Global Journals LATEX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

A Performance Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network

Mr. Rupinder Singh[1] and Dr. Jatinder Singh[2]

[1] Khalsa College, Amritsar, Punjab, India.

Received: 11 December 2011 Accepted: 4 January 2012 Published: 15 January 2012

Abstract

Wireless Intrusion Detection System (IDS) performance metrics are used to measure the ability of a wireless IDS to perform a particular task and to fit within the performance constraints. These metrics measure and evaluate the parameters that impact the performance of a wireless IDS.Wireless IDS analyze wireless specific traffic including scanning for external users trying to connect to the network through access points and play important role in security to the wireless network. Design of wireless IDS is a difficult task as wireless technology is advancing every day, performance metrics can play an important role in the design of efficient wireless IDS by measuring the factors concern with the performance of a wireless IDS. In this paper we provide a performance metrics scorecard based approach to evaluate intrusion detection systems that are currently popular for wireless networks in the commercial sector. We provide a set of performance metrics that are relevant to wireless IDS and use a "scorecard" containing the set of values as the centerpiece of testing and evaluating a wireless IDS. Evaluation of a wireless IDS is done by assigning score to various performance metrics concern with wireless IDS. We apply our performance metrics scorecard evaluation based approach to three popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. Finally we discuss the results and the opportunities for further work in this area.

Index terms— IDS, Performance metrics, Performance Constraints Access Points, Wireless, Metrics, Scorecard.

1 Introduction

ireless network is a novel technology involving the deployment of hundreds of low-cost, microhardware, and resource-limited sensor nodes. Wireless technologies are becoming increasingly ubiquitous in modern networks; however, this new technology comes with its own set of challenges. Wireless networks are inherently 'open' and viewable by all network scanners. There are no physical barriers between data sent through the air. As such, it is relatively easy to intercept data packets in a wireless network.

The biggest concern with wireless network is its security, for some time wireless has had very poor, if any, security on a wide-open medium. Wireless Intrusion Detection System (WIDS) is a new solution to help Author ? : Rupinder Singh, Department of Computer Science, Khalsa College, Amritsar, Punjab, India. E-mail : rupi_singh76@yahoo.com Author ? : Dr. Jatinder Singh, Principal, Golden College of Engg. & Tech., Gurdaspur, Punjab, India. E-mail : bal_jatinder@rediffmail.com combat this problem. An Intrusion Detection System (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a management station ??Wikipedia, 2012). A wireless IDS performs this exclusively for the wireless network. This system monitors traffic on network looking for and logging threats and alerting personnel to respond.

Lord Kelvin said ”If you cannot measure it, you cannot improve it”. This fact also applies to wireless network security issues. An activity cannot be managed if it cannot be measured, this is a widely accepted management principle and security falls under this rubric. Metrics can be an effective tool for detecting the capability of a wireless IDS. Metrics can help in raising the level of security awareness within the network. Security metrics that are related to wireless network are hard to generate because the discipline itself is still in the early stages of development. There is not yet a common vocabulary and not many documented best practices to follow [4].

In this paper we provide a performance metrics scorecard based approach to evaluate intrusion detection systems that are currently popular for wireless network in the commercial sector. We describe a testing methodology we developed to evaluate Wireless IDS by assigning score to various performance metrics concern with wireless IDS. The approach followed in this paper do not compare wireless IDS against each other, but against a set of performance metrics concern with wireless IDS.

The generalized approach of this paper will allow systems with any wireless requirements to tailor evaluation of ID technologies to their specific needs. Since evaluation is against a static set of performance metrics the evaluation may be extended for other metrics like logistical metrics, architectural metrics, quality metrics etc. The standard approach of comparison used in this paper also gives us scientific repeatability.

2 II.

3 Snort, airdefense guard and kismet wireless ids

In order to explain performance metrics scorecard based evaluation approach to wireless IDS, Snort works by implementing a detection engine that allows registering, warning, and responding to attacks previously defined. Snort is available under GPL (General Public License) and runs under Windows and GNU/Linux. It is among the most widely used, has a number of predefined signatures and continuously updated. Snort can be configured in three modes namely sniffer, packet logger, and network intrusion detection. In addition to all of these basic Snort features, Snort can be set up to send real-time alerts. This provides with the ability to receive alerts in real time, rather than having to continuously monitor Snort system. Snort is like a vacuum that takes packets and allows doing different things. Center piece of testing and evaluating wireless IDS will be a ”scorecard” containing the set of performance metrics and their definitions. Each metric can have low (+), average (++), or high (+++) score, where higher scores will be interpreted as more favorable ratings.

