on the MAC Frame features by using backpropagate neural networks (BNN). Any other type of attacks are not included in this dissertation.

As a basic assumption for the research, the feature considered for IDS development should be well-known or at least reasonable that means in must be a part of the MAC Frame and some of the MAC frame features will excluded because it is useless such as the MAC addresses features. Moreover if features come from different layers, cross referencing can ease anomalous traffic detection. Since the wireless medium owns interesting and difficult to forge features, and since higher layers should not be addressed by WIDS, features should be MAC layers features.

1.3 Research Objectives:

The main objective of this dissertation is to enhance the WIDS by using the backpropagate NN against the DoS attacks in the infrastructure WLANs. The following objectives can be extracted from the main:

- Review WLANs security issues and the current WIDSs.
- Capturing the WLANs for Normal and different DoS attacks traffics to collect and build a data set for the research study.
- Determine the relevant attributes (features) from the collected data set for the mining process.
- Reduce the feature set by using feature ranking algorithm to reduce the classification process' computations.
- Finding the best NN classifier architecture.
- Reduce the false positive alerts of the WIDS in comparison with related systems such as [30][60] .

1.4 Research Outcomes:

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

- Review the WLANs security issues and the state of the art of WIDSs.
- Forming useful data set for WLANs it can consider as basic for a benchmark data set.
- Create a high accurate BNN anomaly WIDS.
- Define the optimal feature set for the BNN model.
- Determine the best BNN architecture for both all feature set and optimal feature set.

1.5 Thesis Structure:

This dissertation has been divided into five major chapters, which are structured around the objectives of the research.

Chapter 2 provides a Literature Review for the IEEE 802.11, IDS, NN, and the feature selection importance.

Chapter 3 provides the state of art of the WIDSs and the NN anomaly IDS as a related works to the research.

Chapter 4 provides the experimental works for this dissertation, which starting from the data set creation, building the BNN model, examining the BNN model accuracy, define the optimal features set, examining the accuracy on BNN based on the optimal features set, and finally determining the best architecture for both the all features set and optimal features set BNN models.

Finally, the conclusion and the future work direction in the area will be drawn in chapter5.

Chapter 2: Literature Review

This chapter provides a brief introduction about 802.11 wireless networks and its security threats and evolutions; Intrusion Detection Systems (IDS) and its detection techniques; neural networks, its learning techniques and the ability to provide high prediction. Data mining and feature selection importance and there techniques will be provided finally.

2.1 802.11 WLANs Security

This section provides a background in WLAN; Frame structure and contents; WLAN operations; reviews the WLAN security evolution; also reviews the outstanding security issues and attacks that can be used against WLANs and the latest WLAN security defense mechanisms. This section is mainly based on [21].

2.1.1 IEEE 802.11 standards

IEEE 802.11 standard [21] 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 Open System Interconnection (OSI) model -Physical and Data link. All 802 networks implement a Media Access Control (MAC) component and a Physical (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). IEEE 802.11 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 802.11a, 802.11b and 802.11g amendments differ from the original 802.11 standard only in the 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[17][36][3].

2.1.2 WLAN Network Topologies

The IEEE 802.11 WLANs consist of four fundamental architectural components namely [21]:

- ***Wireless Medium (WM)*** -The medium used to transfer 802.11 WLAN frames between WLAN nodes[2].
- ***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.

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

- ***Access Point (AP)*** -An AP is a specialized STA that provides connectivity between the various STAs and between the STAs and the DS.

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 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:

Infrastructure BSSBI: (Figure 2-1(a)) use APs to relay all information between the BSS STAs and the DS and between the STAs themselves [21][53]. 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 [53]. In an infrastructure BSS, the BSSID is the MAC address of the wireless interface of the AP.

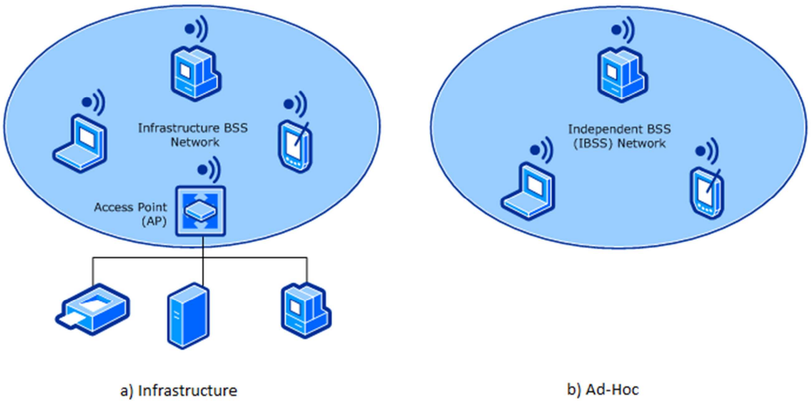


Figure 2-1: WLAN Structural Configurations

Ad-Hoc or Independent BSS: (Figure 2-1(b)) has no central control entity such as an AP, but comprises of STAs in direct communication with each other over the wireless medium [53][13]. STAs in an Ad-Hoc communicate directly with each other and hence must be within direct radio communication range. BSSID of IBSS WLANs is generated using random 46 bits, the individual/group bit of the address is set to 0 and the universal/local bit of the address is set to 1 [13].

While ad-hoc BSSs are typically used for creating short live 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 [13].

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

2.1.3 WLAN Operations

In a WLAN, all nodes (STAs and APs) are identified by their 48 bit IEEE 802 MAC address and the frames are delivered based on the MAC address. This sub-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.

2.1.3.1 Media Access Control

IEEE 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) [21][3][57].

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, IEEE 802.11 requires 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 [21][3].

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 [21]. Hence, besides physical carrier sensing, IEEE 802.11 also implements *virtual carrier sensing* [21]. 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) [21][31], which maintains a prediction of future traffic on the medium. It is a timer that represents the amount of time the medium will be reserved, in microseconds. The WLAN nodes reserve the medium by setting the *duration* field (described in the next sub-section) 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* [21][58][41]. 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 Short Interframe Space (SIFS) period. The *duration* field in the MAC headers [21] 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. [21][41]

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 same physical channel would receive the NAV and hence defer access appropriately [21][58][41].

2.1.3.2 IEEE 802.11 Frame Details

IEEE 802.11 frames consist of four fields as shown in Figure 2-2 [21]:

- ***The Preamble***: it is PHY dependent and contains training bit sequence for the antenna, the start frame delimiter and other synchronization information.

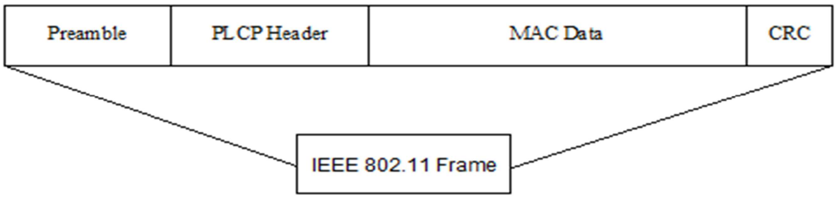


Figure 2-2: IEEE 802.11 Frame Structure

- ***Physical Layer Convergence Protocol*** (***PLCP***): PLCP's 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***: it contains the transmitted data.
- ***Cyclic Redundancy Code*** (***CRC***): it contains an error detection checksum for the frame.

MAC Data field of an IEEE 802.11 frame (simply referred to as the MAC frame) consists of the following features, as shown in Figure 2-3[21]:

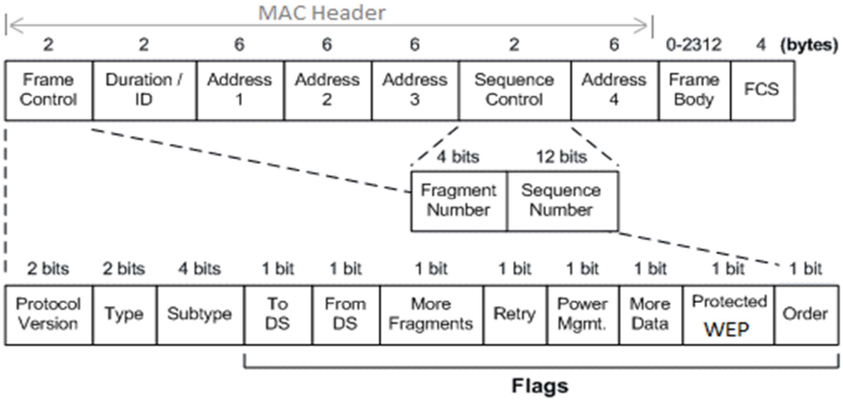


Figure 2-3: MAC Frame Format [21]

- **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 [21].
- **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[21].

- **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 [21].
- **Frame Body**: The frame body is variable in length and specific to the frame [21].
- **Frame Check Sequence**: The frame check sequence (FCS) contains an IEEE 32bit cyclic redundancy check (CRC) [21].

MAC frames used in 802.11 can be divided into three categories (types) namely[21]:

Control: Control frames provide MAC-layer reliability functions and assist in delivery of data frames, The Control frame subtypes are [21]:

- *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.

Management: These frames implement various services in WLANs and manage communication between STAs and APs, The Management frame subtypes are [21]:

- *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 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).

Data: Data frames are used to encapsulate upper layer data to be exchanged between WLAN nodes, the data frame subtypes are [21]:

- *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.

2.1.3.3 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 *unassociated and associated*. These variables create three states locally on a node for each remote node it communicates with over the wireless media [55]:

State 1: Initial start state, unauthenticated, unassociated.

State 2: Authenticated, unassociated.

State 3: Authenticated, associated.

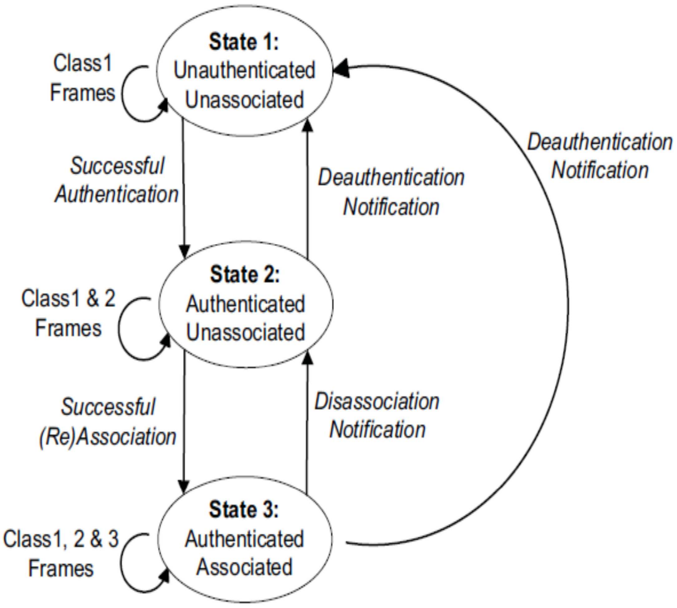


Figure 2-4: 802.11 State Diagram [55]

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 illustrated at Figure 2-4:

Class 1 frames: Class 1 frames are permitted in State 1, State 2 and State 3. 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. 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 nonauthenticated 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. 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 2-4 shows the IEEE 802.11 state diagram where each WLAN node transitions from State 1 to State 3 using Management frames.

2.1.4 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 and other wireless networks which are related to Confidentiality, Integrity, Availability and Access Control. These objectives are further discussed in [40][12][34].

However, the security challenges in WLANs are greater than those in wired networks due to the inherent characteristics of WLANs. The 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. The mobility of the WLAN nodes also leads to more complex trust relationships between network components in WLANs as compared to wired networks.

Now, in the next sub-section shows the threats faced by WLANs due to their unique PHY and MAC protocol will be discussed.

2.1.5 WLAN Threats

The threats to 802.11 WLANs described in [40][18]can be divided into categories such as: Traffic Analysis; Passive Eavesdropping; Message Modification; Deletion and Interception; Message Injection and Active Eavesdropping; Unauthorized Access; Man-in-the-Middle; Session Hijacking; Message Replay and Denial of Service.

This dissertation thesis concerned with the Denial of service (DoS) attacks in WLAN, which 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 Reply Frame (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 [40][18][7].

2.1.6 WLAN Security Evolution

Before ratification of IEEE 802.11i and its *Robust Security Network (RSN)* framework [40][8], IEEE 802.11 suffered from a number of serious security weaknesses. This sub-section explains Pre-RSN security shortcomings and how RSN addresses them.

2.1.6.1 Pre-RSN Security

To satisfy security objectives and threats identified in the previous sub-section, the original IEEE 802.11 specification uses a number of security mechanisms (Figure 2-5).

