Performance analysis of wireless intrusion detection systems

Khalid Nasr

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :
Institut National Polytechnique de Toulouse (INP Toulouse)

Discipline ou spécialité :
Réseaux, Télécommunications, Système et Architecture

Présentée et soutenue par :
Khalid Salih Sayed NASR

Le 09 Janvier 2014

Titre :

Analyse de Performance des Systèmes de Détection d'Intrusion Sans-Fil

Performance Analysis of Wireless Intrusion Detection Systems

JURY

M. Frédéric CUPPENS	Professeur, IMT Télécom Bretagne	Président
M. Abdelmadjid BOUABDALLAH	Professeur, UTC Compiègne	Rapporteur
M. Belhassen ZOUARI	Professeur, Sup'Com de Tunis	Rapporteur
M. Christian FRABOUL	Professeur, INP Toulouse	Examinateur
M. Anas ABOU EL KALAM	HDR, Maître de Conf., INP Toulouse	Examinateur

---

Ecole doctorale : Mathématiques Informatique Télécommunications de Toulouse (MITT)
Unité de recherche : IRIT - UMR CNRS 5505
Directeur(s) de Thèse : M. Christian FRABOUL et M. Anas ABOU EL KALAM
Rapporteurs : M. Abdelmadjid BOUABDALLAH et M. Belhassen ZOUARI

To my homeland Egypt, my parents, my wife, my children, my sisters, my wife's parents, and my family.

Acknowledgement

First and foremost I would like to thank my God “ALLAH” for granting me the power and patience throughout the entire PhD journey. Second, I’m so grateful to my beloved homeland “Egypt” which fully funded my PhD program. I pray to ALLAH to keep Egypt safe, secure, and going to a prosperous future.

I would like to express my sincere gratitude to my supervisors Prof. Christian Fraboul and Dr. Anas Abou El Kalam for their continuous support, guidance, encouragement, scientific advice throughout my PhD study. It has been a great honor for me to work under their supervision.

I’m also so thankful to the members of my PhD committee, Prof. Abdelmadjid Bouabdallah, Prof. Belhassen Zouari, and Prof. Frédéric Cuppens for their time, interest, insightful comments, and valuable evaluation reports of my PhD thesis. I am truly fortunate to have had them as members of my PhD committee.

I’m so grateful to the members of the Egyptian Cultural and Educational Bureau in Paris for their continuous assistance, support, appreciable service, and good management of the administrative aspects throughout my PhD program.

I am especially grateful to the members of our laboratory who have contributed immensely to my personal and professional time, Hisham Slimani, Ahmed Neffati, Mohamed Maachaoui, Abdeljebar Ameziane, Hassan Ait Lahcen, Jalal Alroumy, Mohamed Adnan, Bafing Cyprien, Abdelaziz Nacer, Mahmoud Mostafa, Sokchenda Sreng, Warodom Werapun, and Farouk Mezghani. This group has been a source of friendships as well as good advice and collaboration.

I will forever be thankful to my egyptian friends, Hany Ibrahim, Ahmed Akl, El Awady Attia, Yasser Nassar, Ossama Hamouda, and Mohammed Gad who are helpful persons in general. They didn’t skimp on their time, effort, or advice throughout my PhD study.

Last but not least, I would like to especially thank my beloved mother, father, wife, children, sisters, wife’s parents, and family for supporting me spiritually and for their prayer to ALLAH for me throughout my PhD study and my life. My darling parents have sacrificed themselves for me, my brother, and sisters and they provided unconditional love and care. If I stay all my life to fully serve them, I cannot give them a sample of their rights. I pray to ALLAH to bless them with good health and sheltered life. The best event in the past five years is finding my sweetheart, soul mate, and wife. She has accompanied me during my good and hard times, truly supported me, and alleviated the life challenges. She was there during the thesis writing to help me by quick proofreading and giving suggestions. There are no words to convey my gratitude and love for her. I cannot forget my sweet children; Abdulrahman, Abdullah, and Omar who make my life more beautiful and enjoyable.

Abstract

Wireless intrusion detection system (WIDS) has become a matter of increasing concern in recent years as a crucial element in wireless network security. WIDS monitors 802.11 traffic to identify the intrusive activities, and then alerts the complementary prevention part to combat the attacks. Selecting a reliable WIDS system necessitates inevitably taking into account a credible evaluation of WIDSs performance. WIDS effectiveness is considered the basic factor in evaluating the WIDS performance, thus it receives great attention in this thesis. Most previous experimental evaluations of intrusion detection systems (IDSs) were concerned with the wired IDSs, with an apparent lack of evaluating the wireless IDSs (WIDSs). In this thesis, we try to manipulate three main critiques of most pervious evaluations; lack of comprehensive evaluation methodology, holistic attack classification, and expressive evaluation metrics.

In this thesis, we introduce a comprehensive evaluation methodology that covers all the essential dimensions for a credible evaluation of WIDSs performance. The main pivotal dimensions in our methodology are characterizing and generating the evaluation dataset, defining reliable and expressive evaluation metrics, and overcoming the evaluation limitations. Basically, evaluation dataset consists of two main parts; normal traffic (as a background) and malicious traffic. The background traffic, which comprises normal and benign activities in the absence of attacks, was generated in our experimental evaluation tests as real controlled traffic. The second and important part of the dataset is the malicious traffic which is composed of intrusive activities. Comprehensive and credible evaluation of WIDSs necessitates taking into account all possible attacks. While this is operationally impossible, it is necessary to select representative attack test cases that are extracted mainly from a comprehensive classification of wireless attacks. Dealing with this challenge, we have developed a holistic taxonomy of wireless security attacks from the perspective of the WIDS evaluator. The second pivotal dimension in our methodology is defining reliable evaluation metrics. We introduce a new evaluation metric E_{ID} (*intrusion detection effectiveness*) that manipulates the drawbacks of the previously proposed metrics, especially the common drawback of their main notion that leads to measuring a relative effectiveness. The notion of our developed metric E_{ID} helps in measuring the actual effectiveness. We also introduce another metric R_R (*attack recognition rate*) to evaluate the ability of WIDS to recognize the attack type. The third important dimension in our methodology is overcoming the evaluation limitations. The great challenge that we have faced in the experimental evaluation of WIDSs is the uncontrolled traffic over the open wireless medium. This uncontrolled traffic affects the accuracy of the measurements. We overcame this problem by constructing an RF shielded testbed to take all the measurements under our control without any interfering from any adjacent stations. Finally, we followed our methodology and conducted experimental evaluation tests of two popular WIDSs (*Kismet* and *AirSnare*), and demonstrated the utility of our proposed solutions.

Résumé

La sécurité des réseaux sans fil fait l'objet d'une attention considérable ces dernières années. Toutefois, les communications sans fil sont confrontées à plusieurs types de menaces et d'attaques. Par conséquent, d'importants efforts, visant à sécuriser davantage les réseaux sans fil, ont dû être fournis pour en vue de lutter contre les attaques sans fil. Seulement, croire qu'une prévention intégrale des attaques peut s'effectuer au niveau de la première ligne de défense d'un système (pare-feux, chiffrement, …) n'est malheureusement qu'illusion. Ainsi, l'accent est de plus en plus porté sur la détection des attaques sans fil au travers d'une seconde ligne de défense, matérialisée par les systèmes de détection d'intrusions sans fil (WIDS). Les WIDS inspectent le trafic sans fil, respectant la norme 802.11, ainsi que les activités du système dans le but de détecter des activités malicieuses. Une alerte est ensuite envoyée aux briques chargées de la prévention pour contrer l'attaque. Sélectionner un WIDS fiable dépend principalement de l'évaluation méticuleuse de ses performances. L'efficacité du WIDS est considérée comme le facteur fondamental lors de l'évaluation de ses performances, nous lui accordons donc un grand intérêt dans ces travaux de thèse. La majeure partie des études expérimentales visant l'évaluation des systèmes de détection d'intrusions (IDS) s'intéressait aux IDS filaires, reflétant ainsi une carence claire en matière d'évaluation des IDS sans fil (WIDS). Au cours de cette thèse, nous avons mis l'accent sur trois principales critiques visant la plupart des précédentes évaluations : le manque de méthodologie d'évaluation globale, de classification d'attaque et de métriques d'évaluation fiables.

Au cours de cette thèse, nous sommes parvenus à développer une méthodologie complète d'évaluation couvrant toutes les dimensions nécessaires pour une évaluation crédible des performances des WIDSs. Les axes principaux de notre méthodologie sont la caractérisation et la génération des données d'évaluation, la définition de métriques d'évaluation fiables tout en évitant les limitations de l'évaluation. Fondamentalement, les données d'évaluation sont constituées de deux principales composantes à savoir: un trafic normal et un trafic malveillant. Le trafic normal que nous avons généré au cours de nos tests d'évaluation était un trafic réel que nous contrôlions. La deuxième composante des données, qui se trouve être la plus importante, est le trafic malveillant consistant en des activités intrusives. Une évaluation complète et crédible des WIDSs impose la prise en compte de tous les scénarios et types d'attaques éventuels. Cela étant impossible à réaliser, il est nécessaire de sélectionner certains cas d'attaque représentatifs, principalement extraits d'une classification complète des attaques sans fil. Pour relever ce défi, nous avons développé une taxinomie globale des attaques visant la sécurité des réseaux sans fil, d'un point de vue de l'évaluateur des WIDS. Le deuxième axe de notre méthodologie est la définition de métriques fiables d'évaluation. Nous avons introduit une nouvelle métrique d'évaluation, E_{ID} (*Efficacité de la détection d'intrusion*), visant à pallier les limitations des précédentes métriques proposées. Nous avons démontré l'utilité de la métrique E_{ID} par rapport aux autres métriques proposées précédemment et comment elle parvenait à

mesurer l'efficacité réelle tandis que les précédentes métriques ne mesuraient qu'une efficacité relative. L' E_{ID} peut tout aussi bien être utilisé pour l'évaluation de l'efficacité des IDS filaires et sans fil. Nous avons aussi introduit une autre métrique notée R_R (*Taux de Reconnaissance*), pour mesurer l'attribut de reconnaissance d'attaque. Un important problème se pose lorsque des tests d'évaluation des WIDS sont menés, il s'agit des données de trafics incontrôlés sur le support ouvert de transmission. Ce trafic incontrôlé affecte sérieusement la pertinence des mesures. Pour outrepasser ce problème, nous avons construit un banc d'essai RF blindé, ce qui nous a permis de prendre des mesures nettes sans aucune interférence avec quelconque source de trafic incontrôlé. Pour finir, nous avons appliqué notre méthodologie et effectué des évaluations expérimentales relatives à deux WIDSs populaires (*Kismet* et *AirSnare*); nous avons démontré à l'issue de ces évaluations pratiques et l'utilité de nos solutions proposées.

Table of Contents

List of Figures

List of Tables

List of Acronyms

AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AP	Access Point
BSSID	Basic Service Set Identifier
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	Counter-Mode/CBC-MAC Protocol
C_{ID}	Intrusion Detection Capability
CTS	Clear to Send
DDoS	Distributed Denial of Service
DoS	Denial of Service
DR	Detection Rate
EAP	Extensible Authentication Protocol
E_{ID}	Intrusion Detection Effectiveness
ESSID	Extended Service Set Identifier
FP	False Positive
FN	False Negative
GUI	Graphical User Interface
ICV	Integrity Check Value
IDOC	Intrusion Detection Operating Characteristic
IDS	Intrusion Detection System
IV	Initialization Vector
MAC	Media Access Control
MANET	Mobile Ad Hoc Network
MIC	Message Integrity Check
MITM	Man-In-The-Middle attack
PPV	Positive Predictive Value
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
ROC	Receiver Operating Characteristic

R_R	Recognition Rate
RTS	Request to Send
SSID	Service Set Identifier
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TP	True Positive
TN	True Negative
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WIDS	Wireless Intrusion Detection System
WPA	Wi-Fi Protected Access
WSN	Wireless Sensor Network

I. Chapter 1: Introduction

To meet the growing demand for communication at a distance easily and efficiently, numerous telecommunications techniques and protocols have been developed, especially for wireless networks. Wireless networking technology has emerged as a very popular alternative to wired networking technology in recent years. Flexibility in dealing with these protocols and their vulnerabilities creates a problem of poor security. Consequently, several security efforts have been exerted and many security defense mechanisms have been developed such as authentication, encryption, and firewalls. These mechanisms aim to control the access to the system as a first line of defense. Nevertheless, most of the wireless systems are still susceptible to attacks. Unfortunately, complete attack prevention at the first line of defense is not realistically attainable due to lack of centralized monitoring and management points, dynamically changed network topologies [Bidg06], openness of wireless medium, system complexity, design and implementation flaws, configuration and administration errors, etc. Thus the emphasis on detecting the wireless attacks through a second line of defense, in the form of Wireless Intrusion Detection System (WIDS), has been increasing in this context. Basically, WIDS monitors 802.11 wireless traffic and system activities to identify the intrusive activities, and then alerts the complementary prevention part to combat the detected attacks. Despite the importance of WIDSs in wireless network security, their performance is sometimes not satisfying in practice. Thus evaluating WIDSs performance is a pressing necessity. Evaluation can be defined as a systematic assessment of the ability of a WIDS to meet the intended and expected performance.

1.1. Motivations

The break-ins occur almost daily in wireless networks and the distinct lack of the evaluation of wireless intrusion detection systems (WIDSs) are the main motivations for this work. Despite the great concern of most previous work with the evaluation of the intrusion detection systems (IDSs), their evaluations suffer from some drawbacks. In this thesis, the strengths and weaknesses of the previous work are discussed and analyzed to extract the main problematics of this topic, to subsequently develop reasonable solutions for managing a credible evaluation of WIDSs.

Selecting a reliable WIDS depends significantly on its performance. Basically, there are many different attributes that evaluate the WIDS performance such as *effectiveness, efficiency, interoperability, collaboration* [Axel99], *redundant alerts correlation, the impact on the monitored system resources, attack type recognition, scalability and flexibility, etc*. WIDS effectiveness is considered the basic factor in evaluating the WIDS performance, and it thus receives considerable attention in this thesis. Effectiveness reflects the ability of WIDS to detect the intrusive activities and the absence degree of the false alarms which are considered the main great challenges facing the IDSs performance.

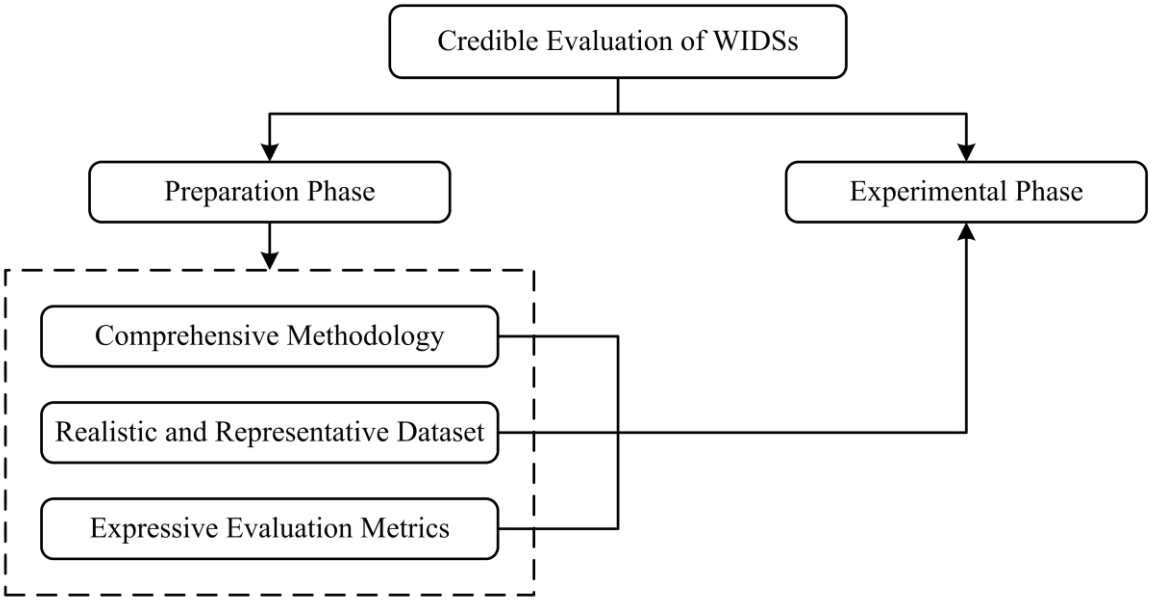

Figure I-1: Key Dimensions of Credible Evaluation of WIDSs.

1.2. Research Goals

Dealing with the above-mentioned motivations, our research goal is performing a credible evaluation of WIDSs (Figure I-1) that can be achieved through two main phases; preparation phase and experimental phase. The preparation phase includes three main pivots that are manifested in preparing a comprehensive evaluation methodology, characterizing real and representative dataset, and defining expressive evaluation metrics. These three pivots altogether are considered in the experimental phase that is managed with regard to predefined conditions to ensure the accuracy of the experimental measurements.

1.3. Contributions

Figure I-1 shows our concept of managing a credible evaluation of WIDSs performance. We commence with introducing a comprehensive evaluation methodology that is considered the road map of our work in the thesis. This methodology takes into account the remaining key dimensions to achieve a credible evaluation.

1.3.1. Comprehensive Evaluation Methodology

Our proposed methodology covers the essential dimensions for a comprehensive and credible evaluation of WIDSs performance. The methodology dimensions or tasks are organized in a sequential and well- engineered manner, starting from the main goals of WIDSs evaluation reaching the intended objectives. This methodology considers some significant dimensions which have been disregarded in the previous work, such as analyzing the evaluation limitations

in order to take the proper measures to overcome them. The pivotal dimensions that receive great attention in our methodology are characterizing and generating representative and real dataset, and defining reliable and expressive evaluation metrics. Basically, the evaluation dataset consists of two main parts; normal traffic (as a background) and malicious traffic. The background traffic, which comprises normal and benign activities in the absence of attacks, can be generated using real or synthetic dataset as described in chapter 3 and chapter 6. In our experimental work in this thesis, we use real background traffic (chapter 6). The second part of the dataset is the malicious traffic which is composed of intrusive activities. No doubt that the credibility of the WIDS evaluation depends significantly on a comprehensive characterization of the malicious traffic. Thus a holistic classification of wireless security attacks is a pressing necessity.

1.3.2. WIDSs Evaluation Centric Taxonomy of Wireless Security Attacks

The ability of WIDS to detect the intrusive activities is an important aspect of the WIDSs effectiveness. Thus, the intrusive traffic used in the evaluation of WIDSs effectiveness should be representative of the possible intrusions in the environment of interest. Dealing with this challenge, we have developed a holistic taxonomy of wireless security attacks from the perspective of the WIDS evaluator. Our proposed taxonomy includes all relevant essential dimensions for wireless attacks classification and it helps in generating and extracting the representative attack test cases. We also consider a new concept of the probability of occurrence of the attack test cases that leads to accurate results of WIDSs evaluation. All these issues are more fully treated in chapter 4.

1.3.3. Novel Evaluation Metrics

Defining expressive evaluation metrics is a crucial task in the evaluation process. Dealing with this issue, we develop a novel metric called *intrusion detection effectiveness* (E_{ID}) for the evaluation of IDSs/WIDSs effectiveness. E_{ID} manipulates the drawbacks of the existing metrics, especially the common main drawback that is manifested in their main notion of measuring the IDSs effectiveness on the basis of comparing two IDSs or more to select the best one, whereas this selected one may be ineffective. The effectiveness measured by this approach can be described as *relative effectiveness*. For measuring the *actual effectiveness,* the notion of our developed metric E_{ID} is based on comparing the operating curve of the IDS/WIDS (system under test) to the *optimal operating curve* (i.e., created as a *zero reference curve ZRC*) by calculating the variation between the two curves. The variation value interprets the deviation of the IDS operation from the intended optimal operation. E_{ID} can be used for evaluating the effectiveness of wired or wireless IDSs. The distinct advantages of E_{ID} over the previously proposed metrics are demonstrated in chapter 5.

We also introduce another metric called *attack recognition rate* (R_R) to measure the proportion of the detected intrusions that are recognized. This metric is related to the diagnosis ability that helps consequently in taking the proper measures.

1.3.4. RF Shielded Testbed

One of the great challenges that we have faced in the experimental evaluation of WIDSs is the uncontrolled 802.11 traffic from the adjacent wireless stations in the open wireless medium which obstructs the accurate measurements of the considered parameters. We overcame this problem by constructing an RF shielded testbed to manage all the measurements under our control without any interfering from any uncontrolled traffic. This significantly facilitates our task of generating and managing real and representative dataset.

As a complement, we follow the remaining dimensions of our methodology to finally conduct experimental evaluation tests of two popular WIDSs (Kismet and AirSnare), to demonstrate the utility of our proposed solutions.

1.4. Thesis Outline

The remainder of the thesis is organized as follows:

Chapter 2 presents an overview of wireless networking technology and the associated benefits and limitations, with a great concern about the wireless network security. A security conceptual model is introduced to clarify the relationships between the network security concepts, the importance of the security countermeasures, and the significant role of WIDS as a second line of defense.

Chapter 3 introduces our proposed methodology for evaluating the WIDSs performance as a consequence of analyzing some existing experimental evaluations of IDSs and the associated critiques. The dimensions of this methodology are described in detail, starting from the main evaluation goals, passing the related subsequent tasks, until reaching the ultimate objective of experimental testing and evaluation of WIDSs.

Chapter 4 presents a new holistic taxonomy of wireless security attacks from the perspective of the WIDSs evaluator. This chapter differentiates between the attack classifications on the basis of the classification orientation, whether it is *evaluation-centric* or *defense-centric* classification; the later one is the main concern of this chapter. The proposed taxonomy helps in extracting the representative attacks test cases. Also, the new concept of the test cases probability is considered in this chapter.

Chapter 5 introduces a novel evaluation metric called *intrusion detection effectiveness* (E_{ID}). This chapter discusses in detail the existing metrics and their advantages and disadvantages. Our developed metric E_{ID} manipulates the drawbacks of the existing ones, taking into account all essential and related parameters for measuring the actual effectiveness of IDSs/WIDSs. Another new metric called *attack recognition rate* (R_R) is also introduced in this chapter.

Chapter 6 is considered as a proof of concept and it presents the experimental evaluation tests of two well-known WIDSs; *Kismet* and *AirSnare*. The results are interpreted and the utility of the proposed methodology, the holistic taxonomy of wireless security attacks, and the developed evaluation metrics are demonstrated.

Chapter 7 summarizes our final conclusions and future work.

II. Chapter 2: Wireless Network Security

Wireless networking technology has become a widespread alternative to wired networking technology in recent years, owing to the associated valuable features such as mobility, scalability, flexibility, and installation simplicity. However, wireless communications suffer from numerous security threats and attacks. Consequently, several security efforts have been exerted to keep the wireless communications systems invulnerable to attacks. This chapter provides an overview of wireless networking technology and the associated benefits and limitations, with a great concern about the wireless network security that is considered the most critical challenge in this context. To understand well the wireless security, we introduce in this chapter a security conceptual model that elucidates the relationships between the network security concepts; vulnerabilities, threats, threat sources, risks, system infection, and countermeasures. These dimensions are discussed in a sequence of cause and consequence until reaching the last dimension which is the security countermeasures to be aware of their great and crucial roles in the network security. The security countermeasures manipulate or neutralize the system vulnerabilities, combat the attack attempts, and mitigate the attack effects. We study the role of each security countermeasure, and how the countermeasures at the first line of defense, such as authentication, encryption, and firewalls, are susceptible to be breached or bypassed by some attacks. This thus necessitates installing wireless intrusion detection systems (WIDSs) at the second line of defense to detect the attacks that eluded the first line of defense.

2.1. Wireless Networking

Basically, there are two main ways for networking the computing devices to communicate with each other, exchange data, and/or share the network resources; via either wired connection using Ethernet cables or wireless connection using radio frequency (RF) waves. Wireless networking technology has been growing to become the norm of networking in universities, enterprises, and homes. Wireless networking makes the life easier and more comfortable without the hassles of cables that are massively used in wired networks. Sometimes a combination of wired and wireless technology is needed to meet the networking requirements. The following subsections describe the advantages of wireless networks over wired networks, and the associated limitations as well.

2.1.1. Wireless Networking Benefits

- ***Mobility*:** Mobility is the prominent attribute and most obvious advantage of wireless networks, and it is manifested in the seamless roaming capabilities. Mobility gives the network users and stations the ability to access the wireless network and maintain the connection as they roam freely and move from one place to another within the network coverage area. Wireless mobility serves the employees within a corporate campus to

manage their work at any convenient location without obligatory physical connection to the network, and it then enhances the productivity gain. Also, the cell phone user can move and drive hundreds of miles during the course of a telephone conversation where the phone maintains the network connection through cell phone towers.

To appreciate the significance of mobility, it is important to understand the difference between the true mobility and mere portability. Portability provides the ability to carry the portable computing device (e.g., laptop) between different locations, but it is still necessary to physically plug into the network and reestablish a network connection at each new location. As for mobility, the network connections stay active even while the portable device is in motion. In short, portability removes only the physical barriers to connectivity, but mobility removes further barriers; most of which are based on the logical network architecture [Gast05]. Mobility is crucial to the domains that require continual network connections such as the health care domain, where mobility supports mobile access to the hospital database and facilitates the communication between patients, doctors and hospital staff, and thus helps in improving the quality of the hospital care.

- ***Installation simplicity and rapidity*:** the installation of wireless networks does not require complex undertakings as that are associated with the wired networks. For wired networks, it is not easy task to wire up traditional Ethernet cables to numerous locations. Besides, many old buildings are preserved by historic preservation laws that increase the difficulty of installing the wired networks. Wireless networking, on the other hand, makes it easier to deploy the wireless equipment and install the network. Moreover, the installation of wireless networks is a time-saving task, in contrast to the installation of wired networks that is a time-consuming task; just deploying the wireless stations and configuring them to associate with the network via RF waves.
- ***Scalability*:** Growing the network size to serve a wider area is a critical issue in the networking technology. The wireless network can be easily scaled up to serve a large number of stations, and this can be achieved by adding extra access points to extend the network coverage area. As for wired networks, scalability requires additional wires and/or routers, and complicated undertakings to properly install the extra part that serves the additional area.
- ***Flexibility*:** Wireless networks offer greater flexibility than wired networks, where the wireless stations are not constrained by physical connections. In modern press conferences, wireless networks allow journalists to take unrestricted locations with privileged access to the network. Moreover, business, research, and academic staff can hold quickly the meetings without predetermination of obligatory locations for the staff members.

2.1.2. Wireless Networking Limitations

- ***Interference*:** Interference is one of the performance limitations of wireless networks. Interference occurs when the receiving node picks up different signals on the same frequency. Many wireless devices such as cordless phones, baby monitors, medical devices, and microwave ovens share the same RF band of 2.4 GHz, and this may cause interference. There are two main types of interference; adjacent channel interference and co-channel interference [Seyb05]. Adjacent channel interference is produced by transmissions on adjacent or partially overlapped channels, but co-channel interference is caused by transmissions carried on the same frequency channels.
- ***Security*:** Network security is the critical issue confronting the wireless networks. Unlike wired networks, where any station should have physical connection and passes many defense lines to gain access to the network, the open wireless medium renders the wireless networks more susceptible to attacks. Consequently, Wireless traffic can be easily intercepted and eavesdropped by attackers within the network coverage area. Moreover, the wireless attacks can come from any direction and target any node. Thus, wireless network security has become a matter of increasing concern in recent years.

Despite these limitations of wireless networking technology, wireless networks nowadays have become widespread, where their benefits dominate their limitations. Since the wireless network security is considered a serious limitation, it receives considerable attention in the following sections.

In the same way as "security" is defined in linguistic dictionaries [Oxfo11][Merr03], we can define "network security" as the procedures followed or measures taken to ensure the safety of a network or system against misuse or malicious activities.

2.2. Wireless Security Requirements

In order to ensure the security of information systems, it is essential to understand the requirements for securing the system. The main requirements for the information security in wireless networks are the same as in wired networks, and they include three main aspects; *confidentiality, integrity,* and *availability*. The malicious activities are usually concerned with compromising one or more of these security requirements.

- ***Confidentiality*:** Confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information [Usc12]. Confidentiality ensures that data is only accessible to the authorized users, and hinders any hostile attempt to get hold of the data from the network. Confidentiality is an important aspect in wireless network security due to the fact that the openness and broadcast nature of wireless networks facilitate eavesdropping. To provide confidentiality and keep the transmitted information secure, access control and cryptographic techniques are used.

- ***Integrity*:** Integrity means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity [Usc12]. Data integrity ensures that the transmitted message is preserved intact and is not illegitimately altered or corrupted during the transmission between the wireless nodes. Typically, this can be achieved by generating checksum of the message with a one-way hash function, or by using cryptographic techniques. As Vines stated in [Vine02], assuring integrity is a three-part endeavor: 1) prevent modification of information by unauthorized users, 2) prevent unauthorized or unintentional modification of information by authorized users, and 3) preserve the internal and external consistency of databases.
- ***Availability*:** Availability means ensuring timely and reliable access to and use of information [Usc12]. Availability ensures the survivability of network service and the absence of denial of service. This means keeping the network service to be accessible to the authorized users whenever needed. The system should be resilient in the face of hardware failures, software faults, and denial of service attacks. Fault tolerance techniques [TDSC02] are commonly used techniques to keep survivability of system services. Also, there are several proposed techniques to combat the denial of service (DoS) attacks.

2.3. Wireless Security Conceptual Model

To understand well the wireless security challenge, it is important to study the main dimensions of wireless network security. This section presents a conceptual model of network security that explains the relationships between the network security concepts as shown in Figure II-1. This conceptual model is considered a general model for either wired or wireless networks; just the difference lies in the nature of vulnerabilities, threats, and countermeasures that are different according to the characteristics of each network. Our concern in this study is the wireless networks. We will explain the dimensions of the security conceptual model (Figure II-1) in a sequence of cause and consequence. The pivotal dimension in this context is the network vulnerabilities that are considered the main cause and motive for the remaining dimensions. Wireless security vulnerabilities expose the network assets to the security threats that could be realized by the threat sources (i.e., accidental events or intentional attacks). When the vulnerabilities are exploited by the threat sources, the likelihood of risks is raised and this could lead ultimately to the system infection. Consequently, security countermeasures are developed to proactively counter the potential threats and manipulate, compensate, or neutralize the system vulnerabilities, and to reactively counter the security risks and alleviate the system infection.

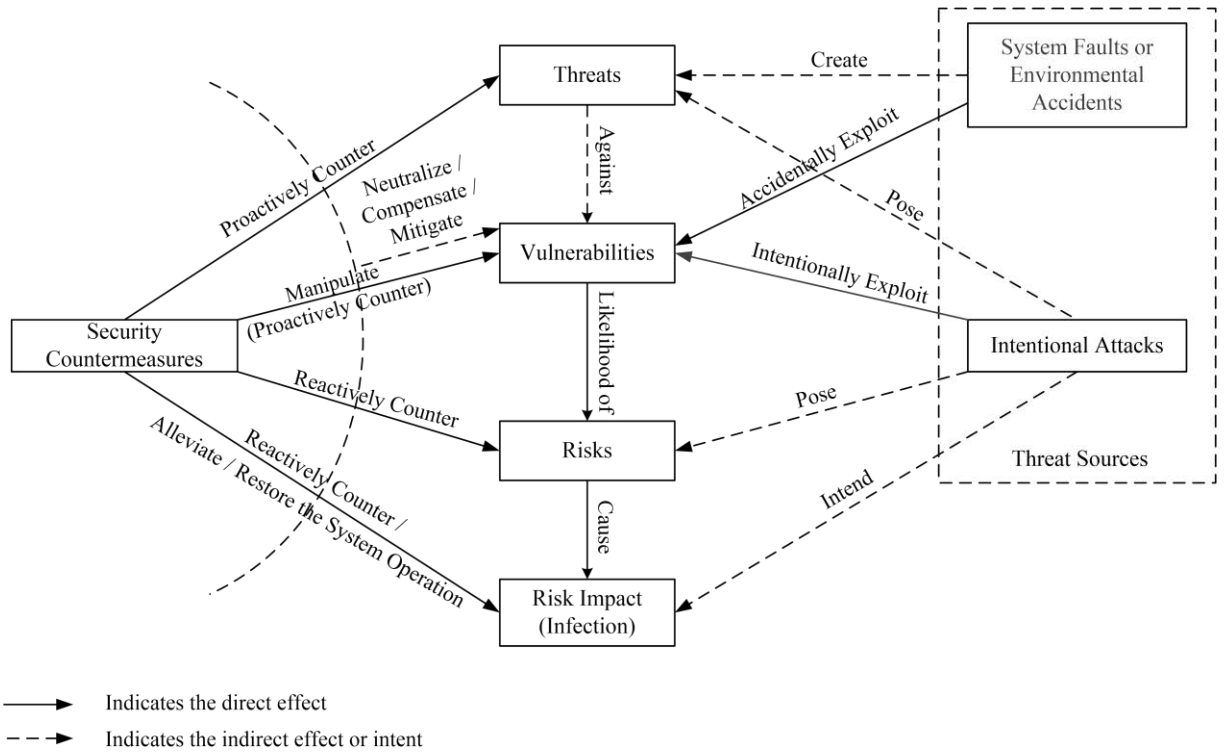

Figure II-1: Security Conceptual Model.

2.3.1. Vulnerabilities

As the vulnerability is defined in [Shir07][Cnss10], with a little adaptation, the vulnerability is a flaw or weakness in a system design, implementation, configuration, or security measures that could be accidentally or intentionally exploited by a threat source, and results in a violation of the system security policy. The open and uncontrolled medium between the communicated nodes in wireless networks is the main critical vulnerability that can be easily exploited and, moreover, opens the door for exploiting the other wireless network vulnerabilities.

We differentiate between two main categories of network vulnerabilities; physical vulnerabilities and logical vulnerabilities. Physical vulnerabilities refer to the weaknesses in the physical security measures (e.g., locks, keys, enclosures and shielding), and they can be exploited by physical tampering and vandalism attacks. Logical vulnerabilities can be found in the network services, protocols and applications besides the logical security measures (e.g., cryptographic algorithms, authentication techniques, etc.), and they can be exploited by logical attacks.

One of the critical weaknesses in physical security of wireless networks is suspending the wireless access points (APs) and wireless sensor network (WSN) nodes in open and unprotected places. This exposes APs and WSN nodes to physical attacks that can damage or steal them. Also, the open wireless medium exposes the wireless communications to eavesdropping, RF jamming and other types of logical attacks. Effect of logical attacks may reach the physical

system, and the same for the physical attacks that may affect the logical system [AnWi11]. It is worth mentioning that our concern in this thesis is the logical security issues that are related to the evaluation of wireless intrusion detection systems (WIDSs).

All wireless vulnerabilities can be categorized under four main classes; exposed medium, design flaws, implementation flaws, and configuration errors; they will be discussed in detail in chapter 4.

2.3.2. Security Threats

As the threat is defined in [StGF02] [Cnss10], with a little adaptation, the security threat is the potential of a threat source to accidentally or intentionally exploit one or more of system vulnerabilities, with adversely impact on the system operation and resources. Briefly, security threat is a potential violation of the system security.

Network security threats and vulnerabilities go hand in hand. The security threat in itself is not an action, it is merely a potential for exploiting the system vulnerabilities. Security threats are realized by the threat sources that represent the real risky action against the system vulnerabilities. Common security threats in wireless networks are manifested in the potential of eavesdropping, spoofing, denial of service, and breaching the security measures.

2.3.2.1. Eavesdropping

Eavesdropping in wireless networks refers to intercepting the radio traffic transmitted over the air. The open wireless medium increases the potential of eavesdropping. The eavesdropper, who is just in the vicinity of a wireless network without any required physical connection, needs only an adequate RF antenna along with wireless sniffing tools, such as NetStumbler [Nets13] and WireShark [Wire13], to capture wireless data stream. The captured and collected data can be decoded, and secret or private information may be easily extracted. Eavesdropping can be countered using encryption mechanisms to safeguard data transmission. Thus, even if the eavesdropper intercepts the encrypted data, he cannot be able to access the original data unless he gets or cracks the encryption key. Eavesdropping is usually used as a preliminary step towards other attacks ranging from spoofing[LiTr07], to information theft, to denial of service (DoS) attacks [BeSa03].

2.3.2.2. Spoofing

Spoofing threat refers to the potential of a malicious node to masquerade as another identity to gain legitimate privileges or deceive the legitimate nodes or stations. Spoofing is a serious threat, where spoofing attacks [YCTC09][LiTr07] can be easily launched in wireless networks with the open medium. For instance, ARP (Address Resolution Protocol) spoofing attack can access and corrupt ARP cache, where MAC and IP pairs are stored, and sends spoofed ARP messages to redirect sensitive data from a legitimate node to another location where the attack

station. Spoofing attacks can facilitate a variety of traffic injection attacks, such as rogue access point [HSTL11], session hijacking [DCTA12], and denial of service [BeSa03] attacks.

2.3.2.3. Denial of Service

The most serious threat facing wired and wireless networks is the denial of service. Wireless networks are highly susceptible to denial of service (DoS) attacks due to the broadcast nature of wireless communications. DoS attacks aim to deplete the network resources and hinder the network services. Many types of DoS attacks [BiTa09] can be launched at the physical layer and MAC layer of wireless network, and cause considerable threat against the network's normal operation. For instance, the attacker can exploit the broadcast and openness nature of wireless medium and launches so-called jamming attack [XTZW05] that causes radio frequency interference and consequently prevents the wireless nodes from accessing the wireless channel.

2.3.2.4. Breaching Security Measures

There is no completely immune security measure. Thus, most security measures have the potential to be breached. For example, the attacker can use cryptanalysis techniques [Swen08] to breach the cryptographic security mechanisms and break ciphers; this is called cryptanalytic attack. This attack exploits the weaknesses in encryption algorithms, plus some probable knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs, to deduce a particular plaintext or encryption key [Stal10]. As another example, the attacker may exploit the weaknesses in authentication techniques to interrupt the connection by deauthentication requests. Moreover, other security systems such as firewalls and WIDSs, may be defeated by some malicious evasion techniques [FoLe06][SmEJ06].

In conclusion, the threat refers to the intent to cause disruption or infection to a secured information system. Basically, the security threats cannot be eliminated, but by using the security countermeasures we can proactively counter the threats, address the vulnerabilities, reactively counter the consequent risks, and finally alleviate the system infection or restore the system operation.

2.3.3. Threat Sources

Threat source is either 1) an intentional attack with an intent and method targeted at the intentional exploitation of the system vulnerabilities [Cnss10], or 2) a system fault or environmental incident that may accidentally exploit the system vulnerabilities.

2.3.3.1. System Faults and Environmental Accidents

Unintentional system faults and environmental accidents are significant events that should be considered in studying and analyzing the threats sources. System faults refer to the operational errors due to software bugs or hardware failures, or faults induced accidently by the system operator. Examples of system faults are failure in wireless access point, nodes, data

storage devices, and battery depletion of sensor nodes in wireless sensor networks (WSNs). Environmental accidents refer to unpleasant events in the system's surroundings and the peripheral components. Environmental accidents include the sudden power failure and the system's components being destroyed by external events, in addition to the natural incidents that affect the system operation such as thunderstorms, floods, etc.

2.3.3.2. Wireless Security Attacks

Wireless security attacks are the focal point of scientific research in wireless network security. Wireless attacks have been receiving great attention, along with appreciable and valuable effort to develop appropriate security countermeasures. In this section, we present a quick review of some wireless attacks that exploit the network vulnerabilities. More details about wireless attacks will be presented in chapter 4.

A) RF Jamming Attack

RF jamming attack is a type of denial of service (DoS) attacks that are the most dangerous attacks against wireless networks. RF jamming attack aims to prevent the wireless stations from exchanging information by keeping the wireless medium busy by emitting jamming signals to interfere with the radio frequency (RF) used by the legitimate stations. Jamming attack is sometimes difficult to be prevented, where the attacker doesn't need to gain access to the network to launch the attack. Xu et al. [XTZW05] differentiate between four models of jamming attacks:

- ***Constant jammer*:** It continuously emits a radio signal with random bits to the channel without following the MAC layer rules. Constant jammer with signal strength higher than the threshold (i.e., used to determine whether the channel is idle or not) can prevent the legitimate stations from using the channel.
- ***Deceptive jammer*:** It constantly injects regular packets, instead of emitting random bits, to the channel without gap between subsequent packet transmissions. Due to the constant stream of incoming packets, the legitimate stations will be deceived and remain in the receiving state even if they have packets to send.
- ***Random jammer*:** It alternates, in pulsing manner, between sleeping and jamming phases. During jamming phase, it can be either constant jammer or deceptive jammer. This model is usable for jammers with limited biasing power to conserve energy.
- ***Reactive jammer*:** It jams the channel only when the transmission activity is detected, and stays quiet when the channel is idle. This evasion technique of reactive jammer makes it difficult to be detected.

There are many security countermeasures have been proposed to combat the jamming attacks. One of these countermeasures is the spread spectrum based techniques. The common used spread spectrum techniques are Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) [Skla01] which are based on secrets that need to be shared between the sender and the receiver before starting the communication. Also, Popper et al.

[PoSC09] proposed so-called Uncoordinated DSSS (UDSSS) that enables spread spectrum anti-jamming broadcast communication without the requirement of shared secrets. Chiang and Hu [ChHu08] developed a scheme for jamming mitigation based on spread spectrum and a binary key tree. Lin and Noubir [LiNo05] introduced Low Density Parity Check (LDPC) codes as a method to defend against the jamming attacks.

B) Wormhole Attack

Wormhole attack is one of the most severe attacks in wireless Ad Hoc networks, especially against many routing protocols and location-based security systems [HuPJ03]. In wormhole attack, the attacker records packets at one location in the network, tunnels them to another location, and replays them from that location into the network. The wormhole attack can be launched by two different modes; hidden mode and participation mode [KhMB09]. In hidden mode, the attackers do not declare their identities and act as two simple transceivers that capture messages at one end of the wormhole and replay them at the other end. In participation mode, wormhole attackers participate in the routing as legitimate nodes and use the wormhole to deliver the packets sooner and/or with a smaller number of hops. In this mode, the attacker uses cryptographic key that can be used to launch a more powerful attack.

For tunneled distances longer than the normal wireless transmission range of a single hop, the wormhole attacker uses either a single long-range directional wireless link or a direct wired link between the transmitting and receiving points to tunnel the packets that arrive before other packets transmitted over the normal multihop route. Also, the attacker can forward each bit of the packet over the wormhole tunnel directly without waiting to aggregate the entire packet before beginning to tunnel the bits of the packet, in order to minimize the delay.