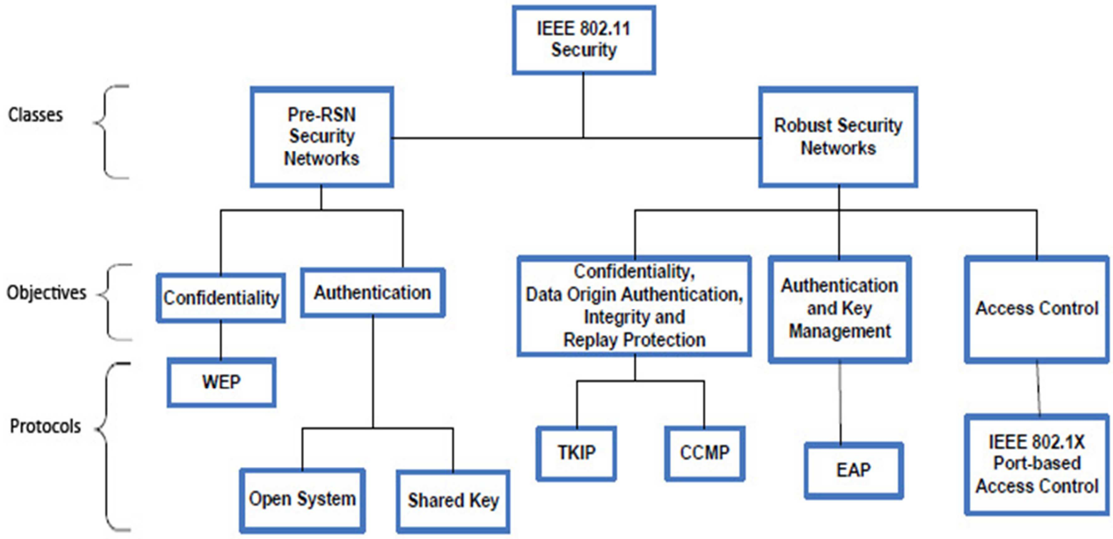

IEEE 802.11 Security
Classes
Objectives
Protocols
Pre-RSN Security Networks
Robust Security Networks
Confidentiality
Authentication
Confidentiality, Data Origin Authentication, Integrity and Replay Protection
Authentication and Key Management
Access Control
WEP
Open System
Shared Key
TKIP
CCMP
EAP
IEEE 802.1X Port-based Access Control

Figure 2-5: Taxonomy of 802.11 Security [40]

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) [40][8] stream cipher algorithm for encryption of data frames.

Access Control and Authentication**:** Pre-RSN WLANs use two methods for authenticating the identities of WLAN devices open system authentication and shared key authentication. The open system authentication is necessary for IEEE 802.11 WLANs, whereas the shared key authentication is optional. Open system authentication and shared key authentication discussed in [53][39].

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 encrypted CRC-32 checksum is called the *Integrity Check Value* (ICV). Weak integrity protection assists in plaintext recovery attacks such as inductive chosen plaintext attacks [40][54].

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 or the MAC layer to either inject a large number of spoofed frames in the WLAN (*flooding*) , hence causing a DoS [40].

2.1.6.3 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)*[40][8]. A RSN is a WLAN security 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.* Moreover, RSNs achieves the data confidentiality and access control security objectives but there is no amendment to achieve the availability security issues.

Table 2-1 summarizes the differences (the used techniques) between RSN and Pre-RSN securities to achieve the security issues. Note that neither Pre-RSN nor RSN performs protection against PHY and MAC layer DoS attacks.

Table 2-1: Comparison between RSN and Pre-RSN [40][8]

	Pre-RSN Security Technique(s)	**Pre-RSN Security** Technique(s)
Data Confidentiality & Integrity	▪ WEP Protocol	▪ TKIP protocol ▪ CCMP
Access Control and Authentication	▪ Open System ▪ Pre Shared Key	▪ IEEE 802.1X standard ▪ Pre Shared Key
Availability	▪ No protection against PHY and MAC layer DoS attacks	▪ No protection against PHY and MAC layer DoS attacks

2.1.7 Outstanding WLAN Security Issues

IEEE 802.11i has been designed to address all security issues related to Pre-RSN WLANs as shown in sub-section 2.1.6 except the Availability security issues. In this subsection list some of the remaining security issues in the WLANs.

For the sake of completeness, there is no mitigation for DoS attacks based on PHY jamming or spoofed Management, Control or Extensible Authentication Protocol (EAP) frames. The following attacks that can still be launched against RSNs: Man-in-the-middle Attacks [16][38]; Session Hijacking Attacks[4]; Security Level Rollback Attack[11]; Rogue AP[11]; Denial of Service Attacks. Next DoS attacks will discussed in more details.

2.1.7.1 Denial of Service Attacks:

As mentioned before this thesis concerned with the DoS attacks, some of these attacks will listed according to their base as follow:

I. ***Algorithm and Protocol Based Attacks***: A number of DoS vulnerabilities exist in RSNs due to flaws in RSN security protocols and algorithms, such as: Michael Algorithm Countermeasures [11], RSN IE Poisoning [40][11], 4-Way Handshake Blocking [11][10].

II. ***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 Extensible Authentication Protocol over LAN (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. Some of EAP and EAPoL based DoS attacks: Security Association Deterioration Attacks[4][11], EAP ID Exhaustion Attack [11].

III. **Management Frame Based DoS Attacks:** 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 [11]. 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 2.4 page 16). 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 [22]. 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.

IV. **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 [11]. 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 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. 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 [11]. 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 [6].

V. **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. Some of these attacks: Radio Jamming Attacks [11], NAV Based Attacks.

2.1.7.2 RSN Vulnerabilities

Figure 2-6 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 before, RSNs still suffer from multiple vulnerabilities which negatively impact their security. Figure 2-6 also shows the vulnerabilities that allow various attacks to manifest in a RSN (labeled as Cause).

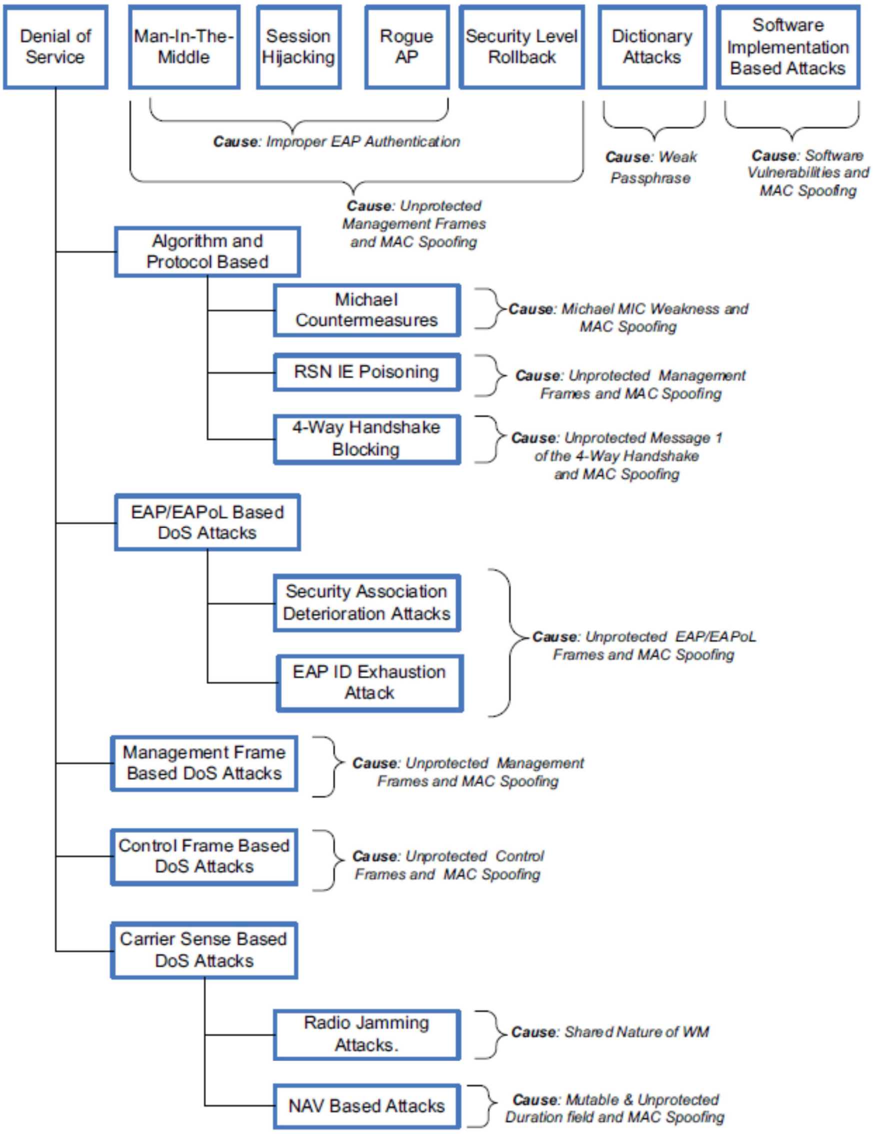

Denial of Service
Man-In-The-Middle
Session Hijacking
Rogue AP
Security Level Rollback
Dictionary Attacks
Software Implementation Based Attacks
Cause: Improper EAP Authentication
Cause: Weak Passphrase
Cause: Software Vulnerabilities and MAC Spoofing
Cause: Unprotected Management Frames and MAC Spoofing
Algorithm and Protocol Based
Michael Countermeasures
Cause: Michael MIC Weakness and MAC Spoofing
RSN IE Poisoning
Cause: Unprotected Management Frames and MAC Spoofing
4-Way Handshake Blocking
Cause: Unprotected Message 1 of the 4-Way Handshake and MAC Spoofing
EAP/EAPoL Based DoS Attacks
Security Association Deterioration Attacks
EAP ID Exhaustion Attack
Cause: Unprotected EAP/EAPoL Frames and MAC Spoofing
Management Frame Based DoS Attacks
Cause: Unprotected Management Frames and MAC Spoofing
Control Frame Based DoS Attacks
Cause: Unprotected Control Frames and MAC Spoofing
Carrier Sense Based DoS Attacks
Radio Jamming Attacks.
Cause: Shared Nature of WM
NAV Based Attacks
Cause: Mutable & Unprotected Duration field and MAC Spoofing

Figure 2-6: RSN attacks' taxonomy [40]

This dissertation focuses on the MAC layer DoS attacks on the RSN such as: 4-Way Handshake Blocking; EAP and EAPoL Based DoS Attacks; Management Frame Based DoS Attacks; Control Frame Based DoS Attacks; Carrier Sense Based DoS Attacks; Radio Jamming Attack and NAV Based Attacks.

2.2 Intrusion Detection Systems

This section will cover an introduction to the concept of intrusion detection system. Consequently it will look at the different variants of available IDS techniques and at the end specify what kind of properties we would like to have regarding the supervised IDS which will be built for the WLAN.

2.2.1 Introduction to Intrusion Detection System

Intrusion prevention measures, such as encryption and authentication, can be used in LANs to reduce intrusions, but cannot eliminate them. For example, encryption and authentication cannot defend against compromised mobile nodes, which often carry the private keys.

When an intrusion defined as "*any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource*" [51] takes place, intrusion prevention techniques, such as encryption and authentication, are usually the first line of defense. However, intrusion prevention alone is not sufficient because as systems become ever more complex, and as security is still often the after-thought, there are always exploitable weaknesses in the systems due to design and programming errors, or various "socially engineered" penetration techniques. For example, even though they were first reported many years ago, exploitable "buffer overflow" security holes, which can lead to an unauthorized root shell, still exist in some recent system software.

Generally, IDS is a tool for detecting abnormal behavior patterns in a system[27]. An abnormal pattern covers many definitions but in general it is likely described as unwanted, malicious and/or misuse activity occurring within a system. The two main techniques of intrusion detection are called *misuse detection* and *anomaly detection*[56][14]:

- ***Misuse detection systems*** (some articles such as [14] refer to it as signature base detection) use patterns of known attacks or weak spots of the system to match and identify intrusions. For instance, if someone tries to guess a password, a signature rule for this kind of behavior could be that ’too many failed login attempts within some time’ and this event would result in an alert. Misuse detection is not effective against unknown attacks that have no matched rules or patterns yet.
- ***Anomaly detection*** flags observed activities that deviate significantly from the established normal usage profiles as anomalies, that is, possible intrusions. For instance a profile of a user may contain the averaged frequencies of some system commands in his/her logging sessions, and for a logging session that is being monitored if it has significantly lower or higher frequencies an anomaly alert will be raised. Anomaly detection is an effective technique for detecting novel or unknown attacks since it does not require knowledge about intrusion attacks without having to be reconfigured or updated in any manner. But at the same time it tends to raise more alerts than misuse detection because whatever event happens in a session, normal or abnormal behavior, if its frequencies are significantly different from the averaged frequencies of the user it will raise an alert [33].

The two general techniques described are two different ways of spotting intrusions. Intrusion detections can be deployed on different areas, host-based IDS, or network-based IDS [56][14]:

- ***Host-based ID***: A host-based IDS (HIDS) monitors all or parts of the dynamic behavior and the state of a computer system. HIDS might detect which program accesses what resources and discover that, for example, a word-processor has suddenly and inexplicably started modifying the system password database. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appear as expected.
- ***Network-based IDS***: In a computer network there are a lot of data exchanges between computers within a local network and between a computer and another network (e.g. the Internet), see Figure 2-7.

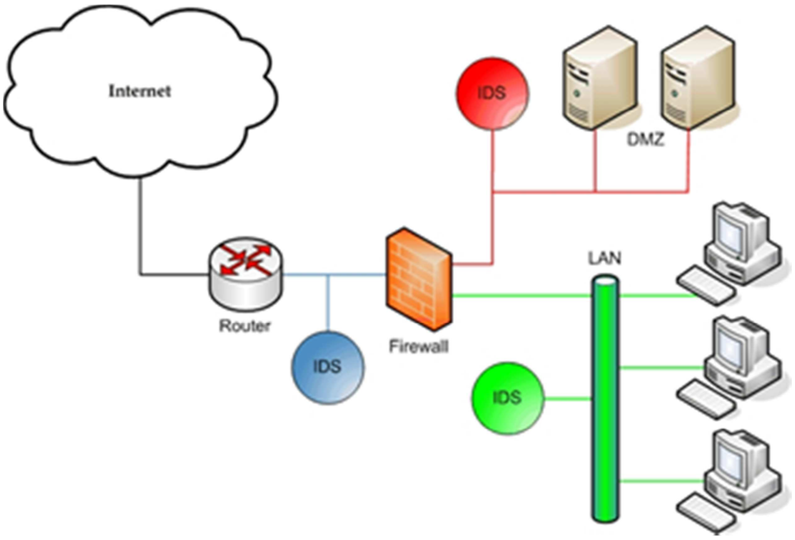


Figure 2-7: A network with intrusion detection systems

The IDS systems can be deployed in different areas of a network having different detection tasks. Being connected to a large network like the Internet plunges the computers into a world where the risk of getting in touch with harmful network traffic activity is relatively high. Several security precautions can be taken, like deploying antivirus, firewall, access control etc. in order to prevent such activities from intruding upon your computer or network. They all concentrate on different aspects of how to protect and secure a computer/network. Some well-known methods of IDS systems are based on either comparing patterns of network traffic to saved patterns of network activities of known attacks in [56] or statistical methods used to measure how abnormal a behavior in [27].

The reliability and robustness of IDSs is usually measured using the following three characteristics [56][27]:

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

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 anomaly-based IDS is directly proportional to the comprehensiveness and completeness of the statistical models or the specification used.

The IDSs differ in whether they are online or offline [27]. Offline IDSs are run periodically and they detect intrusions after-the-fact based on system logs. Online systems are designed to detect intrusions while they are happening, thereby allowing quicker intervention. However, offline systems slow down the process of intervention as they are monitoring network connections offline. Online systems continuously monitor network and thereby detect intrusions while they are happening but compared to offline systems they are more expensive in the sense of computation time due to continuous monitoring. But this expense should not scare us from making online intrusion detection, because it is more important to detect attacks faster and while they are happening, rather than after the attack has taken place and maybe caused harm.

Finally, for this dissertation concentrates the efforts on online anomaly-based IDSfor the wireless networks.

2.3 Neural Networks

This section will cover an introduction to NN by introducing a definition and description of the NN models. Categorically we will dig into to the essences of NN, presenting the core elements like learning processes and paradigms and eventually indicating why these are important to clarify before making a decision on which type of NNs will be used. It will be clarified why a NN is a good tool for developing WIDSs.

2.3.1 Introduction to Neural Network

NNs are an attempt at modeling the information processing capabilities of nervous systems [47]. The concept of NN is highly inspired by the recognition mechanism of the human brain. The human brain is a complex, nonlinear and parallel computer, whereas the digital computer is entirely the opposite, it is a simple, linear and serial computer. The capability to organize neurons to perform computation is many times faster than a modern digital computer in existence today [48].

So, it is obvious there is no universally accepted definition of neural network, but there are some architectural and fundamental elements that are the same for all neural networks. First of all, a NN is a network with many simple processors which are known as the neurons [47][48]. These neurons often possess a small amount of local memory. They have the task to receive input data from other neurons or external sources and use this to compute new data as output for the neural network or input data to the neurons of the next layer. The received or computed data is carried by communication channels, better known as the weights. The weights which connect two neurons possess certain values and will be adjusted upon network training. The adjustment of the weights is processed in parallel, meaning that many neurons can process their computations simultaneously. The magnitude of the adjustment of the neurons depends on the training data and is carried out with a so-called training rule (also known as learning rule). Another common characteristic for most NN is that the network can be parted into layers. An example of a basic neural network model is shown in Figure 2-8, it has three layers where the layers are organized as follows [47][48]: the first layer is the *input layer* that receives data from a source; the second layer is called *hidden layer*, whose input and output signals remain within the neural network; the third is the *output layer* that sends computed data out of the neural network.

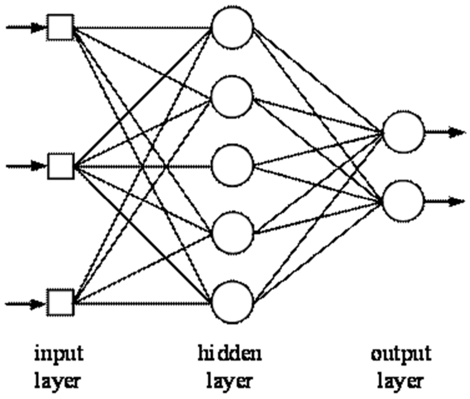


Figure 2-8: A Simple Fully Connected NN with three layers

In the particular example the network is fully-connected, which means that every neuron in one layer is connected with all neurons in the preceding layer and so on. Although it is not a rule and a neural network does not need to be fully-connected. Roughly, the overall task of a neural network is to predict or make approximately correct results for a given condition. NNs are trained with training data and the elements (e.g., neurons and weights) of the network will be adjusted on the basis of this training data. When further training does not change the network significantly or a given criterion is fulfilled the network is ready to produce results. Test data can be put into the network, be processed and the network will come up with a result.

2.3.2 Learning processes

Learning processes are important to the NNs. These sets of rules formulate how the weights of a network are to be adjusted [48]. From a higher perspective these rules can be considered to be the mechanism that makes the networks learn from their environment and improve their performance accordingly. If networks are trained carefully, networks can exhibit some capability for generalization beyond the training data, for example how much is it going to rain the next year? Based on the rain behaviors for the past 30 years a neural network, if trained with the proper learning algorithm, which is determined by the analysis and preprocessing of the data, can produce a reasonable prediction on how much it is going to rain the next year.

The definition of the learning process implies the following sequence of events: the neural network is stimulated by an environment; the NN undergoes changes in its free parameters as a result of the stimulation; the network responds in a new way to the environment due to the changes that occurred in its internal structure [48].

2.3.3 Learning paradigms

In NNs there are two different overall learning paradigms [47][48]: the first one is supervised learning; the second one is called unsupervised learning.

2.3.3.1 Supervised learning

In conceptual terms the supervised learning can be seen as a teacher having knowledge of the environment derived from input-output examples. The teacher provide consultancy to the NN telling it (for example) what is normal and abnormal traffic pattern, in the sense of what is classified as malicious and non-malicious. In general a supervised learning IDS operates as depicted in Figure 2-9[5].

A portion of network connection is to be analyzed and labeled with the help of the teacher. Afterwards the labeled training data is used by the learning algorithm to generalize the rules. Finally the classifier uses the generated rules to classify new network connections and gives alert if a connection is classified to be malicious.

Multi-Layer Perceptron (MLP) with Backpropagation algorithm is a well-known supervised learning NNs.

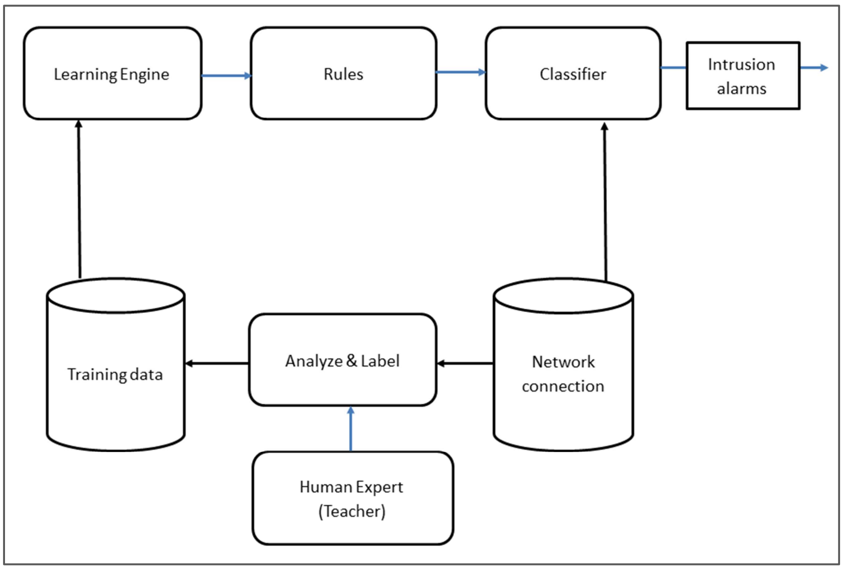


Figure 2-9: Supervised Intrusion Detection System[5]

Backpropagation algorithm: backpropagation algorithm is the most well-known supervised learning algorithms. In multilayer preceptron NN After choosing the weights of the network randomly, the backpropagation algorithm is used to compute the necessary corrections. The algorithm can be decomposed in the following four steps: Feed-forward computation; Backpropagation to the output layer; Backpropagation to the hidden layer and Weight updates. The algorithm is stopped when the value of the error function has become sufficiently small [47]. It usually uses the sigmoid function and expressed as two phases of computations as follow [47][48][33]:

- *Forward Pass*

1. Apply an input vector X and its corresponding output vector Y.
2. Propagate forward the input signals through all the neurons in all the layers and calculate the output signals.
3. Calculate the Err_j for every output neuron j as for example

$$Err_j \ = Y_j - O_j \qquad (1)$$

where Y_j is the j^{th} element of the desired output vector Y.

- *Backward Pass*

1. Adjust the weights between the hidden/intermediate neurons k and output neurons j according to the calculated error.

$$\Delta W_{jk}(t+1) = \ lrate \ \ O_k \ \ (1 - O_k)\, Err_j \ O_j \ + \ \alpha \ \Delta w_{jk}(t) \qquad (2)$$

where $\alpha\Delta \mathrm{w}_{\mathrm{jk}}(\mathrm{t})$: is called momentum term to accelerate the learning.

$lrate$ is a momentum constant 0 <= $lrate$ <= 1, and α is a small value called learning coefficient

2. Calculate the error Err_i for neurons i in the hidden layer :

$$Err_i \ = \ \sum Err_j * w_{ij} \qquad (3)$$

where n is the number of outputs

3. Propagate the error back to the neurons i of lower level

$$\Delta W_{ij}(t+1) = \ lrate.O_j\, (1 - O_j) Err_i\, O_i \ + \ \alpha \Delta w_{ij}(t) \qquad (4)$$

4. Update each network weight w_{ij}

$$W_{ij}(t+1) = w_{ij}(t) + \Delta w_{ij}(t+1) \qquad (5)$$

2.3.3.2 Unsupervised learning

Unlike the supervised learning, unsupervised learning does not have a teacher to tell what is a ’good’ or ’bad’ connection. It has the ability to learn from unlabeled data and create new classes automatically.

In general unsupervised learning IDS operates as depicted in Figure 2-10[5] with the use of a clustering algorithm it is illustrated how unsupervised learning operates. First, the training data is clustered using the clustering algorithm. Second, the clustered weight vectors can be labeled by a given labeling process, for example by selecting a sample group of the data from a cluster and label that cluster center with the major type of the sample. Finally, the labeled weight vectors can be used to classify the network connections. Self-Organizing Map (SOM) is a well-known unsupervised learning NN.

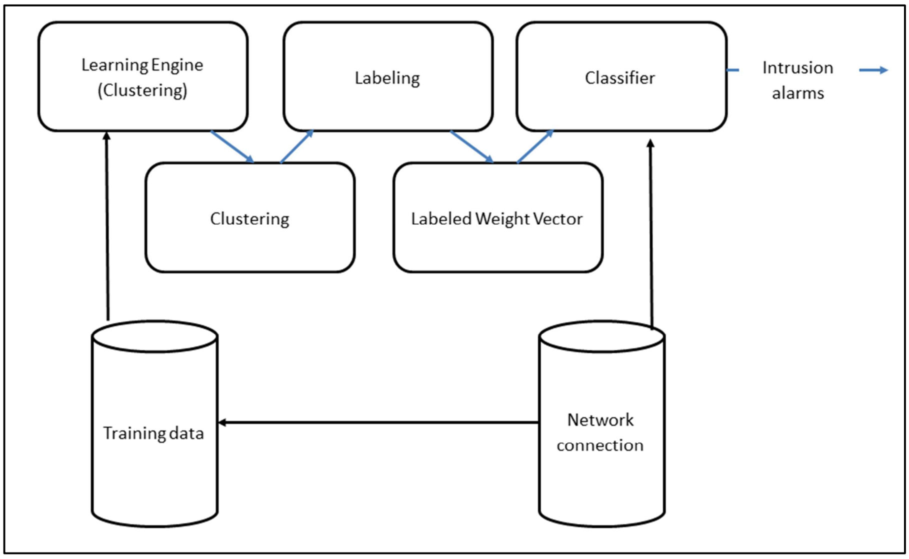


Figure 2-10: Unsupervised intrusion detection system[5]

2.3.4 Neural Networks for Intrusion Detection Systems

Using NNs in building anomaly IDS brings some advantages to the IDS such as: it provides more accurate statistical distribution than statistical models; neural network has low cost for development; it is highly scalable compared to other techniques; good in reducing both false positive error and false negative error rate [61].