Many security mechanisms and approaches were proposed to combat the wormhole attacks [HuPJ03] [LPMS05] [KhMB09]. Hu et al. [HuPJ03] introduced a new mechanism called packet leashes for detecting and defending against wormhole attacks. They proposed two types of leashes: geographic leashes and temporal leashes. Also, they proposed an authentication protocol called TIK for using it with the temporal leashes. Lazos et al. [LPMS05] introduced theoretic approach with derived conditions for detecting and combating the wormholes. They also proposed a defense mechanism based on local broadcast keys. In the same way, Khabbazian et al. [KhMB09] proposed a timing-based solution to defend against the wormhole attacks.

C) Sybil Attack

In Sybil attack [Douc02], a malicious node illegitimately claims multiple identities and pretends to be multiple and distinct nodes in the system. Sybil attacker obtains Sybil identities by forging new false identities for the Sybil node or by stealing identities of other legitimate nodes.

There are several impacts of Sybil attacks ranging from the possibility of defeating the redundancy mechanisms of distributed storage systems [Douc02], to the malicious effect on

routing protocols in sensor networks [KaWa03], to bypass the reputation system in peer-to-peer system. Also, in Facebook-style Social Network Systems (FSNS), where the authorization decision is the function of the topology of the social graph, it is possible for Sybil attack by a group of pseudonymous identities to manipulate the social graph topology and gain access privileges that would otherwise be forbidden [Fong11].

Yu et al. [YKGF06] proposed *SybilGuard* decentralized protocol for limiting the corruptive influences of Sybil attacks. Also, Yu and Gibbons [YGKX08] proposed another protocol called *SybilLimit* that leverages the same notion of *SybilGuard* with an improvement to reduce the number of Sybil nodes accepted per attack edge.

2.3.4. Security Risks

Security risk is the likelihood that the vulnerability will be exploited by the threat sources, and losses will occur. Threat sources and vulnerabilities are the key drivers of the security risk.

As attempts to address the risk impact, numerous literatures were concerned with risk management in the last few years, such as [Gibs11] [StGF02]. Risk management is the practice of identifying, assessing, controlling, and mitigating risks [Gibs11]. Risk management helps in identifying and differentiating severe risks from minor risks and their impact to manage the security measures, taking into account the trade-off between the security cost, potential loss, and quality of service (QoS).

2.3.5. Risk Impact

Risk impact is manifested in losing one or more of security requirements; confidentiality, integrity, and availability. Risk impact translates the attack intent or objective to a system infection. Attack objectives are ranging from merely nuisance, to spy, to information theft, to compromising data integrity, to denial of service, to vandalism. The realized attack objectives can be categorized as a loss of confidentiality, integrity, or availability.

- ***Loss of Confidentiality*:** Loss of confidentiality means the unauthorized access to confidential information that can lead to disclosing secret and proprietary information. This disclosed information may be used in theft or extortion of users and organizations; the objective may rise until threatening national security.
- ***Loss of Integrity*:** Loss of data integrity means unauthorized alteration or corruption of the transmitted messages or data, and that results in many unpleasant impacts. Compromising data integrity can be attained either by intentional alteration of the data for the objective of revenge or vandalism, or by unintentional alteration of the data caused by operator mistakes, software errors, or hardware faults [Vine02].
- ***Loss of Availability*:** Loss of availability refers to denial of service which means that the network service is unavailable or inaccessible to the authorized users. The consequent impact of the lost availability can be observed by the harmful effect on the operational performance, commercial services, and financial services of the system. For instance, in

February 2000, Yahoo, Amazon, eBay, and other popular sites were targets of denial of service (DoS) attacks that cause cumulative loss, estimated by Yankee Group, of almost $1.2 billion [Step01].

2.3.6. Security Countermeasures

Security countermeasure can be defined as actions, devices, procedures, or techniques that counter a threat, vulnerability, or attack by eliminating or preventing it, minimizing the harm it can cause, or discovering and reporting it so that corrective action can be taken [Cnss10]. There are two main types of the security countermeasures: *proactive countermeasures* and *reactive countermeasures.*

- ***Proactive countermeasures***: Proactive countermeasures help in reinforcing the system immunity by proactive techniques to hinder or even decrease the potential malicious activities against the system vulnerabilities. Proactive defense techniques play a vital role in manipulating, neutralizing, and compensating the system vulnerabilities. Access control, authentication, and encryption mechanisms are clear examples of proactive countermeasures.
- ***Reactive countermeasures***: As a complement, reactive countermeasures are concerned with countering the malicious activities at the violation phase and infection phase. Thus, there are two main dimensions of the reaction of these countermeasures: 1) detecting and preventing the attacks that attempt to exploit the vulnerabilities at the violation phase, and 2) detecting and combating the attacks that already occurred and infected the system resources at the infection phase, as well as alleviating the malicious impact.

Some security countermeasures play the two roles; as a proactive and reactive countermeasure, such as firewalls. When the firewall rules are adjusted to block traffic on certain ports and allow traffic on other ports, in this case the firewall acts as a proactive countermeasure. On the other hand, when the firewall detects malicious activities with the incoming traffic on a certain port and consequently blocks the malicious traffic on this port, then the firewall acts as a reactive countermeasure in this case. The intrusion detection system IDS (whether wired or wireless) is purely reactive countermeasure. In the following sections, we present wireless security countermeasures with a major concern with the wireless intrusion detection system (WIDS) that is the focal point of this study.

2.3.6.1. Authentication

Authentication is the first barrier to wireless stations to gain access to wireless networks. This is comparable to physical plugging of Ethernet cable into Ethernet jack in wired networks. IEEE 802.11 standard basically specified two approaches of authentication; *open system authentication* and *shared key authentication.* These approaches were improved by other developed authentication mechanisms such as WPA-PSK authentication and IEEE 802.1X-based EAP authentication as shown in the following.

- ***Open system authentication***: open system authentication involves a two-step authentication frame exchange. The wireless station initiates the authentication process by sending an authentication request to the access point. When the access point receives the authentication request, it replies by authentication response containing approval or disapproval of authentication. In open system authentication, the access point accepts the wireless station wishing to join the network without verifying its identity. Open system authentication does not offer any level of security, and it is then advisable to use it along with an auxiliary security mechanism such as encryption techniques, MAC address filtering, or higher level authentication such as 802.1X-based EAP authentication. The encryption algorithm is not used as a part of the open system authentication process, but it is used to provide verification after the authentication and association occur. To boost security level, many access points offer a security option of MAC (Media Access Control) address filtering that provides network access solely for wireless stations with specific MAC addresses.
- ***Shared key authentication*:** shared key authentication basically relies on using WEP (Wired Equivalent Privacy) key shared between the access point and wireless stations willing to join the network. It is similar to open system authentication but it includes additional challenge and response exchanged between the wireless stations and access point; it involves a four-way authentication frame exchange. The wireless station sends an authentication request frame to the access point, and the access point replies by a challenge text in a response frame to the wireless station. The wireless station encrypts the challenge text by the configured WEP key, and then sends it back to the access point. The access point then decrypts the received frame and compares it to the original challenge text to determine if they are matched or not, and accordingly sends the final authentication response to the wireless station with approval or disapproval.

However, WEP offers weak security and it can be broken by trivial attacks. This can be overcome by another security algorithm WPA (Wi-Fi Protected Access) that improves the encryption mechanism and boosts the security level.

2.3.6.2. Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the optional cryptographic algorithm specified by IEEE 802.11 to provide data confidentiality that is subjectively equivalent to the confidentiality of the wired local area network (LAN) medium. WEP [Ieee12] helps in protecting the data streams by encrypting them, thus preventing unauthorized disclosure or alteration of the data. It also helps in managing the network access control by verifying the authorized access to the network. WEP algorithm was not designed for ultimate security in wireless networks, but rather to be at least as secure as wired networks.

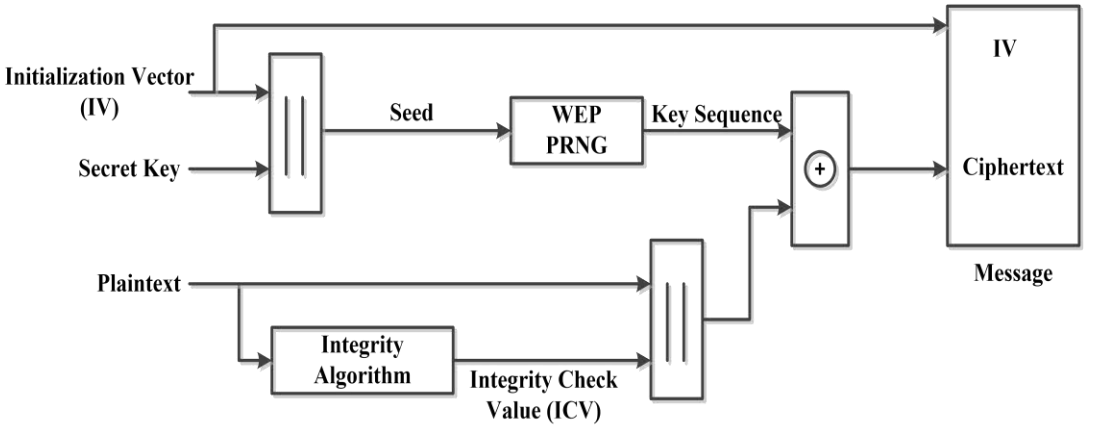

Figure II-2: WEP Encryption.

WEP encryption process is shown in Figure II-2, and it includes two crucial branches; a branch of computing the integrity check value (ICV), and another one of generating the key sequence. The results of the two branches are XORed to produce the ciphertext. The encryption process can be described as follows:

ICV generation;

1- The plaintext is firstly manipulated by the integrity algorithm - Cyclic Redundancy Check (CRC-32) - to produce the integrity check value (ICV).
2- The resulting ICV is concatenated with the plaintext payload.

Key sequence generation;

3- The secret key is concatenated with an initialization vector (IV) to produce WEP seed.
4- The resulting WEP seed is fed to pseudo-random number generator (PRNG) - RC4 encryption algorithm - to produce a key sequence of pseudo-random bytes equal in length to the number of data bytes of plaintext plus 4 bytes, since the key sequence is used to encrypt the plaintext data in addition to the integrity check value (ICV).

Encipherment;

5- The resulting key sequence is XORed with the plaintext concatenated with the ICV to produce the ciphertext.
6- The final output of this encryption process is a message containing the ciphertext and IV.

WEP PRNG is the actual encryption engine in WEP encryption process, and it uses RC4 encryption algorithm [Rive92] that transforms a relatively short secret key into a long pseudo-random key sequence. RC4 algorithm is a variable key-size stream cipher with byte-oriented operations, and it is based on the use of a random permutation. The initialization vector (IV) extends the useful lifetime of the secret key and provides the self-synchronous property of the algorithm. The secret key remains constant while the IV may be changed as frequently as every

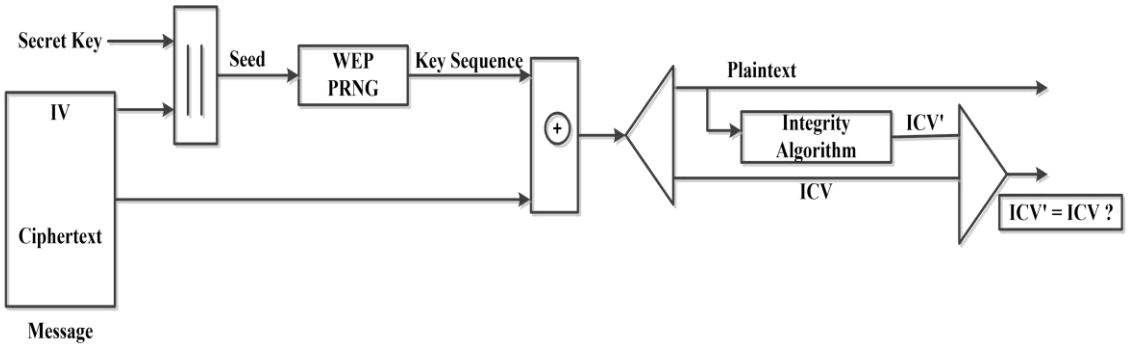

Figure II-3: WEP Decryption.

plaintext. Each new IV results in a new seed and key sequence. The IV travels with the encrypted message to the receiver.

The initially deployed standard of WEP key length was 64-bit WEP seed that consists of 40-bit shared secret key concatenated with a 24-bit initialization vector (IV). Then 128-bit WEP seed was deployed to boost the security by a longer key length. 128-bit WEP includes 104-bit secret key and a 24-bit initialization vector (IV). Many manufacturers of access points implement and support an option of using 256-bit WEP, although the incremental security by using this long key is dubious due to inherent weaknesses in WEP mechanism.

To recover the original message, the receiver should decrypt the ciphertext with identical secret key. The decryption process shown in Figure II-3 can be described as follows:

Key sequence generation;

1- The IV of the received message is concatenated with the secret key, and the result is fed into the WEP PRNG to generate the key sequence that is necessary to decrypt the received message.

Decipherment;

2- As a reverse process, the ciphertext is XORed with the key sequence to extract the original plaintext and ICV.

Data Integrity Check;

3- The decryption is verified by applying the integrity check algorithm on the recovered plaintext and comparing the produced ICV' to the ICV transmitted with the message.

4- If ICV' matches ICV, then the original message is correctly recovered. on the other hand, if they do not match, then there is an error in the received message and consequently an error notification is sent back to the sending end.

Unfortunately, WEP has serious security flaws in the main used and implemented algorithms (the encryption algorithm RC4 or the integrity check algorithm CRC-32), thus it is susceptible to attacks such as FMS attack [FlMS01] and chopchop attack [Kore04].

2.3.6.3. Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) [Wpa03] was mainly developed to address WEP vulnerabilities, and to boost more robust security mechanism. WPA is a subset of the ratified IEEE 802.11i [Ieee04] security specification, and it is also compatible and can be implemented on majority of 802.11 products out today and old ones by updating their firmware; WPA is both forward and backward compatible.

WPA uses Temporal Key Integrity Protocol (TKIP) to provide data encryption enhancements including a per-packet key mixing function. It also adds a message integrity check (MIC) to protect against packet forgery. WPA2 is the second generation of WPA that provides a stronger encryption mechanism. It includes a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES).

- ***Temporal Key Integrity Protocol (TKIP)*:** WPA uses TKIP to address the encryption deficiencies of WEP and minimize the problem of encryption key reuse. TKIP uses the RC4 encryption algorithm with increasing in the key size to 128-bit temporal key, and generates a unique encryption key to every packet. TKIP replaces the single static key used in WEP with keys that are dynamically generated and distributed by the authentication server. Also, TKIP uses a key hierarchy and key management methodology that obstructs the malicious attempts to predict and exploit the key.
- ***Message Integrity Check (MIC)*:** As a second important component to ensure the data integrity, WPA uses a message integrity check (MIC) (sometimes called *Michael*) that protects the transmitted data against the malicious altering attempts. Unfortunately, MIC does not provide perfect integrity. It is particularly vulnerable to bit-filliping, where the attacker can change a bit in the message, then changes the integrity check of the resulting message.
- ***Advanced Encryption Standard (AES-CCMP)*:** Advanced Encryption Standard (AES) [Aesa01] is a block cipher, and it is considered a stronger alternative to RC4 encryption algorithm. Variety of modes can be used in conjunction with AES. CCMP security protocol defines a set of rules which are built around AES for data encryption. CCMP uses AES with 128-bit key and 128-bit block size. AES-CCMP combines AES CTR (counter mode) for encryption and ensuring data confidentiality and AES CBC-MAC (Cipher Block Chaining Message Authentication Code mode) for data integrity. AES-CCMP is used by WPA2 and 820.11i to enhance the encryption mechanism.

WPA and WPA2 operate in two different modes [Wpaw05], *personal mode* and *enterprise mode*:

- ***Personal Mode*:** Personal mode is designed for Small Office Home Office (SOHO) environments, where authentication server is not required. This mode uses a Preshared Key (PSK) approach for authentication. A preshared key can be configured manually on both the access point and wireless stations. This mode is considered as unmanaged mode.

- ***Enterprise Mode*:** Enterprise mode is designed for enterprises, and it operates in managed mode to meet the rigorous measures of enterprise security. This mode requires an authentication server, which typically is a Remote Authentication Dial-In User Service (RADIUS) server, with IEEE 802.1X and the Extensible Authentication Protocol (EAP) to strengthen mutual authentication between the wireless station and authentication server via the access point.

***WPA-Preshared Key (WPA-PSK) Authentication*:** WPA-Preshared Key (WPA-PSK) [Gast05] authentication is based on distributing a preshared key (WPA-PSK) to all wireless stations. Key derivation for the wireless link is based on random numbers exchanged along with the preshared key. This authentication approach is vulnerable to dictionary attacks due to the distributed preshared key. In most cases, a single preshared key is used for all stations in the same SSID (Service Set Identifier). Then all stations share the same master key. With the preshared key, the attacker can monitor the four-way handshake and derive the unique keys for any other station which shares the same preshared key. The attacker can also forge the messages to make re-authentication, and then he may be able to capture the four-way handshake.

***IEEE 802.1X-based EAP Authentication*:** IEEE 802.1X is a port-based authentication method for wired and wireless networks. Extensible Authentication Protocol (EAP) is defined in IETF – RFC 3748 [ABVC04] as an authentication framework that supports multiple authentication mechanisms such as EAP Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), and Protected Extensible Authentication Protocol (PEAP) [StWA05].

In 802.1X/EAP authentication, the access point acts as a pass-through agent that tunnels EAP request/response messages between the wireless station and the authentication server, typically is RADIUS. When a station sends an EAP authentication request to access a network, the access point firstly allows the station to communicate solely with the authentication server to verify the access privileges of the station. Once the authentication process is completed successfully, the access point then allows the authenticated station to communicate over the network with other entities. The mutual authentication with the authentication server using 802.1X and EAP protects the wireless stations from accidental connection to rogue access points, and also ensures the access privilege of the wireless stations that join the network.

2.3.6.4. Association

When the wireless station is authenticated, it should be associated with the access point to gain full access before sending data frames. Association is a record keeping procedure that allows the network to track the location of each wireless station, so frames from the wireless station can be delivered to the correct access point. Association is necessary to synchronize the station and access point with important information, such as supported data rates. The station initiates the association by sending an association request frame containing elements such as SSID (Service Set Identifier) and supported data rates. The access point responds by sending an association response frame containing Association ID (AID) along with other information

related to the access point. The AID [Gast05] is a numerical identifier used to logically identify the station to which buffered frames need to be delivered, and it is usually used with power saving operation. Once the station is associated with the network, it can send and receive data frames.

2.3.6.5. Reassociation

When a wireless station moves from the coverage area of an access point to another one, it issues a reassociation request to the new access point to keep the connection with the network and to inform the network about its new location. Reassociation request is similar to the association request. The only difference is that the reassociation request frames contain a field of the address of the old access point. The new access point communicates with the old access point to verify the previously registered association. Reassociation process is also used when the station leaves the coverage area of an access point and returns alert to the same access point, to rejoin the network.

2.3.6.6. Disassociation

When a wireless station wants to terminate the existing association with an access point, it sends a disassociation frame to the access point. The access point is also able to remove any station from the network by sending a disassociation frame to the station. Once the station is dissociated, any mobility data stored in the distribution system is removed, and consequently the station is not able to exchange data frames with the access point. Disassociation is a notification, not a request that is considered a polite task to do during the station shutdown process.

2.3.6.7. Deauthentication

The wireless station can send a deauthentication frame to terminate the authentication relationship between it and the access point, then it is disconnected from the network. Deauthentication is also a notification, not a request, to inform the access point about the station leaving the network. Also, the access point is able to deauthenticate any station by sending a deauthentication frame to it. Once the station is deauthenticated, it is no longer able to access the network. Since the authentication is prerequisite of the association, then the side effect of deauthentication is the termination of any current association.

Figure II-4 summarizes the 802.11 authentication and association processes and the relevant parts that form three sequential states:

- **State 1:** unauthenticated and unassociated.
- **State 2:** authenticated and unassociated.
- **State 3:** authenticated and associated.

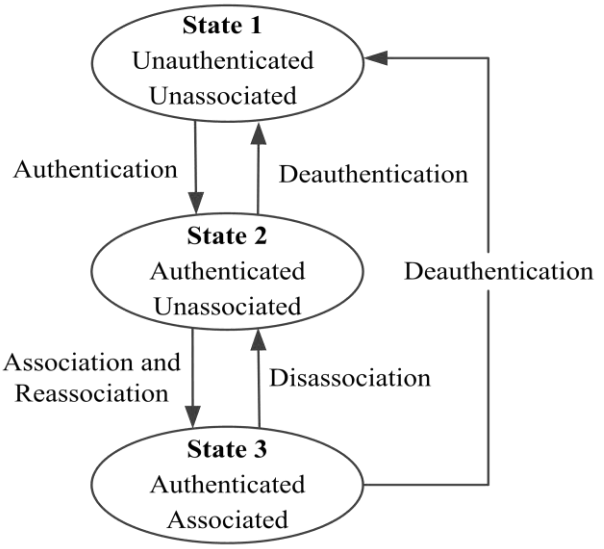

Figure II-4: States and Services.

2.3.6.8. Virtual Private Network (VPN)

Virtual private network (VPN) [RiRa04] provides a way for secure communication over public or unsecured network connections. Wireless networks can use VPNs as a part of their security solutions. In wireless networks, VPN is usually installed on the access points to provide a secure connection to tunnel the wireless stations to the network. Access points in open wireless medium are susceptible to attacks. Then, it is recommended to use a VPN gateway server at the edge of the protected network segment. Using VPN is a mandatory for remote access and it is useful to the researchers and employees who need to access the network from remote locations. VPN uses encryption to ensure that the third party cannot access the transmitted data and authentication to ensure that only the authorized users can access the network.

2.3.6.9. Firewalls

As we mentioned, the firewall can be used as a proactive countermeasure by controlling the access to the network and as a reactive countermeasure by reactively inspecting and detecting the malicious events that threaten the network. Firewalls are a controversial issue in wireless networks. The firewall was initially developed to separate between the wired network segments and filter the network traffic to determine which is allowed and which are denied according to the filtering policies. Security researchers argue about the conception of firewall in wireless networks. Some researchers consider it as a packet filtering firewall, which is mainly designed for wired networks, with some adaptations [TKLB11][NGML08] to be usable and compatible with the wireless network operation and to overcome the wireless network challenges such as the open network architecture, shared wireless medium, and dynamic network topology. The

firewall in this form is unable to monitor the radio spectrum to defend against the wireless attacks. In this case, the firewall is usually used as a part of the overall security system of the wireless network, and it operates in collaboration with other security solutions to reinforce the network security. Other researchers consider the wireless firewall as a security countermeasure installed on the wireless access point to monitor the radio spectrum and detect the malicious traffic besides controlling the access according to the filtering policies. Most firewalls developed in this case are composed of intrusion detection or prevention mechanisms and filtering policies [JNPF10] [YZZW12].

2.3.6.10. Wireless Intrusion Detection Systems (WIDSs)

Although the appreciable roles of the aforementioned security countermeasures which represent the first line of defense, they might be breached or bypassed by attacks that may penetrate into the secured system. This necessitates installing a second line of defense to boost the system security by monitoring and detecting the attacks escaped from the first line of defense. This can be realized using the wireless intrusion detection system (WIDS) which monitors the wireless network traffic and analyzes it for identifying any signs of attack, and then alerts the complementary prevention part to combat the detected attacks. The intrusion can be defined as a malicious event or a set of malicious events that attempt to compromise confidentiality, integrity, availability, or to bypass security mechanisms of a system [BaMe01]. The complementary prevention part is either a system administrator who observes the WIDS output alerts and takes reactions accordingly or a prevention countermeasure that reacts directly according to the WIDS output alerts.

Wireless intrusion detection systems (WIDSs) deviate, but not much more, from the wired intrusion detection systems (IDSs). WIDSs are in accord with IDSs on the main concept of intrusion detection and some characteristics, but they are different in some other characteristics due to the structural and behavioural differences between wired and wireless networks as well as the related differences between wired and wireless attacks. Basically, it is impossible for a wireless network to directly utilize the wired IDS. Characteristics of wireless networks and wireless attacks are considered in the design and implementation of WIDSs. It is worth mentioning that we always use “IDS” to refer to the wired intrusion detection system and “WIDS” to refer to the wireless intrusion detection system.

Most WIDSs operate and monitor the wireless frames at MAC Layer, but there are some WIDSs designed to monitor the potential attacks at the physical layer besides the MAC layer. WIDSs are limited in their ability to identify the upper-layer attacks that are traditionally identified by wired IDSs. Some systems overcame this WIDS limitation by integrating a WIDS with a wired IDS to boost the system security, such as WHIFF system [AmGP03] that integrates Kismet WIDS [Kism13a] with Snort IDS [Snor13].

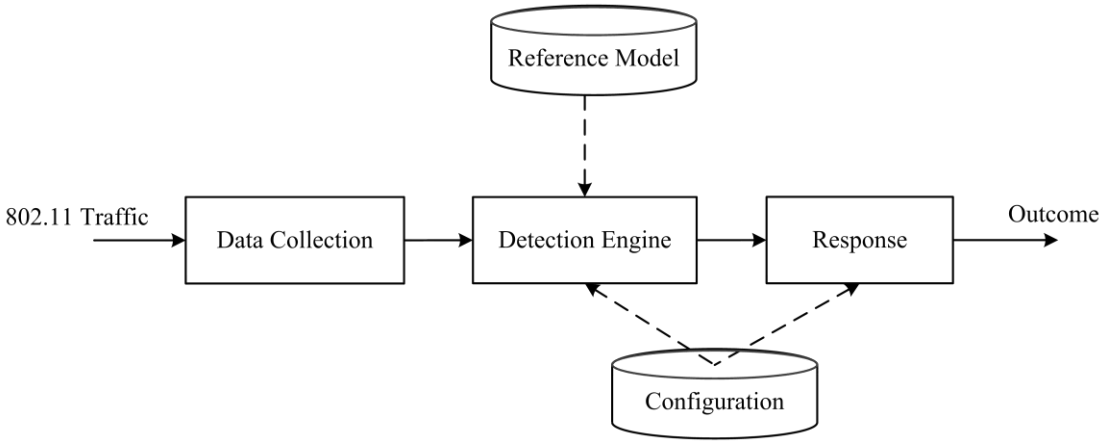

Figure II-5: Wireless Intrusion Detection Process.

Wireless intrusion prevention system (WIPS) operates in the same way as the WIDS with an additional capability to automatically react to prevent intrusions.

The research on intrusion detection systems (IDSs) has been conducted for over 30 years [Ande80] [DeNe85] [Denn87]. Most research efforts are concerned with wired IDSs [LuJa88] [DeDW99] [WaDe01] [Levi02] [DeMo02] [RuJM05] [ArCh07] [JLMY12] with little interest in wireless IDSs (WIDSs) [ZhLH03] [VGSB04] [SuSA06] [GiSC06] [YGXC10].

A) Wireless Intrusion Detection Process

The main concept of the intrusion detection process in WIDS systems is shown in Figure II-5 that explains the sequential manner of collecting the wireless traffic from the network, preprocessing it, and then analyzing it according to the detection technique used to differentiate between the normal and malicious events.

- ***Data Collection*:** at the data collection stage, the WIDS collects the raw 802.11 traffic from the network and preprocesses it to be readable and useable for data analysis and intrusion identification that will be managed at the next stage by the detection engine.
- ***Detection Engine*:** it is considered the core of intrusion detection process, where the WIDS analyzes the outcome of the data collection stage according to the algorithms of the reference model to identify the malicious activities.
- ***Reference Model*:** it is the database unit that includes a model of the normal and expected behaviour of the system, attack signatures, or specification-based profile depending on the detection technique used; anomaly-based, signature-based, or specification-based detection techniques. More details about the detection techniques are available in chapter 3.
- ***Configuration*:** WIDS typically includes a configuration file or settings that can be used to configure the WIDS according to the network characteristics and the Wi-Fi devices used, as well as to adjust the detection engine and the WIDS response according to the system security policy.

- ***Response:*** once the intrusion is detected, the WIDS generates alarms to either notify the network administrator or induce the complementary prevention countermeasure to take the proper action.

Wireless intrusion detection system is considered a mature technology that is coupled with research efforts to produce the intended solutions to the problems of wireless network security. One of the significant features of WIDSs in wireless networks is the deployment characteristic that is manifested in three main architectures of WIDSs; *standalone, distributed,* and *hierarchical* architectures that serve the different modes and topologies of wireless networks. More details about the WIDSs characteristics will be covered in chapter 3. There are many types of commercial WIDSs such as AirMagnet [Airm13] and AirDefense [Aird13], but unfortunately with a lack of availability of open source WIDSs such as Kismet.

1) Kismet

Kismet [Kism13a] is an open source WIDS that operates at 802.11 MAC Layer. Kismet works by placing wireless cards in monitor (RFMON) mode, and thus continuously hopping between 802.11channels to gather data. Monitor mode puts the wireless network interface card into a state to monitor all traffic received from the wireless network. Monitor mode is different from promiscuous (or promisc) mode which is also used for packet sniffing, where it allows capturing the packets without obligatory association with an access point or Ad Hoc network. Monitor mode is only applied to the wireless networks, while promiscuous mode can be used for both wired and wireless networks.

Kismet can collaborate or be combined with a network layer IDS like Snort [Snor13], to reinforce the system security as shown in the following system (WHIFF).

2) WHIFF

In 2002, a research team at Carnegie Mellon University developed WHIFF system [AmGP03] that integrates the two functions of wired and wireless intrusion detection. WHIFF combines two main components; Snort [Snor13] as a wired IDS to monitor the internal state of the host and Kismet [Kism13a] as a WIDS to monitor the RF traffic directed to the host. The WHIFF architecture is a distributed architecture and it comprises four modules; 1) *Listener*, 2) *Correlation*, 3) *Notification*, and 4) *Interface*.

- ***Listener*:** the listeners act as data collectors for the wireless traffic and as intrusion detectors as well. They are machines with proper antenna to passively monitor 802.11 traffic. These machines run Redhat linux 8.0 and use Snort IDS and Kismet WIDS to detect malicious activities and then send them to the correlation server.
- ***Correlation*:** the correlation module receives the data from the listeners and processes it through a series of MySQL tables to be usable by the interface module. It compares all alerts and then eliminates the duplicates. The related alerts in rapid succession are classified under the corresponding classes of alerts.

- ***Notification*:** the notification and correlation modules are conceptually distinct, although they are technically intertwined. The function of the notification module is to gather the alerts data from the correlation module and deliver it to the administrator in real time.
- ***Interface*:** the interface module provides a web-based console to view alerts, IDS incidents, rogue clients, and access points. It also allows the administrator to tag or add comments for subsequent investigations.

B) WIDSs Limitations

Basically, there is no security countermeasure has hundred percent strengths with zero weaknesses. As any security countermeasure, WIDSs suffer from some limitations that affect their performance.

- ***False Responses*:** false responses problem refers to the unexpected responses from the WIDS. There are two main types of false responses; false alarms and false negatives. False alarms (also known as false positives) refer to the generated alarm when the WIDS classifies a benign activity as an intrusion, and false negatives refer to the failure of WIDS to detect the actual intrusive action; the intrusions occur without any raised alarms from the WIDS. The main problem in wireless networks that increases this limitation of false responses is that there is no obvious separation between normal and abnormal operation in wireless environment due to network topology changing. A wireless node may temporarily lose synchronization due to the fast or volatile physical movement, or the false information sent out from another compromised one. It is difficult for WIDS to distinguish the temporary system malfunction from the real intrusion, and this thus could lead to high false responses.
- ***Redundant Alerts*:** WIDS systems may flag a large volume of alarms and thus overwhelm the complementary prevention part or annoy the system administrator. A great part of these alerts are redundant and can be neglected, and the whole volume of alerts can be minimized through correlation analysis of intrusion alerts as stated in [PiMa08]. Also, Debar and Wespi [DeWe01] described an aggregation and correlation algorithm for the intrusion detection alerts that can be used in design and implementation of intrusion detection console.
- ***Weak Attack Recognition*:** one of the observed limitations of WIDSs is the inability to correctly recognize the detected attacks. This consequently affects the diagnosis capability, which is essential for restoring the compromised systems as well as taking corrective and preventive actions [DeMo02].
- ***Weak Immunity*:** due to the openness nature of wireless networks, the WIDS entities are vulnerable and attractive targets for wireless attacks. There is no guarantee of secure communication between the WIDS entities, especially in hierarchical architecture which is commonly used in wireless Ad Hoc networks, where the network is divided into clusters with a set of WIDS-agent nodes that are controlled by an elected cluster-head as a console for each cluster. This gives the opportunity for attackers to listen in the

transmission and messages exchanged between the WIDS agents and the cluster-head [ZhLe00], cut off the control branches between them, and hack the cluster-heads.

- ***Bandwidth (BW) Limitation*:** the limited bandwidth of wireless links is one of the serious challenges facing the WIDSs. In WIDS distributed architecture, the deployed WIDS agents and console communicate with each other to take the collaborative decision about generating global alarms for the detected malicious activities. The communication between the WIDS agents and console must be restricted and respects the network bandwidth to avoid the network bandwidth congestion to give the main stations the ability to communicate without nuisance.

2.4. Conclusion

This chapter provided a survey of wireless network security and introduced a security conceptual model that clarifies and simplifies the relationships between the main security concepts; vulnerabilities, threats, threat sources, risks, system infection, and security countermeasures. We discussed and analyzed the links between these security concepts and we demonstrated the crucial role of the security countermeasures in the network security. We discussed the vulnerabilities and breaches of the security countermeasures at the first line of defense (e.g., authentication, encryption algorithms, and firewalls) and demonstrated the usefulness of installing the wireless intrusion detection systems (WIDSs) at the second line of defense to detect the attacks escaped from the first one. This chapter also introduced a WIDS detection model that summarizes the detection process. We finally discussed the critical challenges facing WIDSs.

III. Chapter 3: WIDSs Evaluation Methodology

Wireless intrusion detection system (WIDS) is considered a crucial element in wireless network security. Selecting a suitable WIDS for a system or network necessitates taking into account the evaluation of WIDSs performance. Evaluation can be defined as a systematic assessment of the ability of a WIDS to meet the intended and expected performance. Many different attributes evaluate the WIDS performance such as *effectiveness, efficiency, interoperability, collaboration* [Axel99], *redundant alerts correlation, the impact on the monitored system resources, attack type recognition, scalability and flexibility, etc*. WIDS effectiveness is considered the basic factor in evaluating the WIDS performance so that it receives great attention in this study.

In this chapter, we present an overview of the previous work on the experimental evaluation of intrusion detection systems (IDSs), and the associated strengths and weaknesses. We discuss three main weaknesses which are summarized in the drawbacks of the followed evaluation methodology, attack classification, and evaluation metrics. These three aspects are considered the main pillars for managing a credible evaluation of IDSs/WIDSs. Thus, we are concerned with developing three novel aspects; comprehensive evaluation methodology, wireless attack taxonomy, and expressive evaluation metrics. We commence, in this chapter, with the novel comprehensive methodology for evaluating WIDSs performance. Our proposed methodology covers all essential dimensions for a credible evaluation. Dimensions of our methodology are organized in a sequential and well-engineered manner, starting from the main goals of WIDSs evaluation reaching the intended objectives. It is worth mentioning that this methodology is applicable to wired and wireless intrusion detection systems (IDSs) by considering the concepts and characteristics of each communications medium and characteristics of the IDSs related; in this chapter we are concerned with WIDSs.

3.1. An Overview of the Existing Experimental Evaluations of IDSs

Most existing experimental evaluations of IDSs were concerned with the wired IDSs, with an observed lack of evaluating the wireless IDSs (WIDSs). This section presents an overview of the previous work on the experimental evaluation of IDSs performance. The previous IDSs evaluations vary in the followed methodology, dataset used, and evaluation metrics. Some of them managed the evaluation tests without clearly defined methodology, some others used trivial or inexpressive evaluation metrics, in addition to using biased dataset. A set of well-known evaluations of IDSs are discussed in this section, such as the University of California-Davis evaluation [PZCB96] [PCOM97], IBM Zurich Research Division evaluation [DDWL98], DARPA evaluations [LFGH00] [LHFK00], and LAAS evaluation [Gade08].

3.1.1. University of California-Davis Evaluation

The first introduced evaluation of IDSs, to our knowledge, is the IDS testing managed by Puketza et al [PZCB96] [PCOM97]. They described a methodology and software platform for testing and evaluating IDSs performance. The methodology includes using simulation scripts for both normal (as a background) and intrusive activities to evaluate the detection ability of the IDS and the absence degree of the false alarms. Also, they evaluated the IDS performance under heavy load. They tested IDSs under automatically launched attacks using interactive telnet, FTP, and rlogin sessions. They evaluated Network Security Monitor (NSM) [HDLM90] which is the early developed network intrusion detection system. The NSM evaluation results show its deficiency in intrusion detection, especially under high CPU loads. Briefly, the test procedures in this methodology were crafted to evaluate three performance attributes: intrusion identification, resource usage and stress testing. There is no clearly defined evaluation metrics used in this work, besides a lack of managing unbiased dataset.

3.1.2. IBM Zurich Evaluation

Another experimental evaluation of IDSs was carried out by IBM Zurich research Division [DDWL98]. The testbed consists of several client machines and server machines under the control of a single workstation used as a workbench controller. The attacks were obtained from a vulnerability database maintained internally by IBM; several attacks on FTP. In this experimental evaluation, four host-based IDSs (HIDSs) were compared, but unfortunately the report detailed neither which metrics were used nor which results were obtained.

3.1.3. DARPA Evaluations

The most well-known evaluations of IDSs are DARPA98 [LFGH00], and DARPA99 [LHFK00] evaluations. The implemented testbed contained various traffic types similar to what may be generated by hundreds of users on thousands of hosts. Seven weeks of training data, containing background traffic and labeled attacks, plus two weeks of unlabeled test data were recorded; many types of attacks embedded in a large amount of normal background traffic. The evaluation results were presented by *Receiver Operating Characteristic* (*ROC*) curve. *ROC* is used to analyze the trade-off between the *false alarms rate* and *detection rate*. The drawbacks of using *ROC* curve in evaluating the intrusion detection systems are discussed in detail in chapter 5; where a set of existing evaluation metrics of IDSs performance are discussed there. DARPA evaluated the IDSs against a set of attacks classified under four categories; *probe, denial of service* (*DoS*)*, remote-to-local* (*R2L*)*,* and *user to root* (*U2R*) *attacks*. This classification of attacks does not help in credible and unbiased evaluation, where it does not cover all dimensions of attacks that ensure a holistic classification. More details of the critiques of DARPA evaluations are available in [Mchu00].

3.1.4. LAAS Evaluation

Gad El Rab [Gade08] evaluated two IDSs, *Snort* and *Bro*, under sponsorship of LASS-CNRS. Methodology of this evaluation missed some vital tasks for evaluating the IDSs, such as the evaluation challenges. The methodology seems at first glance as an engineered methodology, but the organization and sequence of some methodology dimensions violate the logical ordering. He depended, in evaluating the IDSs, on two trivial metrics, *detection ratio* (*DR*) and the *detection ratio per attack type* (*DRPAT*). These separated metrics are neither expressive nor meaningful in evaluating the IDSs effectiveness that relies on using a unified metric for measuring the detection ability and the absence degree of false alarms, with taking into account the hostility of the environment (i.e., it is measured by the probability of intrusions in the environment). The results show that *Snort* (with the out of box configuration) detects one attack out of the 19 test cases, but *Bro* has correctly detected more than half of the attacks included in the dataset.

3.2. Critiques of the Existing Work

There are some critiques associated with most of the previous evaluations, and they may affect the evaluation credibility. As a result of our research, the apparent lack of comprehensive evaluation methodology, holistic attack classification, and/or expressive evaluation metrics are the main critiques which the existing evaluations suffer from. These three aspects are matter of concern in this study, due to their significance as main pivots for managing unbiased evaluation.

3.2.1. Evaluation methodology

It was observed that most previous evaluations didn't follow a comprehensive methodology in their evaluations of IDSs. Evaluation methodology is a crucial element in IDSs/WIDSs evaluation, where it gives the guidelines for the evaluation process. Evaluation methodology must satisfy some essential requirements: 1) methodology dimensions or tasks should be organized in sequential and practical manner, 2) it should cover all dimensions tasks for a credible evaluation. We propose in this chapter a comprehensive evaluation methodology that respects these requirements as possible to ensure a credible evaluation of WIDSs

3.2.2. Attack Taxonomy

The second critique of most previous evaluations of IDSs is the lack of using representative attack test cases that need a holistic taxonomy of attacks. Most previous evaluations tested the IDSs under a set of attacks that were not representative of the possible attacks against the monitored system. This consequently leads to biased evaluation of IDSs. We propose (in chapter 4) a holistic taxonomy of wireless security attacks from the perspective of the WIDSs evaluator, to subsequently extract the representative attack test cases.

3.2.3. Evaluation Metrics

No doubt that the evaluation metrics dimension is the most significant aspect in the evaluation process owing to its great role in assessing the IDSs/WIDSs performance. Unfortunately, most previous evaluations depended on ordinary trivial metrics, except DARPA98 [LFGH00] and DARPA99 [LHFK00] evaluations which depended on *ROC* curve that seems at first glance as a valuable metric, but it has some drawbacks that are discussed in detail in chapter 5. Any evaluation metric should consider some important requirements; it should, 1) consider all essential parameters related to the IDSs/WIDSs performance, 2) be meaningful, 3) be quantifiable; composed of quantitatively measurable variables, 4) be relative; not absolute, 5) be unified; to facilitate the evaluation. Chapter 5 presents new evaluation metrics E_{ID} (*intrusion detection effectiveness*) and R_R (*attack recognition rate*) that respect and satisfy these requirements.