This dissertation project concerns working with supervised learning model with backpropagation algorithm.

2.4 Data Mining

This section provides an introduction to defining Data Mining and feature selection techniques.

2.4.1. Introduction to Data Mining:

Data mining is the search for new, valuable, and nontrivial information in large volumes of data [35]. It is a cooperative effort of humans and computers. Best results are achieved by balancing the knowledge of human experts in describing problems and goals with the search capabilities of computers [35]. Data mining functionalities are used to specify the kind of knowledge patterns to be found in the data mining tasks, these tasks categorized into takes: Classifications, Association Rules, Clustering and Outlier Analysis.

NN with supervised learning is one of the most powerful classification techniques[35]. So that NN classifier will be used in this dissertation.

2.4.2. The Impact of Feature Selection

Feature Selection is one of the most effective ways which used to reduce the data size, data reduction are used because while large data sets have the potential for better mining results, there is no guarantee that they will yield better knowledge than small data sets [35][37][29. Choosing features which are relevant to our data mining application in order to achieve maximum performance with the minimum measurement and processing effort. The feature reduction process should result in:

- less data so that the data mining algorithm can learn faster;
- higher accuracy of a data mining process so that the model can generalize better from data;
- simple results of data mining process which are easier to understand and use; and
- for fewer features, the next round of data collection can be made easily by removing redundant or irrelevant features.

Different feature-selection methods will give different reduced data sets, and we can globally classify all this methods into two [35][37]:

- ***Feature-ranking algorithm***, in this algorithm one can expect a ranked list of features that are ordered according to a specific evaluation measure. A measure can be used on accuracy of available data, consistency, information content, distances between samples, and finally, statistical dependencies between features. These algorithms do not tell you what the minimum set of features for further analysis is; they indicate only the relevance of a feature compared to others.

- ***Minimum subset algorithms***, on the other hand, return a minimum feature subset and no differences are made among features in the subset-all have the same ranking. The features in the subset are relevant for the mining process; the others are irrelevant. In both types of algorithms, it is important to establish a feature-evaluation scheme: the way in which the features are evaluated and then ranked, or added to the selected subset.

This thesis will examine different feature-ranking algorithms such as: *Information Gain*; *Information Gain Ratio* and *Support Vector Machine* algorithms in experimental study to find the best suitable features, high ranking features, for our application domain, since there is no best feature ranking algorithm can be used in all application types according to [37].

2.4.2.1 Information Gain Attribute Ranking:

The Information Gain (IG) [35][37] of a given attribute A with respect to the class attribute C is the reduction in uncertainty about the value of C when we know the value of $A, I(C\,; A)$. The uncertainty about the value of C is measured by its entropy, $H(C\,)$. The uncertainty about the value of C when we know the value of A is given by the conditional entropy of C given A, $H(C\,|A)$.

$$I(C\,;\,A) = H(C\,) - H(C\,|A) \qquad (1)$$

When C and A are discrete variables that take values in $\{c_1 \ldots c_k\,\}$ and $\{a_1 \ldots a_l\}$ then the entropy of C is given by:

$$H\ (C\ )\ =\ -\sum_{i=1}^{i=k} P\ (C\ =\ c_i) \log_2 P\ (C\ =\ c_i) \qquad (2)$$

The conditional entropy of C given A is:

$$H\ (C\ |A) = -\sum_{j=1}^{j=l} P\left(A\ = a_j\ \right) H\left(C\ \middle|A\ =\ a_j\ \right) \qquad (3)$$

alternatively the information gain is given by:

$$I(C\ ;\ A) =\ H(A) +\ H(C\ ) -\ H(A, C\ ) \qquad (4)$$

where $H(A, C\ )$ is the joint entropy of A and C :

$$H\ (A, C\ ) = -\sum_{i,j} P\left(A\ =\ a_j\ , C\ =\ c_j\ \right) \log_2 P\left(A\ =\ a_j\ , C\ =\ c_i\right) \qquad (5)$$

2.4.2.2 Information Gain Ratio (IGR) Attribute Ranking

It is a modification of the information gain that reduces its bias on high-branch attributes; it should be large when data is evenly spread or small when all data belong to one branch.

IGR takes number and size of branches into account when choosing an attribute and it corrects the information gain by taking the *intrinsic information* of a split into account (i.e. how much info do it need to tell which branch an instance belongs to)[27][30].

$$IGR(C; A) = \frac{IG(C; A)}{SplitInfo(C; A)} \qquad (6)$$

where

$$SplitInfo\ (C;A) = -\sum \frac{|\{n \in C\}|}{|C|} * log_2 \frac{|\{n \in C\}|}{|C|} \qquad (7)$$

where n is the number of instances belongs to the class C.

2.4.2.3 Support Vector Machine Attribute Ranking

Support Vector Machine (SVM) is an algorithm of data mining technique, recently received increasing popularity in machine learning community. Support vector machines have been introduced in [52] for solving pattern recognition and nonlinear function estimation problems. Beside for classification problem, the SVM can be used to feature selection [42][50]. The linear programming formulation of SVM has been shown to have one of the best feature selection properties among all norms including the conventional support vector machines [42].

$$\boldsymbol{Y} = \boldsymbol{w}.\boldsymbol{x} - b \qquad (8)$$

Equation (8) is dot product formula and used for the output of linear SVM, where *x* is a feature vector of classification documents composed of words. *w* is the weight of corresponding *x*. *b* is a bias parameter determined by training process. The following summarizes SVM steps[42][50][52]:

- Map the data to a predetermined very high-dimensional space via a kernel function.
- Find the hyperplane that maximizes the margin between the two classes.
- If data are not separable find the hyperplane that maximizes the margin and minimizes the (a weighted average of the) misclassifications.

SVM can be used for both linear and nonlinear data. It uses a nonlinear mapping to transform the original training data into a higher dimension. With the new dimension, it searches for the linear optimal separating hyperplane (i.e., “decision boundary”). With an appropriate nonlinear mapping to a sufficiently high dimension, data from two classes can always be separated by a hyperplane. SVMs finds this hyperplane using support vectors (“essential” training tuples) and margins (defined by the support vectors)[42][52]. In this dissertation *w* vector is the desired output for ranking the features.

Chapter 3: Related Works

This chapter provides a state-of the art for the applied techniques in the WIDS and provides an overview of the success on the neural networks in the IDS system, for the traditional –wired networks.

3.1. WIDS State of the Art

Different techniques and different characteristics of the wireless technology were used on the WIDS to provide a high detection rate. This section study the most used techniques in WIDS such as: MAC frame sequence number, Received Signal Strength, the frame Round Trip Time and the fingerprinting techniques.

3.1.1. Sequence Number Field:

Sequence Number field is a 12 bits field in MAC header of Management frame is widely used by researchers for the MAC spoofing DoS attacks detection

Guo and Chiuen in [19] monitor the wireless traffic looking for any gap between the sequence numbers of the received frame. If a gap is found “gap more than a threshold” 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 Address Resolution Protocol (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 [15] 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 address by using the difference (modulo 4096), The sequence numbers only range from 0 to 4096, 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 DoS attacks.

Some of the techniques for detecting spoofing based attacks have been implemented in some open source WIDSs such as *Snort-Wireless* [32]. Snort-Wireless claims to be capable of detecting MAC spoofing by monitoring for inconsistencies in MAC frame sequence numbers.

3.1.2. Physical Characteristics of the transmission radio:

Two parameters appear to be useful, including the received signal strength (RSS) which provides a numeric indication of the strength of a received signal, and observations of round trip time (RTT) measurements. RSS monitoring have been reported by Gill et al. in [45]. They also report preliminary success on implementing RTT monitoring. A significant advantage of using physical layer parameters in an IDS is that they are much more difficult to accurately predict, and therefore fabricate, given the dynamic nature of the wireless environment. The use of such parameters, however, requires considerable fine tuning to the deployment environment, in order that appropriate thresholds are selected to minimize false positives and reduce the likelihood of false negatives.

Abu Samra and Abed in [2] evaluate the passive MAC spoofing DoS attacks detection by doing laboratory experiments with eight different scenarios to verify the effectiveness of the Received Signal Strength Technique and the Round Trip Time in detecting MAC spoofing DoS attacks. The verification done by applying three new different DoS attacks: TKIP DoS attack; Channel Switch DoS attack; and Quit DoS attack. As a result the experiments show that: there is no false positive, with some false negative alerts were raised. Then they provide in [1] an enhanced algorithm to measure the RSS and RTT with modified threshold.

3.1.3 Fingerprinting:

Other 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 [23] 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 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. [24] 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. [25] suggest using Radio Frequency Fingerprinting (RFF) for MAC spoof detection where the

RFF uniquely identifies a transceiver based on the transceiver print of the signal it generates. By using the transceiver print 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 [26]. Such PHY layer watermarking can assist in distinguishing adversaries from legitimate clients.

3.2. Neural Network and IDS:

Sani et al. in [61] present an overview of NNs and their use in building anomaly IDS, and list the advantages of using NN in IDS: it provides more accurate statistical distribution than statistical models; neural network has low cost for development; It is highly scalable compared to other techniques; Good in reducing both false positive error and false negative error rate.

A NN-based intrusion detection method was presented by Shun and Malki [28] for the internet-based attacks on a computer network, In particular, feedforward neural networks with the backpropagation training algorithm was used. The data for both training and testing were obtained from the Defense Advanced Research Projects Agency (DARPA) depository and the experimental results on the used data showed promising results on detection intrusion systems. The result was 100% of classification accuracy for the known traffic, normal and attack traffic, and 76% of accuracy for the unknown traffic.

Wang and Ma in [20] propose an optimization of NNs for network IDS, they propose a reduced number of features extracted from LAN traffic as input to BNN. The reported detection rates up to 88.4% with false positive rates less than 1%, and the analysis of the results indicates that: the best architecture for the used BNN is 18-36-1(18 inputs neurons, 36 hidden neurons, and 1 output neuron).

For wireless networks, *Khalil El-Khatib* in [30] generate a wireless traffic by using four DoS attacks (Deauthentication Attack, ChopChop Attack, Fragmentation Attack, and Duration Attack) to collect a data set based on the MAC Frame features. Information Gain Ratio (IGR) as a measure to determine the weight of each feature then the reduced feature set and the original data set were used by three different neural networks classifiers: Perceptron; Multilayer backpropagation (MLBP) and Hyprid network, the experimental results show that the performance of the three classifiers is improved by an average of 15 percent when they are tested using the reduced set of features. If the perceptron classifier is excluded, the combined false positives rate of the MLBP and Hybrid classifiers is reduced by 67% and the false negatives rate is reduced by 84%. The achieved results for the all features set (38 features) are 88%, 3% and 9% for accuracy, false negative and false positive rates respectively; and for the optimal features set (8 features) are 95.6%, 0.4 and 4% for accuracy, false negative and false positive rates respectively.

Y. Liu et al. in [60] propose an intrusion detection method based on Dynamic Growing Neural Network (DGNN) for wireless networking. They use DGNN as a supervised learning NN and used The Synthetic Control Chart Time Series[3], to simulate WLAN traffic. The propose method usually falsely alarm new normal adding mobile client as intruder, and some abnormal behavior of added station cannot be found. Some famous attacks such as RTS/CTS based DoS cannot be prevented by this method.

[3] this benchmark can be found in UCI Knowledge Discovery in Databases Archive (http://kdd.ics.uci.edu/)

N.P. Pathack et al. in [43] proposed unsupervised NN for building anomaly based IDS. They generate input space in a two dimensional space with predetermined four clusters on different variances $\sigma = 0.5$ and $\sigma = 0.05$. The clusters are centered at (0, 1.5), (0, -1.5), (1.5, 0) and (-1.5, 0) for $\sigma = 0.5$ and centered at (0, 0.5), (0, -0.5), (0.5, 0) and (-0.5, 0) for $\sigma = 0.05$, the input space's points are assigned to each center according to Gaussian distribution. The proposed NN learned by 5.5x104 instances and the testing show a highly false alarm rate 17.2%. Finally they found the proposed NN failed in detecting RTS/CTS DoS attack.

Chapter 4: WIDS enhancement by using Backpropagate Neural Network

Since there is no data set considered as a benchmark for the WIDS, in this chapter a data set for the WIDS was created. This chapter provides an experimental works to: measure the BNN's performance in the anomaly intrusion detection for WLANs, define the optimal features set, measure the BNN's performance based on the optimal features set, and finally finding the best BNN's architecture.

To achieve the enhancement on the WIDS by using BNN the following steps construct the methodology which will be followed as shown in Figure 4-1:

- Collecting a suitable data set
- Examining the BNN accuracy based on the collected data set
- Define the optimal features set and examining the BNN model accuracy based on the optimal features set(s).
- Confirming the results
- Determine the best BNN architecture for both the all features set and the optimal features set(s).

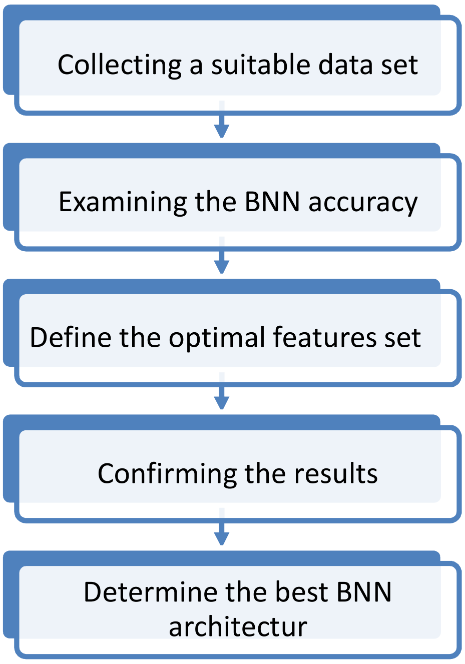

Collecting a suitable data set
Examining the BNN accuracy
Define the optimal features set
Confirming the results
Determine the best BNN architectur

Figure 4-1: Proposed Methodology

4.1 Dataset Creation:

Until now there is no real WLAN traffic which can consider as benchmark to be used in this area of researches.

The features from MAC layer were selected to construct the data set features. All IEEE 802.11 frames are composed by Preamble, PLCP Header, MAC Data, and CRC.

Section 2.1 shows the contents of the MAC Data in IEEE 802.11. All these information can be used to construct features.

To create a real dataset an infrastructure environment was constructed which consists of AP, two mobile computers for a legitimate client (STA) and attacker, a desktop computer (MON) for passive monitoring the WLAN traffic using Wireshark [66] to capture the WLAN traffic. Four different new attacks against a legitimate station; TKIP

Cryptographic DoS attack [63], Airflood DoS attack [63],Channel Switch DoS attack [7], and Quiet DoS attack [7].

The wireshark exports the captured frames in a raw data in text files(see Appendix A), a simple Java file has been built (see Appendix B) to fill that text file data into columns. Some of manual data preprocessing have been done to generate data set which is suitable for the goals and experiments in this dissertation thesis.

The Addresses were removed because it is useless in the classification methods since the attacker can use any faked or real MAC address and also it can targeted any legitimate STA. The frame body also removed because it may contain any data, also frame body which contains the message data will be removed because it is not accessible at the MAC layer.

The traffic has been generated, to collect the dataset, in different scenarios to emulate all the possible case in the real life. The AP, the MON and the victim STA were always stationary in all of these scenarios. The other scenarios were based on the distance between the attacker/STA from the AP, and the motion state of the attacker/STA. These scenarios are valuable because the obstacles and the motion states affect the PHY/MAC Frames' features such as RSS, RTT, Duration field, FCS, Power Mgmt…etc. The scenarios were as follow:

- Scenario I, the legitimate STA and the attacker are stationary in the same room;
- Scenario II, the legitimate STA stationary in the room while the attacker is stationary outside the room;
- Scenario III, the legitimate STA and the attacker are stationary outdoor;

- Scenario IV, the legitimate STA and the attacker are stationary as far as possible from the AP.
- Each of these scenarios yields another three scenarios where the legitimate SAT or the attacker is in motion within the coverage area of the AP.

The dataset contains about 12000 instances (frames). Table 4-1 shows the dataset classes (labels) and the percentage of each of them, each of the launch attacks has approximately 25% of the over all of the attack traffic. All different attacks traffic was labeled as attack and the legitimate traffic was labeled as Normal.

Table 4-1: Dataset classes' distribution

Type Of traffic	Count Of frame	Percentage
Normal	4500	37.5%
Attack	7500	62.5%

4.2 Experiments and Results analysis:

In this subsection, four different types of experiments have been constructed. These experiments categorized according its goals: model efficiency measures; MAC frame’s feature reduction; confirming the results by using other tool; and determining the model’s best architecture.

4.2.1 BNN’s efficiency in the WIDs:

To measure the efficiency of BNN model in the anomaly WIDs, four experiments have been done. Three subset of the whole dataset extracted by using stratified sampling, the size of each of them is 25%, 50% and 75% respectively and whole data set (100%) was used for the last experiment that prove the effectiveness of the data set size on the model accuracy. RapidMiner tool [65] has been used to create the BNN and to measure its performance the cross-validation performance measure [62] was used.

BNN's with 15-10-2 (15 input neurons, 10 hidden neurons, 2 output neurons) was constructed by the Rapid Miner, the hidden neurons is 10 neurons because the Rapid Miner uses the rule "the number of hidden neurons equal to the half of the sum of the input and output neurons plus 1". The experiments' results occur as Table 4-2 through 4-5 respectively.

Table 4-2: BNN's accuracy measurement Experiment 1

Experiment 1		
Goal:	Measure BNN's accuracy	
Data set:	25%	
Result:	Accuracy:	98.20%
	False Negative:	0.0%
	False Positive:	1.8%

Table 4-3: BNN's accuracy measurement Experiment 2

Experiment 2		
Goal:	Measure BNN's accuracy	
Data set:	50%	
Result:	Accuracy:	99. 0%
	False Negative:	0.2%
	False Positive:	0.8%

Table 4-4: BNN's accuracy measurement Experiment 3

Experiment 3		
Goal:	Measure BNN's accuracy	
Data set:	75%	
Result:	Accuracy:	99. 4%
	False Negative:	0.1%
	False Positive:	0.5%

Table 4-5: BNN's accuracy measurement Experiment 4

Experiment 4		
Goal:	Measure BNN’s accuracy	
Data set:	100%	
Result:	Accuracy:	99. 6%
	False Negative:	0.1%
	False Positive:	0.3%

Figure 4-1 shows that accuracy of the four experiments, it is clearly noted whereas the size of the dataset increased the accuracy of the neural network model is increased.

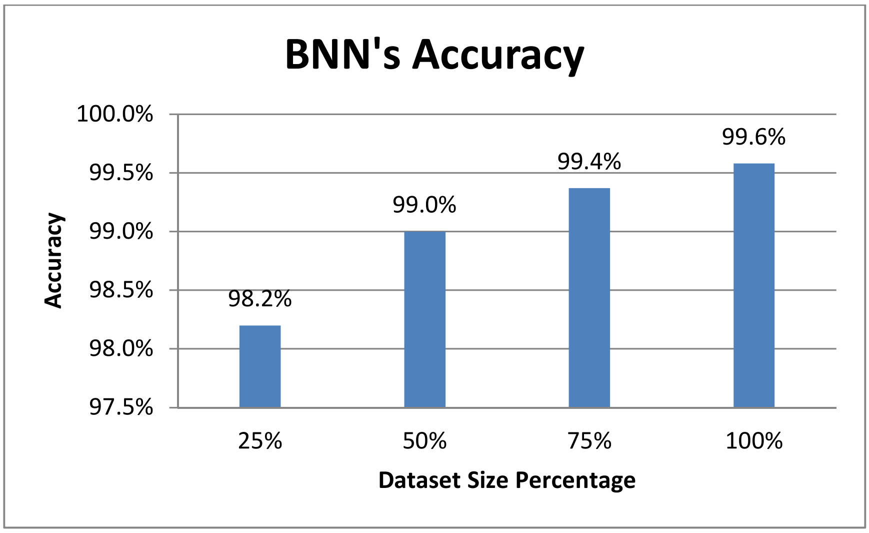


Figure 4-2: BNN's Model Accuracy

The false negative and the false positive rates according to the previous experiments have shown in Figure 4-2.

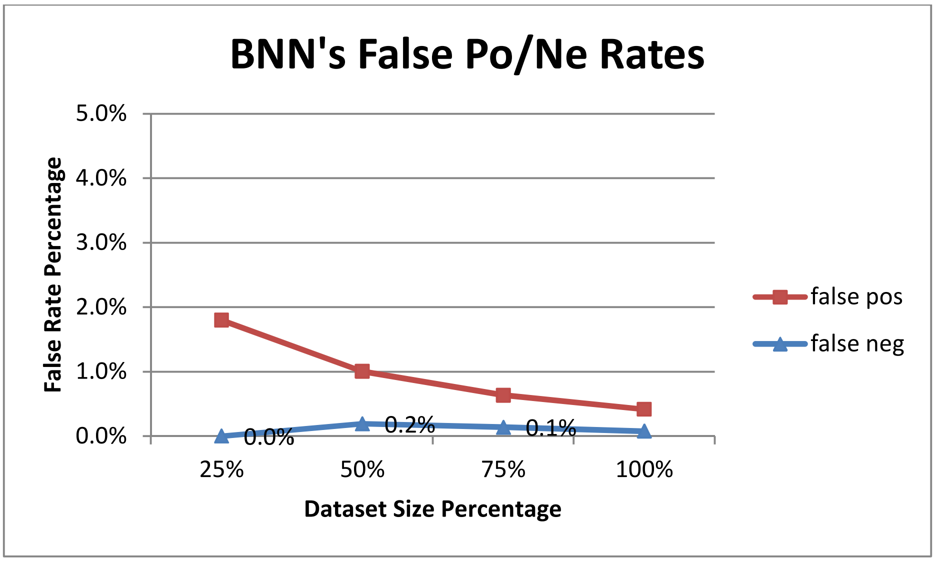
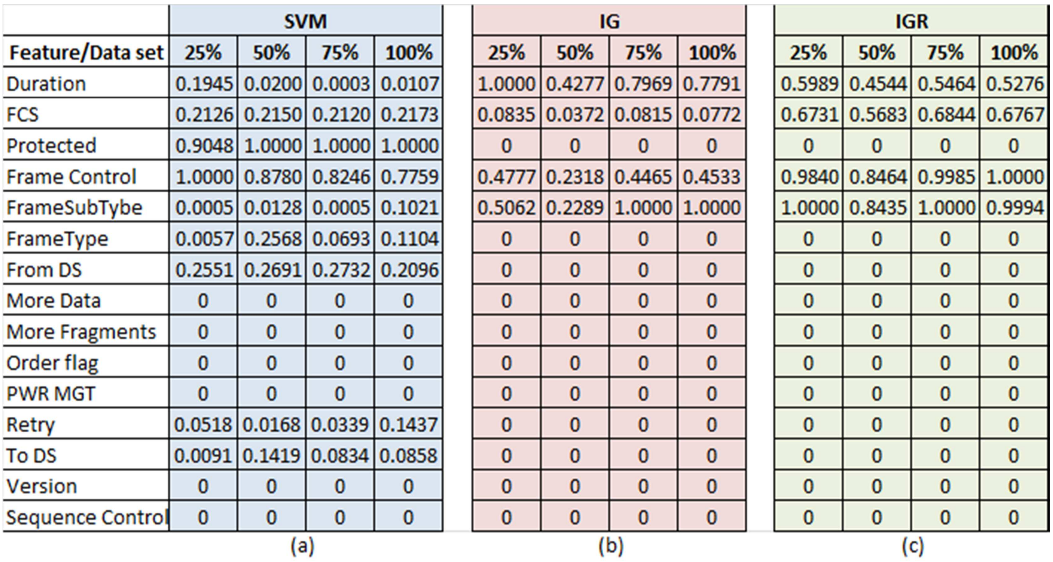


Figure 4-3: BNN's Model False Negative and False Positive Rates

The results of the previous experiments come as it was expected from the BNN, as the training set size increased the prediction accuracy increased, the accuracy is too closed to 100% and the false negative and the false positive are 0.1% and 0.9% respectively.

4.2.2 MAC Frame feature Reduction:

Attributes reduction will decrease the learning time since the total number of the input attributes will decrease as consequence the overall computations will decreased too. Three attributes ranking algorithm have been used to rank the input attributes, Support Vector Machine (SVM), Information Gain (IG) and Information Gain Ratio (IGR). IG and IGR show that only four attributes {*FrameControl, FrameSubType, Duration*, *FCS*} which affect the prediction process, while SVM show that they are nine attributes {*Duration*, *FCS*, *Protected*, *FrameControl*, *FrameSubType*, *FrameType*, *FromDS*, *Retry*, *ToDS*}. Figure 3 shows the attributes' weights according to the whole dataset.