3.3. New Evaluation Methodology

We have commenced our evaluation of WIDSs with a simple proposed evaluation methodology [NaAF11], but due to some evaluation challenges that we have faced during the experimental evaluation of WIDSs, we have modified the evaluation methodology accordingly to produce a new comprehensive one [NaAF12] as shown in Figure III-1. In our developed methodology, we believe that the premier logical step in any evaluation process is determining the main goals of the evaluation. In this study, our goal is evaluating the wireless intrusion detection systems (WIDSs) performance in wireless networks. It is obvious that our evaluation goal consists of three main parts; evaluation, WIDSs performance, and wireless networks. Then, our methodology starts accordingly from this evaluation goal towards three main directions; studying the evaluation challenges, WIDSs performance attributes, and operating environment characterization. By analyzing the evaluation challenges, we can extract the satisfactory requirements and take all possible measures to ensure the credibility of the evaluation. This can be managed by selecting the proper evaluation techniques and tools, and designing a robust testbed as well. Regarding the analyzed attributes of the WIDSs performance, the evaluation metrics can be defined and developed. Also, depending on the defined evaluation metrics and what we need to measure, the helpful and suitable techniques and tools will be selected. As a complement, the operating environment (i.e., wireless networks in this study) should be characterized, where it is considered the base for the deployment and configuration of the system under test (WIDS). Regarding the characteristics of operating environment and WIDS system, the evaluation dataset or workload can be characterized, and then the suitable generation tools can be selected. Basically, evaluation dataset consists of two main parts; normal traffic (as a background) and malicious traffic. Then, the testbed can be designed and configured on the basis of the characteristics of the operating environment and WIDS, and the selected evaluation techniques and tools, taking into account the avoidance of the evaluation limitations. Now, the evaluator can manage the evaluation tests using the evaluation tools and techniques, considering

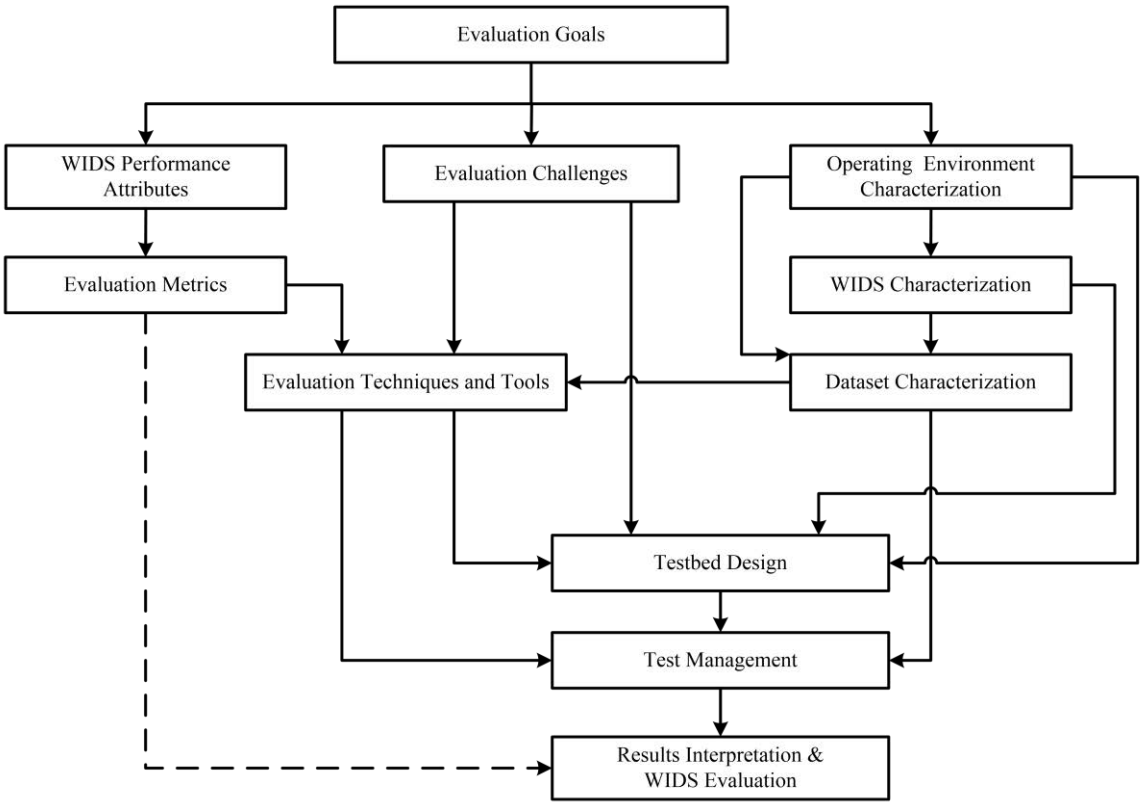

Figure III-1: Evaluation Methodology.

the dataset characterization. Finally, using the defined evaluation metrics, the results can be interpreted and the WIDS is evaluated. In the following sections, we will discuss each dimension in our methodology in more details.

3.3.1. Evaluation Goals

Evaluation goals, in general, interpret the evaluator's objectives such as evaluating one or more of the WIDS performance attributes in a specific operating environment. The evaluator should be aware of the main aspects of his goal and the associated limitations to be able to determine the main dimensions and related subsequent ones.

3.3.2. Evaluation Challenges

There are many critical challenges and limitations of evaluating WIDSs in wireless networks. We summarize these challenges as follows.

3.3.2.1. Openness of Wireless Environment

One of the great problems in WIDSs evaluation is the openness of wireless environment which is rich in uncontrolled RF (Radio Frequency) traffic. Due to the continuous broadcasting of RF traffic from the adjacent wireless nodes in the range of the evaluation testbed, it is

difficult to accurately measure neither the WIDSs detection rate, nor false positive rate, nor BW (Bandwidth) utilization. Basically, in the evaluation domain, measuring the false positive rate is based on observing and calculating the WIDSs response (i.e., whether it generates an alarm or not) for the generated and controlled benign traffic. No doubt that this generated traffic will be aggregated with the already existing RF traffic emitted from other adjacent wireless nodes at the receiving end of the WIDS. This leads to inaccurate measures of the false positives, and in the same way the detection rate (i.e., which is based on testing the WIDS response for the generated malicious traffic) and BW utilization. Another important challenge that must be taken into account is that some experimental evaluation tasks test the WIDSs under certain type of attacks that can overwhelm all the Wi-Fi devices in the range, such as "deauthentication/disassociation (Amok mode)" attack (chapter 4, section 4.5.8). When we launched this type of attacks for the first time in open space, we found that all the Wi-Fi devices in the range either the stations which participate in the test or the other ones in the vicinity are disconnected.

The two main solutions to overcome the above mentioned limitations are managing the test and measurements either through RF isolated workspace or through virtually created environment using VM (virtual machines) software. To our knowledge, until now there is no VM software supports virtual creation of wireless environments. Then, the remaining solution is the former one that is manifested in managing the test and measurements through RF isolated enclosure or chamber such as "*RF anechoic chamber*" [WSPH08] that isolates and protects the testbed and measurements from the exterior uncontrolled RF traffic. For our experimental evaluation of WIDSs, since we have not in our laboratory RF shielded workspace such as *RF anechoic chamber*, we have constructed RF isolated testbed by building RF shielded enclosure to keep the access point and Wi-Fi adapters (i.e. connected to the stations which participate in the test) isolated from any exterior uncontrolled RF traffic; it will be discussed in detail in chapter 6.

As a third solution that seems at first glance as a good solution, but in fact it has some limitations. The solution is changing the communications channels between the nodes of interest and selecting a specific one to operate on it. Unfortunately, this option is not supported by all WIDSs. This option is usually supported by WIDSs that include network traffic analyzer; this is available on some advanced WIDSs which most of them are commercial. This option of managing the test on a specific unique channel does not guarantee the absence of attacks in the range of the testbed, where the attacker can easily scan and sniff the communications in the testbed, and then affects the measurements by annoying attacks or even broadcasting normal traffic on the tuned test channel. This option seems useful for collecting the dataset (specially the normal background dataset) from the stations of interest, to replay it again in the testbed under the evaluator control, but the collected data must be reviewed and sanitized from any unwanted data. For example, AirMagnet, which is a commercial WIDS, gives the option of selecting a specific channel to filter and isolate the particular packets of interest.

3.3.2.2. Biased Testbed

The second critical challenge that the evaluator faces in WIDSs evaluation is the difficulty of benchmarking different WIDSs in a completely common testbed. The prominent reasons for that are the restricted compatibility of the WIDS with certain determined types of wireless network interface cards (WNICs) (i.e., usually commercial issue) and the supporting operating systems (e.g., Linux, Windows, or Mac). It might be difficult to find a WIDS that is compatible with multiple operating systems or different WNICs. This biasing in the evaluation testbed decreases the fairness of the benchmarking and evaluation.

3.3.3. WIDS Performance Attributes

This section presents the WIDSs performance attributes and the associated challenges. Some of the IDS performance attributes were stated in [Axel99], but the author didn't consider all the related attributes. In this section, we consider all related attributes that can be used for a comprehensive evaluation of the WIDSs performance. The WIDS performance attributes include the WIDS *effectiveness, efficiency, interoperability, collaboration* [Axel99]*, redundant alerts correlation, the impact on the monitored system resources, attack type recognition, scalability and flexibility*, etc. The following subsections summarize these attributes.

3.3.3.1. Effectiveness

The WIDS effectiveness is considered the main focal attribute in evaluating the WIDSs performance. Effectiveness reflects the ability of an IDS/WIDS to detect the intrusive activities in the monitored system, and the degree of keeping the benign activities pass without any raised alarms (i.e., the absence degree of the false alarms). The main challenge associated with the effectiveness attribute is the false responses problem which refers to the unexpected response from the IDS. There are two main types of false responses as discussed in chapter 2; false alarms (also known as false positives) which refer to the generated alarm when the IDS classifies a benign activity as an intrusion, and false negatives which refer to the failure of IDS to detect the actual intrusive action. False responses are considered the great challenge that the wired and wireless IDSs suffer from.

3.3.3.2. Efficiency

WIDS efficiency includes many parameters related to the WIDS operation such as real-time detection, computing resources, biasing power resources, operation decay, etc. For the real-time detection, the WIDSs detect the intrusive activities in real-time (or near real-time), or process audit data with some delay and in turn postpone the detection (non-real-time detection). For the computing and biasing power resources, to avoid confusion, we should first distinguish between the types of resources in the context of WIDSs evaluation. In some cases the WIDS entities depend, in their operation, on the monitored system resources, but in other ones they are

standalone entities where they depend on their own resources. Also, operation decay is one of the practically observed weaknesses in the WIDS operation in the presence of heavy processing load. Hsiu et al [HKKJ05] proposed a scenario-based search algorithm to improve the IDS/WIDS efficiency by minimizing the number of rules selected by a rule selector module, to test them through a detection engine module. A part of operation decay might depend on the computing resources. The efficiency attribute can be fairly evaluated for the standalone WIDS system (as a hardware), where it depends on its own resources, but for the other case where the WIDS software is installed and depends on the monitored system resources, it is unfair to evaluate the WIDS efficiency, where the measurements will depend heavily on the monitored system capabilities, memory, loaded programs, etc.

3.3.3.3. Interoperability

The WIDS interoperability measures the ability of a WIDS to interoperate with other ones. Unfortunately, different WIDSs rarely interoperate with each other. Thus, it is difficult to consolidate different WIDSs to work together for monitoring the same system. This problem is clearly observed in the commercial WIDSs. If an organization uses and distributes through its network a certain type of WIDSs, and after a period of time it wants to enhance the system security by adding another different type of WIDSs, it may face a problem of un-interoperability between the different WIDSs. Then, the organization may be compelled to replace the whole old WIDS system by a new one.

3.3.3.4. Collaboration

No doubt that the additional effectiveness can be achieved when two or more of the security countermeasures work together in a synergy manner. WIDS collaboration measures the ability of a WIDS to collaborate with other security countermeasures to achieve the intended level of effectiveness. The combination of the security countermeasures should ensure providing at least the same level of security when each countermeasures applied singly would provide, and it does not lower the overall security of the monitored system [Axel99].

3.3.3.5. Redundant Alerts Correlation

Redundant alerts limitation is one of the critical challenges that the IDSs/WIDSs suffer from as mentioned in chapter 2. Redundant alerts correlation refers to the ability of a WIDS to correlate the redundant alerts that do not indicate significant events in intrusion detection process. Example of the redundant alerts, the numerous generated alerts from Kismet WIDS [Kism13a] (i.e., observed in our experimental evaluation) which indicate suspicious traffic, even though a great part of this traffic is benign traffic and has the same properties. Many of these alerts indicate repeated traffic from the same source MAC addresses.

3.3.3.6. The Impact on the Monitored System Resources

WIDS should not cause a load on the monitored system. The impact of WIDS on the monitored system is reflected in the system resources utilization; e.g., processor, memory, and BW utilization. For wireless devices with limited biasing power such as wireless sensor nodes in wireless sensor networks (WSNs), it is important to take into account the impact of WIDSs on the power consumption of the sensor nodes. It is also important to consider the network BW utilization that affected by the exchanged traffic between the WIDS entities in the distributed and hierarchical WIDSs architectures.

3.3.3.7. Attack Type Recognition

For IDSs/WIDSs, it is not enough to only notify of the intrusion detection, but also the intrusion type must be recognized. The criterion of interest here is evaluating the ability of the IDS/WIDs to recognize the type of the detected intrusion. This ability can be clearly observed with the signature-based IDSs than the anomaly-based IDSs, where the signature-based IDS inspects the system activities on the basis of detecting any evidence of attacks according to a predefined and established model of specific known attacks signatures, but the anomaly-based IDS inspects the system activities on the basis of detecting any deviations from a pre-established model of the normal and expected behaviour through the system. The main limitation associated with the signature-based IDSs is the difficulty of detecting the novel attacks or variants of the existing defined attacks.

3.3.3.8. Scalability and Flexibility

WIDS should be scalable and flexible to accommodate expansion of the networks scale. Expansion can be achieved via clustering, multi-hop delivery, localization of computation, and data processing. Also, the WIDS should be adaptive to network topologies and configuration changes.

3.3.4. Evaluation Metrics

One of the pivotal tasks in our methodology is defining the evaluation metrics that translate the criteria of evaluating the WIDSs performance into mathematical expressions to facilitate the results interpretation and conclusion. The main parameters that measure the ratio between the IDS's input and output events are sometimes used as traditional metrics for evaluating the IDSs performance such as *true positive rate* (*TPR*) (also known as *detection rate DR*) which is the proportion of the malicious activities that are flagged as intrusive by generated alarms, *false positive rate* (*FPR*) which is the proportion of the benign activities that are flagged as intrusive with raised alarms, *false negative rate* (*FNR=1-TPR*) which is the proportion of the malicious activities that are not flagged as intrusive, and *true negative rate* (*TNR=1-FPR*) which is the proportion of the benign activities which pass without any raised alarms. The main drawback

lies in the inexpressive outcome of using these metrics individually for evaluating any attribute of IDSs/WIDSs performance. For example, the effectiveness evaluation is dispersed among these parameters, but it is preferred mathematically to use a unified metric that collects all the parameters related to the intrusion detection effectiveness in a unified expressive formula or equation.

In addition to these trivial metrics, there are other valuable metrics proposed for evaluating the IDSs effectiveness such as *Receiver Operating Characteristic* (*ROC*) curve which was used by DARPA evaluations [LFGH00] [LHFK00], *Bayesian Detection Rate* ($P(I|A)$) [Axel99], *Cumulative Cost* [SFLP00], *Expected Cost* [GaUl01], *Intrusion Detection Capability* (C_{ID}) [GFDL06], and *Intrusion Detection Operating Characteristic* (*IDOC*) [CaBS06]. The benefits and drawbacks of these metrics will be discussed in detail in chapter 5, and also a novel evaluation metrics E_{ID} (*intrusion detection effectiveness*) and R_R (*attack recognition rate*) will be introduced.

3.3.5. Operating Environment Characterization

According to the evaluation goals, the wireless operating environment can be characterized on the basis of the network type, mode, and architecture.

3.3.5.1. Network Type

Network type differentiates between military, commercial, academic networks, etc. Each of these networks has different security policies that determine the security level required and help in determining the accepted level of false alarms, thus adjusting the WIDS configuration file accordingly. Also, knowing the network type helps in determining the hostility of the operating environment.

3.3.5.2. Network Mode

Network mode refers to the communications approach among the wireless stations, and the protocols that organize that communications. There are two main modes in wireless networks; *wireless infrastructure mode* and *wireless Ad Hoc mode*. It is worth mentioning that the deployment and configuration of the WIDS systems depend significantly on the wireless network mode.

A) Infrastructure Network

In wireless infrastructure network, the wireless nodes associate themselves with a wireless access point (AP) to get the network services and/or communicate with each other. The AP is usually connected to a wired network and provides a communication link between the associated wireless nodes and the wired network services (usually Internet). Also, AP operates as a radio relay to forward the information between the wireless nodes that are too distant to communicate directly with each other.

Based on the wireless infrastructure mode, we can differentiate between two main architectures; *standalone* and *distributed system* modes.

1) Standalone Mode

Standalone infrastructure network is mainly configured around a central access point (AP). The basic architecture of this mode is called infrastructure basic service set (BSS). However, a BSS covers a small limited area around the AP that serves the adjacent nodes in the range. It is worth noting that there is no restriction on the distance between the mobile nodes in the BSS coverage area.

2) Distributed System Mode

The coverage area of wireless infrastructure network can be extended by joining BSSs to the backbone network to form extended service set (ESS) that serves the distributed system mode. In the distributed system mode, multiple APs are interconnected with each other by wired or wireless backbone system. This enables the wireless nodes to roam between the APs, thus providing greater range and mobility. In this mode, if a mobile wireless node moves out the coverage area of an AP, but it keeps its existence in the ESS range, it will re-associate with the next AP in the ESS range.

B) Ad Hoc Network

Wireless Ad Hoc network is a self-organized network which is a collection of autonomous wireless nodes that can be deployed and communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. In Ad Hoc networks, the wireless nodes can interact as routers to forward packets without relying on any fixed infrastructure support such as access points, routers, or base stations.

Ad Hoc networks are also called *independent BSS* (*IBSS*), where the nodes communicate directly with each other through their direct communication range. Basically, Ad Hoc networks generate a random BSSID with the Universal/Local bit set to 1 to prevent conflicts with officially assigned MAC addresses.

3.3.5.3. Network Architecture

Wireless networks can be configured as either flat or multi-layered network infrastructure. In flat network infrastructure, all nodes are considered homogeneously equal and may participate in routing functions, while in multi-layered networks all nodes are not considered equal [BrKo03] and they are partitioned in clusters with an elected cluster head for each cluster. The communication between the clusters is managed through the cluster heads.

3.3.6. WIDS Characterization

The deployment and configuration of WIDS system depend on the characteristics of the operating environment. For example, in infrastructure wireless networks, WIDS systems are

often deployed wherever the access points (APs) located, where the APs are the attractive targets of attacks. On the contrary, in Ad Hoc networks each wireless node may be a target of attacks, thus they necessitates specific deployment of WIDSs agents. Then, the standalone architecture of WIDS may be appropriate for infrastructure networks, but WIDS distributed or hierarchical architectures are required for Ad Hoc networks.

Characteristics of wireless IDSs (WIDSs) do not deviate much more from the wired IDSs; wireless communications characteristics and wireless intrusions features are taken into account for WIDSs. There are a number of proposed classifications of wired and wireless IDS systems [DeDW99] [Sobh06], but they did not cover all characteristics related to WIDS systems. Some of the previous classifications focused only on some common characteristics such as detection techniques and IDS response. Some others considered also the detection time and granularity of data-processing. In addition to all these characteristics, it is important to take into account two important dimensions related to the WIDS architecture and WIDS administration that significantly serve the monitoring and attack detection in the wireless networks.

Figure III-2 summarizes the holistic taxonomy of WIDSs. One of the basic differences between IDSs and WIDSs classifications is the information source. In IDSs, the source of input information can be: 1) *audit trails* and *system logs* on a particular host, or 2) *network traffic*. On the other hand, in pure WIDS, the information source is the wireless traffic, and this can be achieved through RF (Radio Frequency) monitor mode (RFMON).

3.3.6.1. Detection Techniques

Detection techniques describe the detection approaches for distinguishing the suspicious traffic from the benign traffic. There are two main mechanisms for identifying the intrusions; *signature-based* and *anomaly-based* detection techniques. In the recent past there has been a growing interest in developing the third advanced technique which is called the specification-based detection technique [SGFS02] [TSBK05] [GiSC06].

A) Signature-based Detection Technique

Signature-based WIDS analyzes the network traffic on the basis of detecting any evidence of attacks with regard to a predefined and established model of specific attack signatures. This technique is used for identifying instances of known attacks; the only attack signatures that are registered in the databases are identified. The challenges facing the signature-based WIDSs are the difficulty of gathering information about all current attacks as well as the potential failure to characterize the new attacks or the variations in the existing ones. Thus, signature-based WIDSs may lack the ability to detect the newly invented or unknown intrusions. It is also susceptible to evasion techniques. Then, it is more prone to high rate of false negatives.

B) Anomaly-based Detection Technique

Anomaly-based WIDS analyzes the network traffic and system activities on the basis of identifying any deviation from a predefined model of the normal and expected activities through

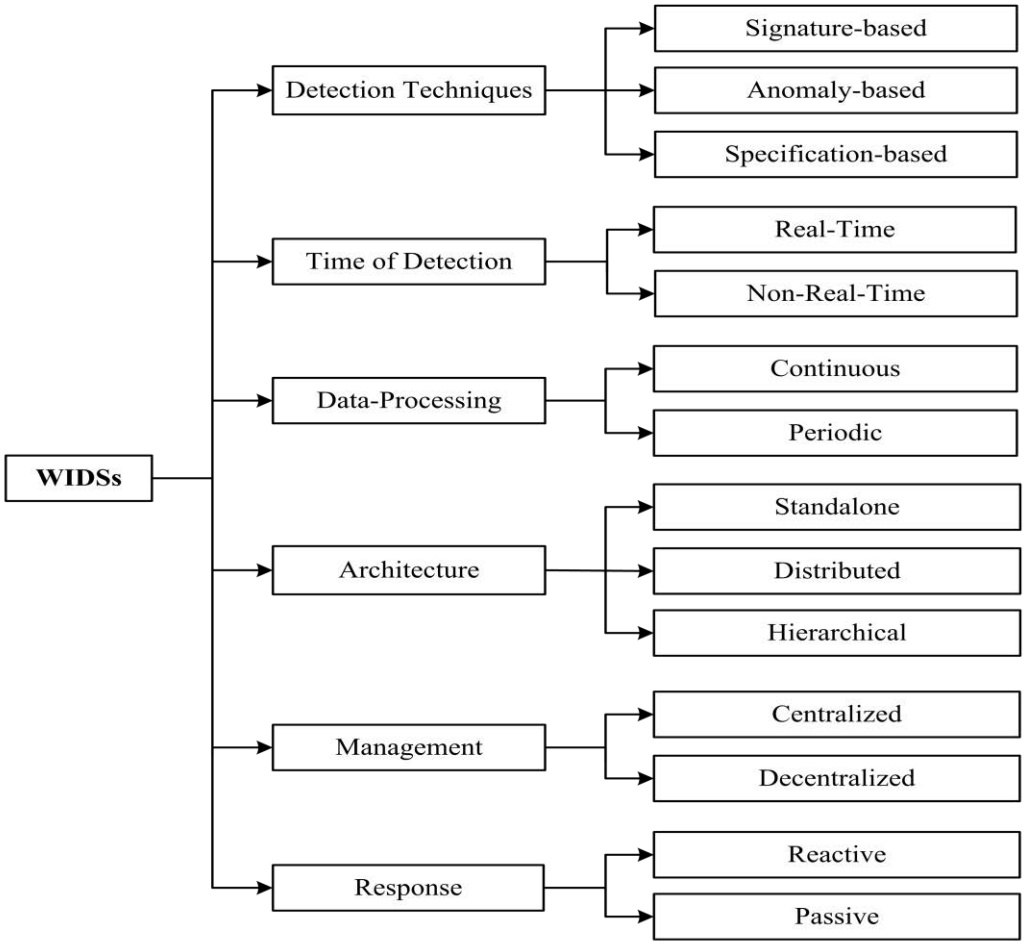

Figure III-2: WIDSs Classification.

the system. The reference model can be characterized by taking statistical samples of the system over a period of normal activities. This technique does not require a prior knowledge of attacks, where it is based on behavior identification; not specific patterns of traffic. Then, it could be able to detect the new attacks that may not be detected by the signature-based technique.

Disadvantages of this technique are manifested in lack of the ability to detect the attacks that do not introduce significant anomaly behavior, false detection of non-attack events that may cause a momentary anomaly in the system, and lack of recognizing the type of the detected attacks. Anomaly-based WIDSs are more prone to high rate of false positives due to the ever-changing nature of wireless networks and applications. The analytical behaviour of this approach may impose a heavy processing load on the system.

C) Specification-based Detection Technique

Specification-based techniques identify the malicious activities on the basis of detecting the deviation from a reference model that is created by combining between the trained normal behaviour of the system with the constraints imposed by the security policy of the system. This combination could enhance the attack detection capability to achieve the goals of high detection

rate and low false alarms rate. Some researchers refer to the specification-based detection approach as an enhanced anomaly-based detection approach [GiSC06].

3.3.6.2. Time of detection

Based on the time of detection, there are two main groups. Those that attempt to detect intrusions in real-time or near real-time, and those that process audit data with some delay, which in turn postpones the detection (non-real-time detection).

3.3.6.3. Granularity of data-processing

It differentiates between WIDS systems that process data continuously and those that process data in batches at regular intervals.

Continuous: The WIDS collects information about the actions taken on the environment immediately after they happened, and analyzes it continuously.

Periodic: The WIDS periodically takes and analyzes a snapshot of the traffic.

This dimension is linked with the time of detection dimension, but they do not overlap, where the system could process the data continuously with considerable delay or process it in patches in real-time.

3.3.6.4. Architecture

Architecture refers to the collaboration degree of WIDS agents on the monitored system. Based on the WIDS architecture, we differentiate between autonomous, distributed, and hierarchical WIDSs.

A) Standalone WIDS

In Standalone WIDS architecture, each WIDS node or agent operates independently and is responsible for detecting attacks on its own accord; there is no interaction between the network nodes. This architecture is more proper for the flat networks than the multi-layered networks.

B) Distributed WIDS

Distributed WIDS architecture comprises a number of network nodes which are responsible for collecting data and detecting signs of intrusions locally and independently, and then investigate them collaboratively in a broader range in order to carry out global decisions. Distributed WIDS is the suitable architecture for the decentralized nature of Ad Hoc wireless networks. Figure III-3 shows the distributed WIDS architecture for wireless Ad Hoc Network. The different WIDSs nodes exchange two types of data; security data and intrusion alerts. The nodes are distributed, but they share the information locally and detect the intrusions collaboratively. This architecture is applicable to flat networks and multi-layered networks as well.

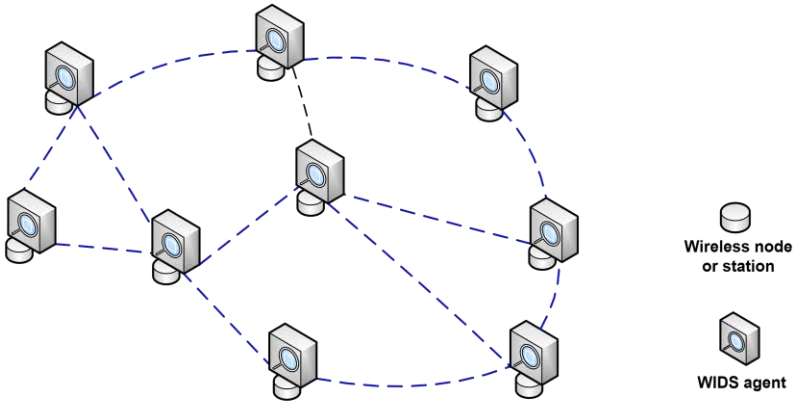

Figure III-3: Distributed WIDS Architecture.

C) Hierarchical WIDS

In this architecture, the network is divided into clusters with the formation of cluster-head nodes. These head-nodes are responsible for routing within the cluster, collect alert messages from local agents or nodes within the cluster, and accept all the accusation messages from the other cluster members indicating malicious activities. The cluster-head nodes may also detect the attacks against the other cluster-head nodes of the network as they constitute the backbone of the routing infrastructure. The cluster-head nodes collaborate to detect the intrusions in distribution manner (Figure III-4, a)) or pass the collected data to a centralized base-station which manages the whole network (Figure III-4, b)). There are several techniques to select the cluster head, such as voting [PXYN08] and spontaneous watchdog [RoJL06] techniques. This architecture is more suitable for multi-layered network.

3.3.6.5. Management

WIDS system can manage the detection and response processes either in centralized or decentralized manner depending on the network characteristics.

***Centralized WIDS*:** In a centralized WIDS, a combination of individual sensors or agents sniff the local traffic and then pass the collected data to a centralized management console, where the collected data is processed and analyzed for identifying the intrusions.

***Decentralized WIDS*:** It consists of one or more devices that can perform the functions of both the IDS agents and the centralized management console.

3.3.6.6. Response

Reponses of WIDS to the detected intrusions can be classified as passive or reactive. Passive systems notify the proper authority; and they do not try to hinder or mitigate the effects of attacks. On the other hand, the reactive WIDSs react to stop the attack (e.g., terminate the attack session); this function is more related to the wireless intrusion prevention systems (WIPSs).

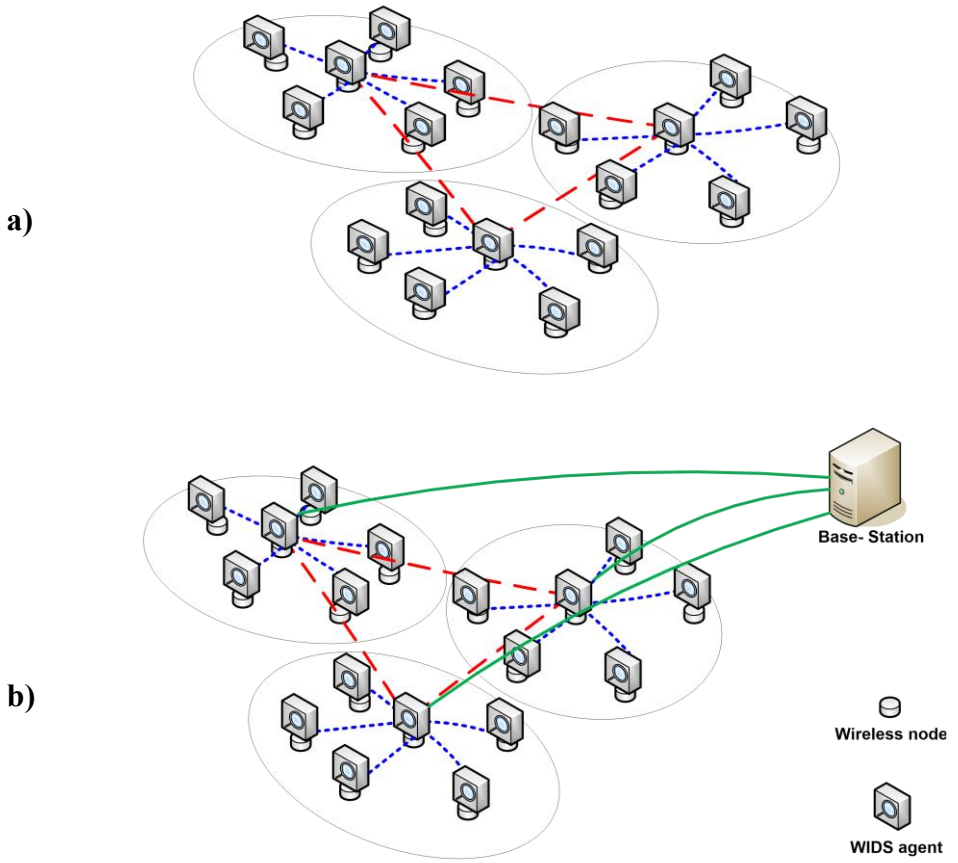

Figure III-4: Hierarchical WIDS Architecture.

3.3.7. Dataset Characterization and Generation

One of the focal points in our methodology is characterizing the evaluation dataset that includes two main parts of traffic; normal benign traffic (as background) and malicious traffic. The background traffic, which comprises normal and benign activities in the absence of attacks, can be generated as real traffic or synthetic traffic. The synthetic traffic can be generated artificially using traffic generation tools such as MGEN [Mgen13] and Rude/Crude [Rude13]. The main advantage of generating synthetic traffic is that it doesn't include secret information, but the main drawback is that it doesn't represent the real operation in the network. As for the real traffic, its generation can be managed by collecting and capturing the operational traffic during the normal operation of the network, and then replaying or injecting it into the testbed. *Airodump-ng* [Airo13] is an example of the capturing tools of the raw 802.11 traffic that can be replayed by aireplay-ng [Aire13] tool. Unfortunately, the collected real traffic may contain credential and confidential data besides some unwanted malicious traffic. This necessitates hence sanitizing the collected dataset before using it.

The second part of the evaluation dataset is the malicious traffic which is composed of intrusive activities. No doubt that the credibility of the WIDS evaluation test results depends significantly on comprehensive characterization of the malicious traffic. It is thus necessary to develop an attack classification that groups the common attack characteristics under expressive categories. This facilitates generating and extracting the representative attack test cases by combining the terminal classes of the classification. Therefore, we have developed a holistic taxonomy of wireless security attacks that classifies the attacks from the perspective of the WIDS evaluator as shown in chapter 4. The most well-known tools for generating the malicious traffic are Metasploit [Meta13a], CANVAS [Canv13], aircrack-ng suite [Airc13], and other Linux command line tools.

3.3.8. Evaluation Techniques and Tools

The selection of the proper techniques depends on the available tools, resources and the desired level of accuracy. Basically, there are three main techniques for the system evaluation; analytical modeling, simulation, and experimental measuring [Jain91].

Analytical modeling: It refers to the analytical analysis of the system under evaluation, mainly by mathematically abstracting the features of the system as a set of parameters or parameterized functions.

Simulation: It is the imitative representation of the operation of a system or process by means of the operation of another synthetic tool; software program or simulating device.

Experimental measuring: It refers to the practical measuring of the system features. This can be managed through an actual real system or using a prototype.

3.3.9. Testbed Design and Test Management

We reach now the penultimate task (i.e., the testbed level) that collects all aforementioned conditions and requirements to manage unbiased tests of WIDSs. These tasks of testbed design and test management are realized practically in chapter 6, with the experimental evaluation of WIDSs (Kismet & AirSnare).

3.4. Conclusion

Due to the complexity of the evaluation process of WIDSs, developing a reliable evaluation methodology is a pressing necessity and it is considered the first logical step in the way of the evaluation process. Thus, this chapter introduced a comprehensive evaluation methodology that considered all essential dimensions for managing a credible evaluation of WIDSs. Since the WIDSs evaluation is not a trivial task, our developed methodology consists of sequential tasks that facilitate and clarify the evaluation procedures. The developed methodology considered some important dimensions that were ignored in the previous evaluations of IDSs such as the evaluation challenges.

IV. Chapter 4: WIDSs Evaluation Centric Taxonomy of Wireless Security Attacks

Comprehensive and unbiased evaluation of WIDSs necessitates logically taking into account all possible attacks. While this is operationally impossible, it is necessary to develop an attack classification that groups the common attack characteristics under expressive categories. This facilitates generating and extracting the valid and representative attack test cases by combining the terminal classes of the classification. In this chapter, we study a set of previous classifications of attacks (wired and wireless), where we differentiate between them on the basis of the classification orientation, whether it is *evaluation-centric* or *defense-centric* classification. Regarding our concern in this thesis, we study and classify holistically the wireless attacks from the perspective of the WIDS evaluator, and how the possible and valid representative attack test cases can be extracted accordingly. Our proposed taxonomy of wireless attacks considers all essential dimensions for holistic classification of wireless attacks. The term "taxonomy" can be defined as a classification system that ensures a systematic arrangement into groups or categories according to established criteria [Merr03]. Besides considering the aspect of extracting the representative attack test cases that was ignored in most of the previous evaluations of intrusion detection systems (IDSs), we also consider another important aspect which is the probability of occurrence of each extracted test case. To the best of our knowledge, this aspect of the test cases probability was not considered before in the concept of IDSs evaluations.

4.1. Orientation of Security Attack Classifications

In the network security domain, we believe that the classification of security attacks can be oriented towards one of the following two objectives: *1) security defense* or *2) security countermeasure evaluation*.

In the first orientation, the attacks are classified from the perspective of the security defender. The considered taxonomy is created by extracting the attack signs or signatures from all possible attacks and assembling the common attack signs under representative dimensions. These dimensions guide to the techniques and mechanisms that can be followed by the security defender to prevent the attacks. This taxonomy can be called *defense-centric taxonomy*.

In the second orientation, the attacks are classified from the perspective of the security countermeasure evaluator. The dimensions of this taxonomy guide to the attack generation process and help in extracting the representative attack test cases. In this taxonomy, the evaluator generally describes the main phases of attack; preparation phase, exploiting phase and infecting phase. This taxonomy can be called *evaluation-centric taxonomy*.

Several considerable attempts of attack classification were developed, but much more of them were concerned with wired network attacks [Loug01][HaHu05][GaAD07]. Also, some

taxonomies focused on the security flaws [LBMC94], others focused on the exploited vulnerabilities, and others just listed the terms and types of attacks [Cohe97][Cohe95][IcSV95]. There is a lack of developing holistic taxonomy of wireless security attacks that can cover all essential dimensions for attack classification, especially from the perspective of the security countermeasure evaluation. We thus develop, regarding our concern with evaluating the wireless intrusion detection systems (WIDSs), a WIDS evaluation-centric taxonomy of wireless security attacks.

4.2. An overview of the Existing Security Attack Classifications

This section presents some of the previous work on the attack classification. We study and categorize these taxonomies from the perspective of the defense-centric and evaluation-centric as mentioned in the previous section. It is worth mentioning that many of the proposed taxonomies, that have been originally developed to help the security defender, followed the direction of the security countermeasure evaluation.

4.2.1. Defense-Centric Taxonomy

Kumar [Kuma95] proposed an attack taxonomy that is considered a defense-centric one. This classification was based on inspecting the attack signatures, to help ultimately in designing and building a signature-based IDS. The author classified the attack signatures under the following dimensions: *existence, sequence, regular expression patterns,* and *other patterns* that contain all other intrusion signatures that cannot be represented directly in one of the earlier categories. *Existence patterns* look for the evidence that may have been left behind by an intruder. For *sequence patterns*, some attacks manifest themselves as a sequence of events. *Regular expression patterns* include events that often specify several activities to be done jointly.

Killourhy et al. [KiMT04] classified the attacks from the perspective of the anomaly-based IDS defender. This classification is based on observing the anomalies of attack manifestation: *foreign symbol, minimal foreign sequence, dormant sequence,* and *non-anomalous sequence*. In *foreign symbol*, the attack manifestation contains a system call which never appears in the normal record. For *minimal foreign sequence*, the attack manifestation contains a system call sequence which never appears in the normal record, but all subsequences appear in the normal record. In *dormant sequence*, a sequence of system calls in the attack manifestation matches a subsequence in the normal record, but does not match the full sequence. In *non-anomalous sequence*, the attack manifestation entirely matches the normal sequence without any anomaly. In the same way, Barse and Jonsson [BaJo04] were concerned with extracting the attack manifestations for intrusion detection.

4.2.2. Evaluation-Centric Taxonomy

In this section, we study the attack taxonomies that followed one step or more towards the evaluation-centric taxonomy.

Most of the popular taxonomies in this direction concerned with two main dimensions: *passive* and *active* attacks [Bidg06][Stal10]. These two broad dimensions or classes are then subdivided into terminal subclasses. Passive attacks are subdivided into *traffic analysis* and *eavesdropping*. Active attacks are subdivided into *masquerading*, *relay*, *message modification*, and *denial of service*. This type of classification is not much more useful, as a complete taxonomy, for the security countermeasure evaluation or designing appropriate security countermeasures. This taxonomy can be used as an assistant object in the preparation phase of the evaluation-centric taxonomy, but to be efficient it needs more details about the attack features, attack techniques, exploited vulnerabilities, and attack objectives.

The taxonomies presented by Wood and Stankovic [WoSt04] and Howard [Howa97] followed close methodologies and provided nearly similar categorizations. Due to space limitations, we couldn't list all dimensions of these taxonomies. These taxonomies can be adapted to become a complete evaluation-centric taxonomy; by deleting some unuseful redundant dimensions and adapting others according to the evaluator's point of view.

Gad El Rab et al. [GaAD07] proposed an attack taxonomy to use it in evaluating the wired IDSs. This taxonomy has five dimensions; 1) *Firing source*: indicates the launching point of attack, 2) *Privilege escalation*: refers to the elevated access gained by an attacker to the system resources, 3) *Vulnerability*: specifies the exploited network vulnerabilities, 4) *Carrier:* describes the auxiliary means by which the attack reaches the victim; either via network traffic or through a local action, 5) *Target*: refers to the attack objectives. Although this taxonomy is an interesting one, it does not cover all dimensions of attacks from the perspective of the IDSs evaluator.

In the following section, we treat the shortcomings of the previous attempts of attack classification in the direction of the evaluation-centric, and accordingly we develop a new taxonomy of wireless attacks.

4.3. Our Proposed Taxonomy of Wireless Security Attacks

Before defining our classification attributes, it is important first to define some important requirements for the satisfactory and holistic taxonomy:

- ***Orientation****:* The orientation of attack classification must be clearly determined and defined; *defense-centric* or *evaluation-centric*.
- ***Completeness/exhaustive****:* Taxonomy should consider all possible attacks and develop the corresponding representative categories.
- ***Methodical:*** Taxonomy classes should be organized on the basis of a clearly defined methodology.
- ***Mutually exclusive:*** Each attack should be classified into only one category.

- ***Repeatable**:* Taxonomy should be repeatable and ensures always the same classification of an attack regardless of who is classifying.
- ***Unambiguous**:* Each category of the taxonomy should be clearly and precisely defined.

In this section, we propose the essential dimensions for creating a holistic and satisfactory taxonomy of wireless attacks from the perspective of the WIDS evaluator. Basically, these dimensions can be extracted from the conception of the attack generation process. The logical sequence of this process begins by determining what does the attacker want? i.e., attack objectives. Then, according to the *network mode* and *access privileges*, the *attack objectives* can be achieved via exploiting the *network vulnerabilities* using certain *attack techniques and mechanisms*. This sequence interprets the *methodology* of our classification. In the following subsections, we will explain the importance of each dimension in our taxonomy which is summarized in Figure IV-1.

We try by our proposed taxonomy to consider the essential dimensions without overkill or disregard, to finally have main categories that cover the existing attacks and novel attacks in the future. It may seem, for some, at first glance that the wireless attacks at MAC layer do not necessitate a grand or holistic classification, but there are two reasons necessitate developing a holistic taxonomy of wireless attacks. *First*, due to the enormous progress in information technology and programing in recent years, each attack can be launched by numerous tools and techniques ranging from simple command lines to GUI (Graphical User Interface) tools. For example, WEP Cracking attacks can be managed passively by AirSnort [Airs13a] based on FMS attack [FlMS01] notion or actively by aircrack-ng suite [Airc13]. Thus, we will consider not only the attack type, but also the attack tools and techniques as shown in Appendix A; it is clear from the different tools used for each attack that some of these tools follow the same attack process and some others deviate by one dimension or more. *Second*, the novel attacks appear overnight. The endless vulnerabilities of wireless network and security systems open the door for novel and unlimited potential attacks, so that we also consider in our taxonomy the potential attacks. For example, we consider the misfeasor as a class under the access privileges dimension, despite its rarity of occurrence, but it is not far to happen; the future hides many potential attacks.