	SVM				IG				IGR			
Feature/Data set	25%	50%	75%	100%	25%	50%	75%	100%	25%	50%	75%	100%
Duration	0.1945	0.0200	0.0003	0.0107	1.0000	0.4277	0.7969	0.7791	0.5989	0.4544	0.5464	0.5276
FCS	0.2126	0.2150	0.2120	0.2173	0.0835	0.0372	0.0815	0.0772	0.6731	0.5683	0.6844	0.6767
Protected	0.9048	1.0000	1.0000	1.0000	0	0	0	0	0	0	0	0
Frame Control	1.0000	0.8780	0.8246	0.7759	0.4777	0.2318	0.4465	0.4533	0.9840	0.8464	0.9985	1.0000
FrameSubTybe	0.0005	0.0128	0.0005	0.1021	0.5062	0.2289	1.0000	1.0000	1.0000	0.8435	1.0000	0.9994
FrameType	0.0057	0.2568	0.0693	0.1104	0	0	0	0	0	0	0	0
From DS	0.2551	0.2691	0.2732	0.2096	0	0	0	0	0	0	0	0
More Data	0	0	0	0	0	0	0	0	0	0	0	0
More Fragments	0	0	0	0	0	0	0	0	0	0	0	0
Order flag	0	0	0	0	0	0	0	0	0	0	0	0
PWR MGT	0	0	0	0	0	0	0	0	0	0	0	0
Retry	0.0518	0.0168	0.0339	0.1437	0	0	0	0	0	0	0	0
To DS	0.0091	0.1419	0.0834	0.0858	0	0	0	0	0	0	0	0
Version	0	0	0	0	0	0	0	0	0	0	0	0
Sequence Control	0	0	0	0	0	0	0	0	0	0	0	0
	(a)				(b)				(c)			

Figure 4-4: MAC Frame - Attributes' Weights

As a result, IG and IGR give the same subset of attributes {FrameControl, FrameSubType, Duration, FCS}. Eight experiments have been done based on the ranked attributes and the dataset size.

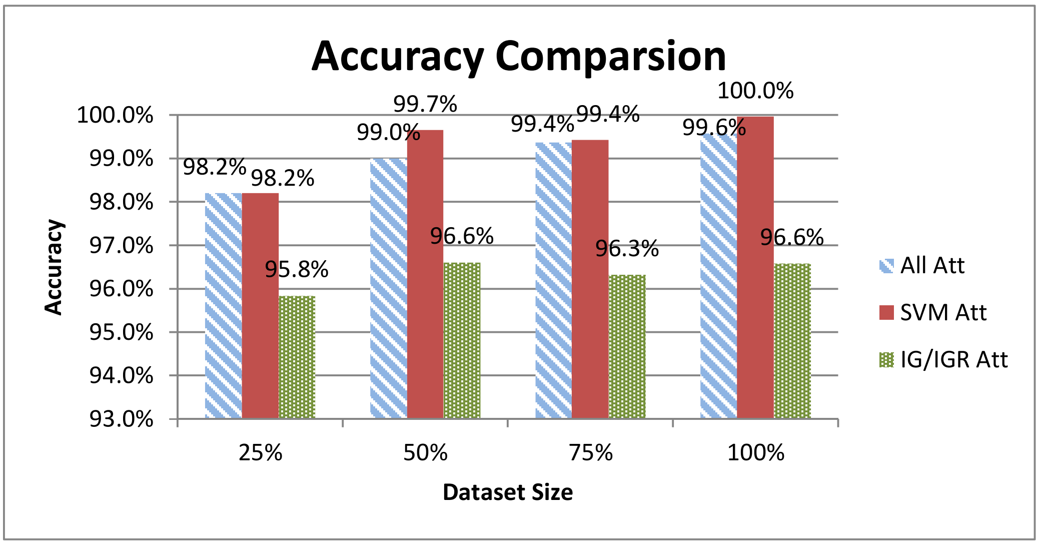


Figure 4-5: Accuracy Comparison for three different features set

Figure 4-5(a) shows the false negative and Figure 4-5(b) shows the false positive rates for each experiment.

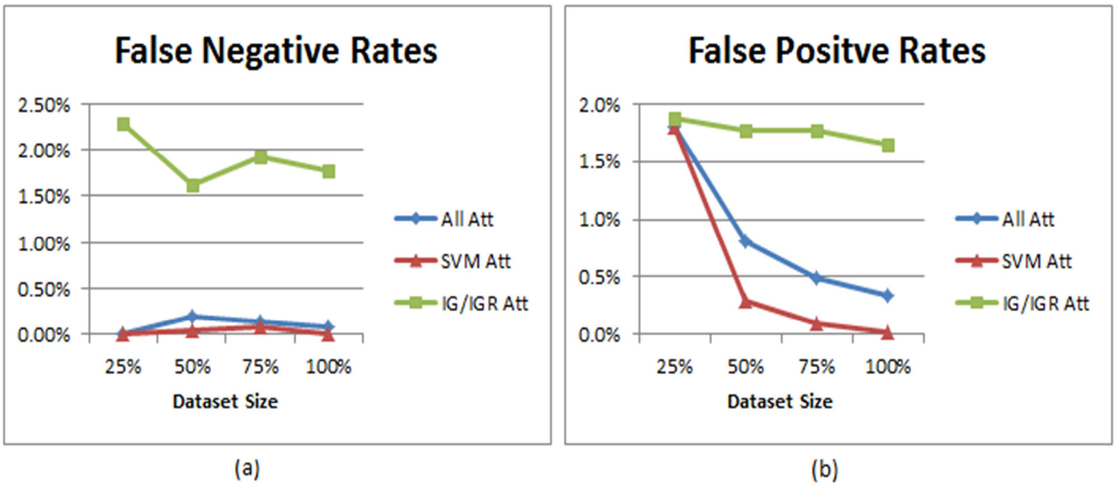


Figure 4-6: False Negative/Positive Rates Comparison

The experiments show the performance of the SVM optimal features set is better than the all features set that due the existence of irrelevant attribute in the second set which will detract from the model accuracy.

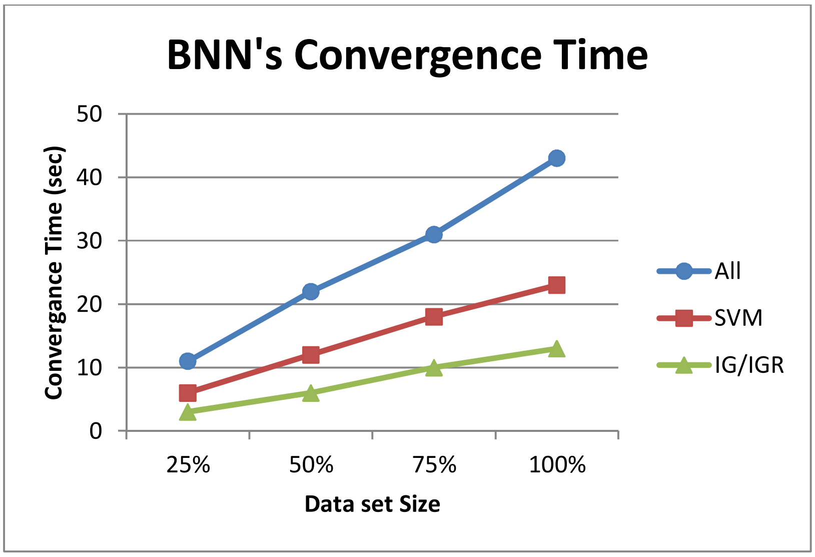


Figure 4-7: BNN's convergence time for three feature sets

It also shows that reducing the feature set will reduce the BNN's convergence time. Figure 4-6 shows the convergence time for the three features sets, the all feature set, SVM feature set and IG feature set.

From Figures 4-4 through 4-6 we can conclude that the IG/IGR ranking is not suitable for the anomaly BNN's WIDS since the feature set provides accuracy less than the accuracy of the full feature data set by 3% and provides higher false negative and false positive rates 2.8% and 3% respectively. While the SVM ranking provides accuracy higher than the accuracy of the full feature data set and provides lower false negative and false positive rates, so that is more suitable for anomaly BNN's WIDS.

4.2.3 Confirming the Results

To get more realistic results all experiments have been repeated on other tool which is MATLAB [64] version 7.6.0 (R2008a), the dataset of each experiment divided into two subsets 60% for training and 40% for testing. The used BNN structure used as in the previous experiments which are 15-10-2 for the all attributes dataset, 9-7-2 for the SVM attribute dataset and 4-4-2 for the IG/IGR attributes dataset. Table 4-7 shows the experiments results and Figure 4-7 shows the accuracy average of all the experiments by the two tools.

The difference in the results return to that:

- In RapidMiner the X-Validation were used, which encapsulates a cross-validation in order to estimate the performance of a learning operator. The input dataset S is split up into number of validations subsets S_i. The BNN is applied number of validations times using S_i as the test set and S \ S_i as training set. And it returns Performance Vector, which contains the average of the S_i times of applying the BNN model.

Table 4-6: MATLAB's experiments results for all the Dataset

Dataset Size	All	SVM	IG
25%	100%	98.03%	91.32%
50%	99.91%	100%	95.10%
75%	100%	100%	92.73%
100%	100%	100%	94.60%

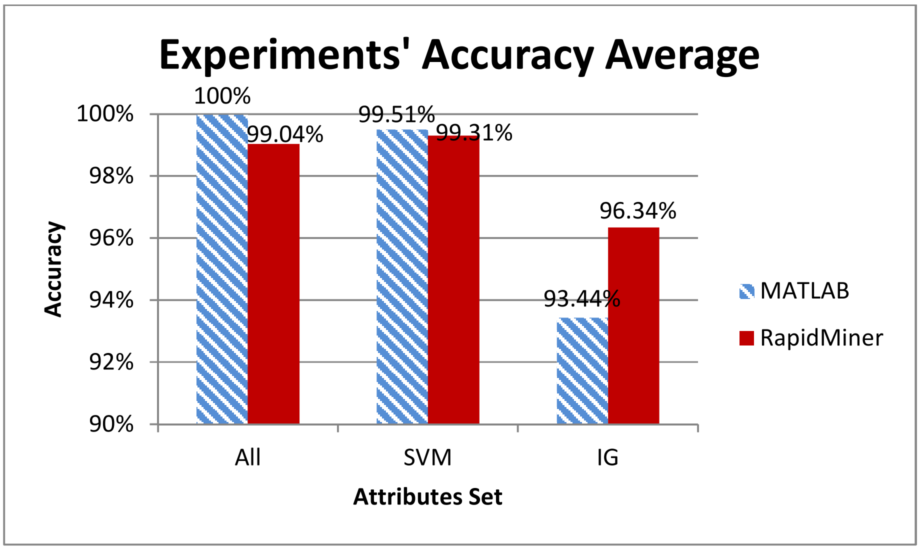


Figure 4-8: MATLAB vs RapidMiner Accuracy Average

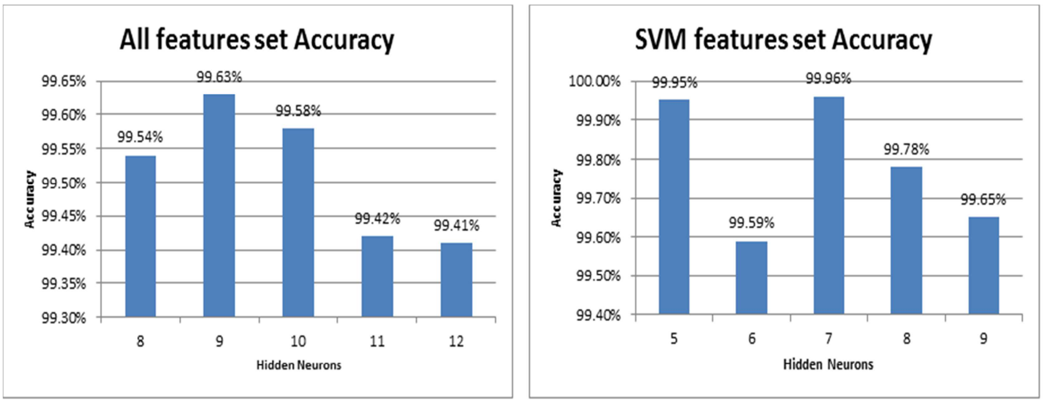
- Rapid Miner always return the accuracy with some error, e.g. in the first experiments with the All attributes data set as example it returns 98.20%±0.79%. This error (±0.79%) fill the gap between the MATLB's results and the RapidMiner's results.

- For more assurance the Iris[4] benchmark dataset, the result by using RapidMiner is 97.33% ± 3.27% and the result by using MATLAB is 97.2%.

4.2.4 The Best Architecture for BNN:

In this sub section the experiments have been done to find the best architecture of the BNN for both attribute sets the whole attribute set and the SVM attribute set. These experiments were done on the RapidMiner by fixing the following BNN's parameters and changing the number of the hidden neurons: training cycle = 500 epochs; learning rate = 0.3; momentum = 0.2; error epsilon = 1.0E-5.

For the full attribute set 15-9-2 is the best architecture of the BNN model as shown in Figure 4-8(a), while for the SVM attribute set 9-7-2 is the best architecture of the BNN model as shown in Figure 4-8(b).



(a)

(b)

Figure 4-9: All/SVM features sets hidden neurons accuracy

[4] it can be found in UCI machine learning repository at http://archive.ics.uci.edu/ml/support/iris.

4.3 Results Comparison

The experimental results show that the proposed work is more accurate than all the discussed related works. It achieved based on the all features set (15 features) 99.6%, 0.08% and 0.32% for accuracy, false negative and false positive rates respectively and it achieved based on the optimal features set (8 features) 99.6%, 0.08% and 0.32% for accuracy, false negative and false positive rates respectively 99.96%, 0.026% and 0.017% for accuracy, false negative and false positive rates respectively.

Since El-khatib’s works[30] is the most related works, Table 4-7 and Table 4-8 provide a comparison between the proposed work in this thesis and El-khatib’s works.

Table 4-7: Comparison with El-khatib's work

Parameter	Proposed Work	El-kahtib’s Work
Used attacks	Channel switch, TKIP Cryptographic, Airflood and Quiet DoS attacks.	Deauthentication, Duration, Chopchop and Fragmentation DoS attacks
Data set Size	12000	24000
All features set	15 features (MAC Frame features)	38 features (all the IEEE frame features)
Features ranking algorithm(s)	IG, IGR and SVM	IGR
Optimal features set	9 features {*Duration, FCS, Protected, FrameControl, FrameSubType, FrameType, FromDS, Retry, ToDS*}	8 features {*IsWepValid, DurationRange, MoreFlag, ToDS, WEP, Casting Type,Type, SubType, andSubType*}

It’s must be noted that isWepValid are WEP redundant features which equivalent to the Protected feature in the MAC Frame features, which is a single bit flag to check the validity of the WEP protocol in the IEEE Frame. Also the size of the data set in this work is 50% of El-khatib’s work, but it provides a higher accuracy by using the MLBP classifier which used in this work.

Table 4-8: Comparison El-khatib's results

	Proposed Work			El-kahtib’s Work		
	Accuracy	**F. Negative**	**F. Positive**	**Accuracy**	**F. Negative**	**F. Positive**
All features set	99.6%	0.08%	0.32%	88%	3%	9%
Optimal features set	99.96%	0.026%	0.017%	95.6%	0.4%	4%

Chapter 5: Conclusion and Future Work:

This chapter concludes the work, its results and discussion. Finally the future work directions were remarked.

5.1 Conclusion:

WLANs have great benefits and have a wide spread at the level of organizations and individuals. Through its evolution stages, the security issues were added to bring more protection to it. Confidentiality and data integrity are improved, while the availability security issues still considered as danger threats faced the WLANs. IDS is a major component of the defense lines in the networks, BNN is a good participant for the anomaly IDS but there is no any benchmark data set for WIDS to train its model.

This dissertation project consists of 6 stages:

- ***Stage I***: four different DoS attacks were used to create data set of 12000 instances which are classified as normal/attack traffic, this data set used to train the BNN anomaly IDS; MAC Frame features (Figure 2-3, page 13) constructed the data set's features; four data subsets extracted randomly form that data set their sizes 25%, 50%, 75% and 100% respectively.
- ***Stage II***: Four BNNs has been built by using RapidMiner base on the four data sets to measure the effectiveness of the data set size on the BNN's accuracy. The accuracy of the four BNN models are 98.20%, 99.00%, 99.4% and 99.6% respectively. The false negative rates are 0%, 0.19%, 0.14% and 0.08% respectively. The false positive rates are 1.8%, 0.8%, 0.5% and 0.3% respectively.

- ***Stage III***: Three features ranking algorithms (SVM, IG and IGR) were used to determine the optimal features set, by using the four data sets four experiments for each algorithm were done. Each algorithm ranked for the same features but with different ranked value according to the data set size. The results came as follow: IG and IGR algorithm ranked for the same features set which is {FrameControl, FrameSubType, Duration, FCS}; and SVM algorithm ranked for 9 features {Duration, FCS, Protected, FrameControl, FrameSubType, FrameType, FromDs, Retry, ToDs}.
- ***Stage IV***: measure the performance of the BNN model based on the two features sets. Four experiments were done based on the four data sets, the average of the model's accuracy are 96.3%, 99.0% and 99.3% for IG, All and SVM features sets respectively. The false negative rates are 1.9%, 0.1% and 0.04% for IG, All and SVM features sets respectively. The false positive rates are 1.76%, 0.86% and 0.55% for IG, All and SVM features sets respectively.
- ***Stage V***: Confirming the results by using MATLAB. The data set was divided into 60% as training set and 40% as testing set, the average of the model's accuracy are 93%, 100% and 100% for IG, All and SVM features sets respectively.

  Differences in results between the two tools are due to the usage of different performance measurement techniques, the RapidMiner uses the cross-validation method then provides the accuracy average with certain error ratio but the MATLAB uses single round of testing.

- ***Stage VI***: determine the best BNN's architecture (input-hidden-output) for the All, SVM and IG features sets. The results are 15-9-2, 9-7-2 and 4-4-2 respectively.

5.2 Future Work Directions:

The future work direction of this dissertation extracted from the scope and limitation of the dissertation itself and from the experimental results. These directions can be summarized on the following points:

- Examining the proposed WIDS against other DoS attacks such as the used attacks in[30].
- Increase the data set by adding Unknown traffic label then using the Fuzzy logic to distinguish between the traffic types.
- Applying the used IDS on other WLAN's structure such as Ad-hoc structure.
- According to the continuous modification on the attacks' strategies the WIDS need be extended dynamically, so that the efficiency of the dynamic growing NN must be investigated.

References

[1] AbuSamra A. and Abed R.; “Enhancement of Passive MAC Spoofing Detection Techniques”; (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 1, No. 5, November 2010

[2] AbuSamra A. and Abed R.; “Evaluation of Passive MAC Spoofing Detection Techniques”; The 6th International Symposium on Electrical & Electronics Eng. and Computer Systems (EEECS’10); November 2010

[3] Athanasopoulos A., Topalis E., Antonopoulos C. and Koubias S.; "Evaluation Analysis of the Performance of IEEE 802.11b and IEEE 802.11g Standards"; Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. vol., no., pp.141, 23-29 April 2006

[4] Mishra A. and Arbaugh W.; “An Initial Security Analysis of the IEEE 802.11X Standard”; Technical report; [Online] Available: http://citeseer.ist. psu.edu/566520.html [Accessed: June 2010], 2003.

[5] Oks¨uz A.; “*Unsupervised Intrusion Detection System*”; Master thesis, Technical University of Denmark, Informatics and Mathematical Modeling; 2007.

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

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

[8] O'Hara B. and Petrick A.; *“IEEE 802.11i security enhancements” in IEEE 802.11 Handbook: A Designer's Companion*; IEEE; pp.95-135; 2005

[8] Schneider B.; “Applied Cryptography: Protocols, Algorithms, and Source Code in C”; John Wiley & Sons; 1996.

[10] He C. and Mitchell J.; “Analysis of the 802.11i 4-way handshake”; In WiSe ’04: Proceedings of the 2004 ACM workshop on Wireless security; pp.43–50; ACM Press; 2004.

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

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

[13] Murthy C.S.R. and Manoj B.S.; “ Ad Hoc Wireless Networks: Architectures and Protocols”; Prentice Hall PTR Upper Saddle River, NJ, USA; 2004

[14] Bolzoni D., Etalle S., Hartel P.H. and Zambon E.; “Poseidon: a 2-tier anomaly-based network intrusion detection system”; In Proceedings of the 4th IEEE International

Workshop on Information Assurance;13-14 April 2006;Egham, Surrey, UK; pp. 144-156; 2006.

[15] Madory D.; “New Methods of Spoof Detection in 802.11b Wireless Networking”. PhD thesis; Dartmouth College; 2006.

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

[17] Vassis D., Kormentzas G., Rouskas A. and Maglogiannis I.; “The IEEE 802.11g standard for high data rate WLANs”; Network, IEEE , vol.19, no.3, pp.21- 26, May-June 2005

[18] Welch D. and Lanthrop S.; “Wireless Security Threat Taxonomy”; In Proceedings of the 2003 IEEE Workshop on Information Assurance; pp.76 – 83; West Point, NY, USA; June 2003.

[19] Guo F. and Chiueh T.; “Sequence number- based MAC address spoof detection”; In Proceedings of the 8th International Symposium on recent Advances in Intrusion Detection Seattle; WA,USA; Sept. 2005.

[20] Wang H. and Ma R.; “Optimization of Neural Networks for Network Intrusion Detection”; Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on, vol.1; pp.418-420; 2009

[21] IEEE; IEEE Standard 802.11-1997. Information Technology-telecommunica¬tions And Information exchange Between Systems-Local And Metropolitan Area Networks-speci?c Requirements-part 11: Wireless LAN Medium Access Control (MAC) And

Physical Layer (PHY) Speci?cations; Institute of Electrical and Electronics Engineers; 1999.

[22] Bellardo J. and Savage S.; “802.11 Denial-of-Service Attacks: Real Vulnerabili¬ties and Practical Solutions”; In Proceedings of the USENIX Security Symposium. Washington D.C., USA, 2003.

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

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

[25] Hall J., Barbeau M. and Kranakis E.; “*Radio Frequency Fingerprinting for Intrusion Detection in Wireless Networks*”; IEEE Transactions on Defendable and Secure Computing; 2005.

[26] Kleider J., Gifford S., Chuprun S. and Fette B.; “Radio frequency watermarking for OFDM wireless networks”; IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP’04); Vol. 5; 2004.

[27] Ryan J., Lin M.J. and Miikkulainen R.; “Intrusion detection with neural networks”; In Michael I. Jordan, Michael J. Kearns, and Sara A. Solla, editors; Advances in Neural Information Processing Systems; Vol. 10; The MIT Press; 1998.

[28] Shun J. and Malki H.A.; “Network Intrusion Detection System Using Neural Networks”; Natural Computation, 2008; ICNC '08; 4th International Conference on, vol.5, no.; pp.242-246; 2008.

[29] Quinlan J.R.; “Induction of Decision Trees”; Machine Learning; Vol.1; pp.81-106; 1986.

[30] El-Khatib K.; “Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems”; Parallel and Distributed Systems, IEEE Transactions on; vol.21, no.8; pp.1143-1149; Aug. 2010

[31] Sugantha K. and Shanmugavel S.; "Anomaly detection of the NAV attack in MAC layer under non-time and time-constrained environment"; Wireless and Optical Communications Networks, 2006 IFIP International Conference on , vol., no., pp.5, 2006

[32] Andrew L.; Snort-Wireless. [Online] Available: http://www.snort.org/ [Accessed: March 2011], 2005.

[33] Torres L.M., Magana E., Izal M., Morato D. and Santafe G.; "An anomaly-based intrusion detection system for IEEE 802.11 networks"; Wireless Days (WD), 2010 IFIP , vol., no., pp.1-6, 20-22 Oct. 2010

[34] Wang Li and Srinivasan B.; "Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard"; Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on , vol.2, no., pp.109-113, 24-25 April 2010

[35] Kantardzic M.; “Data Mining: Concepts, Models, Methods, and Algorithms”; ebook ed.; John Wiley & Sons ©; 2003.

[36] Zargari M., Su D.K., Yue C.P., Rabii S., Weber D., Kaczynski B.J. , Mehta S.S. , Singh K. , Mendis S. and Wooley B.A.; “A 5-GHz CMOS transceiver for IEEE 802.11a wireless LAN systems”; Solid-State Circuits, IEEE Journal of , vol.37, no.12, pp.1688-1694, Dec 2002

[37] Hall M.A. and Holmes G.; “Benchmarking attribute selection techniques for discrete class data mining”; Knowledge and Data Engineering; IEEE Transactions on; vol.15, no.6; pp.1437- 1447; Nov.-Dec. 2003

[38] Asokan N., Niemi V. and Nyberg K.; “Man-in-the-Middle in Tunnelled Authentication Protocols”; 11th Security Protocols Workshop; pp.28–41; 2003.

[39] Borisov N., Goldberg I. and Wagner D.; ”Intercepting mobile communications: the insecurity of 802.11”; in proceedings of the 7th annual international conference on Mobile computing and networking; pp.180–189; 2001.

[40] NIST; “Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i”, Feb 2007; National Institute of Standards and Technology; Special Publication 800-97. [Online] Available: http://csrc.nist.gov/publications/ nistpubs/800-97/SP800-97.pdf

[41] Chatzimisios P., Boucouvalas A.C. and Vitsas V.; “Optimisation of RTS/CTS handshake in IEEE 802.11 wireless LANs for maximum performance”; Global Telecommunications Conference Workshops, 2004. GlobeCom Workshops 2004. IEEE; vol., no., pp.270- 275, 29 Nov.-3 Dec. 2004

[42] Bradley P.S. and Mangasarian O.L.; "Feature selection via Concave Minimization and Support Vector Machines"; Machine Learning Proceedings of the 15th International Conference (ICML), California; pp.82-90; 1998.

[43] Pathack N.P., Kulkarni M.R. and Joshi S.D.; *"A Wireless Intrusion Detection Method Based on Neural Network*"; Advance Computer Vision and Information Technology; pp.244-250; 2006 [online at: http://books.google.com/books accessed at Jun, 2011]

[44] Ahlawat R. and Dulaney K.; "Magic Quadrant for Wireless LAN Infrastructure"; Gartner Research; 2006.