4.3.1. Network Modes

The first dimension in our taxonomy focuses on specifying the wireless network mode which is considered as the base of the attack test cases in wireless environments. It helps in determining the manifestation and launching point of attack. As mentioned in chapter 3, there are two main modes in wireless networks; wireless *infrastructure* mode and wireless *Ad Hoc* mode. Most attacks objectives depend on the network mode; for example, in wireless infrastructure mode the wireless access point is the most attractive target for attacks, but in wireless Ad Hoc mode all the nodes are equal in their susceptible to attacks.

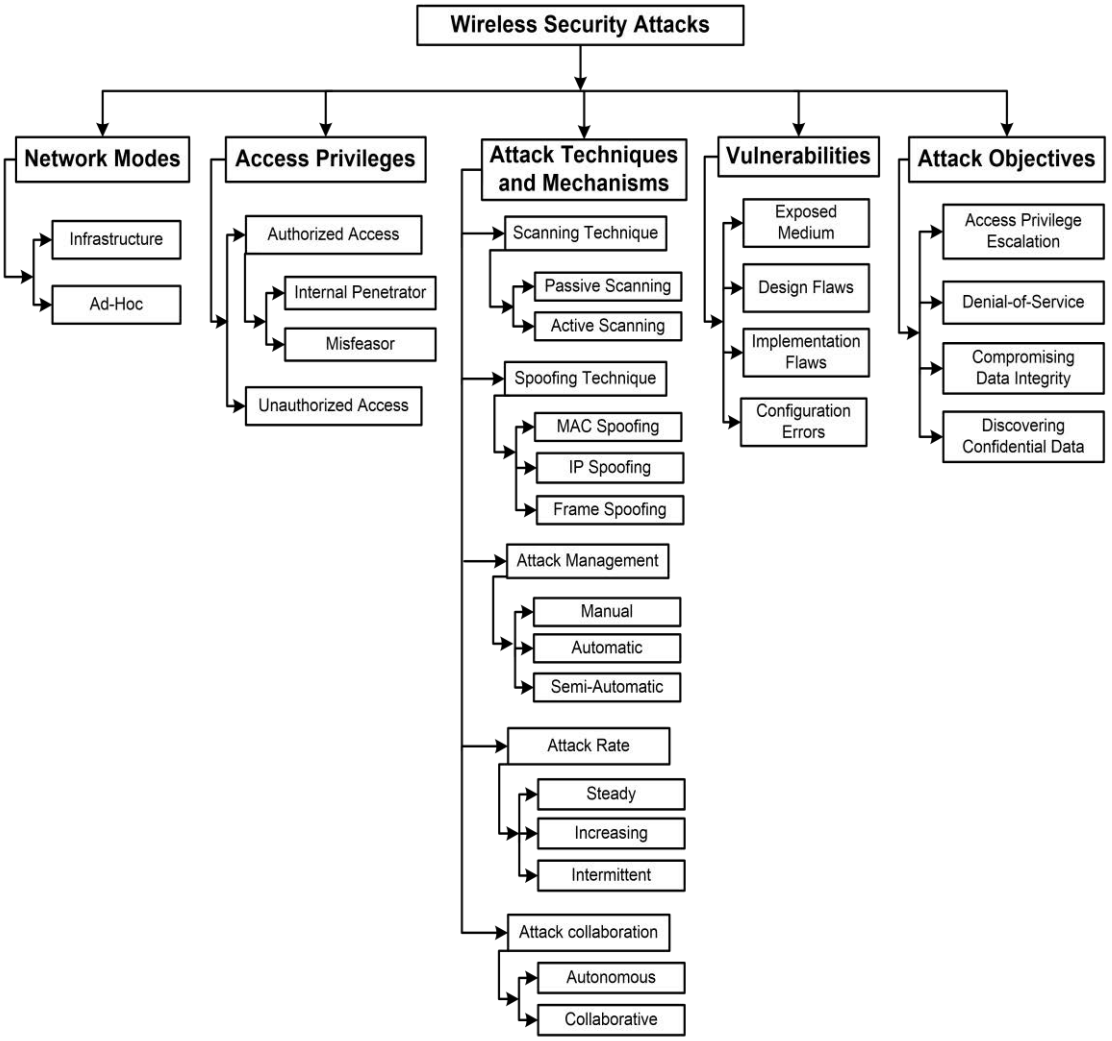

Figure IV-1: WIDSs Evaluation Centric Taxonomy of Wireless Security Attacks.

4.3.1.1. Infrastructure Mode

In wireless infrastructure mode, the wireless nodes associate themselves with a wireless access point to get the network services and/or communicate with each other. Basically, the access point announces its presence to the wireless nodes in the range by periodically broadcasting beacon frames that carry a service set identifier (SSID). SSID is used to identify WLAN by 1-32 characters unique ID as a network name. Basically, in infrastructure networks, SSID may consist of one or more Basic SSIDs (BSSIDs) which present the MAC addresses of the access points in the range. SSID helps in the differentiation between the wireless LANs (WLANs) in the range. The wireless node scans SSIDs in the range, and selects the intended one to associate with. Sometimes the access point may resort to conceal the SSID by disabling its broadcasting, and consequently the wireless nodes would not be able to identify and associate with the access point and they instead need foreknowledge of the SSID. This mechanism is not

considered as an effective security mechanism, where despite stopping the broadcast of SSID on the beacon frame, it may be sent out in other management frames.

It is worth mentioning that the access point can buffer frames unicast to a specific node when it goes to the sleeping mode. When the node wakes up, it sends PS Poll (Power Save Poll) request frame to the access point to retrieve the buffered data. An attacker could spoof the PS poll frame to activate the retrieval of the buffered data instead of the node, and then hinders it from receiving its buffered data.

4.3.1.2. Ad Hoc Mode

Wireless Ad Hoc network is a decentralized network which allows the wireless nodes to communicate with each other without need to infrastructure organization. Each node, in a wireless Ad Hoc network, participates in routing by forwarding data to the other nodes

Usually, mobile nodes in mobile Ad Hoc network (MANET) work with limited power, and the efficient utilization of this power is important for increasing the lifetime of the individual nodes as well as the overall network. The attacker can exploit this vulnerability to exhaust the energy of the mobile nodes. For example, an adversary may consume the biasing power of the sensor nodes in wireless sensor networks (WSNs) by sending several fake requests in order to cause denial of service (DoS) attacks.

4.3.2. Access Privileges

Access privilege restriction is one of the important security measures for organizing the access rights of users, and limiting the data exposure and system resources utilization. Based on the access privilege, we differentiate between *authorized* and *unauthorized access*.

4.3.2.1. Authorized Access

Authorized access privilege determines which level of access a particular authorized user should have to join the secured network data and resources. Each of them, the system user and administrator, has a determined access privilege to perform his assigned tasks. From the perspective of the authorized access violation, we can differentiate between the *internal penetrator* and *misfeasor*.

A) Internal Penetrator

Usually, the system user has a restricted access privilege where he is authorized to access a certain determined area of the network services and resources, but he is not authorized to access another specific one. Internal penetrator is the malicious user who may violate this restriction by performing a number of malicious activities to hack the restricted area of the network services and resources. For example, the malicious user who is already associated with a network via an access point, could be able to exploit the existing vulnerabilities to breach the access point security and change its configuration, steal MAC control list, discover confidential information,

or recruit the access point to launch attacks against the associated stations or stations in the range. There are many real examples [Cve09a][Cve13a] about compromising the access points and wireless control devices by internal penetrators. As registered in [Cve09a], the access point Netgear WNDAP330 which uses Atheros wireless driver, can be easily exploited by an authenticated user to cause denial of service attacks or execute arbitrary code via a truncated reserved management frame. Also, Cisco WLAN Controller (WLC) devices with software 7.0, such as Cisco Wireless Intrusion Prevention System (WIPS), are vulnerable to be exploited by an authenticated user to bypass wireless management settings and read or modify the device configuration [Cve13a].

B) Misfeasor

Misfeasor refers to the malicious administrator who misuses his authorized access privilege to the system resources and databases. However, system administrator has a superior level of authorized access to the system and its data. He is able to assign the users' access privileges, monitor and log the activity of users' sessions, and know where the highest value of information resides. He may discover the users' private information such as users' profile data, bank account details, and confidential data.

4.3.2.2. Unauthorized Access

Unauthorized access can be defined as an accidental or deliberate violation of the system security policy or bypassing the system security countermeasures to disclose, alter, or steal private accounts, messages, files, or confidential information without legal permission, superintendence, or authority. The attacker tries to penetrate the security system by exploiting the system vulnerabilities, using several compromising and hacking techniques, to achieve the intended malicious objectives.

4.3.3. Attack Techniques and Mechanisms

Attack techniques and mechanisms clarify the tactics that can be followed to prepare and execute the attack. Based on the attack techniques and mechanisms, we differentiate between *scanning techniques, spoofing techniques, attack management, attack rate organization,* and *attack collaboration*.

4.3.3.1. Scanning Techniques

The premier intuitive procedure in the preparation phase of wireless attacks is the scanning process. It helps to locate the access points, wireless stations, vulnerable services, in addition to discovering the secret data, passwords, and so on. Based on the scanning techniques, we differentiate between *passive* and *active scanning*.

A) Passive Scanning

In wireless networks, the attacker can use the radio channels in the RF (radio frequency) monitor mode to listen in the network traffic which broadcasts over the wireless medium. One of the intended attack objectives of passive scanning technique is sniffing the service set identifier (SSID) which leads to discovering the MAC addresses of the access points and the associated stations to determine after that the next step in the attack. As mentioned, each access point announces its presence by broadcasting beacon frames that carry SSID. The attacker could exploit this broadcasting process to sniff the beacons and SSIDs. At a certain level of network security, the network administrator may disable the SSID broadcasting. In this case, the attacker can wait and sniff any associate request from a legitimate station that already carries the network SSID. Then, the attacker can take steps to scan passively and collect the MAC addresses. KisMAC [Kism13b] and AirTraf [Airt13] are examples of passive scanning tools.

B) Active Scanning

When the attacker is unable to collect the intended information using passive scanning technique, or if he does not wish to wait patiently for voluntary associate requests from the legitimate stations that carry the networks SSIDs, he resorts to use active scanning technique. In active scanning technique, the attacker sends out probe request frames [Ieee12] or artificially constructed packets that contain a spoofed MAC address to discover the network activity or trigger useful responses from the target. The probe response frames from the access points contain the SSIDs and other information similar to which in the beacon frames. The attacker sniffs these probe responses and extracts SSIDs, and consequently collects the MAC addresses. NetStumber [Nets13], Wellenreiter [Well13], and WiFiFoFum [Wifi13a] are popular tools for wireless active scanning.

4.3.3.2. Spoofing Techniques

Using spoofing techniques, the attacker can forge his identity to masquerade as another one, or even creates a single or multiple illegitimate identities. The attacker may resort to use this technique to evade detection by security defense systems, impersonate another network device, bypass access control mechanisms, gain authorized access, or falsely advertise services to wireless clients. On the basis of the spoofing techniques, we differentiate between *MAC address spoofing*, *IP address spoofing*, and *Frame spoofing*.

A) MAC Address Spoofing

MAC address is a layer 2 unique identifier that is burned into network devices or network interface cards (NICs) during manufacturing. However, MAC address is 6-bytes long, the first 3-bytes are assigned by IEEE and indicate which manufacturer fabricated the NIC, and the last 3-bytes are assigned by the manufacturer to differentiate between the NICs. MAC spoofing refers to altering the manufacturer-assigned part. Using MAC address spoofing, the attacker

may be able to bypass the access control mechanisms or advertise fake services to achieve intended objectives.

In wireless networks, typical access points usually predefine access permission for a set of machines or nodes with MAC addresses registered in an assigned address-set (MAC control list). The attacker may spoof a legitimate MAC address of a node that already exists in the MAC control list to have the ability to associate with the access point. Also, the attacker can create a fake access point with spoofed MAC address to deceive the wireless nodes in the range to associate with it, thus he may be able to capture secret information of the associated nodes or overwhelm the adjacent nodes by beacon flood attack.

In certain attacks such as DoS attacks, the attacker needs a heavy number of MAC addresses than he could collect by sniffing. Therefore, the attacker resorts to generate random MAC addresses. However, the attacker generates a random MAC address by selecting an IEEE-assigned part appended with additional 3-bytes manufacturer-assigned [Bidg06]. SMAC [Smac13], MAC MakeUP [Make13], and Macchnager [Macc13] are examples of MAC spoofing tools that alter the software based MAC addresses; not the hardware burned-in MAC addresses. Sheng et al. [STCK08] has discussed three methods for detecting MAC address spoofing; sequence-number analysis, transceiver fingerprint and signal strength analysis.

B) IP Address Spoofing

IP address is a layer 3 unique identifier for the host connection and packet routing in the network. Every IP address consists of 32-bits that are divided into two parts, one of them identifies the network and the other identifies the host, according to the address class and the subnet mask. IP addresses are usually assigned as static or dynamic addresses. Static IP address is the fixed permanent address that is assigned to the host on the network by the administrator or Internet service provider (ISP). Dynamic IP address is a temporary address assigned to the host each time it accesses the network. The main difference between MAC address and IP address is that although the MAC address is a unique identifier for the network devices, it doesn't know how to route the packets through the network; which is the main function of IP address. In other words, direct connected transmission uses MAC addresses for frame delivery, and routed transmission uses IP addresses for packet delivery.

IP spoofing refers to the creation of IP packets with a forged source IP address. Using IP address spoofing, the attacker may intercept the link between two communicated nodes and pretends alternately as an end-point to each one of them. Then, the attacker can control the traffic, alter or eliminate information exchanged between the two points, i.e. this type of attack is called man-in-the-middle (MITM) attack. In the same way, the attacker can disclose confidential information by deceiving the victim.

Another type of attacks that depend significantly on IP spoofing is the denial of service (DoS) attacks that aim to consume network resources and bandwidth. However, there are many scenarios of DoS attacks. One of these scenarios is flooding the victim by heavy traffic with spoofed IP address to conceal the attack origin. Another scenario is sending request to a set of

network nodes with a spoofed IP address of a targeted victim to redirect the reply to the victim to exhaust its resources. RafaleX [Rafa13] and SendIP [Send13] are examples of IP spoofing tools.

C) Frame Spoofing

Frame spoofing is the most popular spoofing in wireless networks, where most wireless attacks at MAC layer depend on it. Frame spoofing usually includes by default MAC spoofing. The lack of authentication for the management frames in wireless communications leads to numerous types of attacks, especially DoS attacks, depending on the frame spoofing technique. For instance, when a wireless station selects an access point to associate with, it must first authenticate itself to the access point before establishing further communication. A part of the authentication process is the deauthentication frame that can be sent by the station to the access point to notify it about its disconnection. Unfortunately, this frame itself is not authenticated using any keying material. Consequently, the attacker could spoof this deauthentication frame, either pretending to be the access point or the station, and directs it to the other party to break the connection between the station and the access point. Similarly, a part of the association process is the disassociation frame that may be also sent to notify the network about the station leaving. This disassociation frame can be also spoofed and exploited to terminate the station connection and cause denial of service. Also, the authentication frames can be used for launching authentication flood attacks that overwhelm the access point by several authentication requests. Much more tools can be used for these attacks, such as AirJack [Airj13], KisMAC [Kism13b], Void11 [Void13], etc.

4.3.3.3. Attack Management

This dimension refers to the management of the attack phases. Basically, depending on the system immunity, exploited vulnerabilities, attack objectives, attack techniques, and attack tools, one or more of the attack phases (i.e., preparation, exploiting, and infecting phases) can be managed either *manually*, *automatically*, or *semi-automatically*. With the notable progress in the software used for wireless network analysis in the recent past, this task of attack management depends greatly on the attack tools rather than the other conditions.

A) Manual

Manual management of the attack refers to executing all phases of the attack process, from the preparation phase until the infecting phase, manually. The attacker scans the system vulnerabilities manually and exploits them to reach the intended objectives manually as well. This technique is rarely used in the present, especially by the skillful attackers, where a lot of time is spent and much more efforts are exerted to perform the intended objectives of infecting victims or obtaining information. Manual management of attacks can be observed clearly in using the Linux command line tools such as aircrack-ng suite [Airc13]; airmon-ng, airodump-ng, aireplay-ng, aircrack-ng, etc. The attacker who uses command line tools should be more

technically literate and aware of using these tools to successfully manage the attacks. Recently, there is a trend towards implementing the aircrack-ng suite tools in GUI (Graphical User Interface) tools to facilities their utilization, and to be an easy task to manage automatic or even semi-automatic of attack.

B) Automatic

The automatic attack technique refers to performing all phases of attack automatically. All attack features such as attack type, rate, duration, and victim addresses are pre-programmed in a specified field for firing the attack by a keystroke. Some tools help in managing the attack automatically such as CommView toolset [Comm13]; just select the attack type, specify the attack features, and then launch the attack by a keystroke.

It is worth mentioning that the attacker could compromise and recruit one or more of the stations or access points in the range to launch certain attacks. This type of attacks can be managed automatically and remotely; just firing the command of attack with the specified features.

C) Semi-automatic

Semi-automatic attack technique merges between both the manual and automatic techniques. In the semi-automatic attack, not all the attack phases are launched automatically by a simple unique command. There are a number of attacks that should be managed semi-automatically at the preparation phase and may be at the exploiting phase as well, but the infection phase is performed automatically. On the contrary, some other attacks can be performed automatically at the preparation and exploiting phases, but the infection phase should be managed manually by specifying the attack type, onset, and rate. Some attackers prefer to use this technique to have more control on the victim. During the attack, the attacker might be able to manage all the attack features according to the state of the victim and the intended attack objectives.

4.3.3.4. Attack Rate Organization

One of the pivotal techniques that are used to reinforce the attack impact is the attack rate organization. Basically, the attack rate can be organized according to the analysis of the real-time state of the targeted system and the intended attack objectives. The attack can be managed at *steady*, *increasing*, or *intermittent* rate.

A) Steady Rate

Using several tools, the attacker may be able to generate a steady number of attack packets during the attack interval. DoS attack, which is the most dangerous attack in wireless network security, can use this tactic to overwhelm and flood the victim resources by a heavy steady rate of traffic to exhaust the victim resources. The main challenge of combating DoS attack is the difficulty of distinguishing the malicious traffic from the legitimate traffic. DoS attack is more

severe when the attacker recruits agent machines to overwhelm simultaneously the victim resources; this is a form of distributed DoS (DDoS) attack.

B) Increasing Rate

Typical successful attack resorts to many tactics to evade the attack detection. One of these tactics is generating the attack at a gradually increasing rate. This can lead to a slow exhaustion of the victim resources, as aimed by some flooding attacks, and it thus delays the early detection of attack.

C) Intermittent Rate

Another successful tactic with low probability of revealing the attack is generating the attack at an intermittent rate. In the intermittent rate tactic, the attacker generates the attack in alternate intervals, where he launches attack during a certain interval (*on-state*), and holds it during another alternative interval (*off-state*). At the end of *off-state*, the attacker resumes the attack again and so on. The attacker can adjust the *on* and *off* intervals according to the real-time state of the victim. Also, during *on-state*, the attacker may use steady constant rate or gradually increasing rate.

4.3.3.5. Attack collaboration

This dimension determines the collaboration degree between the attack entities. Based on the attack collaboration, there are two main strategies to prepare and perform the attack; *autonomous* or *collaborative* attack.

A) Autonomous Attack

Autonomous attacker can prepare and launch the attack independently without any contribution or help from any other entity. In this category, the attacker is responsible for discovering the system vulnerabilities, determining the targets, planning the attack, selecting the appropriate tools and techniques, launching and managing the attack autonomously. However, autonomous attack is commonly used and easy to be managed, where the attacker doesn't need any arrangement with any other entity for intervention or managing the attack.

B) Collaborative Attack

Collaborative attack refers to the collaboration between the attack entities to perform intended objectives. However, collaborative attack can be performed by one of two strategies. The first strategy is manifested in the contribution between autonomous attackers to reach and achieve a common goal. In the second strategy, the attacker can compromise and recruit multiple agents (centrally controlled) to be collaborated in launching an intended attack against a certain victim.

4.3.4. Vulnerabilities

Vulnerability is a flaw or weakness in a system design, implementation, configuration, or security measures that could be accidentally or intentionally exploited by a threat source, and results in a violation of the system security policy. In this section, we classify the vulnerabilities into four main categories; *exposed medium, design flaws, implementation flaws,* and *configuration errors*.

4.3.4.1. Exposed Medium

Due to the openness of the exposed wireless medium, the attacker can easily eavesdrop on the wireless connection, intercept the messages exchanged between wireless nodes, and access the wireless network with poor authentication. However, most of the wireless networks are not configured securely and often only MAC address spoofing is required to gain full access. Radio jamming and man-in-the-middle (MITM) attacks are examples of attacks that exploit the openness vulnerability of wireless medium. Radio jamming attack overwhelms wireless communications or corrupts the received signals using radio interference by transmitting radio signals to the intended victim at the same frequency band or sub-band as the transmitter uses. In MIMT attack, the adversary eavesdrops on the communications between the communicated points and intercepts the data transferred between them to discover secret information and/or inject false information. It is worth mentioning that the exposed medium vulnerability is the gate that facilitates the exploitation of the other vulnerabilities; design flaws, implementation flaws, and configuration errors.

4.3.4.2. Design Flaws

Design flaws refer to the weaknesses in the services or protocol design that can be exploited to violate the assumption of normal behaviour in the network. As an example of the design flaws, 802.11 authentication is a one-way authentication which is useful and commonly used in infrastructure networks. The one-way authentication is attractive to some serious attacks that rely on using rogue access points. Although the access points authenticate the wireless stations to ensure that only the authorized stations access the network, it is not obligatory for the access point to authenticate itself to the station wants to join the network, then a rogue access point could spoof SSID and steal authentication credentials to deceive the wireless stations in the range to associate with it to steal confidential data.

Also, there is a lack of authenticating the management frames in 802.11 networks, and this may lead to exposing the wireless stations to many attacks ranging from spoofing, to deauthentication, to authentication flood attacks.

4.3.4.3. Implementation Flaws

Implementation flaws refer to errors in hardware construction or software coding due to the unfamiliarity with the programming language or the ignorance of security issues. For example,

inadequate boundary checking which may result in a buffer overflowing with attacker controlled contents [HsSL08]. Some implementation flaws are the translation of design flaws. For example, some wireless network cards reset the initialization vector (IV) to zero each time they are re-initialized and regularly increase the IV by one for each packet transmitted [BoGW01].

Example of implementation flaws is the vulnerability CVE-2001-0160 [Cve01] of Lucent/ORiNOCO WLAN cards that generate predictable initialization vector (IV) values of WEP protocol which might allow attackers to quickly compile the information to decrypt the transmitted messages. More examples of implementation flaws can be found in Appendix A with the registered vulnerabilities CVE-2007-5651 [Cve07a], CVE-2007-4012 [Cve07b], CVE-2009-0052 [Cve09a], and CVE-2009-0282 [Cve09b].

4.3.4.4. Configuration Errors

Configuration errors are the result of improper settings of a particular environment, threat model, or program utilities that are installed in a wrong place, or incorrect installation of program parameters. As registered in CVE-2013-4613 [Cve13b], the default configurations of the administrative interface on the Canon MG3100, MG5300, and MX922 printers do not require authentication, then the attacker could modify the configuration by open access.

4.3.5. Attack Objectives

Attack objectives are the ultimate goals of attack. They can be classified into four main categories; access *privilege escalation*, *denial of service*, *compromising data integrity*, and *discovering confidential data*.

4.3.5.1. Access Privilege Escalation

Access privilege escalation is the act of exploiting the system vulnerabilities to gain elevated access to the system resources that are normally protected against any unauthorized use. However, the malicious unauthorized user can escalate the access privilege of an authorized user (i.e., remote-to-local (R2L) privilege escalation), or the authorized user may escalate to the administrator level (i.e., user-to root (U2R) privilege escalation). Usually, this task is considered as a penultimate goal that is used to achieve another ultimate goal. For example, the authenticated user can exploit the vulnerability of Cisco WLAN Controller (WLC) software (4.2 through 6.0) [Cve10] to bypass the access restrictions and modify the configuration to gain administrative privileges.. Also, the vulnerability CVE-2005-3802 [Cve05] (Appendix A) shows another example of access privilege escalation.

4.3.5.2. Denial of Service

Denial of service (DoS) goal can be achieved by obstructing the normal operation of the targeted stations or preventing the targeted system from serving the legitimate stations. DoS attacks aim to disrupt the normal operation of the system by exhausting its resources (CPU time,

memory, band-width, battery power, etc.) or creating fake requests to deauthenticate and disconnect the legitimate nodes from the network. Despite the exerted effort to combat DoS attacks or mitigate their impact, the wireless communications still suffer from their threats. The main challenge associated with DOS attack is the difficulty of distinguishing the legitimate traffic from the malicious traffic, where the DoS malicious traffic seems usually compliant with the specification of the legitimate traffic. Most wireless attacks are denial of service (DoS) attacks and this is obvious from the huge number of the registered DoS attacks. As shown in [Cvew13] and Appendix A, most of the registered cases (CVE-2013-1105, CVE-2011-0196, CVE-2009-0052, CVE-2006-6059, CVE-2009-2861, etc.) are DoS attacks.

4.3.5.3. Compromising Data Integrity

Data integrity refers to the accuracy, consistency, and completeness of data during operation of transfer, storage, and retrieval; data is never altered and reaches the destination intact. Usually, data integrity is imposed on the database at its design stage through using standard rules and procedures, and it is maintained through using error checking and validation routines. Data integrity can be compromised by altering the data stream. However, the attacker may intend to modify the contents of the system data or inject complete created packets into the data stream, or replace relevant information with nonsensical or offensive content. Airpwn [Airp13] and File2air [File13] are examples of attack tools used to compromise the data integrity. Airpwn is a wireless packet injection tool. It listens in the transmitted packets, and if the data matches a pattern specified in the configuration files, then Airpwn spoofs the response from the access point with custom content and injects it to the client; this is similar to, but not identical, the classic MITM attack. File2air tool is a command line utility for injecting 802.11 frames from binary files into the wireless channel using AirJack drivers [Airj13].

4.3.5.4. Discovering Confidential Data

Due to the exposed wireless medium and other network vulnerabilities, the attacker can sniff and probe the wireless beacon frames or access illegitimately the system database to look for and discover the secret and confidential data. They attempt to discover private and secret data by eavesdropping and intercepting it over the wireless link, escalating to gain access to the confidential data under a fake identity, or deceiving the wireless nodes in the range to associate with a fake access point. Eavesdropping, encryption key cracking, rouge access point phishing, and MITM attacks are examples of confidentiality attacks. For example, the attacker may intend to discover the WEP shared secret key. One of the available tools for WEP cracking is AirSnort [Airs13a] that passively monitors and captures the transmitted packets. Once enough packets have been gathered, AirSnort can compute and extract the WEP key. Also, one of the available eavesdropping tools is WireShark [Wire13] which is a packet analyzer used to passively capture 802.11 packets being transmitted over the wireless link.

4.4. Attack Test Cases Generation

On the basis of our proposed taxonomy of wireless attacks, we can generate all the possible attack test cases and extract the valid and representative ones. The most appropriate tool in this context is the Classification Tree Editor (CTE) [Cte13] that helps in automatic generation of the attack test cases. CTE is a graphical editor tool that is based on the Classification Tree Method (CTM) which supports test cases design using descriptive tree-like notation. Using CTE, the test cases are designed with regard to systemic classification of the test objects into a finite number of mutually exclusive terminal classes. CTE gives a compact and clear presentation of the overall test objects.

Regarding our concern in this study, the attack test cases can be generated using CTE through two main steps. The first step is specifying the dimensions or classes relevant to the test of interest, and organizing them in a tree-like classification according to our classification of wireless attacks. The second step is generating the attack test cases by combining the terminal classes using the logical combination rules that are supported by CTE.

The logical combination rules are organized according to the scope of the test. Since the generated test cases may contain some invalid ones, then the evaluator can revise them and extract the valid representative ones which are the input situations to be tested. The main advantages of using CTE are that the evaluator can easily modify the test specification when necessary, and can control the complexity and number of test cases according to the scope of the test.

The logical combination rules organize the relationship between the taxonomy dimensions in mathematical formula. For example, the following formula (Eq. IV-1) that collects all the main dimensions of our taxonomy generates all possible test cases that are 6912 test cases. It is worth mentioning that not all these test cases are available or valid, so that they need an intervention to extract the valid ones.

$$[Network\_Modes * Access\_Privileges * Attack\_Techniques * Vulnerabilities * Attack\_Objectives] \quad \text{Eq. IV-1}$$

Where "*" and "+" represent AND and OR logic operators respectively. The generated test cases are controlled according to the dimensions of interest. For example, if we want to extract the attack test cases in wireless infrastructure mode only with the concern about two vulnerabilities (implementation flaws and design flaws), and two attack objectives (DoS and discovering confidential data), then the CTE formula will be:

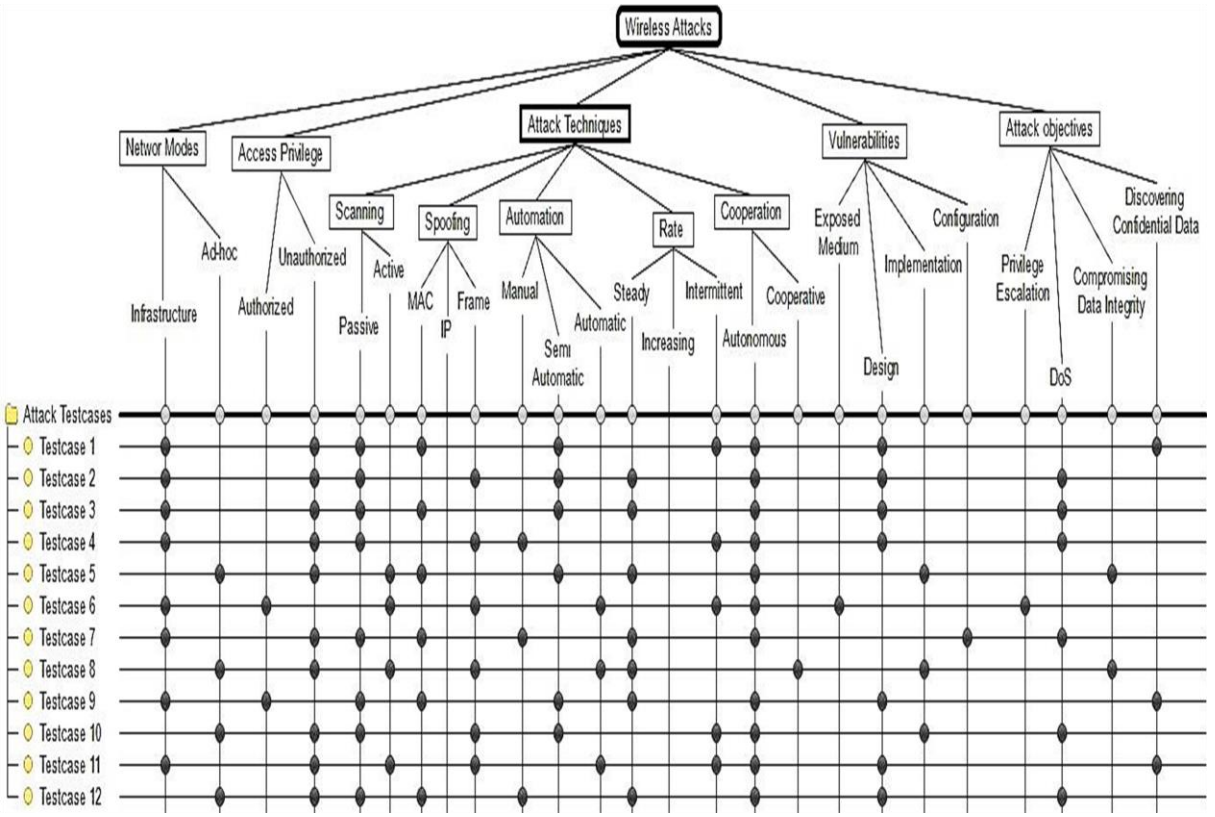

Figure IV-2: Sample of the Attack Test Cases.

$$[Infrastructure * Access\_Privileges * Attack\_Techniques * (Implementation\_Flaws + Design\_Flwas) * (DoS + Discovering\_Confidential\_Data)] \quad \textbf{Eq. IV-2}$$

This formula (Eq. IV-2) generates a set of test cases that are limited and related to these dimensions only. For example, Figure IV-2 shows a sample of the attack test cases generated according to our taxonomy of wireless attacks. The generated test cases can be also minimized by using the logical dependency rules that are also supported by CTE. In conclusion, CTE helps the evaluator to avoid time consuming and error prone that may be caused by the manual creation of the test cases, especially if the classification is too large. The evaluator is also able to intervene, revise, and modify the generated test cases according to the scope of the test.

4.5. Classification of Some Wireless Attacks

In this section, we study and classify some of wireless attacks from the perspective of our proposed taxonomy.

4.5.1. WEP-based Attacks

Wired equivalent privacy (WEP) algorithm suffers from some security breaches. These security breaches which can be easily exploited demonstrate the ineffectiveness of WEP algorithm. Basically, WEP uses two main algorithms, encryption algorithm RC4 and the integrity check algorithm CRC-32 that are susceptible to attacks due to their design flaws. Examples of the attacks that can exploit RC4 and CRC-32 weaknesses are FMS attack and chopchop attack.

4.5.1.1. FMS Attack

FMS attack is the first key recovery attack against WEP. Fluhrer et al [FlMS01] analyzed the weaknesses in the key scheduling algorithm of RC4 and they demonstrated how it can be easily cracked and WEP secret key is derived. They introduced FMS attack that exploits the correlation between the initialization vector (IV) and the key sequence produced by RC4 algorithm to recover the secret key. FMS attack is based on collecting numerous encrypted packets including the initialization vectors (IVs), and analyzing them analytically to derive the secret key. WEPCrack [Wepc13] and AirSnort [Airs13a] are open source WEP cracking tools that realize and implement the theoretical idea of FMS attack.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Unauthorized
Scanning Technique:	Passive / Active
Spoofing Technique:	
Attack Management:	Manual / Automatic
Attack Rate:	
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	Discovering confidential data

4.5.1.2. Chopchop Attack

The chopchop attack was initially posted on the NetStumbler Internet forum by an individual under the pseudonym KoreK [Kore04]. Chopchop can decrypt a WEP packet without knowing the encryption key. This attack does not recover the WEP key itself, but it merely reveals the plaintext. Chopchop attack exploits the weaknesses of integrity algorithm (CRC-32) that is used to compute the integrity check value (ICV). In chopchop, the attacker intercepts the encrypted packet and truncates it by chopping the last byte. The attacker guesses the value of the last byte and patches the truncated packet, and then computes the new ICV of the modified packet. Then, the attacker sends the new packet to the access point with a multicast destination address. When

the access point receives the packet, the access point decrypts it and checks the ICV value. If the ICV is correct, the access point retransmits the packet to the network, then the attacker knows that his guess of the last byte of the packet is correct, and he can continue with the second last byte and so on, until guessing and revealing all clear byte of the plaintext. If the ICV is incorrect, the packet is silently discarded, and accordingly the guess at the last byte is incorrect and this induces the attacker to make another different guess. After at most 256 trials, the attacker can guess the correct value of the last byte, and so on. Chopchop attack can be managed by tools such as aircrack-ng suite [Chop13]

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Unauthorized
Scanning Technique:	Active
Spoofing Technique:	MAC
Attack Management:	Manual
Attack Rate:	Steady
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	Discovering confidential data

4.5.2. RF Jamming Attack

RF jamming attack exploits the openness of wireless medium and uses a high gain antenna to send powerful RF signals to interfere with the radio frequency (RF) used by legitimate stations, to prevent them from exchanging information[KhMM08]. Sometimes, RF jamming attack is used to damage the electronic components of the access point by high power RF signals and make the access point permanently out of service. Wifi jammer [Wifi13b] and AirHORN [Airh13] are examples of RF jamming tools.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure / Ad Hoc
Access Privilege:	Unauthorized
Scanning Technique:	Active
Spoofing Technique:	Frame
Attack Management:	Manual / Automatic
Attack Rate:	Steady
Attack Collaboration:	Autonomous
Vulnerability:	Exposed Wireless Medium
Attack Objective:	DoS

4.5.3. Authentication flood attack

Authentication flood attack is a type of denial of service (DoS) attack that generates a flood of authentication frames requesting to join a network through an access point. Thus, the access point or authentication server will be overwhelmed and cannot respond to the flood of authentication requests and it consequently fails to respond or establish successful connections to the legitimate stations. The attacker can easily adjust the hacking rate to be either steady rate or intermittent rate. Void11 (gvoid11) [Void13], MDK3 [Mdk13], and KisMAC [Kism13b] are examples of tools that can be used to control the authentication attack rate.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Unauthorized
Scanning Technique:	Passive
Spoofing Technique:	Frame
Attack Management:	Manual / Automatic
Attack Rate:	Steady
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	DoS

4.5.4. Association Flood Attack

Association flood attack is another type of DoS attacks, like authentication flood, which generates a flood of association frames to interrupt the wireless services by depleting the resources of the access point, particularly the association table. When the association table overflows, the legitimate stations cannot get associated. Void11 [Void13] is also used for association flood attacks.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Unauthorized
Scanning Technique:	Passive
Spoofing Technique:	Frame
Attack Management:	Manual / Automatic
Attack Rate:	Steady
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	DoS

4.5.5. Deauthentication Attack

A part of the authentication framework (Figure II-4) is the deauthentication message which allows the wireless node and access point to explicitly request deauthentication from each other. Unfortunately, this message itself is not authenticated. Therefore, the attacker can spoof this message, pretending to be either the access point or the wireless node, and directs it to the other part to terminate the authentication state between the wireless station and access point. Once the station is deauthenticated, it is no longer able to access the network until the authentication is re-established. This attack is usually called deauthentication attack and it causes denial of service.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Unauthorized
Scanning Technique:	Passive / Active
Spoofing Technique:	Frame
Attack Management:	Manual / Automatic
Attack Rate:	
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	DoS

4.5.6. Disassociation Attack

Disassociation is a part of the association framework. The disassociation suffers from vulnerability as that found with the deauthentication frame, where it is also unauthenticated. This vulnerability gives the attacker an ability to spoof the disassociation frame and terminates the association session. The disassociation attack is slightly less efficient than the deauthentication attack, where the victim can return to the associated state by a small effort than that can be done with the deauthentication attack; it is clear in Figure II-4 that shows the states of authentication and association processes and their relevant parts.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Unauthorized
Scanning Technique:	Passive / Active
Spoofing Technique:	Frame
Attack Management:	Manual / Automatic
Attack Rate:	
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	DoS

4.5.7. Deauthentication flood attack

Deauthentication flood attack is an advanced form of the deauthentication attack. In the simple form of deauthentication attack, when the attacker sends a deauthentication frame to break the connection between the wireless station and access point, the station would attempt to reauthenticate. If the attacker wants to hinder the station from connecting the network, he needs to send a stream of deauthentication frames, usually in steady rate. This is called deauthentication flood attack and it is considered one of the severe DoS attacks. Metasploit [Deau13], Void11 (gvoid11) [Void13], and aireplay-ng [Aire13] are examples of tools that can be used in performing deauthentication flood. Metasploit command lines can be managed easily by Armitage [Armi13] through GUI.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Unauthorized
Scanning Technique:	Passive / Active
Spoofing Technique:	Frame
Attack Management:	Manual / Automatic
Attack Rate:	Steady
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	DoS

4.5.8. Deauthentication / Disassociation (Amok Mode)

Deauthentication attack (Amok mode) does not merely disconnect a specific station from the access point as the aforementioned deauthentication attacks, but it effectively breaks the connections between the wireless stations and access points in the range. The most popular tool for this type of attacks is MDK3 [Mdk13].

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Unauthorized
Scanning Technique:	Passive
Spoofing Technique:	Frame
Attack Management:	Manual
Attack Rate:	Steady
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	DoS

4.5.9. Fake authentication Attack

Fake authentication attack performs the two steps of authentication and association. It can be used for authentication/association with the access points that use WEP algorithm, but it cannot be used against WPA/WPA2 access points. Aireplay-ng [Aire13] is a premier used tool for managing the fake authentication attack.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Unauthorized
Scanning Technique:	Active
Spoofing Technique:	Frame
Attack Management:	Manual
Attack Rate:	Steady / Intermittent
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	Access Privileges Escalation

4.5.10. Rogue AP

Rogue Access Point (Rogue AP) is a wireless access point that is either installed on a network by a legitimate user without authorization from the network administrator or created by an attacker to discover the confidential data. Airsnarf [Airs13b] and KARMA [Karm13] tools can be used in creating a simple rogue AP to steal usernames and passwords.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Internal Penetrator / Unauthorized
Scanning Technique:	None / Active
Spoofing Technique:	Frame
Attack Management:	Manual
Attack Rate:	Steady
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	Discovering confidential data

4.5.11. PS Poll Attacks

Power management is one of the critical features of wireless devices. IEEE 802.11 standard provides a power save (PS) mode to conserve the wireless node energy. Actually, before entering the power save mode, the wireless node informs the access point that it will go to the

sleeping state. At this state, the access point starts to buffer data that is destined to this node. When the wireless node wakes up, it checks the Traffic Indication Maps (TIM) [GuCh05], and sends power save (PS) poll frame to demand the buffered data (referenced by its MAC address). When the access point receives the poll message, it delivers the buffered data to this wireless node and subsequently discards the contents of its buffer. The attacker can exploit this vulnerability and spoofs a PS poll frame on behalf of the wireless node while it is in sleep state, and then hinders it from receiving the buffered data which is consequently discarded from the access point.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure
Access Privilege:	Unauthorized
Scanning Technique:	Passive
Spoofing Technique:	Frame
Attack Management:	
Attack Rate:	
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	DoS

4.5.12. RTS/CTS Attacks

Basically, RTS (request-to-send)/CTS (clear-to-send) mechanism [RCS03] is used to avoid frame collision among the wireless nodes. In RTS/CTS mechanism, a wireless sending node transmits RTS frame to a destination node, to reserve the radio link for the transmission. When the destination node receives the RTS request, it responds by CTS frame that confirms the reservation of the link. Using RTS and CTS frames, the radio link between the sending and receiving nodes will be reserved and all the nodes in the transmission range will be silent and refrained from using the link by the transmission duration that is determined by the value of NAV (Network Allocation Vector). The attacker can exploit the vulnerability of this mechanism to launch two types of denial of service attacks; RTS flood and CTS flood.

4.5.12.1. RTS Flood Attack

The attacker can send a great amount of RTS frames to the wireless nodes in the transmission range to block and hinder them from sending data. Sensor nodes in wireless sensor networks (WSNs) can be easily hacked by a flood of RTS frames, where the receiving node will respond by equivalent CTS frames and this may lead to exhausting its biasing power battery or preventing it from pursuing its normal operation.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure / Ad Hoc
Access Privilege:	Unauthorized
Scanning Technique:	
Spoofing Technique:	Frame
Attack Management:	Semi-Automatic
Attack Rate:	Steady
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	DoS

4.5.12.2. CTS Flood Attack

Also, the attacker can flood the stations in the range by periodic spurious CTS frames with the objective of forcing other nodes to update their NAV values and then preventing them from using the channel until the attacker stops transmitting the CTS frames.