[45] Gill R., Smith J., Looi M. and Clark A.; "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): Refer¬eed R&D Stream; pp.26 – 38; 2005.

[46] Hecht-Nielsen R.; "Theory of the backpropagation neural network"; Neural Networks, 1989. IJCNN.; International Joint Conference on , vol., no., pp.593-605 vol.1; pp.18-22 Jun 1989

[47] Rojas R.; "Neural Networks: A Systematic Introduction"; (PDF); Springer-Verlag; Berlin; 1996; pp.151-170 Available: http://page.mi.fu-berlin.de/rojas/neural/neuron.pdf [March 10, 2011]

[48] Haykin S.; "Neural Networks, A Comprehensive Foundation"; Prentice Hall, 2nd edition, 1999.

[49] Purnami S.W., Rahayu S.P. and Embong A.; "Feature selection and classification of breast cancer diagnosis based on support vector machines"; Information Technology, 2008. ITSim 2008. International Symposium on , vol.1, no., pp.1-6, 26-28 Aug. 2008

[50] T.B. Trafalis, B. Santosa, and M.B. Richman; “Feature Selection with Linear Programming Support Vector Machines and Applications to Tornado Prediction”; WSEAS Transactions on Computers; Vol. 4, no.8; pp.865-873; 2005.

[51] Khoshgoftaar T.M., Nath S.V., Zhong S. and Seliya N.; “Intrusion detection in wireless networks using clustering techniques with expert analysis”; In Proceeding of the ICMLA 2005: Fourth International Conference on Machine Learning and Applications; pp.120-125; 2005.

[52] Vapnik V.; “Statistical Learning Theory”; John Wiley & Sons ©; New York; 1998.

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

[54] Arbaugh W.; “An inductive chosen plaintext attack against WEP/WEP2”; IEEE Document, 802(01); pp.230; 2001.

[55] Hsieh W., Lo C., Lee J. and Huang L.; “The implementation of a proactive wireless intrusion detection system”; In Procedding for The 4th International Conference on Computer and Information Technology; CIT ’04. 14-16 Sept; pp.581–586; 2004.

[56] Lee W. and Stolfo S.J.; “A framework for constructing features and models for intrusion detection systems”; ACM Transaction; Information System Security; 3(4); pp.227-261; 2000.

[57] Wang X. and Giannakis G.B.; "CSMA/CCA: A Modified CSMA/CA Protocol Mitigating the Fairness Problem for IEEE 802.11 DCF"; Multimedia Services Access Networks, 2005. MSAN '05. 2005 1st International Conference on , vol., no., pp.88- 95, 13-15 June 2005

[58] Xiaodong Zah. and Maode Ma; "Security improvements of IEEE 802.11i 4-way handshake scheme" Communication Systems (ICCS), 2010 IEEE International Conference on , vol., no., pp.667-671, 17-19 Nov. 2010

[59] Xinyu Xing, Shakshuki E., Benoit D. and Sheltami T.; "Security Analysis and Authentication Improvement for IEEE 802.11i Specification"; Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE , vol., no., pp.1-5, Nov. 30 2008 - Dec. 4 2008.

[60] Liu Y., Tian D. and Li B.; "A Wireless Intrusion Detection Method Based on Dynamic Growing Neural Network"; Computer and Computational Sciences, 2006; IMSCCS '06. First International Multi-Symposiums on , vol.2, no., pp.611-615, 20-24 June 2006.

[61] Sani Y., Mohamedou A., Ali K., Farjamfar A., Azman M. and Shamsuddin S.; "An Overview of Neural Networks Use in Anomaly Intrusion Detection Systems"; Research and Development (SCOReD); 2009 IEEE Student Conference on ; vol.; pp.89-92; 16-18 Nov. 2009

[62] Yong Liu; "Create Stable Neural Networks by Cross-Validation"; Neural Networks, 2006. IJCNN '06. International Joint Conference on; vol., no.; pp.3925-3928; 2006

[63] Aircrack, http://www.aircrack-ng.net; [Accessed March, 2011]

[64] MATLAB - The Language Of Technical Computing; www.mathworks.com/products/matlab/

[65] Rapid Miner 5.0.010; http://www.rapidminer.com ; [Accessed March, 2011]

[66] Wireshark; http://www.wireshark.org ; Plugin with Backtrack 4 Lunix Operating System.

Appendix A:

IEEE Captured Frame Format

A WLANs frame as exported by wireshark, the following frame is only a sample of the frames. The following frame is a Beacon frame.

```
No.     Time        Source               Destination          Protocol Info
  3225 122.981167  Netgear_41:39:82      Broadcast            IEEE 802.11 Beacon frame, SN=3237, FN=0,
Flags=........C, BI=100, SSID="NETGEAR - 0"

Frame 3225: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits)
    Arrival Time: Mar 13, 2011 16:21:07.217726000 Jerusalem Standard Time
    Epoch Time: 1300026067.217726000 seconds
    [Time delta from previous captured frame: 0.048991000 seconds]
    [Time delta from previous displayed frame: 0.048991000 seconds]
    [Time since reference or first frame: 122.981167000 seconds]
    Frame Number: 3225
    Frame Length: 168 bytes (1344 bits)
    Capture Length: 168 bytes (1344 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan]
Radiotap Header v0, Length 32
    Header revision: 0
    Header pad: 0
    Header length: 32
    Present flags: 0x0000482f
        .... .... .... .... .... .... .... ...1 = TSFT: True
        .... .... .... .... .... .... .... ..1. = Flags: True
        .... .... .... .... .... .... .... .1.. = Rate: True
        .... .... .... .... .... .... .... 1... = Channel: True
    .... .... .... .... .... .... ...0 .... = FHSS: False
    .... .... .... .... .... .... ..1. .... = DBM Antenna Signal: True
    .... .... .... .... .... .... .0.. .... = DBM Antenna Noise: False
    .... .... .... .... .... .... 0... .... = Lock Quality: False
    .... .... .... .... .... ...0 .... .... = TX Attenuation: False
    .... .... .... .... .... ..0. .... .... = DB TX Attenuation: False
    .... .... .... .... .... .0.. .... .... = DBM TX Attenuation: False
    .... .... .... .... .... 1... .... .... = Antenna: True
    .... .... .... .... ...0 .... .... .... = DB Antenna Signal: False
    .... .... .... .... ..0. .... .... .... = DB Antenna Noise: False
    .... .... .... .... .1.. .... .... .... = RX flags: True
    .... .... .... .0.. .... .... .... .... = Channel+: False
    0... .... .... .... .... .... .... .... = Ext: False
MAC timestamp: 5328384146
Flags: 0x10
    .... ...0 = CFP: False
    .... ..0. = Preamble: Long
    .... .0.. = WEP: False
    .... 0... = Fragmentation: False
    ...1 .... = FCS at end: True
    ..0. .... = Data Pad: False
    .0.. .... = Bad FCS: False
    0... .... = Short GI: False
Data Rate: 1.0 Mb/s
Channel frequency: 2452 [BG 9]
Channel type: 802.11b (0x00a0)
    .... .... ...0 .... = Turbo: False
    .... .... ..1. .... = Complementary Code Keying (CCK): True
```

```
            .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
            .... .... 1... .... = 2 GHz spectrum: True
            .... ...0 .... .... = 5 GHz spectrum: False
            .... ..0. .... .... = Passive: False
            .... .0.. .... .... = Dynamic CCK-OFDM: False
            .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
            ...0 .... .... .... = GSM (900MHz): False
            ..0. .... .... .... = Static Turbo: False
            .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
            0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
        SSI Signal: -46 dBm
        Antenna: 1
        RX flags: 0x0000
            .... .... .... .... .... ..0. = Bad PLCP: False
    IEEE 802.11 Beacon frame, Flags: ........C
        Type/Subtype: Beacon frame (0x08)
        Frame Control: 0x0080 (Normal)
            Version: 0
            Type: Management frame (0)
            Subtype: 8
            Flags: 0x0
                .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
                .... .0.. = More Fragments: This is the last fragment
                .... 0... = Retry: Frame is not being retransmitted
                ...0 .... = PWR MGT: STA will stay up
                ..0. .... = More Data: No data buffered
                .0.. .... = Protected flag: Data is not protected
            0... .... = Order flag: Not strictly ordered

    Duration: 0

    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

    Source address: Netgear_41:39:82 (00:22:3f:41:39:82)

    BSS Id: Netgear_41:39:82 (00:22:3f:41:39:82)

    Fragment number: 0

    Sequence number: 3237

    Frame check sequence: 0xd7265263 [correct]

        [Good: True]

        [Bad: False]

IEEE 802.11 wireless LAN management frame

    Fixed parameters (12 bytes)

        Timestamp: 0x000000013D98B181

        Beacon Interval: 0.102400 [Seconds]

        Capability Information: 0x0421

            .... .... .... ...1 = ESS capabilities: Transmitter is an AP

            .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS

            .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)

            .... .... ...0 .... = Privacy: AP/STA cannot support WEP

            .... .... ..1. .... = Short Preamble: Short preamble allowed

            .... .... .0.. .... = PBCC: PBCC modulation not allowed

            .... .... 0... .... = Channel Agility: Channel agility not in use

            .... ...0 .... .... = Spectrum Management: dot11SpectrumManagementRequired FALSE

            .... .1.. .... .... = Short Slot Time: Short slot time in use

            .... 0... .... .... = Automatic Power Save Delivery: apsd not implemented

            ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed

            .0.. .... .... .... = Delayed Block Ack: delayed block ack not implemented

            0... .... .... .... = Immediate Block Ack: immediate block ack not implemented
```

```
Tagged parameters (96 bytes)
  SSID parameter set
    Tag Number: 0 (SSID parameter set)
    Tag length: 11
    Tag interpretation: NETGEAR - 0: "NETGEAR - 0"
  Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) 6.0 12.0 24.0 36.0
    Tag Number: 1 (Supported Rates)
    Tag length: 8
    Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) 6.0 12.0 24.0 36.0  [Mbit/sec]
  DS Parameter set: Current Channel: 9
    Tag Number: 3 (DS Parameter set)
    Tag length: 1
    Tag interpretation: Current Channel: 9
  Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
    Tag Number: 5 (Traffic Indication Map (TIM))
    TIM length: 4
    DTIM count: 0
    DTIM period: 1
    Bitmap Control: 0x00 (mcast:0, bitmap offset 0)
  Country Information: Country Code: KR, Any Environment
    Tag Number: 7 (Country Information)
    Tag length: 6
    Tag interpretation: Country Code: KR, Any Environment
     Start Channel: 1, Channels: 13, Max TX Power: 20 dBm
  ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
    Tag Number: 42 (ERP Information)
    Tag length: 1
    Tag interpretation: ERP info: 0x0 (no Non-ERP STAs, do not use protection, short or long
preambles)
           Extended Supported Rates: 9.0 18.0 48.0 54.0
             Tag Number: 50 (Extended Supported Rates)
             Tag length: 4
             Tag interpretation: Supported rates: 9.0 18.0 48.0 54.0  [Mbit/sec]
           Vendor Specific: Autocell
             Tag Number: 221 (Vendor Specific)
             Tag length: 45
             Vendor: Autocell
             Tag interpretation: Not interpreted
```

Appendix B:

Java Program to fill Text data into Columns

The used Java program to fill the raw data to columns

```
package RawData2Columns;

import java.io.BufferedReader;

import java.io.BufferedWriter;

import java.io.File;

import java.io.FileReader;

import java.io.FileWriter;

import java.util.ArrayList;


/**

 *

 * @author eshami

 */

public class RawData2Columns{


    /**

     * @param args the command line arguments

     */

    public static void main(String[] args) {

        // TODO code application logic here

        // determine the input and output file

        File fname = new File("D://Cases/Case1.txt");
File tfile = new File("D://Cases/Case1Result.txt");

// define BufferedReader,BufferredWriter to read/write form/to
// input/output files
BufferedReader reader = null;
BufferedWriter writer = null;

// store the frame temporarlly in RAM
ArrayList<String> strAr = new ArrayList<String>();

// just a frame counter
int FrameCount = 0;



try{
  // open the input/output files
  reader = new BufferedReader(new FileReader(fname));
  writer = new BufferedWriter(new FileWriter(tfile));

                  String t="";
  String str;
  String sub = "";
  String conStr = "";
```

```
// reading the raw input file line by line
while((str=reader.readLine()) != null){

 t = str.substring(0,3);
 sub = sub +"$"+str;

 // if the line is a starting of a new frame
 // write the the previous string to the output
 // file as a new line
 if(t.compareTo("No.")==0)
 {
                   strAr.add(conStr);
                   writer.write(conStr);
   writer.newLine();

                   conStr = "";

                   // print the frame counter on screen to tell how
                   // many frames were writen in the output file
                   System.out.println("Frame No.:" + ++FrameCount);

 }
```

```
      else
            // if the t is not a starting of a new
            // line then concatenate it to the existing
            // line (frame)
            conStr = conStr + "\t"+str;

     }
     reader.close();

     writer.close();
    }
    catch(Exception e){
      System.out.println("Error: " + e.getMessage());
    }

  }

}
```