Taxonomy Dimensions	Attack Classification
Network Mode:	Infrastructure / Ad Hoc
Access Privilege:	Unauthorized
Scanning Technique:	
Spoofing Technique:	Frame
Attack Management:	Semi-Automatic
Attack Rate:	Steady
Attack Collaboration:	Autonomous
Vulnerability:	Design flaws
Attack Objective:	DoS

Other wireless attacks and vulnerabilities have been classified in Appendix A. It is worth mentioning that some of wireless vulnerabilities that are registered in website Common Vulnerabilities and Exposures [Cvew13] are already exploited by some wireless attacks, and some others are merely registered weaknesses of some network devices and they are susceptible to be exploited by known attacks or under design attacks, such as FMS attack that was firstly an idea and cryptanalysis of WEP weaknesses by Fluhrer et al [FlMS01], and then it was realized by many hacking tools such as WEPCrack [Wepc13]and AirSnort [Airs13a]. As another example, the registered vulnerability CVE-2006-6059 [Cve06] describes the buffer overflow in the driver of NetGear MA521 PCMCIA adapter that may allow the attacker to execute arbitrary code via beacon or probe 802.11 frame responses with long supported rates. This vulnerability has been already exploited by an attack which is designed by the hack community as shown in the Metasploit module [Netg13]. In addition to our classification of some well-known wireless

attacks, we also analyzed, in Appendix A, some popular wireless vulnerabilities and studied the relevant attacks from the perspective of our taxonomy of wireless attacks. Even the existing vulnerabilities that are not yet exploited by specific attacks, we analyzed them and considered the potential attacks. Most of these vulnerabilities are relevant to specific wireless devices that are widely used in wireless networks. If the operating environment uses one or more of vulnerable devices, then their vulnerabilities and the relevant potential attacks should be taken into account to ensure a comprehensive evaluation of WIDSs. The potential attacks are considered by the representative attack test cases and their probabilities that ensure the fairness of the evaluation.

4.6. Test Cases Probability

The important aspect that should be taken into account is that each test case has probability of occurrence among all possible attacks in a specific network. Most previous evaluations of IDSs tested the IDSs under a set of selected attacks, and they calculated the detection rate according to this set of attacks. These evaluations are considered biased and unfair ones, where they calculated the detection rate by only the proportion of the selected attacks that are flagged as intrusions, although the selected attacks may not be representative of other potential attacks under the same conditions. Moreover, to the best of our knowledge, there is no IDSs evaluation took into account the probability of each attack or test case in calculating the detection rate, despite the importance of this concept in managing unbiased evaluation. In this study, we try to follow the best way towards unbiased and fair evaluation of WIDSs, where we extract the test cases of attacks to be representative of all the potential attacks relevant to each test case, and then we calculate the probability of each test case accordingly taking into account the conditions of the operating environment. This concept is considered the main factor in calculating the actual representative ratio of each test case among all the test cases. The significance of this concept is demonstrated in chapter 6.

4.7. Conclusion

The growing exploitation of the system vulnerabilities and enormous progress in hacking tools and techniques ranging from simple command lines to GUI tools necessitate combining the possible attacks under representative attack test cases. This chapter introduced a new taxonomy of wireless security attacks from the perspective of the WIDS evaluator. Our proposed taxonomy considered the essential dimensions without overkill or disregard, to finally have main categories that cover the existing attacks and novel attacks in the future. This taxonomy helps in extracting the representative attack test cases rather than evaluating the WIDSs under the all possible attacks. We also considered a new important concept of the probability of occurrence of attack test cases that was ignored in most previous work. This concept reflects the actual occurrence of possible attacks according to the operating environment conditions, and this is crucial in calculating the actual intrusion detection rate and effectiveness of IDSs/WIDSs.

V. Chapter 5: Evaluation Metrics

Evaluation metrics play a significant role in evaluating IDSs/WIDSs performance. Various appreciable efforts have been exerted in the recent past for developing reliable evaluation metrics. In this chapter, we discuss the most valuable and well-known metrics for IDSs evaluation, their benefits, and their drawbacks. The common conspicuous drawback of most existing metrics is building their main notion on the basis of comparing two or more IDSs to select the best one, although this selected one may be ineffective. We thus develop a novel metric called *intrusion detection effectiveness* (E_{ID}) that manipulates the drawbacks of the existing metrics for evaluating the IDSs/WIDSs effectiveness. Effectiveness attribute is considered the basic factor in evaluating the IDSs/WIDSs performance, where it reflects the ability of IDS to detect the intrusive activities against the monitored system, and the absence degree of the false alarms. Our developed metric E_{ID} helps in measuring the actual effectiveness of IDSs/WIDSs instead of measuring the relative effectiveness as followed by the previously proposed metrics. The notion of E_{ID} is based on comparing the operating curve of the IDS under test to the optimal operating curve (i.e., created as a zero reference curve for the optimal operating state) by calculating the variation between the two curves. The variation value interprets the deviation of the IDS operation from the intended optimal operation. We also propose another metric called *attack recognition rate* (R_R) that measures the proportion of the detected intrusions that are recognized.

5.1. An Overview of the Existing Evaluation Metrics

Many different evaluation metrics of IDSs performance have been proposed; most of them are concerned with the effectiveness attribute that is considered the main aspect in the evaluation of IDSs/WIDSs performance. Besides the well-known evaluation metric called *receiver operating characteristic* (*ROC*) curve that was used by DARPA evaluations [LFGH00] [LHFK00], there are other valuable metrics proposed for IDSs evaluating such as *Bayesian detection rate* ($P(I|A)$) [Axel99], *cumulative cost* [SFLP00], *expected cost* [GaUl01], *intrusion detection capability* (C_{ID}) [GFDL06], and *intrusion detection operating characteristic* (*IDOC*) [CaBS06]. Each of these metrics was based on a different theoretical approach such as *decision theory* [GaUl01], *information theory* [GFDL06], *cost-based analysis* [SFLP00] [GaUl01], etc. Some of these metrics have specific drawbacks, in addition to the common drawback which they all suffer from. We discuss the benefits and drawbacks of these metrics in the following sections,

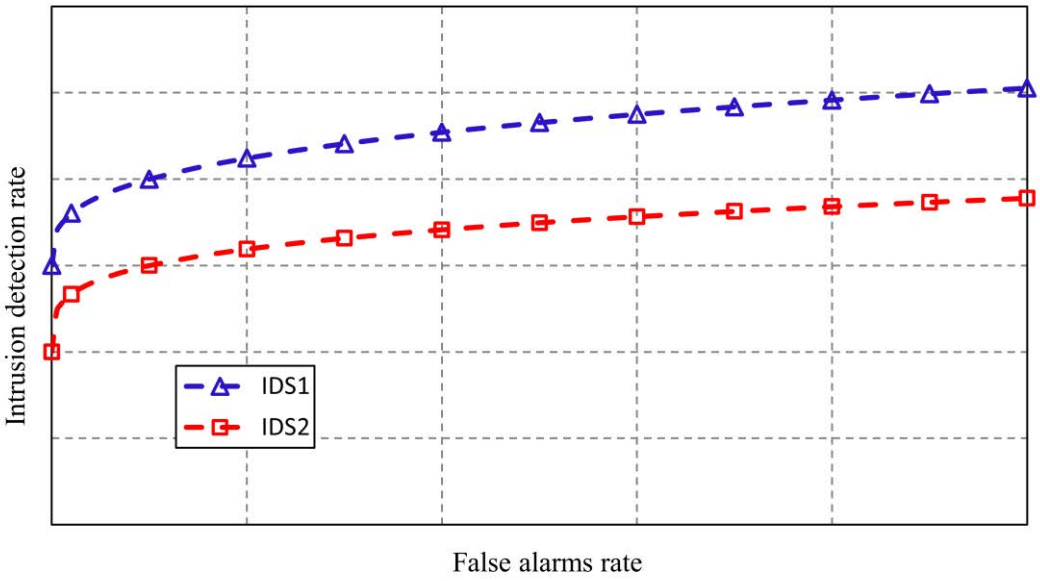

Figure V-1: *ROC* Curves of IDS1 and IDS2.

and we consequently propose a novel evaluation metric called *intrusion detection effectiveness* (E_{ID}) to manipulate the drawbacks of the previously proposed metrics.

5.1.1. Receiver Operating Characteristic (*ROC*)

Receiver operating characteristic (*ROC*) curve is the first unified metric used in the experimental evaluation of intrusion detection systems [LFGH00] [LHFK00]. *ROC* curve is used to analyze the trade-off between the *detection rate* and *false alarms rate*. *Detection rate* (*DR*) (i.e., also known as *true positive rate* (*TPR*)) is the proportion of the malicious activities that are flagged as intrusive by generated alarms, and *false alarms rate* (i.e., also known as *false positive rate* (*FPR*)) is the proportion of the benign activities that are flagged as intrusive with raised alarms. The *ROC* curve can be generated by plotting the *detection rate* and *false alarms rate* values associated with different IDS operating points. The main notion of using *ROC* curve in IDSs evaluation is based on comparing the IDSs curves to select the best one. For example, if we have two IDSs, e.g., IDS_1 and IDS_2, with two *ROC* curves which do not cross as shown in Figure V-1. Since IDS_1 with the upper *ROC* curve has higher values of *DR* than IDS_2 for every *FPR* values, then IDS_1 is considered better than IDS_2. As another example, if we have two IDSs, e.g., IDS_3 and IDS_4, with two *ROC* crossed curves as shown in Figure V-2. Then, it is difficult to differentiate between them on the basis of the curve level where the two curves interchange their levels. In this case the differentiation between the two IDSs is calculated on the basis of the area under each curve. *ROC* curve was initially used in the domains and applications concerned with signal detection [HaWi66] such as communications and radar, then it was applied successfully to

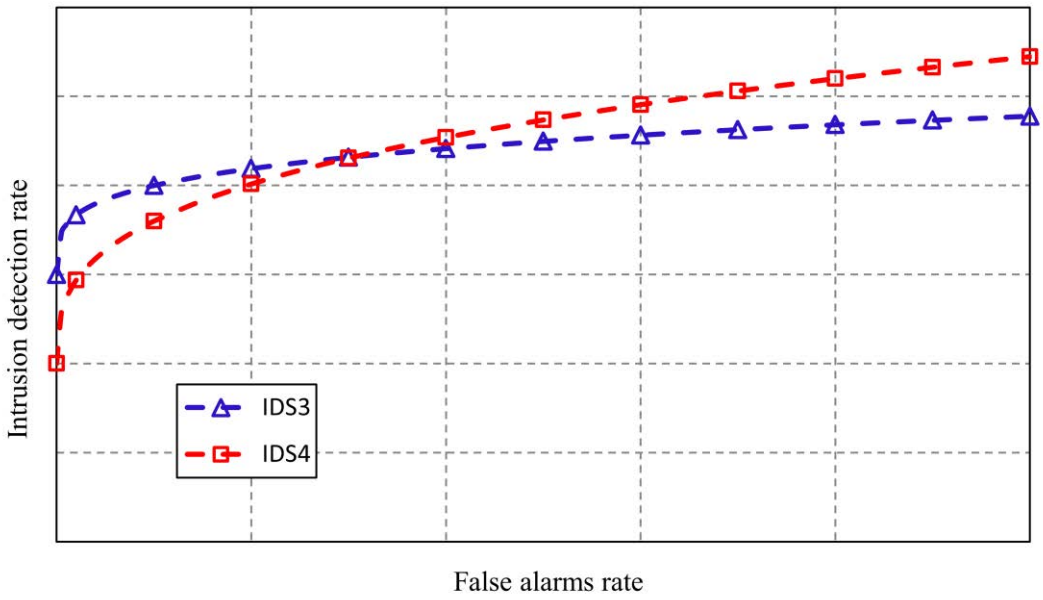

Figure V-2: *ROC* Curves of IDS3 and IDS4.

other fields. One the drawbacks of using *ROC* curve as an evaluation metric of IDSs effectiveness is that the IDSs effectiveness depends on more parameters than those considered in *ROC*. The important parameter that was ignored in *ROC* is the *base-rate* parameter [Axel99] that refers to the *probability of intrusion* $P(I)$ that reflects the hostility of the operating environment.

5.1.2. Bayesian Detection Rate (*P(I|A)*)

Bayesian detection rate $(P(I|A))$ [Axel99] defines a mathematical relation, in a unified equation, between the parameters related to intrusion detection effectiveness, i.e., *detection rate, false alarms rate,* and *base-rate*. The main advantage of this metric is its considering the *base-rate* or *intrusion probability* $(P(I))$ that was ignored in other evaluation metrics, despite its importance in achieving credible evaluation of IDSs/WIDSs effectiveness. Axelsson [Axel99] derived *Bayesian detection rate* $(P(I|A))$ from the Bayes' theorem as follows:

$$P(A|B) = \frac{P(A) \cdot P(B|A)}{P(B)} \qquad \textbf{Eq. V-1}$$

The probability $P(B)$ can be expanded for a set of n possible mutually exclusive outcomes A, then $P(B)$ can be defined by the following equation Eq. V-2:

$$P(B) = \sum_{i=1}^{n} P(A_i)\ .\ P(B|A_i) \qquad \textbf{Eq. V-2}$$

Combining the above two equations Eq. V-1and Eq. V-2 to reach to:

$$P(A|B) = \frac{P(A) \cdot P(B|A)}{\sum_{i=1}^{n} P(A_i)\ .\ P(B|A_i)} \qquad \textbf{Eq. V-3}$$

It was easy for Axelsson, by applying equation Eq. V-3 on the IDSs case with the two possible events, to get the *Bayesian detection rate* ($P(I|A)$) as follows:

$$P(I|A) = \frac{P(I) \cdot P(A|I)}{P(I) \cdot P(A|I) + P(\neg I) \cdot P(A|\neg I)} \qquad \textbf{Eq. V-4}$$

Where, *Bayesian detection rate* $P(I|A)$ (also known *as positive predictive value PPV*) is the posterior probability of an intrusion given the IDS output is an alarm, $P(I)$is the probability of intrusion, $P(\neg I)$ is the probability of no intrusion, $P(A|I)$ is the probability of the output is a generated alarm given an intrusion at the input (i.e., it refers to the detection rate *DR* or true positive rate *TPR*), $P(A|\neg I)$ the probability of the output is a generated alarm given no intrusion at the input (i.e., it refers to the false alarms or false positive rate *FPR*).

Axelsson studied the effect of the base-rate fallacy on the intrusion detection. He demonstrated that due to the base-rate fallacy problem, the limiting factor for the IDS performance is not the ability to correctly identify the intrusions, but rather its ability to suppress the false alarms. We totally agree with him in this point, where the effectiveness of IDSs/WIDSs depends not only on the ability of intrusion detection ability, but also on the absence degree of false alarms.

Unfortunately, despite the prominence of *Bayesian detection rate* and its considering the three main parameters $P(A|I), P(A|\neg I),$ and $P(I)$ that are significant for evaluating the IDSs effectiveness, it is not completely expressive metric for measuring the IDSs effectiveness or even the detection rate. Equation Eq. V-4 demonstrates that *Bayesian detection rate* $P(I|A)$ mainly measures the proportion of the generated alarms that correspond to intrusions. To prove that, we need to analyze mathematically $P(I|A)$ (Eq. V-4) to reach the following results:

***Case* 1**: if $P(A|I) = P(A|\neg I) = 1$

Combining these values with equation Eq. V-4, then;

$$P(I|A) = \frac{P(I)}{P(I) + P(\neg I)}$$

Since $P(I) + P(\neg I) = 1$, then;

$$P(I|A) = P(I) \qquad \textbf{Eq. V-5}$$

Case 2: if $P(A|I) = 0$

Combining this value and equation Eq. V-4, then;

$$P(I|A) = 0 \qquad \textbf{Eq. V-6}$$

We can observe that *Bayesian detection rate* $P(I|A)$ gives a reasonable expression for the IDSs effectiveness, just in the above two cases. In *case* 1 of passing all the traffic with raised alarms ($P(A|I) = P(A|\neg I) = 1$), $P(I|A)$ equals the probability of intrusion $P(I)$ (Eq. V-5) that is considered the perfect expression in this case; where the ratio of the detected intrusions to the generated alarms corresponds to the ratio of intrusions to the input traffic. In *case* 2, $P(I|A)$ equals zero when the *detection rate* $P(A|I)$ is zero (Eq. V-6), where the *detection rate* $P(A|I)$ is the predominant parameter in equation Eq. V-4. However, one of the drawbacks of *Bayesian detection rate* $P(I|A)$ can be observed when the *false alarms* or *false positive rate* $P(A|\neg I)$ is close to zero as shown in the following case.

Case 3: as *P(A|¬I)* approaches 0, then equation Eq. V-4 can be written as follows;

$$\lim_{P(A|\neg I)\to 0} P(I|A) = \lim_{P(A|\neg I)\to 0} \frac{P(I) \cdot P(A|I)}{P(I) \cdot P(A|I) + P(\neg I) \cdot P(A|\neg I)}$$

$$= \frac{P(I) \cdot P(A|I)}{P(I) \cdot P(A|I)} = 1 \qquad \textbf{Eq. V-7}$$

It is obvious from equation Eq. V-7 that when the *false positive rate* $P(A|\neg I)$ equals or approaches "0", the *Bayesian detection rate* $P(I|A)$ is equal to constant value "1" for any value of the *detection rate* $P(A|I)$; this unfortunately seems illogical. How the IDSs effectiveness can be evaluated in disregard of the *detection rate* $P(A|I)$? Merely considering the complete absence of false alarms is insufficient. Thus the *Bayesian detection rate* $P(I|A)$, in this case, is inexpressive metric for measuring the IDSs effectiveness or even the detection rate. However, we propose a reasonable solution for this drawback through our adaptation of *Bayesian detection*

Table V-1: Cost Types in Credit Card Fraud and Network Intrusion.

Cost Type	Credit Card Fraud	Network Intrusion
Damage	$tranamt(t)$	$DCost(service, attack)$
Challenge	*overhead*	*overhead*
Operational	*subsumed in overhead*	$OpCost$

rate to become *enhanced Bayesian detection rate* (EBD) (section 5.3.1.1) that is used as a base for our developed metric E_{ID} (*intrusion detection effectiveness*) shown in section 5.3.1.

5.1.3. Cost-Based Metrics

Cost-based metrics analyze the intrusion detection from the perspective of costs. We focus on studying two noted cost-based metrics; *Cumulative Cost* [SFLP00], and *Expected Cost* [GaUl01].

5.1.3.1. Cumulative Cost

The first cost-based metric for evaluating the fraud and intrusion detection in financial information systems is *Cumulative Cost* metric which was proposed by Stolfo et al. [SFLP00]. They defined three types of *costs*; *operational, damage,* and *challenge costs*. These costs are derived from the credit card fraud case. *Operational cost* refers to the resources needed to run the IDS. *Damage cost* is the amount of damage caused by the intrusions without detection. *Challenge cost* is the cost of acting upon an intrusion when it is detected. It is clearly observed that the *damage cost* indicates the false negatives (FN), and the *challenge cost* indicates the true positives (TP).

Stolfo et al. discussed and analyzed the results of JAM project [SPTL97]. Table V-1 illustrates their perspective on the three types of costs in credit card fraud and intrusion detection. In the credit card case, the damage cost is the amount of a fraudulent transaction that the bank losses and it is denoted by $tranamt(t)$. The challenge cost is the cost of acting upon an alarm and it is denoted by *overhead*, but the operational cost was not considered.

In the IDS case, the damage cost was characterized as a function that depends on the type of service and attack on that service, and it is denoted by $DCost(service, attack)$. The challenge cost, as considered in the credit card case, is the cost of acting on an alarm; also denoted by *overhead*. The operational cost is the feature costs and it is denoted by $OpCost$.

Stolfo et al. applied challenge and damage costs on the outcome parameters of intrusion detection (false negative (FN), false positive (FP), true positive (TP), and true negative (TN))

Table V-2: Cost Model for Connection.

Outcome	$Cost(c)$	
FN	$DCost(s,a)$	
FP	$Overhead$	$if\ DCost(s,a) > overhead$
	0	$if\ DCost(s,a) \leq overhead$
TP	$Overhead$	$if\ DCost(s,a) > overhead$
	$DCost(s,a)$	$if\ DCost(s,a) \leq overhead$
TN	0	

and added to them the operational cost to develop a $CumulativeCost(S)$ metric (Eq. V-8) to evaluate an IDS over some test set "*S*" of labeled connection "*c*".

$$CumulativeCost(S) = \sum_{c \in S} (Cost(c) + OpCost(c)) \qquad \textbf{Eq. V-8}$$

$Cost(c)$ is calculated by Table V-2, where $DCost(s,a)$ indicates the damage cost associated with the particular type of service "*s*" and attack "*a*".

This cost-based metric is more suitable for and applicable to financial information systems than other systems that are interested in other important impacts than the prior determining of the costs in the system. Also, this metric didn't consider the base-rate in the operating environment that indicates the hostility degree.

5.1.3.2. Expected Cost Metric

Another metric which takes the costs into account is the *expected cost* metric which was proposed by Gaffney et al. [GaUl01]. They argued that both the *ROC* analysis and *Cumulative Cost* metric are incomplete metrics. They used decision analysis techniques to combine and extend *ROC* analysis and cost-based analysis methods to provide an expected cost metric. The expected cost metric depends not only on the system *ROC* curve, but also on the IDS operational and damage costs, and hostility of the operating environment.

The formula of the expected cost metric can be derived from analyzing the decision tree shown in Figure V-3. This decision tree shows the sequence of actions (represented by squares) that describe the responses on the basis of the reports, the events (represented by circles) that may be a normal or intrusive event, and the consequences (corresponding costs) of the combinations of actions and events. The formula is derived for the minimum expected cost.

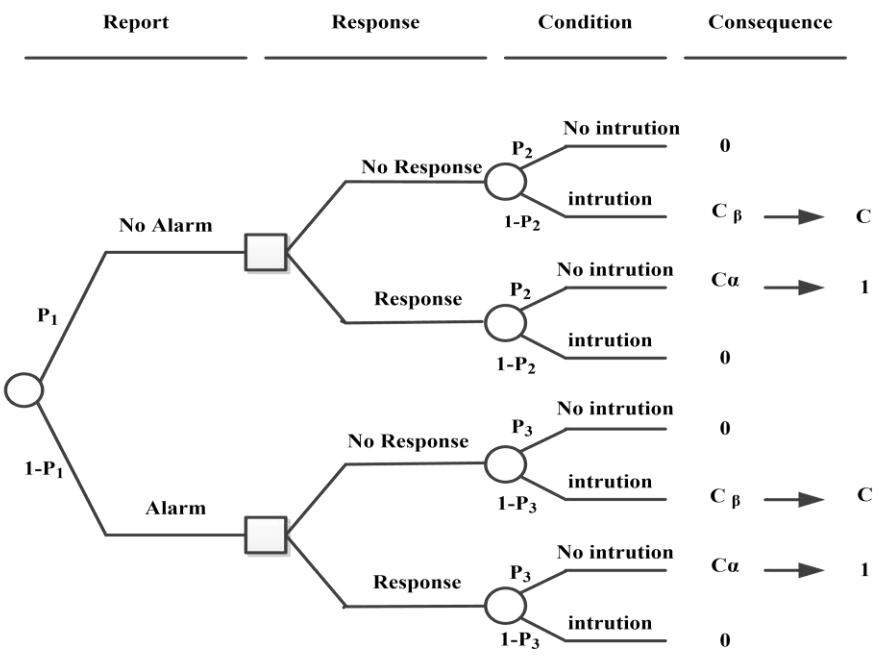

Figure V-3: Decision Tree of The Detectors Expected Cost.

There are three probabilities specified in the decision tree; P_1 is the probability of no generated alarm, P_2 is the conditional probability of no intrusion given that the detector reports no alarm, and P_3 is the conditional probability of no intrusion given that the detector reports an alarm. Consequences of the combinations of the system inputs and responses are specified by the costs. The cost of responding as though there is an intrusion when actually there is none is denoted by C_α. The cost of failing to respond to an intrusion is denoted by C_β. The costs of correct responses are assumed to be zero. Gaffney et al. rescaled costs and defined the cost ratio $C=C_\alpha/C_\beta$, thus this substitution results in costs of 1 and C as shown in Figure V-3. The conditional probabilities of the detector reports given the state of the system are shown in Table V-3. Then, the expected cost formula can be derived as follows.

$$P_1 = P(\neg A) = (1-\alpha)(1-\ P(I)) + \beta\ P(I)$$
$$1-\ P_1 = P(A) = \alpha(1-P(I)) + (1-\beta)\ P(I)$$
$$P_2 = P(\neg I \mid \neg A) = [(1-\alpha)(1-P(I))\ ]/[\ (1-\alpha)(1-P(I)) + \beta\ P(I)]$$
$$1-P_2 = P(I \mid \neg A) = \beta\ P(I)/[(1-\alpha)(1-P(I)) + \beta\ P(I)]$$
$$P_3 = P(\neg I \mid A)\ =\ \alpha(1-\ P(I))/[\alpha(1-\ P(I)) + (1-\beta)\ P(I)]$$
$$1-P_3 = P(I \mid A) = (1-\beta)\ P(I)/[\alpha(1-P(I)) + (1-\beta)\ P(I)]$$

Then, the expected cost (Eq. V-9) is:

Table V-3: Conditional Probabilities of the Detector Reports given the State of the System.

Detector Report	State of the system	
	No Intrusion ($\neg I$)	**Intrusion (I)**
No Alarm ($\neg A$)	$1-\alpha$	β
Alarm (A)	α	$1-\beta$

$$Expected\ Cost = Min\{C\beta P(I), (1-\alpha)(1-P(I))\} + Min\{C(1-\beta)P(I), \alpha(1-P(I))\} \quad \textbf{Eq. V-9}$$

5.1.4. Intrusion Detection Capability (C_{ID})

Gu et al.[GFDL06] proposed another evaluation metric called *intrusion detection capability* (C_{ID}). They argued that the main motivation for introducing this metric is that the cost measures in information security domain are often determined in a subjective way. Then, the authors proposed an information-theoretic measure of the intrusion detection capability as an objective metric. They depended on the notion of having less uncertainty about the IDS input given the IDS output. They introduced *intrusion detection capability* (C_{ID}) metric (Eq. V-10) as the ratio of the mutual information between IDS input and output, and the entropy of the input (as a normalization factor). The C_{ID} is maximized by calculating the operating point that minimizes the uncertainty of the input.

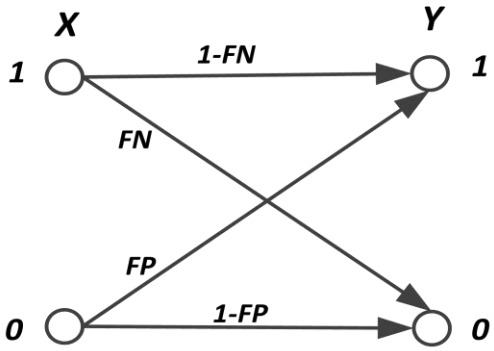

Figure V-4: Abstract Model for Intrusion Detection.

$$C_{ID} = \frac{I(X;Y)}{H(X)} = \frac{H(X) - H(X|Y)}{H(X)} \quad \textbf{Eq. V-10}$$

Where, $I(X;Y)$ is the mutual information that indicates the amount of information shared between the two random variables *X* and *Y*, and it can be defined as:

$$I(X;Y) = \sum_x \sum_y p(x,y) \log \frac{p(x,y)}{p(x)\,p(y)} \quad \textbf{Eq. V-11}$$

And $H(X)$ is the entropy (or self-information) of a discrete random variable *X*, and it is defined by:

$$H(X) = -\sum_x p(x) \log p(x) = -B \log B - (1-B) \log(1-B) \quad \textbf{Eq. V-12}$$

Where, *X* is a random variable represents the input of the IDS (*X=1* represents an intrusion, and *X=0* represents no intrusion), and *Y* a random variable indicates the output alarms of an IDS (*Y=1* indicates an alarm, and *Y=0* indicates no alarm). Figure V-4 shows the intrusion detection model that was used with this metric C_{ID}. It is worth mentioning that $p(x)$ and $p(y)$ are the probability of random variables *X*, and *Y* respectively, and $p(x,y)$ is the joint probability of them. Also, B denotes the base-rate ($P(I)$).

As for $H(X|Y)$, that is the entropy of X given Y, can be defined as follows:

$$\begin{aligned} H(X|Y) = -\sum_x \sum_y p(x)p(y|x) \log \frac{p(x)p(y|x)}{p(y)} &= -B(1-\beta)\log \frac{B(1-\beta)}{B(1-\beta)+(1-B)\alpha} \\ &- B\beta \log \frac{B\beta}{B\beta + (1-B)(1-\alpha)} - (1-B)(1-\alpha)\log \frac{(1-B)(1-\alpha)}{(1-B)(1-\alpha)+B\beta} \\ &- (1-B)\alpha \log \frac{(1-B)\alpha}{(1-B)\alpha + B(1-\beta)} \end{aligned} \quad \textbf{Eq. V-13}$$

Where β and α denote false negative rate and false positive rate respectively. The main advantage of this metric is that it takes into account all main parameters related to intrusion detection effectiveness.

Basically, information theory is the science of operations on data such as communications, data compression, and statistical signal processing. We believe that the notion of C_{ID} for minimizing the uncertainty of the input is practically inapplicable to the IDSs/WIDSs evaluation.

5.1.5. Intrusion Detection Operating Characteristic (*IDOC*)

Cardenas et al. [CaBS06] used the *Bayesian detection rate* $P(I|A)$ (Eq. V-4) and introduced another evaluation metric called *intrusion detection operating characteristic* (*IDOC*) as a trade-off curve between the *probability of intrusion detection* $P(A|I)$ and the *positive predictive value PPV* or $P(I|A)$. *IDOC* is basically derived from the *Bayesian detection rate* [Axel99]; just the graphical representation curves (which are based on the same equation Eq. V-4) are the main difference between the *IDOC* and Axelsson's proposal [Axel99]. Axelsson studied graphically the trade-off between the *PPV* and the *false alarms*, but Cardenas et al. [CaBS06] studied the trade-off between the *PPV* and the *probability of intrusion detection* to introduce the *IDOC*. As a consequence of the dependence of *IDOC* on the *Bayesian detection rate,* it carries all its drawbacks (section 5.1.2).

5.2. The Common Drawback of the Existing Metrics

The common drawback of most existing metrics is manifested in their main notion that is based on comparing two or more IDSs to select the best one, whereas this selected one may not be effective. This direct comparison between the IDSs is performed by the differentiation between the curves level, the area under the curves, or the values of the measured attributes or costs. This is considered a deficient approach that leads to measuring the *relative effectiveness* rather than the *actual effectiveness*. We are concerned with manipulating this drawback and the aforementioned ones.

5.3. Novel Evaluation Metrics

The second pivotal dimension in our methodology (chapter 3), which is the fundamental task in WIDSs evaluation process, is defining the evaluation metrics. In this section, we present two metrics for evaluating IDSs/WIDSs.

Before defining our developed metrics, it is important first to define some important requirements for reliable and satisfactory evaluation metrics:

- ***Meaningful***: Evaluation metrics should have a meaning that is easy to understand and makes sense [Long09].
- ***Quantifiable***: Evaluation metrics must be composed of quantitatively measurable variables.
- ***Expressive:*** Evaluation metrics should be expressive and sensitive to the parameters that reflect the IDS/WIDS performance.
- ***Relative:*** The formulas and equations of evaluation metrics should represent the relationship between the parameters in a relative form (not absolute).

- ***Unified.*** For each performance attribute, all the related parameters should be collected and defined in a unified metric; this facilitates the evaluation.

5.3.1. Intrusion Detection Effectiveness (E_{ID})

The logical approach for measuring the *actual effectiveness* is comparing the IDS under test to the optimal operating level (as a reference). We thus propose a new evaluation metric E_{ID} (*intrusion detection effectiveness*) that is based on the notion of comparing the operating curve of the IDS under test to the optimal operating curve (created as a zero reference curve *ZRC*) by calculating the variation between the two curves. The variation value interprets the deviation of the IDS from the intended optimal operation. We believe that the main parameters which the IDS effectiveness depends on are *detection rate, false alarms rate,* and *base-rate*. To realize the notion of E_{ID}, we need an expressive formula or equation that considers these parameters to be used as a base for E_{ID}. As a result of our research, we discovered that *Bayesian detection rate* (Eq. V-4) regards the needed parameters, but it is inappropriate as a base equation due to its drawback when the *false alarms* equals or approaches "0" (Eq. V-7). We thus manipulate this drawback to derive a new completely expressive formula called *enhanced Bayesian detection rate* (EBD) to become the base for E_{ID}.

5.3.1.1. Deriving *EBD* (Enhanced Bayesian Detection Rate)

As a brief summary of our analysis of *Bayesian detection rate* in section 5.1.2, in *Case* 1 ($P(A|I) = P(A|\neg I) = 1$) and *Case* 2 ($P(A|I) = 0$), *Bayesian detection rate* $P(I|A)$ gives a reasonable expression for the IDSs effectiveness, but it is inexpressive in *Case* 3 when $P(A|\neg I)$ equals or approaches "0". Consequently, we are concerned with manipulating *Case* 3 to make *Bayesian detection rate* an expressive metric in this case. By analyzing *Case* 3, we found that the logical expressive formula for *Bayesian detection rate* in the absence of *false alarms* should be equal to the *detection rate* $P(A|I)$. This can be achieved by modifying the denominator of equation Eq. V-7 to produce the following new formula.

$$\lim_{P(A|\neg I)\to 0} P(I|A) = \lim_{P(A|\neg I)\to 0} \frac{P(I)\cdot P(A|I)}{P(I)\cdot P(A|I)_{\rightsquigarrow=1} + P(\neg I)\cdot P(A|\neg I)}$$

$$= \frac{\cancel{P(I)}\cdot P(A|I)}{\cancel{P(I)}\cdot P(A|I)_{\rightsquigarrow=1}} = P(A|I) \qquad \textbf{Eq. V-14}$$

From equations Eq. V-4 and Eq. V-14, *Case* 1 (Eq. V-5), and *Case* 2 (Eq. V-6), we can produce a new *Bayesian detection rate* that is completely expressive metric under all the operating conditions. We called this new formula *enhanced Bayesian detection rate* (EBD) (Eq. V-15).

$$EBD = \frac{P(I) \cdot P(A|I)}{P(I) + P(\neg I) \cdot P(A|\neg I)} \qquad \textbf{Eq. V-15}$$

Property 1

Enhanced Bayesian detection rate (EBD) can be defined as the posterior probability of detected intrusion (TP) given the total output of intrusion-related responses ($TP + FN$) and false alarms (FP).

Proof

The intrusion detection can be summarized by the simple model shown in Figure V-5, where I, $\neg I$, A, $\neg A$, TP, FP, FN, and TN denote *intrusion, normal traffic, alarm, no alarm, true positive, false positive, false negative,* and *true negative* respectively.

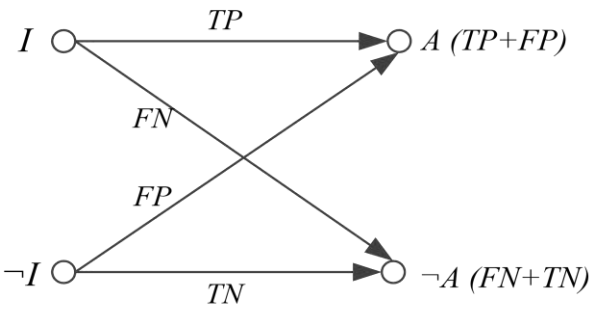

Figure V-5: Intrusion Detection Model.

Basically,

$P(I) = I/(\neg I + I)$

$P(\neg I) = \neg I/(\neg I + I)$

$P(A|I) = TP/I = TP/(TP + FN)$

$P(A|\neg I) = FP/\neg I = FP/(FP + TN)$

Recalling equation Eq. V-15 and solving it by the parameters of intrusion detection model (Figure V-5), then;

$$EBD = \frac{P(I) \cdot P(A|I)}{P(I) + P(\neg I) \cdot P(A|\neg I)} = \frac{1}{\frac{1}{P(A|I)} + \frac{P(\neg I) \cdot P(A|\neg I)}{P(I) \cdot P(A|I)}}$$

$$= \frac{1}{\frac{TP + FN}{TP} + \frac{\cancel{\neg I} \cdot FP / \cancel{(FP + TN)}}{\cancel{I} \cdot TP / \cancel{(TP + FN)}}} = \frac{TP}{TP + FN + FP} \qquad \textbf{Eq. V-16}$$

Equation Eq. V-16 shows the significance of *enhanced Bayesian detection rate* (EBD) for measuring the proportion of the intrusion-related responses ($TP + FN$) and false alarms (FP) that correspond to the detected intrusions (TP). This is considered one of the great advantages of *enhanced Bayesian detection rate* (EBD) over *Bayesian detection rate* $P(I|A)$ that disregards the *false negatives* (*FN*) parameter, as demonstrated in the following.

We can analyze *Bayesian detection rate* $P(I|A)$, in the same way, by recalling equation Eq. V-4 and solving it by the parameters of intrusion detection model (Figure V-5), then;

$$P(I|A) = \frac{P(I) \cdot P(A|I)}{P(I) \cdot P(A|I) + P(\neg I) \cdot P(A|\neg I)} = \frac{1}{1 + \frac{P(\neg I) \cdot P(A|\neg I)}{P(I) \cdot P(A|I)}}$$

$$= \frac{1}{1 + \frac{\cancel{\neg I} \cdot FP / \cancel{(FP + TN)}}{\cancel{I} \cdot TP / \cancel{(TP + FN)}}} = \frac{TP}{TP + FP} \qquad \textbf{Eq. V-17}$$

From Equation Eq. V-17, *Bayesian detection rate* $P(I|A)$ represents the proportion of the generated alarms that correspond to intrusions. This interprets the notion of *Bayesian detection rate* that is related to the *Positive Predictive Value* (*PPV*) which is defined as the posterior probability of an intrusion given the IDS output is an alarm. Then, *Bayesian detection rate* ignores the *FN* parameter that boosts the expressiveness of the metrics concerned with the IDSs effectiveness.

To clarify more the benefit of EBD over $P(I|A)$ about taking the whole *false responses* ($FP + FN$) into account, the relationships between the IDS's input and output events are depicted through Venn diagram as shown in Figure V-6. The intersections between the different events are represented by the areas denoted by numbers from 1 to 4. Area 1 represents the tranquil area of no intrusion and no alarm, but areas 2, 3 and 4 represent the challenge areas of false responses (area 2 and 4) and detected intrusions (area 3). These events in areas 2, 3 and 4 have a great significance in evaluating the IDSs effectiveness, where the intrusion detection and false responses are considered the main limitations and challenges of the effectiveness attribute.

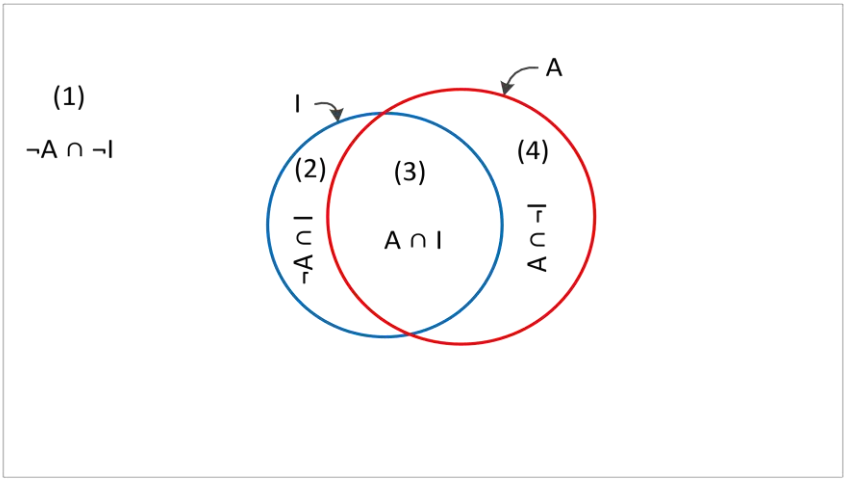

Figure V-6: The Relationships between the IDS's Input and Output Events.

Thus, they should be represented by the evaluation metric. This is attained by enhanced Bayesian detection rate (EBD) as shown in equation Eq. V-16. On the other hand, *Bayesian detection rate* $P(I|A)$ considers only areas 3 and 4 of the detected intrusions and false positives only.

Property 2

EBD is an expressive metric under different operating conditions.

Proof

***Case* 1**: if $P(A|I) = P(A|\neg I) = 1$

Combining these values with equation Eq. V-15, then;

$$EBD = \frac{P(I)}{P(I) + P(\neg I)}$$

Since $(I) + P(\neg I) = 1$, then;

$$EBD = P(I) \qquad \textbf{Eq. V-18}$$

Equation Eq. V-18 shows that EBD presents the intrusion probability $P(I)$ in the case of passing all the traffic (intrusive and normal) with raised alarms ($P(A|I) = P(A|\neg I) = 1$). $P(I)$ represents the logical expressive formula in this case, where it matches the proportion of the generated alarms that correspond to intrusions.

***Case* 2**: if $P(A|I) = 0$
Combining this value and equation Eq. V-15, then;

$$EBD = 0 \qquad \textbf{Eq. V-19}$$

Equation Eq. V-19 shows that EBD equals "0" when the *detection rate* $P(A|I)$ is "0". This is considered the expressive result in this case, where logically the IDS is considered ineffective when it is unable to detect the intrusions.

Case 3: as $P(A|\neg I)$ approaches 0, then equation Eq. V-15 can be written as;

$$\lim_{P(A|\neg I)\to 0} EBD = \lim_{P(A|\neg I)\to 0} \frac{P(I)\cdot P(A|I)}{P(I) + P(\neg I)\cdot P(A|\neg I)} = \frac{P(I)\cdot P(A|I)}{P(I)}$$

$$= P(A|I) \qquad \textbf{Eq. V-20}$$

As shown in equation Eq. V-20, EBD is equal to the *detection rate* $P(A|I)$ in the case of the absence of false alarms ($P(A|\neg I)$ equals or approaches "0"). $P(A|I)$, which refers to the proportion of intrusions that are detected, is the expressive formula for the IDSs effectiveness in this case.

***Case* 4**: if $P(A|\neg I) = 1$
Combining this value with equation Eq. V-15, then;

$$EBD = \frac{P(I)\cdot P(A|I)}{P(I) + P(\neg I)}$$

Since $(I) + P(\neg I) = 1$, then;

$$EBD = P(I)\cdot P(A|I) = \frac{\cancel{I}}{(\neg I + I)}\cdot\frac{TP}{\cancel{I}} = \frac{TP}{TP + FN + FP} \qquad \textbf{Eq. V-21}$$

Equation Eq. V-21 demonstrates the expressiveness of EBD in the worst case of *false alarms* ($P(A|\neg I) = 1$).

***Case* 5:** if $P(A|I) = 1$

Combining this value with equation Eq. V-15, then;

$$EBD = \frac{P(I)}{P(I) + P(\neg I) \cdot P(A|\neg I)} = \frac{1}{1 + \frac{P(\neg I) \cdot P(A|\neg I)}{P(I)}}$$

$$= \frac{1}{1 + \frac{\cancel{\neg I} \cdot FP / \cancel{(FP + TN)}}{TP}} = \frac{TP}{TP + FP} \qquad \textbf{Eq. V-22}$$

As shown in equation Eq. V-22, EBD equals the proportion of the generated alarms that correspond to the detected intrusions. This is the expressive formula in this case of the absence of false negatives ($P(A|I) = 1 \Leftrightarrow FN = 0$).

Equations Eq. V-18, Eq. V-19, Eq. V-20, Eq. V-21, and Eq. V-22 show that *enhanced Bayesian detection rate* (EBD) is an expressive metric for measuring IDSs effectiveness under different operating conditions.

5.3.1.2. Deriving E_{ID} (Intrusion Detection Effectiveness)

Following the main notion of our metric E_{ID} (as mentioned in section 5.3.1), we consider the trade-off between *EBD* and $P(\neg I)$ that helps in developing the more expressive metric E_{ID}. To simplify dealing with *EBD* (Eq. V-15), we adapt it to be a function of $P(\neg I)$ as shown in equation Eq. V-23. The first step in deriving E_{ID} is calculating and plotting the *zero reference curve* (*ZRC*) (i.e., *optimal operating curve*) as a trade-off between *EBD* and $P(\neg I)$ with assumption of the optimal operating case of the IDS under test.

$$EBD = \frac{P(A|I) - P(\neg I) \cdot P(A|I)}{1 - P(\neg I) \cdot (1 - P(A|\neg I))} \qquad \textbf{Eq. V-23}$$

To clarify the idea of calculating and plotting *ZRC,* we assume that we have an IDS under test in an operating environment with hostility or probability of intrusion $P(I)$=3*10^{-4}, then the probability of no intrusion (benign traffic) $P(\neg I) = 1 - P(I) = 0.9997$. First, we assume that the IDS (under test) operates at the optimal case with perfect *detection rate* ($P(A|I)$=1) and complete absence of false positive rate ($P(A|\neg I) = 0$). We use these values to plot *ZRC* (Figure V-7) that is a straight line represents the optimal operating case. The second step, we plot the real operating curve of the IDS under test with the actual values of *detection rate* and *false positive rate*; we assume their values $P(A|I) = 0.8$ and $P(A|\neg I) = 0.0095$. Now we have two

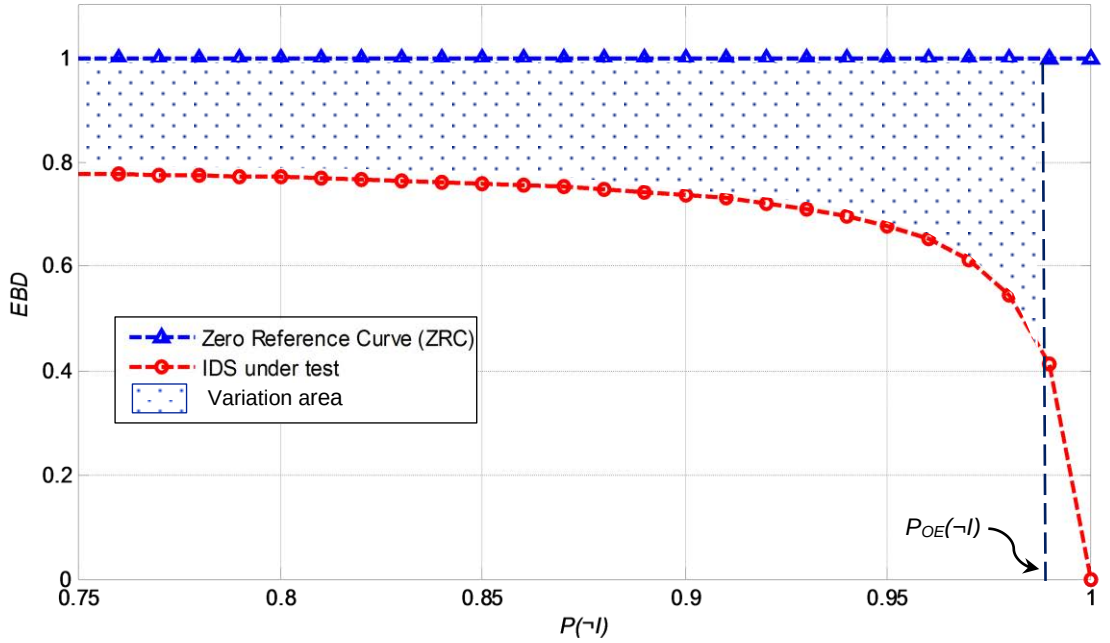

Figure V-7: The Trade-off between *EBD* and *P*(¬*I*).

operating curves; one as a zero reference curve (*ZRC*) for the optimal operation and another represents the real operating curve (Figure V-7). The variation between the two curves is represented by the dotted area. $P_{OE}(\neg I)$ denotes the probability of no intrusion in the operating environment, and it refers to the upper limit of the variation area.

We normalize this variation by the area under *ZRC* (only through $P(\neg I) = [0,\ P_{OE}(\neg I)]$) to have a representative metric E_{ID} of values in the range [0,1]; where "0" indicates zero deviation and then high effectiveness, but "1" indicates the maximum deviation from the intended optimal operation, then zero effectiveness. E_{ID} is represented by equation Eq. V-24, where EBD_{ZRC}, $P_{ZRC}(A|I)$, and $P_{ZRC}(A|\neg I)$ denote *EBD*, detection rate, and false alarms of *ZRC* respectively. Also, EBD_{ID}, $P_{ID}(A|I)$, and $P_{ID}(A|\neg I)$ denote *EBD*, detection rate, and false alarms of IDS under test respectively. $P(\neg I)$ is considered the integration variable.

$$E_{ID} = \frac{1}{\int_0^{P_{OE}(\neg I)} EBD_{ZRC}\, dP(\neg I)} \left(\int_0^{P_{OE}(\neg I)} EBD_{ZRC}\, dP(\neg I) - \int_0^{P_{OE}(\neg I)} EBD_{ID}\, dP(\neg I) \right) \quad \textbf{Eq. V-24}$$

Where,

$$EBD_{ZRC} = \frac{P(I) \cdot P_{ZRC}(A|I)_{\rightsquigarrow=1}}{P(I) + P(\neg I) \cdot P_{ZRC}(A|\neg I)_{\rightsquigarrow=0}} = 1 \quad \textbf{Eq. V-25}$$

$$EBD_{ID} = \frac{P_{ID}(A|I) - P(\neg I) \cdot P_{ID}(A|I)}{1 - P(\neg I) \cdot (1 - P_{ID}(A|\neg I))} \quad \textbf{Eq. V-26}$$

Then equation Eq. V-24 becomes;

$$E_{ID} = 1 - \frac{\int_0^{P_{OE}(\neg I)} EBD_{ID}\, dP(\neg I)}{P_{OE}(\neg I)} \quad \textbf{Eq. V-27}$$

Integration of EBD_{ID} can be solved according to the following integral formulas [ZiWr12].

$$\int \frac{c}{b + ax}\, dx = \frac{c}{a} ln\,|b + ax| \quad \textbf{Eq. V-28}$$

$$\int \frac{x}{b + ax}\, dx = \frac{x}{a} - \frac{b}{a^2} ln\,|b + ax| \quad \textbf{Eq. V-29}$$

Then;

$$\int_0^{P_{OE}(\neg I)} EBD_{ID}\, dP(\neg I) = P_{ID}(A|I)\left(\frac{1}{-\left(1-P_{ID}(A|\neg I)\right)} ln|1 - P(\neg I) \cdot (1 - P_{ID}(A|\neg I))| + \frac{P(\neg I)}{\left(1-P_{ID}(A|\neg I)\right)} + \frac{1}{\left(1-P_{ID}(A|\neg I)\right)^2} ln\left|1 - P(\neg I) \cdot \left(1 - P_{ID}(A|\neg I)\right)\right|\right)\Big|_0^{P_{OE}(\neg I)} =$$

$$\frac{P_{ID}(A|I)}{\left(1-P_{ID}(A|\neg I)\right)}\left(\left(\frac{1}{\left(1-P_{ID}(A|\neg I)\right)} - 1\right) ln|1 - P(\neg I) \cdot (1 - P_{ID}(A|\neg I))| + P(\neg I)\right)\Big|_0^{P_{OE}(\neg I)} =$$

$$\frac{P_{ID}(A|I)}{\left(1-P_{ID}(A|\neg I)\right)}\left(\left(\frac{1}{\left(1-P_{ID}(A|\neg I)\right)} - 1\right) ln|1 - P_{OE}(\neg I) \cdot (1 - P_{ID}(A|\neg I))| + P_{OE}(\neg I)\right)$$

Then equation Eq. V-27 of E_{ID} (*intrusion detection effectiveness*) becomes;

$$E_{ID} = 1 - \frac{P_{ID}(A|I) \cdot \left(P_{OE}(\neg I) + \left(\frac{1}{\left(1 - P_{ID}(A|\neg I)\right)} - 1\right) ln|1 - P_{OE}(\neg I) \cdot (1 - P_{ID}(A|\neg I))|\right)}{P_{OE}(\neg I) \cdot \left(1 - P_{ID}(A|\neg I)\right)} \quad \textbf{Eq. V-30}$$

Property 3

E_{ID} is an expressive metric for measuring the actual effectiveness of IDSs by values in the range [0,1], where "0" indicates the ideal case and supreme effectiveness, but "1" indicates the worst case of zero effectiveness.

Proof

***Case* 1**: when the IDS (under test) detects all the intrusive traffic ($P(A|I) = 1$) and generates no false alarm ($P(A|\neg I) = 0$), its deviation from the optimal operating case can be measured by equation Eq. V-30, as follows;

$$E_{ID} = 1 - \frac{P_{ID}(A|I)_{\rightsquigarrow=1} \cdot (P_{OE}(\neg I) + 0)}{P_{OE}(\neg I) \cdot (1 - P_{ID}(A|\neg I)_{\rightsquigarrow=0})} = 1 - \frac{\cancel{P_{OE}(\neg I)}}{\cancel{P_{OE}(\neg I)}} = 0 \qquad \textbf{Eq. V-31}$$

Equation Eq. V-31 demonstrates the supreme effectiveness of the IDS by its zero deviation from the optimal operating case.

***Case* 2**: when the IDS (under test) detects no intrusion ($P(A|I) = 0$), its deviation from the optimal operating case can be measured by equation Eq. 30 as follows;

$$E_{ID} = 1 - \frac{0}{P_{OE}(\neg I) \cdot \left(1 - P_{ID}(A|\neg I)\right)} = 1 \qquad \textbf{Eq. V-32}$$

Equation Eq. V-32 demonstrates the maximum deviation of the IDS from the optimal operating case and consequently the ineffectiveness of the IDS. It is the logic result for the idle IDS.

It becomes clear from equations Eq. V-31 and Eq. V-32 that E_{ID} is expressive metric for the actual effectiveness of wired or wireless IDSs.

5.3.1.3. Verifying the utility of E_{ID}

This section demonstrates the utility of E_{ID} over the existing metrics under different operating conditions. We start by analyzing the trade-off between E_{ID} and the *intrusion detection rate* $P_{ID}(A|I)$ under different conditions of *false alarms* $P_{ID}(A|\neg I)$ and *intrusion probability* ($P(I)$). To clarify well the relationship between E_{ID} and $P_{ID}(A|I)$, we consider two cases of *intrusion probability* or *hostility of the operating environment* ($P(I) = 1 - P_{OE}(\neg I)$), along with different values of false alarms $P_{ID}(A|\neg I)$ in each case.

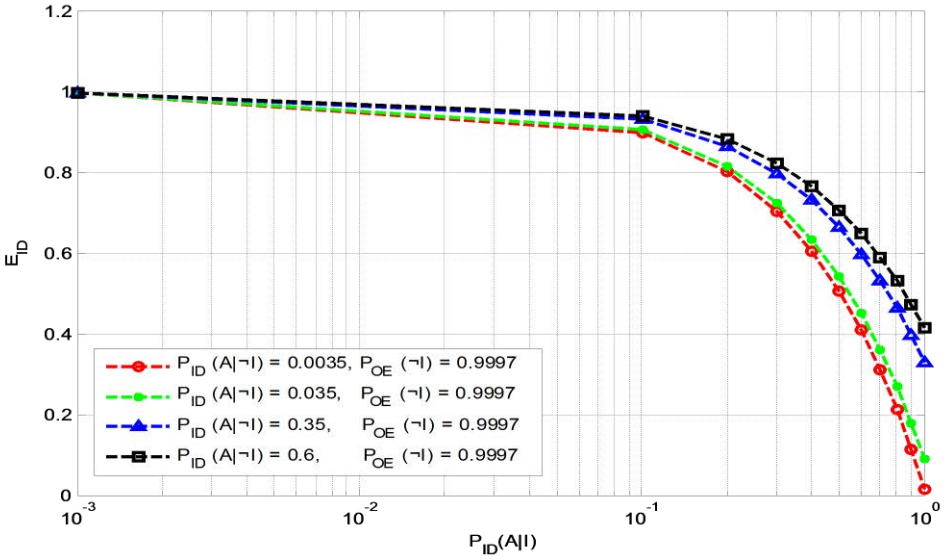

Figure V-8. Case 1 of the Trade-off between E_{ID} and $P_{ID}(A|I)$.

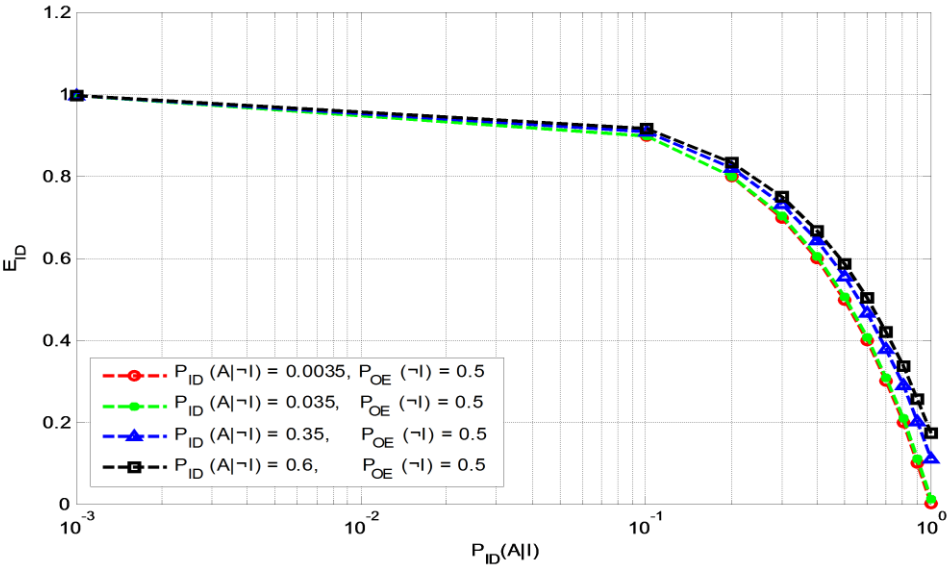

Figure V-9: Case 2 of the Trade-off between E_{ID} and $P_{ID}(A|I)$.

In the first case, we assume an operating environment with little hostility or intrusion probability ($P(I) = 0.0003$), then $P_{OE}(\neg I) = 0.9997$. We consider four different values of false alarms starting from very small value ($P_{ID}(A|\neg I) = 0.0035$) until approximately half of the benign traffic ($P_{ID}(A|\neg I) = 0.6$). This case is described graphically in Figure V-8 that shows the inverse proportion of E_{ID} to $P_{ID}(A|I)$. We can observe that E_{ID} approaches "1" as $P_{ID}(A|I)$ approaches "0", and this proves the aforementioned property and notion of E_{ID} where it measures the deviation of the IDS under test from the optimal operating case. E_{ID} decreases as $P_{ID}(A|I)$

increases with obvious negative slope, especially as $P_{ID}(A|I) \geq 0.1$. The variation between the curves (Figure V-8) increases as $P_{ID}(A|I)$ and $P_{ID}(A|\neg I)$ increase, and it is obvious when $P_{ID}(A|I) \geq 0.1$. We can also observe that the variation between the curves is slight for the small values of false alarms ($P_{ID}(A|\neg I) = [0.0035, 0.035]$), and this explains the slight effect of the small values of false alarms. This agree with important truth, where there is no real system with zero false alarms, but any real system considers an acceptable level of false alarms that is usually very small and does not obstruct the overall system operation. This proves another important feature of E_{ID}, where it reflects mathematically the real effect of false alarms. We need to study the variation between these curves when the hostility of the operating environment increases to approximately fifty percent; this will be discussed in the following case.

In the second case, we assume that the intrusion probability ($P(I) = 0.5$), then $P_{OE}(\neg I) = 0.5$. We also consider the same values of false alarms considered in the first case ($P_{ID}(A|\neg I) = [0.0035, 0.035, 0.35, 0.6]$). Figure V-9 shows the same principle of inverse proportion of E_{ID} to $P_{ID}(A|I)$ and approximately the same slopes of the curves. We can observe that the variation between the curves for the very small values of false alarms ($P_{ID}(A|\neg I) = [0.0035, 0.035]$) is nearly neglected, and it increases as $P_{ID}(A|I)$ and $P_{ID}(A|\neg I)$ increase but not by the same ratio of variation as the first case. This interprets the very slight or neglected effect of small values of false alarms with high hostility of the operating environment. This also prove the importance of considering the base-rate parameter ($P(I)$) in E_{ID} and its effect in evaluating the IDSs effectiveness.

For more comprehensive understanding of the utility of E_{ID}, we need to study it versus the false alarms $P_{ID}(A|\neg I)$. We consider here also two cases of *intrusion probability* along with different values of intrusion detection rate $P_{ID}(A|I)$ in each case.

In the first case, we assume an operating environment with little hostility or intrusion probability ($P(I) = 0.0003$), then $P(\neg I)_{OE} = 0.9997$. We consider also four different values of intrusion detection rates ($P_{ID}(A|I) = [0.2, 0.4, 0.6, 0.8]$). Figure V-10 shows the direct proportion of E_{ID} to $P_{ID}(A|\neg I)$. E_{ID} approaches $(1 - P_{ID}(A|I))$ as $P_{ID}(A|\neg I)$ approaches "0", and this interprets one of the important features of E_{ID} where it does not ignore the detection rate in the case of complete absence of false alarms as followed by *Bayesian detection rat*e (Eq. V-7), but it considers this case and calculates the IDS effectiveness accordingly $(1 - P_{ID}(A|I))$. This proves another aspect of the utility of E_{ID} and how it is expressive metric. From Figure V-10, we can observe that the slopes of the curves increase positively as $P_{ID}(A|\neg I)$ and $P_{ID}(A|I)$ increase, especially when $P_{ID}(A|\neg I) \geq 0.1$. This interprets the considerable effect of high values of $P_{ID}(A|\neg I)$ and $P_{ID}(A|I)$. We need to study these conditions with high hostility of the operating environment.

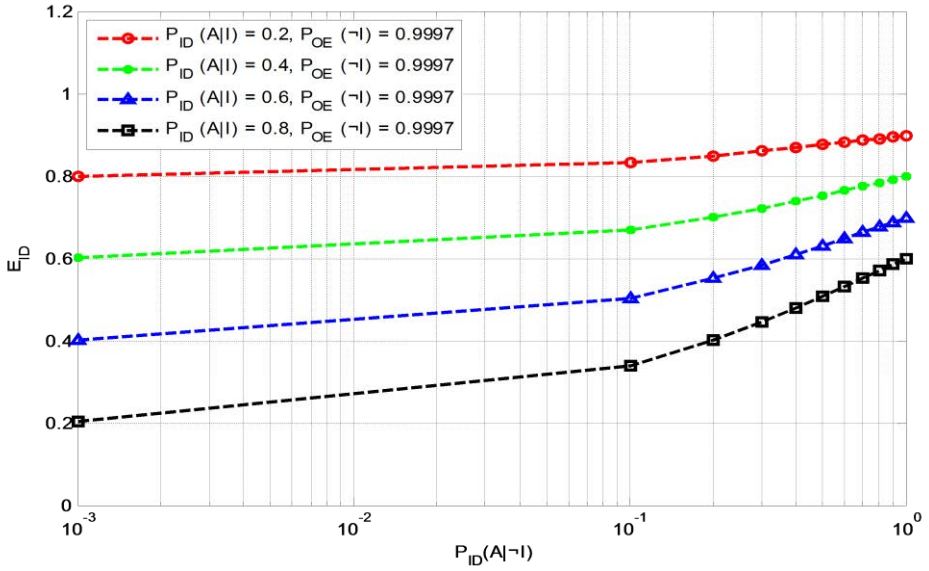

Figure V-10. Case 1 of the Trade-off between E_{ID} and $P_{ID}(A|\neg I)$.

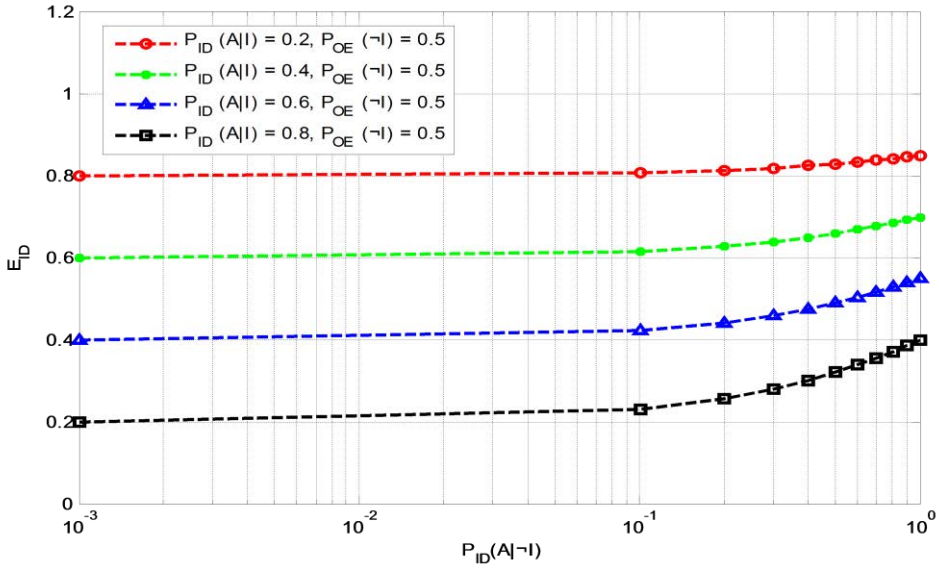

Figure V-11. Case 2 of the Trade-off between E_{ID} and $P_{ID}(A|\neg I)$.

In the second case, we assume that the intrusion probability ($P(I) = 0.5$), then $P_{OE}(\neg I) = 0.5$. We also take into account the same values of the detection rate considered in the first case. Figure V-11 shows the same principle of discussed in the first case, the slopes of the curves increase as $P_{ID}(A|\neg I)$ and $P_{ID}(A|I)$ increase, especially when $P_{ID}(A|\neg I) \geq 0.1$, but not in the same manner where increasing the intrusion probability decreases the effect of $P_{ID}(A|\neg I)$. This concept can be clarified well by analyzing the trade-off between E_{ID} and the environment hostility as shown in Figure V-12. The relationship between them is studied under different

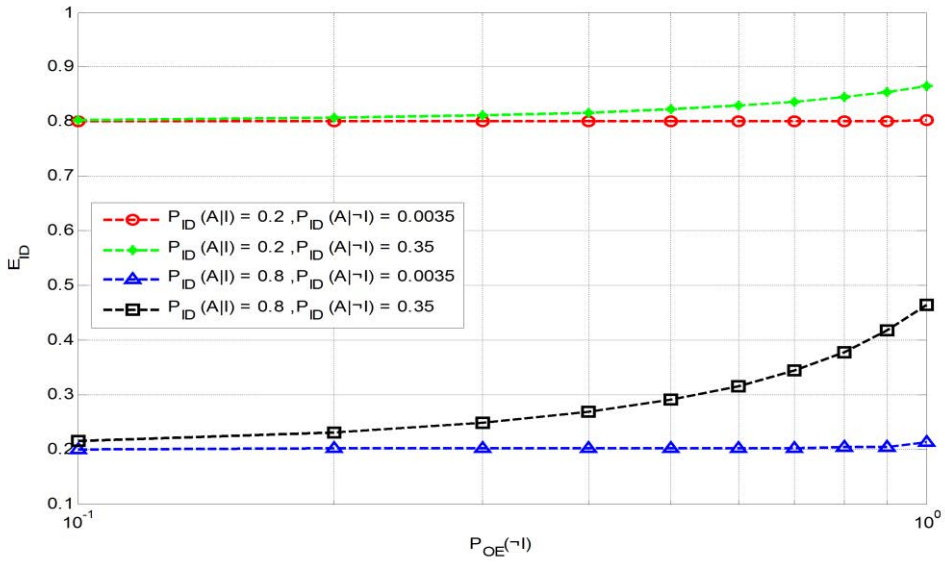

Figure V-12. The Trade-off between E_{ID} and $P_{OE}(\neg I)$.

values of $P_{ID}(A|I)$ and $P_{ID}(A|\neg I)$. We can observe that the slopes of the curves decrease as the environment hostility increases. Also, the slopes of the curves depend largely on $P_{ID}(A|\neg I)$ that has a neglected effect in the very small values. The above studied cases show the importance of considering the three main parameters $P_{ID}(A|I)$, $P_{ID}(A|\neg I)$, and $P(I)$ in the evaluation of IDSs/WIDSs effectiveness, and prove the utility of E_{ID} and how it is an expressive metric. To clarify more the utility of E_{ID}, we suppose the following examples.

***Example 1*:** applying E_{ID} on the above supposed example of the IDS under test with $P_{ID}(A|I) = 0.2$, $P_{ID}(A|\neg I) = 0.0035$, and $P_{OE}(\neg I) = 0.9997$, then;

$$E_{ID} = 1 - 0.1967 = 0.8033$$

E_{ID} value indicates the great deviation of the IDSs operation from the intended optimal operation, then it is not more effective.

***Example 2*:** if we manage, under the same environment hostility ($P(I) = 1 - P_{OE}(\neg I)$) $\Leftrightarrow P_{OE}(\neg I) = 0.9997$, another evaluation of an IDS with results $P_{ID}(A|I) = 0.2$ and $P_{ID}(A|\neg I) = 0.35$, then;

$$E_{ID} = 1 - 0.1338 = 0.8662$$

This value of E_{ID} indicates more deviation of the IDS from the intended optimal operation, due to the increase in the false alarms. This interprets the effect of false alarms in measuring the effectiveness by E_{ID}.

***Example 3*:** we suppose, under the same environment conditions $P_{OE}(\neg I) = 0.9997$, a tested IDS with results $P_{ID}(A|I) = 0.8$ and $P_{ID}(A|\neg I) = 0.35$, then;

$$E_{ID} = 1 - 0.5352 = 0.4648$$

It is easy to observe that the IDS has approximately medium effectiveness, despite the high value of the detection rate. This also interprets the effect of false alarms in measuring the effectiveness by E_{ID}.

***Example 4*:** in this example, we assume the same IDS in the example 3 ($P_{ID}(A|I) = 0.8$ and $P_{ID}(A|\neg I) = 0.35$), but under different environment conditions $P_{OE}(\neg I) = 0.555$, then;

$$E_{ID} = 1 - 0.6965 = 0.30352$$

Comparing example 3 and example 4, we can observe the little effect of false alarms as the environment hostility increased. This also reflects the effect of environment hostility in measuring the effectiveness by E_{ID}.

5.3.2. Attack Recognition Rate

Also, the attack type recognition attribute can be represented by a metric R_R (*attack recognition rate*) which measures the proportion of the detected intrusions that are recognized. *TP* (true positive*)* and TP_R (recognized true positive) denote the truly detected intrusions and the recognized ones respectively.

$$R_R = \frac{TP_R}{TP} \qquad \textbf{Eq. V-33}$$

5.4. Conclusion

In this chapter, the benefits of most existing evaluation metrics were discussed and their drawbacks were criticized. Consequently, we have proposed a novel evaluation metric E_{ID} (intrusion detection effectiveness) that manipulated all the drawbacks of the existing ones. Our metric E_{ID} attained measuring the actual effectiveness through its main notion of comparing the

operating curve of the IDS under test to the optimal operating curve, by calculating the variation between the two curves that interprets the deviation of the IDS operation from the intended optimal operation. E_{ID} was based on the *enhanced Bayesian detection rate* (EBD) which was derived from *Bayesian detection rate* $P(I|A)$ after manipulating its drawbacks to ultimately produce a completely expressive formula. We have proved the great advantages and expressiveness of E_{ID} under different operating conditions. We also demonstrated the importance of considering the main parameters (i.e., detection rate $P_{ID}(A|I)$, false alarms rate $P_{ID}(A|\neg I)$, and intrusion detection $P(I)$) and how they affect directly the evaluation of the IDSs/WIDSs effectiveness. We also proposed another metric R_R (*attack recognition rate*) that is useful in measuring the ability of IDS/WIDS to recognize the attack type.

VI. Chapter 6: Experimental Evaluation of WIDSs

In this chapter, we follow our methodology (chapter 3) to evaluate experimentally two popular WIDSs; Kismet [Kism13a] (for Linux) and AirSnare [Airs13c] (for Windows). As we mentioned in chapter 1, the three main pivots in the preparation phase of WIDSs evaluation are; 1) comprehensive evaluation methodology (achieved in chapter 3), 2) attack classification from the perspective of the WIDSs evaluator (achieved in chapter 4), 3) defining reliable and expressive evaluation metrics (achieved in chapter 5). The remaining phase is the experimental phase that is achieved in this chapter. We commenced the experimental phase with constructing RF shielded environment for hosting our testbed to overcome the evaluation limitations. In this chapter, we demonstrate the utility of our proposed taxonomy of wireless attacks and the importance of considering the probability of the attack test cases in calculating the actual intrusion detection rate of WIDSs. We also prove the benefits of our developed metrics E_{ID} (*intrusion detection effectiveness*) and R_R (*attack recognition rate*), and how they are meaningful and expressive. Finally, we present the evaluation results of the two WIDSs; Kismet and AirSnare.

6.1. RF Shielded Environment

As we mentioned in chapter 3 (section 3.3.2.1), one of the critical problems that we have faced, for the first time, in the experimental evaluation is the problem of uncontrolled 802.11 traffic from the adjacent wireless stations and access points, where it caused Kismet WIDS to generate more than 50 false alarms per hour. It was difficult to take our measurements under these conditions. We thus resorted to isolating our testbed from the uncontrolled RF traffic to take the measurements with only our controlled dataset. Also, some attacks such as deauthentication/disassociation (Amok mode) attack that disconnects the Wi-Fi devices in the range should be managed in an RF isolated workspace. Since we have not, in our laboratory, RF shielded workspace such as "RF anechoic chamber" [WSPH08], we have taken steps in constructing RF shielded enclosure. In fact, it was difficult to isolate a grand place, thus we concerned with isolating only the Wi-Fi adapters and access point together in a small RF shielded chamber or enclosure and pass the wired cables from the Wi-Fi adapters and access point through the enclosure to outside to be connected to main stations or machines. As a result of our research [Tong08] [DeRa97], we found the possibility of constructing a small RF shielded

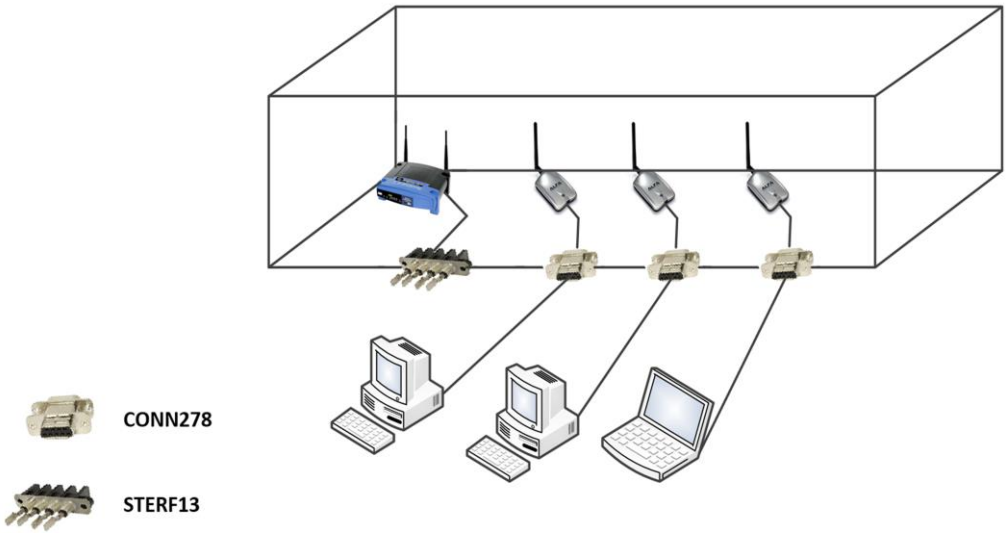

Figure VI-1: RF Shielded Environment.

enclosure using aluminum foil. Basically, radio frequency (RF) is a rate of oscillation in the range of about 3 kHz to 300 GHz, which corresponds to the frequency of radio waves and the alternating currents (AC) which carry radio signals. Then, RF wave is considered as AC current. It is worth mentioning that the skin effect property of AC conductors forces AC current to be distributed within the conductor to become with largest value at the surface and decreases within the inner depth of the conductor. Then, aluminum foil with skin effect property can be used effectively in constructing our RF shielded enclosure.

We used a cuboid box, as shown in Figure VI-1, with dimensions 40x40x70, and we wrapped it completely (internal and external surfaces) by aluminum foil. When the RF traffic arrives at the aluminum foil sheet, it will be distributed within the outer surface with inability to pass to the other side. At first, we tested the RF isolation effectiveness of the enclosure using a mobile phone, and we obtained a good result for a complete RF isolation, but unfortunately the situation was different when we used the Wi-Fi adapters that pick up all the 802.11 traffic outside the enclosure. With many experimental attempts we reached the conclusion that the wired cables, which pass through the enclosure from Wi-Fi adapters to the main stations outside the enclosure, work as parasitic antennas [Mill05] for coupling the interior of the enclosure with its exterior. To solve this problem, we installed on the enclosure three RF filtered connectors, i.e., STERF13 connector [Rams13] for the power connection and CONN278 connectors [Rams13] for data connection, to completely isolate the interior of the enclosure from the exterior uncontrolled RF traffic. Now, the RF shielded environment is ready to host our designed testbed to manage the experimental evaluation of WIDSs. We used three Wi-Fi adapters connected to three base

stations besides one access point; the all were hosted inside the RF Shielded enclosure. The Wi-Fi adapters used CONN278 connectors to be connected to the base stations outside the enclosure, and the access point used only the power connector STERF13 to be connected to the power supply.

6.2. Normal Background Traffic Generation

As we mentioned in chapter 3, there are two main methods to generate the normal background traffic; 1) generating synthetic traffic that doesn't contain secret data, but it doesn't represent the real operation in the network, or 2) generating real traffic by capturing the operational traffic during the normal operation of a network, and then replaying or injecting it into the testbed. The second method is the suitable one for the real measurements, but the main drawback is that the collected dataset must be sanitized from any credential or confidential data or any suspicious traffic before using it. To overcome the complexity of the sanitization process, we have followed the second method with an adaptation by capturing the normal traffic from a private network adjusted for this purpose. This private network includes an access point (i.e., it is connected to the Internet through a Ethernet cable), three workstations (i.e., two machines operate under Windows and the third one operates under Linux) associated with the access point through Wi-Fi adapters, and two mobile phones (i.e., operate under Android system) adjusted to associate with the access point via Wi-Fi connections as well. These devices were running to collect the exchanged traffic between them in a period of two weeks. Figure VI-2 shows a sample of the collected normal traffic, and Table V-1 shows the statistics of the collected traffic.

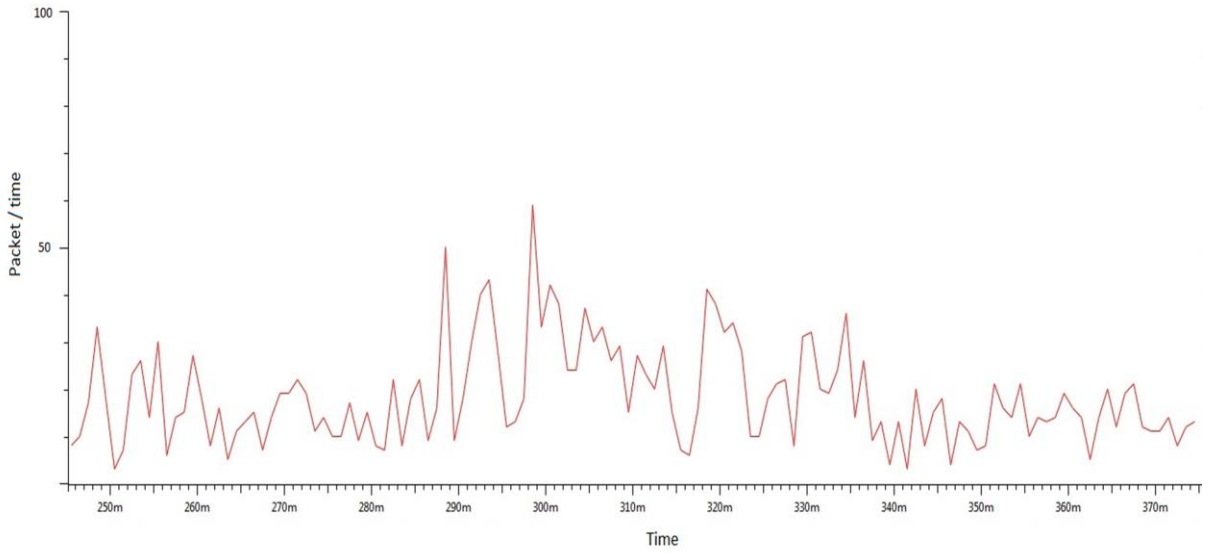

Figure VI-2: Sample of the Collected Normal Traffic.

Table VI-1: The Collected Normal Traffic.

Frame Subtype	Frame Count
Association request	38
Association response	43
Reassociation request	172
Reassociation response	142
Probe request	227081
Probe response	218602
Beacon	378
Disassociation	332
Authentication	169
Deauthentication	80
Action frames	3484
Null data	89920
QoS data	1723
QoS null data	19868
Total	562032

6.3. Malicious Traffic Generation

For generating the malicious traffic or attacks, we used numerous tools such as Metasploit [Meta13a], Armitage [Armi13], Backtrack [Back13], WireShark [Wire13], in addition to the aircrack-ng suite [Airc13] such as airmon-ng, airodump-ng, aireplay-ng, aircrack-ng, etc; each one for specific functions. We didn't find a tool includes all wireless attacks, so that we resorted to use numerous tools to manage the test with the possible attacks. The launched attacks are listed in Table VI-2.

6.4. Test Management

In this section, we manage the experimental evaluation of two popular WIDSs; *Kismet*(for Linux) [Kism13a] and AirSnare (for Windows) [Airs13c]. We used these two WIDSs in the out of box configuration; with just little intervention in Kismet configuration file to configure the

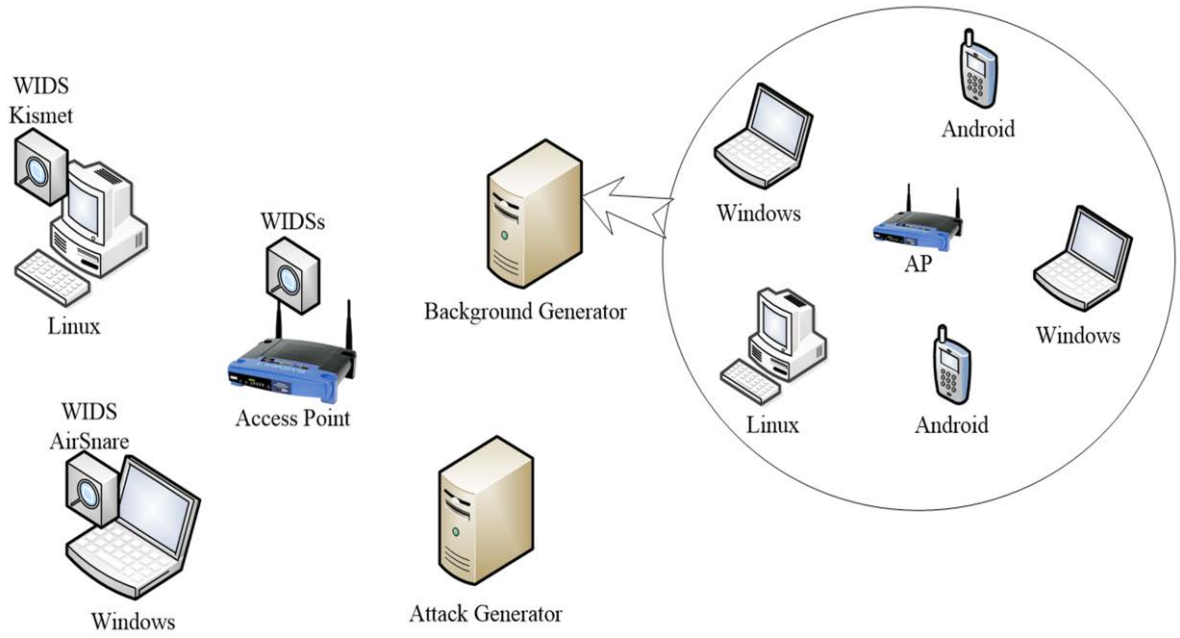

Figure VI-3: Testbed of WIDSs Evaluation.

Wi-Fi adapter deriver and network interface. We used the RF shielded environment (Figure VI-1), an access point Linksys WRT54GL, and three workstations (Linux and Windows) with Wi-Fi adapters ALFA awus036h and D-Link DWA-110 that respect the compatibility with the operating systems and WIDS programs. We concerned ourselves with the wireless infrastructure mode. For this mode, we have two possible scenarios for the installation of WIDSs (Figure VI-3). *Scenario 1*, the WIDS was installed on the access point. *Scenario 2*, the WIDS was installed on a terminal machine which is considered as a victim. Table VI-2 shows the list of the launched attacks, the attack detection and recognition results of WIDSs Kismet and AirSnare. TP and TP_R denote the detected and recognized attacks respectively.

From section 4.4, section 4.5, Appendix A, and Table VI-2, we can extract the attack test cases shown in Figure VI-4 and Table VI-4. From Appendix A and Figure VI-4, we can observe that some attack generations by different tools are classified under the same representative attack test cases. For examples, the deauthentication flood attack generation tools (Appendix A); Metasploit and Armitage follow the same attack process as gvoid11 and MDK3 respectively, thus they are classified under the same representative attack test cases 2 and 3 (Figure VI-4).

For calculating the attack detection rate, if we follow the ordinary method that was used in most previous evaluations of IDSs, then Table VI-2 is sufficient for the calculations and consequently the detection rate is $P_{ID}(A|I) = 0.61$ for Kismet, and $P_{ID}(A|I) = 0.167$ for AirSnare. These values are not real expressive values of the detection rate, and they thus affect negatively the calculation of the real effectiveness of WIDSs. The best way for calculating the

Table VI-2: Attack Detection and Recognition.

Generated Attacks	Kismet		AirSnare	
	TP	TP_R	TP	TP_R
Deauthentication/Disassociation Flood (< 10 Request)	✓	✓	x	x
Deauthentication/Disassociation Flood (< 20 Request)	✓	✓	x	x
Deauthentication/Disassociation Flood (> 30 Request)	✓	✓	✓	x
Deauthentication/Disassociation Flood (> 100 Request)	✓	✓	✓	x
Deauthentication/Disassociation (Amok mode)	✓	✓	x	x
Fake Authentication	✓	✓	x	x
Authentication Flood	✓	✓	x	x
Beacon Flood (evil duplicate AP DoS)	✓	x	x	x
MITM attack	x	x	x	x
ARP Request Replay Attack	x	x	x	x
WPA Downgrade	✓	x	x	x
WPA Cracking	✓	x	x	x
WEP Cracking	x	x	x	x
Chopchop	x	x	x	x
Hidden SSID Brute Force	x	x	x	x
Rogue AP	x	x	x	x
RF Jamming	✓	x	x	x
MAC Spoofing	x	x	✓	✓

expressive detection rate is considering the probability of occurrence of the attack test cases under the operating environment conditions.

In our evaluation tests, we considered and used 100 attack instances of the attacks listed in Table VI-2. We considered the instances of the generated attacks by the ratios that are approximately expressive of the probability of attack occurrence in some real systems. The attack instances were selected according to the registered attacks and vulnerabilities in popular websites such as Common Vulnerabilities and Exposures [Cvew13], National Vulnerability Database – NIST [Nvdn13], and others. It is worth mentioning that we considered in our calculations the deauthentication/disassociation flood attack instances with deauthentication requests > 30 (Table VI-2); we generated it by 8 instances from total of 100 instances of all the

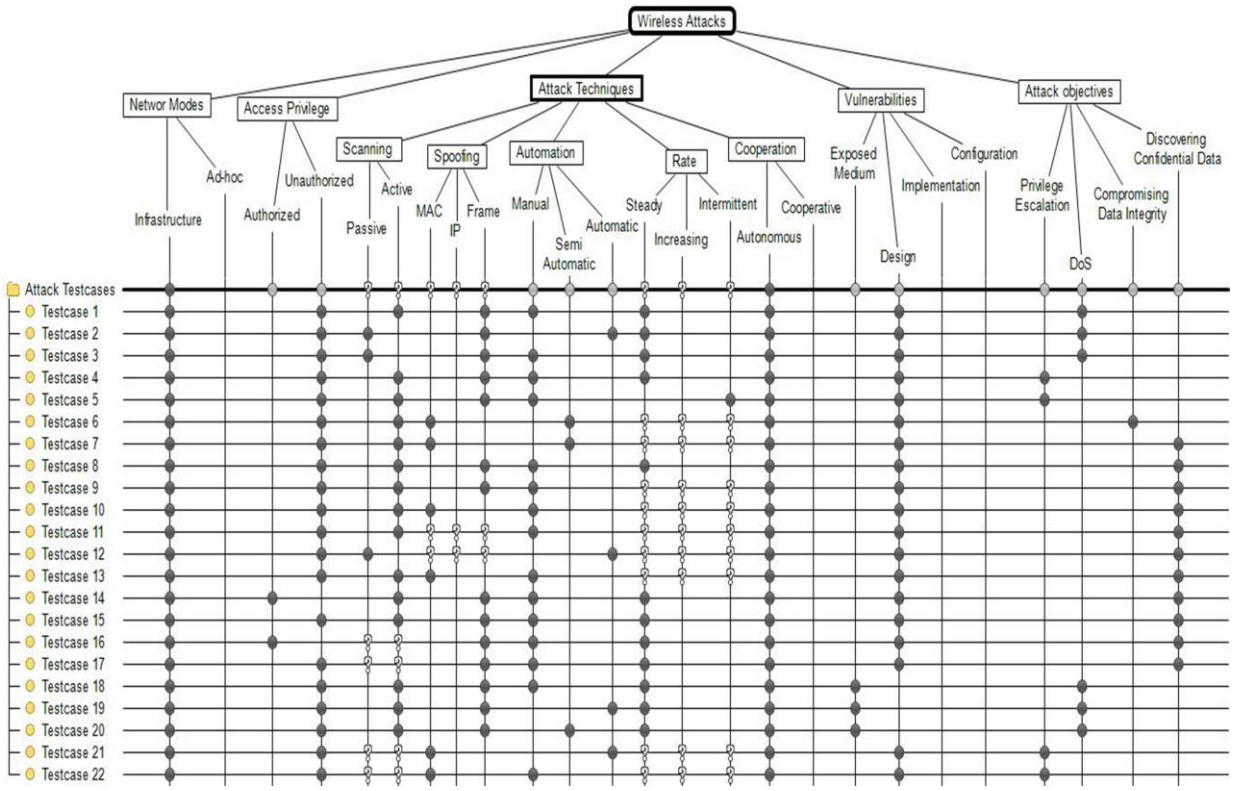

Figure VI-4: Attack Test Cases.

generated attacks. We classified the generated attacks under representative test cases (Figure VI-4 and Table VI-3), and adjusted the estimated probability of occurrence as shown in Table VI-4. Consequently, the expressive detection rate is $P_{ID}(A|I) = 0.65$ for Kismet, and $P_{ID}(A|I) = 0.13$ for AirSnare. As we mentioned in chapter 3 and chapter 4, the detection rate of WIDS varies according to the operating system conditions, since the probability of the system hostility and attack types are varied. Also, it is essential to take into account the special vulnerabilities of specific devices used in the test; these vulnerabilities and the relevant attacks should be considered in the attack test cases and their probabilities. For our testbed, we searched about any vulnerability associated with the used devices (Linksys WRT54GL, ALFA awus036h, and D-Link DWA-110), but we didn't find any specific vulnerability (e.g., some of specific vulnerabilities of some Wi-Fi devices are mentioned in Appendix A). Then, we didn't consider any special attack test case related to the used devices. In our evaluation environment, the used 100 attack instances generated approximately 1500 malicious frames, in addition to the generated background normal traffic (Table VI-1). Then, we have hostility or intrusion probability $P(I) = 2.66889 * 10^{-3}$, and no intrusion probability $P(\neg I) = 0.99733$. Also, the registered false alarms for the two WIDSs are $P_{ID}(A|\neg I) = 0.008967$ for Kismet and $P_{ID}(A|\neg I) = 0.0014946$ for AirSnare.

Table VI-3: Generated Attacks and the Corresponding Test Cases.

Generated Attacks	Representative Attack Test Cases
Deauthentication/Disassociation Flood	1, 2, 3
Deauthentication/Disassociation (Amok mode)	3
Fake Authentication	4, 5
Authentication Flood	2,3
Beacon Flood (evil duplicate AP DoS)	3
MITM attack	6,7
ARP Request Replay Attack	8
WPA Downgrade	3
WPA Cracking	9
WEP Cracking	10, 11, 12
Chopchop	13
Hidden SSID Brute Force	11
Rogue AP	14, 15, 16, 17
RF Jamming	18, 19, 20
MAC Spoofing	21, 22

Table VI-4: Probability of Occurrence of the Generated Attack Instances.

Attack Test Cases	Estimated Probability	WIDSs Detection Ratio	
		Kismet	AirSnare
1, 2, 3, 4, 5	0.46	✓	✓(0.08)
6, 7	0.05	x	x
8	0.04	x	x
9	0.13	✓	x
10, 11, 12	0.1	x	x
13	0.04	x	x
14, 15, 16, 17	0.07	x	x
18, 19, 20	0.06	✓	x
21, 22	0.05	x	✓
Total	1	0.65	0.13

6.5. Results Interpretation

We can now interpret the evaluation results and present some conclusions on the two WIDSs. We commence with evaluating the effectiveness of Kismet and AirSnare using our proposed metric E_{ID} (*intrusion detection effectiveness*).

Recalling E_{ID} (Eq. V-30);

$$E_{ID} = 1 - \frac{P_{ID}(A|I) \cdot \left(P_{OE}(\neg I) + \left(\frac{1}{\left(1 - P_{ID}(A|\neg I)\right)} - 1 \right) ln|1 - P_{OE}(\neg I) \cdot (1 - P_{ID}(A|\neg I))| \right)}{P_{OE}(\neg I) \cdot \left(1 - P_{ID}(A|\neg I)\right)}$$

Then,

$$E_{ID}\ (kismet) = 0.37$$

$$E_{ID}\ (AirSnare) = 0.871$$

As described in detail in chapter 5, we can plot the operating curves of the two WIDSs to show graphically the deviation degree of each one of them from the optimal operating case that is represented by the zero reference curve (*ZRC*). The deviation degree reflects the effectiveness level of each one of them. The operating curves of Kismet and AirSnare besides *ZRC* are shown in Figure VI-5, Figure VI-6, and Figure VI-7. In Figure VI-5, we can observe the increase in the slope of Kismet's operating curve, especially as $P(\neg I) \geq 0.9$. This reflects the effect of false alarms ($P_{ID}(A|\neg I) = 0.008967$) on the operating curve as $P(\neg I)$ increases, and this confirms what we discussed in chapter 5 (section 5.3.1.3). The deviation degree of Kismet's operating curve from *ZRC* interprets the E_{ID} value that shows the acceptable level of Kismet effectiveness. Figure VI-6 shows the straight forward case of AirSnare's operating curve with just little observed change in the slope as $P(\neg I) \geq 0.996$. This also reflects the little effect of false alarms ($P_{ID}(A|\neg I) = 0.0014946$) on the operating curve as $P(\neg I)$ increases. The great deviation of AirSnare's operating curve from *ZRC* interprets its ineffectiveness as shown byE_{ID} value. It is enough to review section 5.3.1.3, especially Figure V-12, to be aware of the important effect of the three parameters, false alarms $P_{ID}(A|\neg I)$, detection rate $P_{ID}(A|\neg I)$, and intrusion probability $P(I)$, on the form and slope of the operating curve, and consequently their effect on the WIDS effectiveness. This proves the utility of our proposed metric E_{ID} that considers these parameters in an expressive formula.

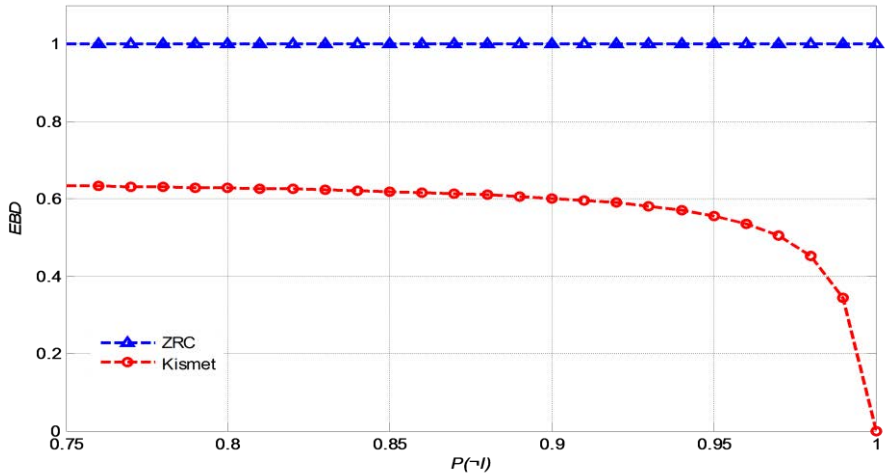

Figure VI-5: The Trade-off between *EBD* and *P*(¬*I*) of Kismet and ZRC.

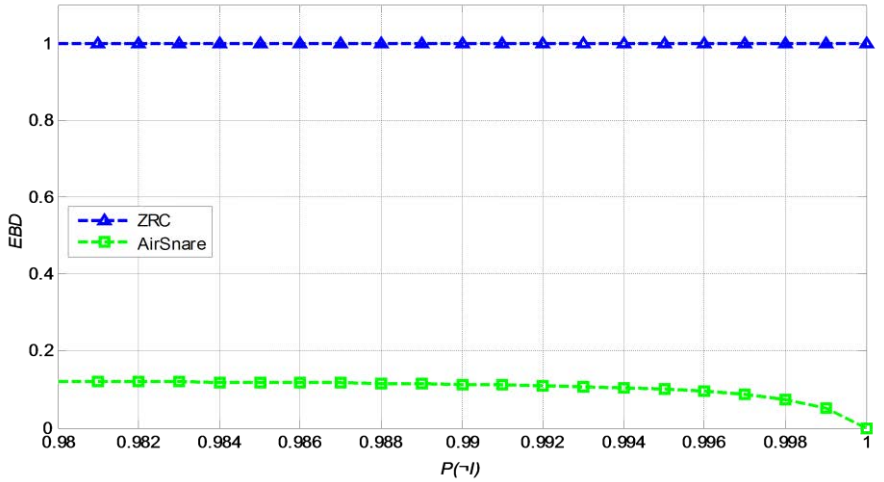

Figure VI-6: The Trade-off between *EBD* and *P(¬I)* of AirSnare and ZRC.

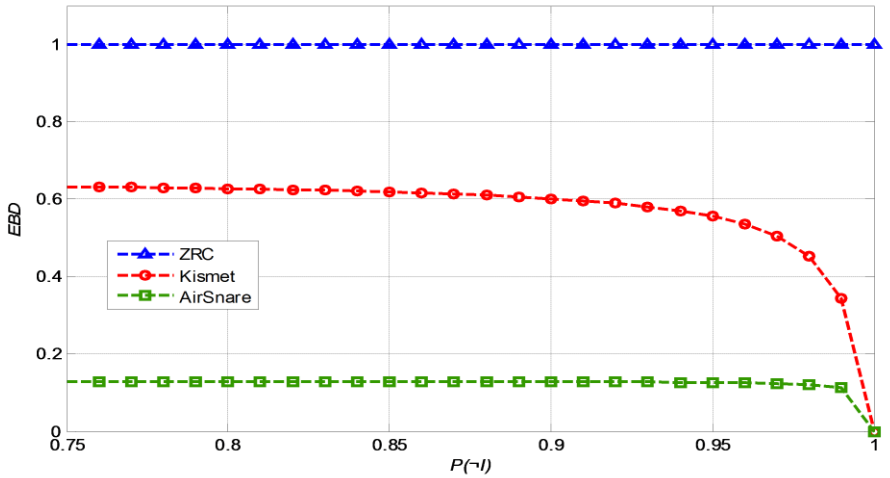

Figure VI-7: The Trade-off between *EBD* and *P(¬I)* of Kismet , AirSnare, and ZRC.

Also, we can apply the second proposed metric R_R (*Attack Recognition Rate*) to Kismet and AirSnare as follows;

Recalling R_R (Eq. V-33);

$$R_R = \frac{TP_R}{TP}$$

From Table VI-2, then,

$$R_R\ (Kismet) = \frac{4}{8} = 0.5$$
$$R_R\ (AirSnare) = \frac{1}{2} = 0.5$$

Figure VI-8 and Figure VI-9 show the impact of the Kismet and AirSnare, respectively, on the monitored system resources.

Kismet. Kismet operation doesn't deviate much more from the optimal case *ZRC*. Kismet is considered a light software with little utilization of the monitored system resources in the absence of intrusions, but its increasing impact on the monitored system appears when the system is under attack (Figure VI-8). The level of its utilization of the system resources depends on the attack type. It has a good ability to recognize the attack type besides the attack detection ability. It is worth mentioning that during launching the beacon-flood attack, which can be performed by creating a lot of fake APs with the same name and the same channel but with different MAC addresses, Kismet didn't generate any alarm for this type of attack; it just notified that there are new APs found. Although all these fake APs are with the same name and the same channel, Kismet considers them as different APs and unfortunately couldn't correlate between them. Also, there is no correlation between the generated redundant alerts that are a heavy load on the complementary prevention part.

AirSnare. It is considered ineffective WIDS where it has high deviation degree from the optimal case. Also, it has a little ability to recognize the intrusion type. It is considered as a light software with nearly the same impact on the system resources in the presence and absence of attacks (Figure VI-9). In fact, AirSnare itself is very weak against attacks, especially flooding attacks, where its operation froze with a heavy traffic of deauthentication flooding attack.

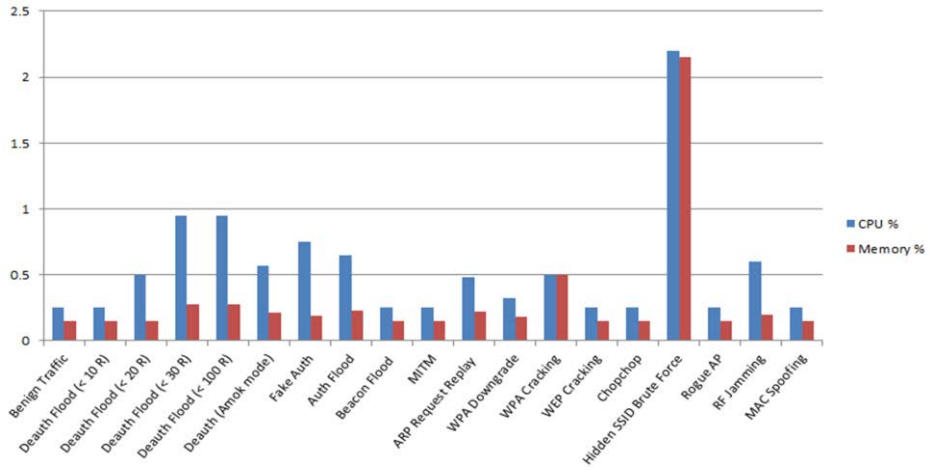

Figure VI-8: The impact of Kismet on the Monitored System Resources.

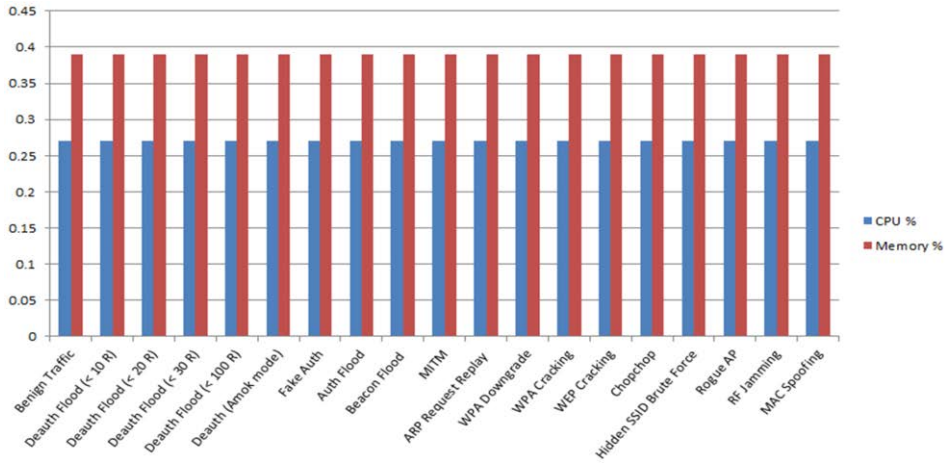

Figure VI-9: The impact of AirSnare on the Monitored System Resources.

6.6. Conclusion

This chapter was concerned with the experimental phase of our work. We have followed our proposed methodology and applied our proposed solutions to evaluate two WIDSs; Kismet and AirSnare. We overcame the problem of uncontrolled traffic from the adjacent wireless stations by constructing an RF shielded environment to host our designed testbed. We generated real representative dataset and managed our test tasks accordingly. The great advantages of our developed metrics for measuring the *intrusion detection effectiveness* (E_{ID}) and attack *recognition rate* (R_R) have been demonstrated. We also demonstrated the difference between the ordinary calculations of intrusion detection rate that were followed by the previous evaluations of IDSs and our proposed notions that lead to the accurate calculation of the actual effectiveness of WIDSs. The results showed the acceptable effectiveness of Kismet and ineffectiveness of AirSnare, and their impact on the monitored system resources.

VII. Chapter 7: Conclusions and Future Work

The evaluation of the IDSs/WIDSs performance is not a trivial task, but it necessitates a comprehensive methodology considers all the necessary related dimensions. This chapter summarizes our conclusions on our proposed solutions and the obtained results. Also, we present some notions and ideas that are taken into account for the future work.

7.1. Conclusions

The growing security violations in wireless networks and the lack of reliable evaluation of WIDSs were the main motivations for our work. We commenced with studying the wireless security concepts and the relationships between them, and we crystallized that in a security conceptual model. This model clarifies well the crucial role of the security countermeasures in manipulating or neutralizing the system vulnerabilities, combating the attack attempts, and mitigating the attack effect. Studying the role of each security countermeasure illuminated the importance of the WIDS as a second line of defense. The question that arises is which WIDS is effective for our system? The answer should inevitably take into account the evaluation of WIDSs performance.

Thus, we have developed an evaluation methodology that provided a comprehensive road map for managing a credible evaluation of WIDSs. The dimensions of our methodology are arranged in a sequential manner starting from the evaluation goals, passing the subsequent tasks, and reaching the intended task of experimental evaluation of the WIDSs. The benefits of our methodology are manifested in the obtained results. The main pivotal tasks in our methodology are characterizing the evaluation dataset, defining the evaluation metrics, and overcoming the evaluation limitations.

For the evaluation dataset, which mainly composed of two parts of normal traffic and malicious traffic, we had a major concern about the malicious activities that affect significantly the management of unbiased evaluation. For the normal traffic, we used real traffic that was mainly collected from a private network (i.e., installed for this purpose) to avoid the irritating sanitization of the data collected from the real system. As for the malicious traffic, we have developed a holistic taxonomy of wireless attacks. The classification methodology of our taxonomy was based on the conception of the attack generation process. This taxonomy helps in generating and extracting the representative attack test cases that are necessary in managing a comprehensive evaluation of WIDSs. We also considered a new concept of the probability of occurrence of the attack test cases that helps in handling accurate calculations of the actual value of intrusion detection rate $P(I)$ that helps consequently in evaluating the actual effectiveness of IDSs/WIDSs. Unfortunately, most existing evaluations of IDSs didn't consider the above-

mentioned concepts, thus their results don't refer to the actual performance of IDSs. The obtained results have proved the advantages of our proposed solutions over the previously proposed ones.

For the second pivotal task of defining the evaluation metrics, we studied the previously proposed metrics and analyzed well their strengths and weaknesses. We subsequently introduced a novel metric called *intrusion detection effectiveness* (E_{ID}) which manipulated the drawbacks of the existing metrics of evaluating the IDS effectiveness, especially the defective main notion of most of them for comparing two or more IDSs to select the best one, although this selected one may be ineffective; this leads to measuring so-called *relative effectiveness*. E_{ID} ensured measuring the *actual effectiveness* depending on its main notion of comparing the *operating curve* of an IDS (system under test) to an *optimal operating curve* (created as a *zero reference curve ZRC*), by calculating the variation between the two curves that indicates the deviation of the IDS operation from the intended optimal operation. We demonstrated in detail the utility of our proposed metric E_{ID} over the existing ones, and the obtained results proved also how it is an expressive and perfect metric. We also developed another metric called *attack recognition rate* (R_R) for measuring the ratio of the detected attacks that are recognized.

As for the third dimension of overcoming the evaluation limitation that was manifested in the uncontrolled traffic in the open wireless medium, we solved this problem by constructing an RF shielded testbed that helped us in taking all the measurements under our control without any interfering from any uncontrolled traffic.

Finally, we have followed our methodology and conducted experimental evaluation tests of two popular WIDSs; Kismet (for Windows) and AirSnare (for Linux). The results showed that Kismet is more effective than AirSnare, but the two have the same value of R_R (*attack recognition rate*) where the ratios of the recognized attacks to the detected ones are matched for the two WIDSs. Kismet had impact on the monitored system according to the attack type, but AirSnare didn't affect the system resources under the different types of attacks.

7.2. Future Work

We are interested in pursuing our scientific research and experimental work to manage some experimental tasks and develop new proposals.

***Attack Scenarios*:** We aim to extract detailed attack scenarios, with the aid of our proposed taxonomy of wireless security attacks. The attack scenarios help in inspecting the intermediate stages between the starting stage and final stage of attacks, thus they could help the WIDSs designers to enhance the WIDSs performance. We picked up this idea from our experimental evaluation of WIDSs, where we observed that some attacks such as WEP cracking can be partially detected in the intermediate stages before reaching the ultimate goal. Most of these

attacks usually interact with the access points or stations by using active scanning or spoofing tools that indicate the malicious preparation of attacks. This could facilitate the early detection of intrusions using the WIDS. For example, one of the known approaches to crack WEP key is using ARP (Address Resolution Protocol) Request Replay attack to capture a large amount of IVs (initialization vectors) for later WEP cracking. ARP Request Replay attack itself requires earlier connection to the network to generate the initial ARP packet, and this connection can be achieved by Fake Authentication attack or spoofing MAC of an authorized station. Early detection can help in protecting the secured system from severe risks.

***New Evaluation Metrics*:** In addition to our proposed evaluation metrics E_{ID} and R_R, we are interested in developing new evaluation metrics to evaluate the remaining attributes of WIDSs performance. We are concerned with deriving a new metric to measure the ability of IDS/WIDS to detect the intrusion in early stage before the infection occurs. This metric is directly linked to the above-mentioned proposal of the attack scenarios that help in discovering the intermediate stages between the starting point and the objective point of attack. The notion of this metric is based on evaluating the WIDS capability which is equivalent to the level or rank of the intermediate stages where the WIDS is able to discover the attacks before reaching the ultimate objectives. The rank of each intermediate stage or point is evaluated by two main parameters. The first parameter measures the deviation of the intermediate point from the objective point. The second parameter refers to the probability of the attack's ferocity at the intermediate point. As a result of our experimental work, the deviation of the intermediate point from the objective point is not the only criterion for evaluating the point rank, but also the attack level should be considered, where there are some penultimate stages of attacks cause very little or neglected impact, but other earlier stages cause an observed harm, and vice versa. We are also interested in deriving a new metric to evaluate the redundant alerts correlation attribute, where the output alarms are analyzed according to some fields of the detected data such as the source address and the alarm type.

***Combating DoS/DDoS*:** Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks are without doubt the most dangerous attacks in wired and wireless networks. There is appreciable work on the classification of DoS/DDoS attacks and defense mechanisms [DoMi04][MiRe04][BiTa09] that could be helpful in understating the DoS attacks as well as designing robust defense mechanisms. Despite the valuable work exerted in developing defense mechanisms [KMMZ06][NiLD08][HCCB12] to prevent or even mitigate the effect of DoS attacks, they are still the most pressing problem facing the network security owing to the difficulty of distinguishing the intrusive traffic from the normal traffic. We are thus interested in emulating some defense mechanisms of the natural immune system to produce artificial robust mechanisms for combatting the DoS attacks. We consider the self-organized and distributed manner of the natural immune system. We also consider the role of the vaccine in training the

immune system to recognize and combat the pathogens. We already commenced with analyzing some defense mechanisms of the natural immune system, and we intend to pursue our work towards the intended objective of developing robust defense mechanisms.

***Penetration Testing*:** We are interested in implementing the wireless attacks using Metasploit framework [MiRe04] to be able to manage automatic generation of the possible wireless attacks according to our concept of the probability of occurrence of the attacks in regard to the system conditions. We have already commenced with the implementation of some wireless attacks, and we are pursuing our work on the remaining possible ones.

Design and implementation of a distributed WIDS: There is an apparent lack of the distributed WIDS that can serve well the distributed architecture of the infrastructure and Ad Hoc wireless networks. We are thus interested in designing and implementing a distributed WIDS with enhanced specification-based detection techniques to manipulate the defects of the existing ones. We consider the data-mining and clustering techniques, besides the helpful techniques to achieve our goal. We also intend to extend our designed testbed to be suitable for some complex tasks of the experimental evaluation of WIDSs.

Appendix A: Wireless Security Attacks and Vulnerabilities

In this Appendix, we classify some possible wireless attacks according to our taxonomy. More details about the security attacks and vulnerabilities are available at the websites of Aircrack-ng suite [Rams13], Metasploit Auxiliary Modules & Exploit Database [Airc13], BackTrack Linux - Penetration Testing Distribution [Meta13b], Common Vulnerabilities and Exposures [Back13], National Vulnerability Database - NIST [Cvew13], and other websites of wireless penetration testing tools.

Attack (Generation Tool) & Vulnerability ID	**Classification and Description**
WEP Cracking (aircrack-ng suite)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** MAC ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** Using aircrack-ng suite, WEP cracking can be managed in five steps: 1) Starting the monitor mode of the wireless interface by *airmon-ng*, to be able to listen in the wireless traffic in the range, 2) Capturing initialization vectors (IVs) from the selected access point by *airodump-ng*, 3) Using *aireplay-ng* to do a fake authentication with the access point, 4) Starting *aireplay-ng* in ARP request replay mode to inject ARP packets into the network, where the access point normally rebroadcasts ARP request packets and generate new IV, and finally 5) Running *aircrack-ng* to obtain the WEP key from the IVs gathered in the previous steps.
WEP Cracking (FMS- WEPCrack)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** ***Attack Management:*** Manual ***Attack Rate:***

	Attack Collaboration: Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** As mentioned in chapter 4, FMS attack is based on collecting numerous encrypted packets including the initialization vectors (IVs), and analyzing them analytically to derive the secret key. WEPCrack tool can be used to realize FMS attack by cracking WEP encryption keys using the latest discovered weakness of RC4 key scheduling. WEPCrack comprises the following Perl scripts: 1) *WeakIVGen.pl* script that generates a file "*IVFile.log*" that contains IVs that can weaken the secret key used to encrypt the WEP traffic, 2) *prism-getIV.pl* script that reads prismdump/Ethereal captured files, and looks for weak IVs in WEP traffic. If weak IVs are found, then they are placed in the file "*IVFile.log*" along with the 1st encrypted output byte, 3) *WEPCrack.pl* script that reads *IVFile.log*, and uses the weak IVs+ encrypted output to determine the secret key used.
WEP Cracking (FMS- AirSnort)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** ***Attack Management:*** Automatic ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** AirSnort is another tool that can realize FMS attack. AirSnort operates by passively monitoring the transmissions, computing the encryption key when enough packets have been gathered. It is nearly automatic tool for WEP cracking; just running it, and then choosing the intended mode that is either "scan" mode to scan through all 802.11 channels at a regular interval or "channel" mode to monitor a specific channel. It can crack WEP key in few minutes.
WEP Cracking (chopchop – aircrack-ng suite)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** MAC ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous

	Vulnerability: Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** Chopchop attack exploits the weaknesses of integrity algorithm (CRC-32) that is used to compute the integrity check value (ICV). It can decrypt a WEP data packet without knowing the key. It does not recover the WEP key itself, but merely reveals the plaintext as explained in chapter 4.
Cracking WPA Migration Mode (aircrack-ng suite)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** WPA Migration Mode is a configuration setting supported by Cisco access points, and it enables both WPA and WEP stations to associate with the access point using the same Service Set Identifier (SSID). Cracking WPA Migration Mode helps in gathering a large number of IVs in a short period, and then accelerates the extraction of WEP key.
WPA/WPA2 Cracking (aircrack-ng suite)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** Unlike WEP, where statistical methods can be used to speed up the cracking process, the brute force techniques can be used against WPA/WPA2 algorithm. WPA/WPA2 cracking can be managed by firstly capturing the WPA/WPA2 authentication handshake by *airodump-ng* and deauthenticating the wireless station by *aireplay-ng* to actively speed up the process of capturing the authentication handshake, to ultimately cracking the pre-shared key by *aircrack-ng.*

WPA/WPA2 Downgrade (MDK3)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** DoS ***Description:*** WPA/WPA2 downgrade attack blocks the stations and access points, only if they use WPA encryption, by deauthenticating them. This induces the system administrator to use a weaker encryption WEP algorithm or disable the encryption.
CTS/RTS Flood (Metasploit)	***Network Mode:*** Infrastructure / Ad Hoc ***Access Privilege:*** Unauthorized ***Scanning Technique:*** ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** DoS ***Description:*** In CTS/RTS flood (Metasploit module), the attacker sends 802.11 CTS/RTS requests to block the transmission between the wireless stations.
Deauthentication Flood (aircrack-ng suite)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** DoS ***Description:*** The attacker can exploit the vulnerability of deauthentication process, as explained in chapter 4, to spoof the deauthentication frame between the wireless station and access point to pretend to be either the access point or the station, and direct the deauthentication frame to the other party. Deauthentication attack can be prepared by firstly discovering the access points and

	associated stations in the range, and this can be managed passively by sniffing the 802.11 traffic using some tools such as AirTraf or actively using other tools such as *airodump-ng* after running the NIC in monitor mode by *airmon-ng*. Then the attacker uses *aireplay-ng* to launch the deauthentication attack between the selected access point and wireless station. *aireplay-ng* supports the ability to control the number of deauthentication requests sent.
Deauthentication Flood (gvoid11)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** Frame ***Attack Management:*** Automatic ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** DoS ***Description:*** gvoid11 is the GUI (Graphical User Interface) implementation of void11 that automates the deauthentication process. Using gvoid11, the attacker just adjusts the network interface and attack type, and then launch the deauthentication attack by a keystroke.
Deauthentication (Amok mode – MDK3)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** DoS ***Description:*** MDK3 is a Linux-based command line tool. MDK3 can be used for deauthentication (amok mode), where it stops the connection between the stations and access points in the range.
Deauthentication Flood (Metasploit) / (Armitage)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** Frame ***Attack Management:*** Manual / Automatic ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous

	Vulnerability: Design flaws ***Attack Objective:*** DoS ***Description:*** 802.11 DEAUTH Flooder (Metasploit module) can be used to break the connection between the wireless stations and access point by deauthentication frames, with a control of the number of the deauthentication frames being sent. Armitage makes the penetration testing easy by adding a GUI to the Metasploit framework.
Fake Authentication (aircrack-ng suite)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** Steady / Intermittent ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Access Privilege Escalation ***Description:*** Fake authentication attack can be used for authentication/association with the access points that use WEP algorithm, but it cannot be used against WPA/WPA2 access points. Fake authentication attack, as other attacks, is prepared by firstly discovering the access points, and this can be managed by active scanning (e.g., by *airodump-ng*). Then the attacker uses *aireplay-ng* to launch the Fake authentication attack between the selected access point and wireless station. *Aireplay-ng* supports the ability to control the number of authentication requests sent.
Wi-Fi DoS Attacks (deauthentication, fake authentication, Jamming attack) (WebSploit)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** Frame ***Attack Management:*** Semi-automatic ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Exposed Medium / Design flaws ***Attack Objective:*** DoS ***Description*:** WebSploit tool is a powerful tool that supports semi-automatic generation of a set of Wi-Fi DoS attacks (i.e., deauthentication, fake authentication, Jamming attack) by in the same time a keystroke.
ARP Request Replay Attack	***Network Mode:*** Infrastructure / Ad Hoc ***Access Privilege:*** Unauthorized

(aircrack-ng suite)	***Scanning Technique:*** Active ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** ARP (Address Resolution Protocol) request replay attack is used to replay ARP packets and quickly generate IVs for WEP cracking. This attack simply captures an ARP packet and replays it to a certain access point. Because it is an ARP request packet, the access point will retransmit the packet and generate a new IV. This allows the attacker to capture a large amount of IVs in a short time for WEP cracking. Before running this attack, the fake authentication is required first, where the attack station needs to be connected to the network to generate the initial ARP packet.
Cafe Latte Attack (aireplay-ng)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** Frame Spoofing ***Attack Management:*** Manual ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** Cafe Latte can be managed by capturing an ARP packet from a station, manipulating it and then sending it back to the station. The station in turn generates packets which can be captured by *airodump-ng*. Then *aircrack-ng* can be used to determine the WEP key.
Beacon flood (evil duplicate AP DoS) (MDK3)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** DoS ***Description:*** Beacon flood (evil duplicate AP DoS) attack can be

	managed by sending out a lot of beacon frames of the network SSID which is targeted to be out of service. While the attack is active, any legitimate station is not able to establish a connection with the targeted network SSID.
Rogue Access Point (AirSnarf)	***Network Mode:*** Infrastructure ***Access Privilege:*** Internal Penetrator / Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** Airsnarf is a simple utility for creating the rogue wireless access points to steal usernames and passwords from the public wireless hotspots.
Rogue Access Point (KARMA)	***Network Mode:*** Infrastructure ***Access Privilege:*** Internal Penetrator / Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** KARMA is originally a set of tools for assessing the security of wireless clients at multiple layers. It can be used for creating rogue wireless access points.
Rogue Access Point (Metasploit)	***Network Mode:*** Infrastructure ***Access Privilege:*** Internal Penetrator / Unauthorized ***Scanning Technique:*** ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** Steady ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** Using Metasploit module - Wireless Fake Access Point Beacon Flood, the attacker can advertise thousands of fake access points, using random SSIDs and BSSID addresses.

MITM (Ettercap & Wireshark)	***Network Mode:*** Infrastructure / Ad Hoc ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** MAC ***Attack Management:*** Semi-Automatic ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Compromising data integrity / Discovering confidential data ***Description****:* Man-in-the-middle (MITM) attack is a form of active eavesdropping in which the attacker intercepts the connections between two stations and pretends alternately as an end-point to each one of them, and relays the messages between them, making them believe that they are talking directly to each other. Thus, the attacker can discover, control, alter, or eliminate the information exchanged between the two stations.
Null Probe Response (Metasploit)	***Network Mode:*** Infrastructure ***Access Privilege:*** Internal Penetrator / Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** Frame ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation flaws ***Attack Objective:*** DoS ***Description:*** Null probe response attack exploits the firmware-level vulnerability in a variety of 802.11 devices. The attacker sends a null probe response to a wireless station to lock up the firmware of its wireless network interface card (NIC).
MAC Spoofing (SMAC)	***Network Mode:*** Infrastructure / Ad Hoc ***Access Privilege:*** Unauthorized ***Scanning Technique:*** ***Spoofing Technique:*** MAC ***Attack Management:*** Automatic ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Access Privilege Escalation ***Description:*** In MAC address spoofing, the attacker spoofs the MAC

	address of a legitimate station in an attempt to be granted that station access privileges or to be used in a next stage of attack. SMAC is a powerful MAC address changer (for Windows) that is easy to use. It helps in changing MAC address in simple steps.
MAC Spoofing (Macchanger)	***Network Mode:*** Infrastructure / Ad Hoc ***Access Privilege:*** Unauthorized ***Scanning Technique:*** ***Spoofing Technique:*** MAC ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Access Privilege Escalation ***Description:*** Macchanger is a Linux-based tool for changing the MAC address of network interfaces. Macchanger gives the ability to change Mac addresses manually by command line tools or automatically using Macchanger GUI (Graphical User Interface).
Cracking hidden SSID (MDK3 – dictionary attack)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data ***Description:*** At a certain level of network security, the access point is configured with disabling the SSID broadcasting. In this case, the attacker can discover the hidden SSID by a dictionary attack, where the attacker uses a wordlist text file to check which dictionary's word matches the hidden SSID.
Cracking hidden SSID (MDK3 – brute force attack)	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Active ***Spoofing Technique:*** ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Design flaws ***Attack Objective:*** Discovering confidential data

	Description: If the dictionary attack is not effective in cracking the hidden SSID of the access point, then the attacker may resort to use a brute force attack. The brute force attack depends on the matter of guessing, and trial and error, where the character set is adjusted in the first trial.
CVE-2001-0160	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** ***Attack Management:*** Manual / Semi-automatic ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** Disclosure confidential Information / Compromising data integrity. ***Description:*** Lucent/ORiNOCO WLAN cards generate predictable Initialization Vector (IV) values of WEP key which might allow the attacker to quickly compile the information to decrypt the transmitted messages.
CVE-2001-0618	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** Discovering confidential data. ***Description:*** Orinoco RG-1000 Wireless Residential Gateway uses the last 5 digits of the routinely broadcast SSID as the default WEP key. Then the attacker could easily determine the WEP key and decrypt the RG-1000 traffic.
CVE-2013-1105	***Network Mode:*** Infrastructure ***Access Privilege:*** Internal Penetrator ***Scanning Technique:*** Passive / Active ***Spoofing Technique:*** ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation flaws

	Attack Objective: Disclosure confidential Information / Compromising data integrity. ***Description:*** Cisco WLAN Controller (WLC) devices with software 7.0, such as Cisco Wireless LAN Controllers Wireless Intrusion Prevention System (WIPS), are vulnerable to be exploited by an authenticated user to bypass wireless management settings and read or modify the device configuration.
CVE-2010-3033	***Network Mode:*** Infrastructure ***Access Privilege:*** Internal Penetrator ***Scanning Technique:*** Passive ***Spoofing Technique:*** ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation flaws ***Attack Objective:*** Access Privilege Escalation / Disclosure confidential Information / Compromising data integrity. ***Description:*** Cisco WLAN Controller (WLC) software (4.2 through 6.0) allows the authenticated user to bypass the access restrictions and modify the configuration to gain administrative privileges.
CVE-2009-0052	***Network Mode:*** Infrastructure ***Access Privilege:*** Internal Penetrator ***Scanning Technique:*** Passive / Active ***Spoofing Technique:*** ***Attack Management:*** Manual / Automatic / Semi-automatic ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation flaws ***Attack Objective:*** DoS ***Description:*** The wireless driver in some Wi-Fi access points, such as the ATHEROS-based AP-Netgear WNDAP330, allows the authenticated user to cause a denial of service (reboot or hang the access point) and possibly execute arbitrary code via a truncated reserved management frame.
CVE-2006-6059	***Network Mode:*** Infrastructure ***Access Privilege:*** unauthorized ***Scanning Technique:*** Passive / Active ***Spoofing Technique:*** Frame ***Attack Management:*** ***Attack Rate:*** steady

	Attack Collaboration: Autonomous ***Vulnerability:*** Implementation flaws ***Attack Objective:*** Disclosure confidential Information / Compromising data integrity / Denial of Service. ***Description:*** The buffer overflow in MA521nd5.SYS driver 5.148.724.2003 for NetGear MA521 PCMCIA adapter allows the attacker to execute arbitrary code via beacon or probe 802.11 frame responses with heavy rate. This vulnerability have been already exploited and the attackers designed an attack for that as shown in the Metasploit module [Nvdn13].
CVE-2013-4613	***Network Mode:*** Ad Hoc ***Access Privilege:*** Internal Penetrator ***Scanning Technique:*** Passive ***Spoofing Technique:*** ***Attack Management:*** Manual ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Configuration error ***Attack Objective:*** Disclosure confidential Information / Compromising data integrity / Denial of Service. ***Description:*** The default configuration of the administrative interface on the Canon MG3100, MG5300, MG6100, MP495, MX340, MX870, MX890, MX920, and MX922 printers does not require authentication, thus the attacker may be able to modify their configuration through open access.
CVE-2012-6371	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** ***Attack Management:*** ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** Disclosure confidential Information ***Description:*** The WPA2 implementation on the Belkin N900 F9K1104v1 router establishes a WPS PIN based on 6 digits of the LAN/WLAN MAC address, which makes it easier for the attacker to obtain access to the network by inspecting the broadcast packets.
CVE-2011-4507	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized

	Scanning Technique: Passive ***Spoofing Technique:*** ***Attack Management:*** ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Configuration Error ***Attack Objective:*** Disclosure confidential Information ***Description:*** D-Link DIR-685 router, where certain WPA and WPA2 configurations are used, does not maintain an encrypted wireless network during the transfer of a large amount of network traffic, thus the attacker may be able to obtain sensitive information or bypass the authentication.
CVE-2011-0196	***Network Mode:*** Ad Hoc ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** ***Attack Management:*** ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** Denial of Service ***Description:*** AirPort in Apple Mac OS X 10.5.8 allows the attacker to cause a denial of service by injecting Wi-Fi frames.
CVE-2012-4366	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** ***Attack Management:*** ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** Disclosure confidential Information ***Description:*** Belkin wireless routers Surf N150 Model F7D1301v1, N900 Model F9K1104v1, N450 Model F9K1105V2, and N300 Model F7D2301v1 generate a predictable default WPA2-PSK passphrase based on eight digits of the WAN MAC address, thus the attacker may access the network by sniffing the beacon frames.
CVE-2009-2861	***Network Mode:*** Infrastructure / Ad Hoc ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive Scanning

	Spoofing Technique: Frame Spoofing ***Attack Management:*** ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** Denial of Service / Compromising data integrity ***Description:*** The Over-the-Air Provisioning (OTAP) functionality on Cisco Aironet Lightweight Access Point 1100 and 1200 devices does not properly implement the access point association, thus the attacker may spoof the controller and cause a denial of service (service outage) via crafted remote radio management (RRM) packets.
CVE-2009-3341	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** ***Attack Management:*** ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** Disclosure confidential Information / Compromising data integrity/ DoS. ***Description:*** Buffer overflow on the Linksys WRT54GL wireless router allows the attacker to execute arbitrary code via unspecified vectors.
CVE-2009-0282	***Network Mode:*** Ad Hoc ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive ***Spoofing Technique:*** ***Attack Management:*** ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** DoS. ***Description:*** The vulnerability of integer overflow in Ralink Technology USB wireless adapter (RT73-3.08), and other wireless card drivers including rt2400, rt2500, rt2570, and rt61, allows the attacker to cause a denial of service and possibly execute arbitrary code via a Probe Request packet with a long SSID.
CVE-2007-5651	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized

	Scanning Technique: Passive Scanning ***Spoofing Technique:*** ***Attack Management:*** ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** DoS. ***Description:*** The vulnerability of the Extensible Authentication Protocol (EAP) implementation in Cisco IOS 12.3 and 12.4 on Cisco Access Points and 1310 Wireless Bridges (Wireless EAP devices), IOS 12.1 and 12.2 on Cisco switches (Wired EAP devices), and CatOS 6.x through 8.x on Cisco switches, may allow an attacker to cause a denial of service via a crafted EAP Response Identity packet.
CVE-2007-4012	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive Scanning ***Spoofing Technique:*** ***Attack Management:*** ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** DoS. ***Description:*** The vulnerability in Cisco 4100 and 4400, Airespace 4000, and Catalyst 6500 and 3750 WLAN Controller (WLC) software 4.1 (before 4.1.180.0), may allow the attacker to cause a denial of service (ARP storm) via a broadcast ARP packet that targets the IP address of a targeted client.
CVE-2007-2927	***Network Mode:*** Ad Hoc ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive Scanning ***Spoofing Technique:*** ***Attack Management:*** Semi-automatic ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** DoS. ***Description:*** The vulnerability in Atheros 802.11 a/b/g wireless adapter drivers before 5.3.0.35 and 6.x (before 6.0.3.67) may allow the attacker to cause a denial of service via a crafted 802.11 management frame.

CVE-2007-2039	***Network Mode:*** Infrastructure ***Access Privilege:*** Unauthorized ***Scanning Technique:*** Passive Scanning ***Spoofing Technique:*** ***Attack Management:*** Semi-automatic ***Attack Rate:*** ***Attack Collaboration:*** Autonomous ***Vulnerability:*** Implementation Flaws ***Attack Objective:*** DoS. ***Description:*** The Network Processing Unit (NPU) in the Cisco WLAN Controller (WLC) before 3.2.171.5, 4.0.x (before 4.0.206.0, and 4.1.x) allows the attackers on a local wireless network to cause a denial of service (loss of packet forwarding) via crafted SNAP packets, malformed 802.11 traffic, or packets with certain header length values.

References

[ABVC04] ABOBA, B. ; BLUNK, L. ; VOLLBRECHT, J. ; CARLSON, J. ; LEVKOWETZ, H.: *Extensible Authentication Protocol (EAP)* : RFC 3748, Internet Engineering Task Force (IETF), 2004

[Aesa01] AES ALGORITHM: Advanced Encryption Standard (AES). In: *Federal Information Processing Standards Publication 197*, National Institute of Standards and Technology (NIST) (2001)

[Airc13] AIRCRACK-NG: *Aircrack-ng - WEP/WPA Cracking Tools*. URL http://www.aircrack-ng.org/doku.php?id=Main

[Aird13] AIRDEFENSE: *AirDefense - Wireless Intrusion Detection System*. URL http://www.airdefense.net

[Aire13] AIREPLAY-NG: *Aireplay-ng - Packet Injection Tool*. URL http://www.aircrack-ng.org/doku.php?id=aireplay-ng

[Airh13] AIRHORN: *AirHORN - RF Generator*. URL http://nutsaboutnets.com/airhorn-signal-generator/

[Airj13] AIRJACK: *AirJack - Device Driver*. URL http://sourceforge.net/projects/airjack/

[Airm13] AIRMAGNET: *AirMagnet - Wireless Intrusion Detection/Prevention System*. URL http://www.airmagnet.com/products/enterprise/

[Airo13] AIRODUMP-NG: *Airodump-ng - Packet Capture Tool*. URL http://www.aircrack-ng.org/doku.php?id=airodump-ng

[Airp13] AIRPWN: *Airpwn - Packet Injection Tool*. URL http://airpwn.sourceforge.net/Airpwn.html

[Airs13a] AIRSNORT: *AirSnort - WEP Cracking Tool*. URL http://airsnort.shmoo.com/

[Airs13b] AIRSNARF: *Airsnarf - Rogue Wireless Access Point Setup Utility*. URL http://airsnarf.shmoo.com/

[Airs13c] AIRSNARE: *AirSnare - Wireless Intrusion Detection System*. URL http://home.comcast.net/~jay.deboer/airsnare/

[Airt13] AIRTRAF: *AirTraf - Wireless Network Analyzer*. URL http://airtraf.sourceforge.net/

[AmGP03] AMETER, C.R. ; GRIFFITH, R. A. ; PICKETT, J. K.: *WHIFF - Wireless Intrustion Detection System*. Technical Report, Foundstone, Inc. and Carnegie Mellon University, 2003

[Ande80] ANDERSON, J. P.: *Computer Security Threat Monitoring and Surveillance*. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, 1980

[AnWi11] ANDRESS, J. ; WINTERFELD, S.: *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 1st. ed. : Syngress, Elsevier, 2011

[ArCh07] ARTAN, N. S. ; CHAO, H.J.: TriBiCa: Trie Bitmap Content Analyzer for High-Speed Network Intrusion Detection. In: *Proceedings of the 26th IEEE International Conference on Computer Communications (IEEE INFOCOM'07)*. Anchorage, Alaska, USA : IEEE, 2007, pp. 125–133

[Armi13] ARMITAGE: *Armitage - Cyber Attack Managment for Metasploit*. URL http://www.fastandeasyhacking.com/

[Axel99] AXELSSON, S.: The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection. In: *Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS'99)*. Singapore : ACM Press, 1999, pp. 1–7

[Back13] BACKTRACK: *BackTrack - Linux Penetration Testing Distribution*. URL http://www.backtrack-linux.org/

[BaJo04] BARSE, E.L. ; JONSSON, E.: Extracting Attack Manifestations to Determine Log Data Requirements for Intrusion Detection. In: *Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04)*. Tucson, AZ, USA : IEEE, 2004, pp. 158–167

[BaMe01] BACE, R. ; MELL, P.: *Intrusion Detection Systems*. Technical report, National Institute of Standards and Technology, NIST SP800-31, 2001

[BeSa03] BELLARDO, J. ; SAVAGE, S.: 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In: *Proceedings of the 12th USENIX Security Symposium*. vol. 3. Washington, USA : USENIX, 2003, pp. 15–28

[Bidg06] BIDGOLI, H.: *Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management*. vol. 3. 1st. ed. : John Wiley & Sons, 2006

[BiTa09] BICAKCI, K. ; TAVLI, B.: Denial-of-Service Attacks and Countermeasures in IEEE 802.11 Wireless Networks. In: *Computer Standards & Interfaces,* vol. 31, Elsevier (2009), Nr. 5, pp. 931–941

[BoGW01] BORISOV, N. ; GOLDBERG, I. ; WAGNER, D.: Intercepting Mobile Communications: The Insecurity of 802.11. In: *Proceedings of the 7th ACM Annual International Conference on Mobile Computing And Networking (MOBICOM'01)*. Rome, Italy : ACM, 2001, pp. 180–189

[BrKo03] BRUTCH, P. ; KO, C.: Challenges in Intrusion Detection for Wireless Ad-Hoc Networks. In: *Proceedings of the Symposium on Applications and the Internet Workshops (SAINT'03)*. Florida, USA : IEEE, 2003, pp. 368–373

[CaBS06] CARDENAS, A. A. ; BARAS, J. S. ; SEAMON, K.: A Framework for the Evaluation of Intrusion Detection Systems. In: *Proceedings of the IEEE Symposium on Security and Privacy (S&P'06)*. California, USA : IEEE, 2006, pp. 63–77

[Canv13] CANVAS: *CANVAS - Exploit Framework*. URL http://www.immunitysec.com/products-canvas.shtml

[ChHu08] CHIANG, J. T. ; HU, Y.-C.: Dynamic Jamming Mitigation for Wireless Broadcast Networks. In: *Proceedings of the 27th IEEE International Conference on Computer Communications (IEEE INFOCOM'08)*. Phoenix, AZ, USA : IEEE, 2008, pp. 1211–1219

[Chop13] CHOPCHOP: *Aircrack-ng suite for Chopchop Attack*. URL http://www.aircrack-ng.org/doku.php?id=korek_chopchop

[Cnss10] CNSSI, COMMITTEE ON NATIONAL SECURITY SYSTEMS: National Information Assurance (IA) Glossary. In: *CNSS Instruction No. 4009* (2010)

[Cohe95] COHEN, F.: *Protection and Security on the Information Superhighway*. 1st. ed. : John Wiley & Sons, 1995

[Cohe97] COHEN, F.: Information System Attacks: A Preliminary Classification Scheme. In: *Computers & Security,* vol. 16, Elsevier (1997), Nr. 1, pp. 29–46

[Comm13] COMMVIEW: *CommView - Wireless Network Monitor and Analyzer*. URL https://www.tamos.com/products/commwifi/

[Cte13] CTE: *Classification Tree Editor*. URL http://systematic-testing.com/functional_testing/cte_main.php?cte=1

[Cve01] CVE-2001-0160: *Common Vulnerabilities and Exposures, 2001-0160*. URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0160

[Cve05] CVE-2005-3802: *Common Vulnerabilities and Exposures, 2005-3802*. URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3802

[Cve06] CVE-2006-6059: *Common Vulnerabilities and Exposures, 2006-6059*. URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6059

[Cve07a] CVE-2007-5651: *Common Vulnerabilities and Exposures, 2007-5651*. URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5651

[Cve07b] CVE-2007-4012: *Common Vulnerabilities and Exposures, 2007-4012*. URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4012

[Cve09a] CVE-2009-0052: *Common Vulnerabilities and Exposures, 2009-0052*. URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0052

[Cve09b] CVE-2009-0282: *Common Vulnerabilities and Exposures, 2009-0282*. URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0282

[Cve10] CVE-2010-3033: *Common Vulnerabilities and Exposures, 2010-3033*. URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3033

[Cve13a] CVE-2013-1105: *Common Vulnerabilities and Exposures, 2013-1105*. URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1105

[Cve13b] CVE-2013-4613: *Common Vulnerabilities and Exposures, 2013-4613*. URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4613

[Cvew13] CVE WIRELESS: *Common Vulnerabilities and Exposures - Wireless*. URL http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wireless

[DCTA12] DACOSTA, I. ; CHAKRADEO, S. ; TRAYNOR, P. ; AHAMAD, M.: One-Time Cookies: Preventing Session Hijacking Attacks with Disposable Credentials. In: *ACM Transactions on Internet Technology (TOIT)* vol. 12, ACM (2012), Nr. 1

[DDWL98] DEBAR, H. ; DACIER, M. ; WESPI, A. ; LAMPART, S.: *An Experimentation Workbench for Intrusion Detection Systems*. Technical Report, IBM Research Division, Zurich Research Laboratory, 1998

[Deau13] DEAUTH FLOOD MODULE: *Deauthentication Flood - Metasploit Auxiliary Module & Exploit Database*. URL http://www.metasploit.org/modules/auxiliary/dos/wifi/deauth

[DeDW99] DEBAR, H. ; DACIER, M. ; WESPI, A.: Towards a Taxonomy of Intrusion-Detection Systems. In: *Computer Networks,* vol. 31, Elsevier (1999), Nr. 9, pp. 805–822

[DeMo02] DEBAR, H. ; MORIN, B.: Evaluation of the Diagnostic Capabilities of Commercial Intrusion Detection Systems. In: *Proceedings of the 5th international conference on Recent advances in intrusion detection (RAID'02)*. Zurich, Switzerland : Springer, 2002, pp. 177–198

[DeNe85] DENNING, D. E. ; NEUMANN, P. G.: *Requirements and Model for IDES - A Real-Time Intrusion Detection System*. Technical Report, Computer Science Laboratory, SRI International, 1985

[Denn87] DENNING, D. E.: An Intrusion-Detection Model. In: *IEEE Transactions on Software Engineering,* vol. 13, IEEE (1987), Nr. 2, pp. 222–232

[DeRa97] DEVENDER ; RAMASAMY, S.R.: A Review of EMI Shielding and Suppression Materials. In: *proceedings of the International Conference on Electromagnetic Interference and Compatibility* : IEEE, 1997, pp. 459–466

[DeWe01] DEBAR, H. ; WESPI, A.: Aggregation and Correlation of Intrusion-Detection Alerts. In: *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID'01)*. Davis, CA, USA : Springer, 2001, pp. 85–103

[DoMi04] DOULIGERIS, C. ; MITROKOTSA, A.: DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art. In: *Computer Networks,* vol. 44, Elsevier (2004), pp. 643–666

[Douc02] DOUCEUR, J. R.: The Sybil Attack. In: *Proceedings of the International Workshop on Peer-to-Peer Systems (IPTPS'02)*. Cambridge, MA, USA : Springer, 2002, pp. 251–260

[File13] FILE2AIR: *File2air - Wireless Traffic Injection Tool*. URL http://www.willhackforsushi.com/File2air.html

[FlMS01] FLUHRER, S. R. ; MANTIN, I. ; SHAMIR, A.: Weaknesses in the Key Scheduling Algorithm of RC4. In: *Proceedings of the 8th Annual International Workshop on*

Selected Areas in Cryptography (SAC'01). Toronto, Canada : Springer, 2001, pp. 1–24

[FoLe06] FOGLA, P. ; LEE, W.: Evading Network Anomaly Detection Systems: Formal Reasoning and Practical Techniques. In: *Proceedings of the 13th ACM conference on Computer and communications security (CCS'06)*. Alexandria, VA, USA : ACM, 2006, pp. 59–68

[Fong11] FONG, P. W. L.: Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems. In: *Proceedings of the IEEE Symposium on Security and Privacy (S&P'11)*. Oakland, CA, USA : IEEE, 2011, pp. 263–278

[GaAD07] GAD-EL-RAB, M. ; ABOU EL KALAM, A. ; DESWARTE, Y.: Defining Categories to Select Representative Attack Test-Cases. In: *Proceedings of the ACM Workshop on Quality of Protection (QoP'07)*. Alexandria, VA, USA : ACM, 2007, pp. 40–42

[Gade08] GAD-EL-RAB, M.: *Evaluation of intrusion detection systems*, PhD Thesis, Université de Toulouse - Paul Sabatier, France, 2008

[Gast05] GAST, M.: *802.11 Wireless Networks: The Definitive Guide*. 2nd. ed. : O 'Reilly, 2005

[GaUl01] GAFFNEY, J. E. ; ULVILA, J. W.: Evaluation of Intrusion Detectors: A Decision Theory Approach. In: *Proceedings of the IEEE Symposium on Security and Privacy (S&P'01)*. Oakland, CA, USA : IEEE, 2001, pp. 50–61

[GFDL06] GU, G. ; FOGLA, P. ; DAGON, D. ; LEE, W. ; SKORIC, B.: Measuring Intrusion Detection Capability: An Information-Theoretic Approach. In: *Proceedings of the ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS'06)*. Taipei, Taiwan : ACM, 2006, pp. 90–101

[Gibs11] GIBSON, D.: *Managing Risk in Information Systems*. 1st. ed. : Jones & Bartlett Learning, LLC, 2011

[GiSC06] GILL, R. ; SMITH, J. ; CLARK, A.: Specification-Based Intrusion Detection in WLANs. In: *Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06)*. vol. 141–152. Florida, USA : IEEE, 2006, pp. 141 – 152

[GuCh05] GUO, F. ; CHIUEH, T.-C.: Sequence Number-Based MAC Address Spoof Detection. In: *Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection (RAID'05)*. Washington, USA : Springer, 2005, pp. 309–329

[HaHu05] HANSMAN, S. ; HUNT, R.: A Taxonomy of Network and Computer Attacks. In: *Computers and Security,* vol. 24, Elsevier (2005), Nr. 1, pp. 31–43

[HaWi66] HANCOCK, J. C. ; WINTZ, P. A.: *Signal Detection Theory*. 1st. ed. : McGraw-Hill, 1966

[HCCB12] HE, D. ; CHEN, C. ; CHAN, S. ; BU, J.: DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks. In: *IEEE Transactions on Wireless Communications,*. vol. 11 : IEEE, 2012, pp. 1946 – 1956

[HDLM90] HEBERLEIN, T.L. ; DIAS, G. V. ; LEVITT, K. N. ; MUKHERJEE, B. ; WOOD, J. ; WOLBER, D.: A Network Security Monitor. In: *in Proceedings of the IEEE Symposium on Research in Security and Privacy*. Los Alamitos, CA, USA : IEEE, 1990, pp. 296–304

[HKKJ05] HSIU, P.-C. ; KUO, C-F. ; KUO, T.-W. ; JUAN, E. Y. T.: Scenario Based Threat Detection and Attack analysis. In: *Proceedings of the 39th Annual International Carnahan Conference on Security Technology (CCST '05)*. Las Palmas de G.C., Spain : IEEE, 2005, pp. 279–282

[Howa97] HOWARD, J. D.: *An Analysis of Security Incidents on the Internet 1989-1995*, PhD Thesis, Carnegie Mellon University, USA, 1997

[HsSL08] HSU, Y. ; SHU, G. ; LEE, D.: A Model-based Approach to Security Flaw Detection of Network Protocol Implementations. In: *Proceedings of the IEEE International Conference on Network Protocols (ICNP'08)*. Orlando, Fl, USA : IEEE, 2008, pp. 114–123

[HSTL11] HAN, H. ; SHENG, B. ; TAN, C. C. ; LI, Q. ; LU, S.: A Timing-Based Scheme for Rogue AP Detection. In: *IEEE Transactions on Parallel and Distributed Systems,* vol. 22, IEEE (2011), Nr. 11, pp. 1912–1925

[HuPJ03] HU, Y.-C. ; PERRIG, A. ; JOHNSON, D. B.: Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In: *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM'03)*. vol. 3. San Francisco, California, USA : IEEE, 2003, pp. 1976–1986

[IcSV95] ICOVE, D. ; SEGER, K. ; VONSTORCH, W.: *Computer Crime: A Crimefighter's Handbook*. 1st. ed. : O'Reilly Media, 1995

[Ieee04] IEEE_STD802.11I–2004: *WLAN Medium Access Control (MAC) Security Enhancements* : IEEE Standards Association, IEEE Computer Society, 2004

[Ieee12] IEEE_STD, 802.11-2012: *WLAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* : IEEE Standards Association, IEEE Computer Society, 2012

[Jain91] JAIN, R.: *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*. 1st. ed. : John Wiley & Sons, 1991

[JLMY12] JAMSHED, M. ; LEE, J. ; MOON, S. ; YUN, I. ; KIM, D. ; LEE, S. ; YI, Y. ; PARK, K.: Kargus: A Highly-Scalable Software-Based Intrusion Detection System. In: *Proceedings of the ACM conference on Computer and communications security (CCS'12)*. Raleigh, NC, USA : ACM, 2012, pp. 317–328

[JNPF10] JIACHENG, H. ; NING, L. ; PING, Y. ; FUTAI, Z. ; QIANG, Z.: Securing Wireless Mesh Network with Mobile Firewall. In: *Proceedings of the International Conference on Wireless Communications and Signal Processing (WCSP'10)*. Suzhou, China, 2010, pp. 1–6

[Karm13] KARMA: *KARMA - Wireless Client Security Assessment Tools*. URL http://www.theta44.org/karma/index.html

[KaWa03] KARLOF, C. ; WAGNER, D.: Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. In: *Proceedings of the IEEE International Workshop on Sensor Network Protocols and Applications (SNPA'03)*. vol. 113–127. Anchorage, AK, USA : IEEE, 2003, pp. 113–127

[KhMB09] KHABBAZIAN, M. ; MERCIER, H. ; BHARGAVA, V. K.: Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks. In: *IEEE Transactions on Wireless Communications* vol. 8, IEEE (2009), Nr. 2, pp. 736–745

[KhMM08] KHATTAB, S. ; MOSSÉ, D. ; MELHEM, R.: Jamming Mitigation in Multi-Radio Wireless Networks: Reactive or Proactive? In: *Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks (SecureComm '08)*. Istanbul, Turkey : ACM, 2008

[KiMT04] KILLOURHY, K. S. ; MAXION, R. A. ; TAN, K. M.: A Defense-Centric Taxonomy Based on Attack Manifestations. In: *Proceedings of the International Conference on Dependable Systems and Networks (DSN'04)*. Florence, Italy : IEEE, 2004, pp. 102–111

[Kism13a] KISMET: *Kismet_WIDS*. URL http://www.kismetwireless.net/

[Kism13b] KISMAC: *KisMAC - Wireless Network Discovery Tool*. URL http://trac.kismac-ng.org/

[KMMZ06] KHATTAB, S. ; MELHEM, R. ; MOSSÉ, D. ; ZNATI, T.: Honeypot Back-Propagation for Mitigating Spoofing Distributed Denial-of-Service Attacks. In: *Journal of Parallel and Distributed Computing (JPDC)* vol. 66, Elsevier (2006), pp. 1152–1164

[Kore04] KOREK: *chopchop - Eexperimental WEP Attacks*. URL http://www.netstumbler.org/unix-linux/chopchop-experimental-wep-attacks-t12489.html. — NetStumbler.org Forums

[Kuma95] KUMAR, S.: *Classification and Detection of Computer Intrusions*, PhD Thesis, Purdue University, USA, 1995

[LBMC94] LANDWEHR, C. E. ; BULL, A. R. ; MCDERMOTT, J.P. ; CHOI, W.S.: A Taxonomy of Computer Program Security Flaws. In: *ACM Computing Surveys,* vol. 26, ACM (1994), Nr. 3, pp. 211–254

[Levi02] LEVITT, K.: Intrusion Detection: Current Capabilities and Future Directions. In: *Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC'02)*. Las Vegas, Nevada, USA : IEEE, 2002, pp. 365–367

[LFGH00] LIPPMANN, R. ; FRIED, D. ; GRAF, I. ; HAINES, J. ; KENDALL, K. ; MCCLUNG, D. ; WEBER, D. ; WEBSTER, S. ; ET AL.: Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation. In: *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'00)*. vol. 2. Los Alamitos, CA, USA : IEEE, 2000, pp. 12–26

[LHFK00] LIPPMANN, R. ; HAINES, J. W. ; FRIED, D. ; KORBA, J. ; DAS, K.: Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation. In: *Proceedings of the International Workshop on the Recent Advances in Intrusion Detection (RAID'00)*. Toulouse, France : Springer, 2000, pp. 162–182

[LiNo05] LIN, G. ; NOUBIR, G.: On Link-Layer Denial of Service in Data Wireless LANs. In: *Wireless Communications & Mobile Computing,* vol. 5, Wiley (2005), Nr. 3, pp. 273–284

[LiTr07] LI, Q. ; TRAPPE, W.: Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships. In: *IEEE Transactions on Information Forensics and Security,* vol. 2, IEEE (2007), Nr. 4, pp. 793–808

[Long09] LONGMAN_DICTIONARY: *Longman Dictionary of Contemporary English*. 5th. ed. : Pearson Longman, 2009

[Loug01] LOUGH, D. L.: *A Taxonomy of Computer Attacks with Applications to Wireless Networks*, PhD Thesis, Virginia Polytechnic Institute and State University, USA, 2001

[LPMS05] LAZOS, L. ; POOVENDRAN, R. ; MEADOWS, C. ; SYVERSON, P. ; CHANG, L. W.: Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In: *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'05)*. vol. 2. New Orleans, LA, USA : IEEE, 2005, pp. 1193–1199

[LuJa88] LUNT, T. F. ; JAGANNATHAN, R.: A Prototype Real-Time Intrusion Detection Expert System. In: *Proceedings of the IEEE Symposium on Security and Privacy (S&P'88)*. Oakland, CA, USA : IEEE, 1988, pp. 59–66

[Macc13] MACCHANGER: *Macchanger - MAC Address Changer*. URL http://ftp.gnu.org/gnu/macchanger/

[Make13] MAC MAKEUP: *MAC MakeUp - MAC Address Changer*. URL http://www.gorlani.com/portal/projects/mac-makeup-the-original

[Mchu00] MCHUGH, J.: Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory. In: *ACM Transactions on Information and System Security (TISSEC),* vol. 3, ACM (2000), Nr. 4, pp. 262–294

[Mdk13] MDK3: *MDK3 - WLAN penetration tool*. URL http://distfiles.gentoo.org/distfiles/mdk3-v6.tar.bz2

[Merr03] MERRIAM-WEBSTER EDITORIAL STAFF: *Merriam-Webster's Collegiate Dictionary*. 11th. ed. : Merriam-Webster Inc., 2003

[Meta13a] METASPLOIT: *Metasploit - Penetration Testing Tool*. URL http://www.metasploit.com/

[Meta13b] METASPLOIT-MODULES: *Metasploit Auxiliary Modules & Exploit Database*. URL http://www.metasploit.org/modules/

[Mgen13] MGEN: *MGEN - Traffic Generation Tool*. URL http://cs.itd.nrl.navy.mil/work/mgen/

[Mill05] MILLIGAN, T. A.: *Modern Antenna Design*. 2nd. ed. : Wiley-IEEE Press, 2005

[MiRe04] MIRKOVIC, J. ; REIHER, P.: A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. In: *ACM SIGCOMM Computer Communication Review,* vol. 34, ACM (2004), Nr. 2, pp. 39–53

[NaAF11] NASR, K. ; ABOU EL KALAM, A. ; FRABOUL, C.: A Holistic Methodology for Evaluating Wireless Intrusion Detection Systems. In: *Proceedings of the International Conference on Network and System Security (NSS'11)*. Milan, Italy : IEEE, 2011, pp. 9–16

[NaAF12] NASR, K. ; ABOU EL KALAM, A. ; FRABOUL, C.: Performance Analysis of Wireless Intrusion Detection Systems. In: *Proceedings of the International Conference on Internet and Distributed Computing Systems (IDCS'12)*. Wu Yi Shan, Fujian, China : Springer, 2012, pp. 238–252

[Netg13] NETGEAR OVERFLOW MODULE: *NetGear MA521 Wireless Driver Long Rates Overflow - Metasploit Auxiliary Module & Exploit Database*. URL http://www.metasploit.com/modules/auxiliary/dos/wifi/netgear_ma521_rates

[Nets13] NETSTUMBLER: *NetStumbler - Wireless Network Discovery Tool*. URL http://www.netstumbler.com/2007/04/17/about/

[NGML08] NEIRA, P. ; GASCA, R.M. ; MACCARI, L. ; LEFEVRE, L.: Stateful Firewalling for Wireless Mesh Networks. In: *Proceedings of the IFIP International Conference on New Technologies, Mobility and Security (NTMS'08)*. Tangier, Morocco : IEEE, 2008, pp. 1–5

[NiLD08] NING, P. ; LIU, A. ; DU, W.: Mitigating DoS Attacks Against Broadcast Authentication in Wireless Sensor Networks. In: *ACM Transactions on Sensor Networks (TOSN)* vol. 4, ACM (2008), Nr. 1

[Nvdn13] NVD-NIST: *National Vulnerability Database-National Institute of Standards and Technology*. URL http://nvd.nist.gov/home.cfm

[Oxfo11] OXFORD DICTIONARIES: *Concise Oxford English Dictionary*. 12th. ed. : Oxford University Press, 2011

[PCOM97] PUKETZA, N. ; CHUNG, M. ; OLSSON, R. A. ; MUKHERJEE, B.: A Software Platform for Testing Intrusion Detection Systems. In: *Journal of IEEE Software,* vol. 14, IEEE (1997), Nr. 5, pp. 43–51

[PiMa08] DI PIETRO, R. ; MANCINI, L. V. (eds.): *Intrusion Detection Systems*. 1st. ed. Advances in Information Security Series, vol. 38 : Springer, 2008

[PoSC09] POPPER, C. ; STRASSER, M. ; CAPKUN, S.: Jamming-Resistant Broadcast Communication without Shared Keys. In: *Proceedings of the 18th USENIX Security Symposium*. Montreal, Canada : USENIX, 2009, pp. 231–248

[PXYN08] PING, Y. ; XINGHAO, J. ; YUE, W. ; NING, L.: Distributed Intrusion Detection for Mobile Ad Hoc Networks. In: *Systems Engineering and Electronics,* vol. 19, IEEE (2008), Nr. 4, pp. 851 – 859

[PZCB96] PUKETZA, N. J. ; ZHANG, K. ; CHUNG, M. ; B, MUKHERJEE ; OLSSON, R. A.: A Methodology for Testing Intrusion Detection Systems. In: *IEEE Transactions on Software Engineering,* vol. 22, IEEE (1996), Nr. 10, pp. 719–729

[Rafa13] RAFALEX: *RafaleX Packet Builder*. URL http://www.securityfocus.com/tools/2158

[Rams13] RAMSEY ELECTRONICS, LLC: *RF Filtered Connectors - CONN278 & STERF13*. URL http://www.ramayes.com/ramsey_test_enclosure_connectors.htm

[RiRa04] RITTINGHOUSE, J. W. ; RANSOME, J. F.: *Wireless Operational Security*. 1st. ed. : Elsevier, 2004

[Rive92] RIVEST, R.L.: *The RC4 Encryption Algorithm* : RSA Data Security, Inc., 1992

[RoJL06] ROMAN, R. ; JIANYING, Z. ; LOPEZ, J.: Applying Intrusion Detection Systems to Wireless Sensor Networks. In: *Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC'06)*. vol. 1. Las Vegas, Nevada, USA : IEEE, 2006, pp. 640–644

[Rude13] RUDE/GRUDE: *Rude/Crude - Traffic Generation Tool*. URL http://rude.sourceforge.net/

[RuJM05] RUBIN, S. ; JHA, S. ; MILLER, B. P.S.: Language-Based Generation and Evaluation of NIDS Signatures. In: *Proceedings of the IEEE Symposium on Security and Privacy (P&S'05)*. Oakland, CA, USA : IEEE, 2005, pp. 3–17

[Send13] SENDIP: *SendIP - IP Packet Generation Tool*. URL http://snad.ncsl.nist.gov/ipv6/sendip.html

[Seyb05] SEYBOLD, J.S.: *Introduction to RF Propagation*. 1st. ed. : John Wiley & Sons, Inc., 2005

[SFLP00] STOLFO, S. ; FAN, W. ; LEE, W. ; PRODROMIDIS, A. ; CHAN, P.: Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project. In: *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'00)*. vol. 2. South Carolina, USA : IEEE, 2000, pp. 130–144

[SGFS02] SEKAR, R. ; GUPTA, A. ; FRULLO, J. ; SHANBHAG, T. ; TIWARI, A. ; YANG, H. ; ZHOU, S.: Specification-Based Anomaly Detection: A New Approach for Detecting Network Intrusions. In: *Poceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02)*. Washington, DC, USA : ACM, 2002, pp. 265–274

[Shir07] SHIREY, R.: *Internet Security Glossary*. 2nd. ed. : RFC 4949, Internet Engineering Task Force (IETF), 2007

[Skla01] SKLAR, B.: *Digital Communications: Fundamentals and Applications*. 2nd. ed. : Prentice Hall, 2001

[Smac13] SMAC: *SMAC - MAC Address Changer*. URL http://www.klcconsulting.net/smac/

[SmEJ06] SMITH, R. ; ESTAN, C. ; JHA, S.: Backtracking Algorithmic Complexity Attacks Against a NIDS. In: *Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06)*. Miami Beach, FL, USA : IEEE, 2006, pp. 89–98

[Snor13] SNORT: *Snort - Intursion Detection System*. URL http://www.snort.org/

[Sobh06] SOBH, T.: Wired and Wireless Intrusion Detection System: Classifications, Good Characteristics and State-of-the-Art. In: *Computer Standards and Interfaces,* vol. 28, Elsevier (2006), Nr. 6, pp. 670–694

[SPTL97] STOLFO, S. ; PRODROMIDIS, A. L. ; TSELEPIS, S. ; LEE, W. ; FAN, W. ; CHAN, P. K.: JAM: Java Agents for Meta-Learning over Distributed Databases. In: *Proceedings of the International Conference on Knowledge Discovery and Data Mining (KDD'97)*. CA, USA, 1997, pp. 74–81

[Stal10] STALLINGS, W.: *Cryptography and Network Security: Principles and Practice*. 5th. ed. : Prentice Hall, 2010

[STCK08] SHENG, Y. ; TAN, K. ; CHEN, G. ; KOTZ, D. ; CAMPBELL, A.: Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength. In: *Proceedings of the 27th IEEE International Conference on Computer Communications (IEEE INFOCOM'08)*. Phoenix, AZ, USA : IEEE, 2008, pp. 1768–1776

[Step01] STEPHEN, J.: *The Changing Face of Distributed Denial of Service Mitigation* : SANS Institute, 2001

[StGF02] STONEBURNER, G. ; GOGUEN, A. ; FERINGA, A.: *Risk Management Guide for Information Technology Systems* : National Institute of Standards and Technology, NIST SP800-30, 2002

[StWA05] STANLEY, D. ; WALKER, J. ; ABOBA, B.: *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs* : RFC 4017, Internet Engineering Task Force (IETF), 2005

[SuSA06] SUBHADRABANDHU, D. ; SARKAR, S. ; ANJUM, F.: A Statistical Framework for Intrusion Detection in Ad Hoc Networks. In: *Proceedings of the 25th IEEE International Conference on Computer Communications (IEEE INFOCOM'06)*. Barcelona, Spain : IEEE, 2006, pp. 1–13

[Swen08] SWENSON, C.: *Modern Cryptanalysis: Techniques for Advanced Code Breaking*. 1st. ed. : John Wiley & Sons, Inc., 2008

[TDSC02] TIPPER, D. ; DAHLBERG, T. ; SHIN, H. ; CHARNSRIPINYO, C.: Providing Fault Tolerance in Wireless Access Networks. In: *IEEE Communications Magazine,* vol. 40, IEEE (2002), Nr. 1, pp. 58–64

[TKLB11] TAGHIZADEH, M. ; KHAKPOUR, A. R. ; LIU, A. X. ; BISWAS, S.: Collaborative Firewalling in Wireless Networks. In: *Proceedings of the 30th IEEE International*

Conference on Computer Communications (IEEE INFOCOM'11). Shanghai , China : IEEE, 2011, pp. 46–50

[Tong08] TONG, X. C.: *Advanced Materials and Design for Electromagnetic Interference Shielding*. 1st. ed. : CRC Press, 2008

[TSBK05] TSENG, C. H. ; SONG, T. ; BALASUBRAMANYAM, P. ; KO, C. ; LEVITT, K.: A Specification-Based Intrusion Detection Model for OLSR. In: *Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection (RAID'05)*. Washington, USA : Springer, 2005, pp. 330–350

[Usc12] 44USC, SEC.3542-DEFINITIONS: *Subchapter III - Information security, Chapter 35 - Coordination of Federal Information Policy, Title 44 - Public Printing and Documents, United States Code (44USC)* : United States Code (44USC), 2012

[VGSB04] VIGNA, G. ; GWALANI, S. ; SRINIVASAN, K. ; BELDING-ROYER, E. ; KEMMERER, R.: An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks. In: *Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04)*. Tucson, Arizona, USA : IEEE, 2004, pp. 16–27

[Vine02] VINES, R. D.: *Wireless Security Essentials: Defending Mobile Systems from Data Piracy*. 1st. ed. : John Wiley & Sons, Inc., 2002

[Void13] VOID11: *Void11 - Penetration Testing Tool for Wireless Networks*. URL http://www.wirelessdefence.org/Contents/Void11Main.htm

[WaDe01] WAGNER, D. ; DEAN, D.: Intrusion Detection via Static Analysis. In: *Proceedings of the IEEE Symposium on Security and Privacy (P&S'01)*. Oakland, CA, USA : IEEE, 2001, pp. 156–168

[Well13] WELLENREITER: *Wellenreiter - Wireless Network Discovery and Auditing Tool*. URL http://wellenreiter.sourceforge.net/

[Wepc13] WEPCRACK: *WEPCrack - WEP Cracking Tool*. URL http://wepcrack.sourceforge.net/

[Wifi13a] WIFIFOFUM: *WiFiFoFum - Wardriving Tool*. URL http://www.wififofum.net/

[Wifi13b] WIFIJAMMER: *Wifijammer - RF Jamming Tool*. URL http://code.google.com/p/wifijammer/

[Wire13] WIRESHARK: *WireShark - Network Protocol Analyzer*. URL http://www.wireshark.org/

[WoSt04] WOOD, A. ; STANKOVIC, A.: A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks. In: *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*. 1st. ed. : CRC Press, 2004

[Wpa03] WPA: *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks* : Wi-Fi Alliance, 2003

[Wpaw05] WPA & WPA2: *Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise* : Wi-Fi Alliance, 2005

[WSPH08] WILKERSON, J. ; SKEEN, M. ; PATRICK, D. ; HODGES, R. ; SCHIMIZZI, R. ; VORA, S. ; ZHIPING, F. ; GARD, K. ; ET AL.: Acoustic-RF Anechoic Chamber Construction and Evaluation. In: *Proceedings of the IEEE Radio and Wireless Symposium (RWS'08)*. Orlando, Fl, USA : IEEE, 2008, pp. 331–334

[XTZW05] XU, W. ; TRAPPE, W. ; ZHANG, Y. ; WOOD, T.: The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In: *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking (MobiHoc'05)*. Urbana-Champaign, IL, USA : ACM, 2005, pp. 46–57

[YCTC09] YANG, J. ; CHEN, Y. ; TRAPPE, W. ; CHENG, J.: Determining the Number of Attackers and Localizing Multiple Adversaries in Wireless Spoofing Attacks. In: *Proceedings of the 28th IEEE International Conference on Computer Communications (IEEE INFOCOM'09)*. Rio de Janeiro, Brazil : IEEE, 2009, pp. 666–674

[YGKX08] YU, H. ; GIBBONS, P. B. ; KAMINSKY, M. ; XIAO, F.: SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks. In: *Proceedings of the IEEE Symposium on Security and Privacy (S&P'08)*. Oakland, CA, USA : IEEE, 2008, pp. 3–17

[YGXC10] YANG, J ; GE, Y. ; XIONG, H. ; CHEN, Y. ; LIU, H.: Performing Joint Learning for Passive Intrusion Detection in Pervasive Wireless Environments. In: *Proceedings of the 29th IEEE International Conference on Computer Communications (IEEE INFOCOM'10)*. vol. 1–9. San Diego, CA, USA : IEEE, 2010, pp. 1–9

[YKGF06] YU, H. ; KAMINSKY, M. ; GIBBONS, P. B. ; FLAXMAN, A. D.: SybilGuard: Defending Against Sybil Attacks via Social Networks. In: *Proceedings of the ACM conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '06)*. Pisa, Italy : ACM, 2006, pp. 267–278

[YZZW12] YI, P. ; ZHU, T. ; ZHANG, Q. ; WU, Y. ; LI., J.: Green Firewall: an Energy-Efficient Intrusion Prevention Mechanism in Wireless Sensor Network. In: *Proceedings of the IEEE Global Communications Conference (GLOBECOM'12)*. Anaheim, CA, USA : IEEE, 2012, pp. 3037–3042

[ZhLe00] ZHANG, Y. ; LEE, W.: Intrusion Detection in Wireless Ad-hoc Networks. In: *Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom'00)*. Boston, MA, USA : ACM, 2000, pp. 275–283

[ZhLH03] ZHANG, Y. ; LEE, W. ; HUANG, Y-A.: Intrusion Detection Techniques for Mobile Wireless Networks. In: *Wireless Networks,* vol. 9, Springer (2003), Nr. 5, pp. 545–556

[ZiWr12] ZILL, D. G. ; WRIGHT, W. S.: *Advanced Engineering Mathematics*. 5th. ed. : Jones & Bartlett Learning, 2012