The performance metrics used are general characteristics that are relevant to the design of wireless IDS. The method used for observing each performance metric value can be either analysis (source code analysis) or open source material (such as specifications, white papers or reviews provided by vendors or users). We use open source material to analyze each performance metrics for wireless IDS. We examine publicly available research papers, reports, product documentation, published conference material (proceedings) and other material available for public review. b) Performance Metrics for Wireless IDS Performance metrics are used to measure the ability of a Wireless IDS to perform a particular task and to fit within the performance constraints. These metrics measure and evaluate the parameters that impact the performance of the wireless IDS [15]. The metrics defined in this area are shown in Table 1.

Table 1 In this section of the paper we will apply above mentioned approach to popular wireless IDS Snortwireless, AirDefense Guard, and Kismet. We choose these three for evaluation as they are most widely used and have different ways of working. Below with table **??** we describe how scores to performance metrics related to these three wireless IDS are assigned.

Performance metric False Positive Ratio can be assigned score depending on the following criteria: The weighted average of False Positive and False Negative ratios.

Induced Traffic Latency It measures the delay in the arrival of packets at the target network in the presence and absence of a wireless IDS.

4 Stress Handling and Point of Breakdown

The point of breakdown is defined as the level of network or host traffic that results in a shutdown or malfunction of IDS.

5 IDS Throughput

This metric defines the level of traffic up to which the IDS performs without dropping any packet.

6 Depth of System’s Detection Capability

It is defined as the number of attack signature patterns and/or behavior models known to it.

7 Reliability of Attack Detection

It is defined as the ratio of false positives to total alarms raised.

8 Possibility of Attack

It is defined as the ratio of false negatives to true negatives.

9 Consistency

It is defined as the variations in the performance of a wireless IDS.

10 Error Reporting and Recovery

The ability of a wireless IDS to correctly report and recover.

11 Firewall Interaction

The ability of a wireless IDS to interact with the Firewall systems.

12 User Friendliness

The ability of a wireless IDS to configure according to user's environment.

13 Router Interaction

Degree of interaction of a wireless IDS with the router.

14 Compromise Analysis

It is the ability to report the extent of damage and compromise due to intrusions.

15 Simple Network Management Protocol (SNMP) Interaction

Ability of the wireless IDS to send an SNMP trap to one or more network devices in response to a detected attack.

16 Timeliness

Average/maximal time between an intrusion's occurrence and its being reported.

Table **??** : Scorecard for Snort, AirDefense Guard and Kismet wireless IDS Snort-Wireless is the most advanced Open Source Wireless IDS. It uses the sequence number analysis technique to detect false frame attacks. In [19] authors tested the effectiveness of the Snort-Wireless with the used data applying the purposed analysis technique. It is not capable of identifying the malicious packets as the threshold-based technique used by Snort-Wireless is prone to false negatives. Table **??** provides the results produced by authors. AirDefense Guard wireless IDS produces very low false negative ratio as it has ability to detect 200+ attacks and policy violations. Kismet has less attack definitions and produces average false negative ratio.

Performance metric Cumulative False Alarm Rate can be assigned score depending on the following criteria: Inside the packet processing function, Snort performs several tasks. First, it calls into libpcap using the pcap_dispatch function to process any waiting packets. For each packet that is available, libpcap calls the Pcap Process Packet function, which handles the actual packet processing. This function resets several per-packet counters, collects some statistics about the packet, and calls Process Packet. The Process Packet function handles all of the details of decoding the packet, printing the packet to the screen and either directly calling the packet logging functions or calling into the pre-processors. If no packets are available, Snort performs basic housekeeping chores such as checking for pending signals. In order to perform all this functions, Snort-Wireless IDS delays the arrival of packets at the target network. Air Defense has the most detailed available wireless forensic database in the industry. It has more than 300 wireless statistics per device per minute logged and has instant analysis using the forensic wizard [20]. The point of breakdown is defined as the level of network or host traffic that results in a shutdown or malfunction of IDS. Air Defense. Kismet IDS identifies networks by collecting passively packets The detection engine is the time-critical part of Snort wireless. Depending upon how powerful user machine is and how many rules have been defined, it may take different amounts of time to respond to different packets. If traffic on the network is too high when Snort wireless is working in NIDS mode, it may drop some packets and may not get a true real-time response. The load on the detection engine of snort wireless depends upon the following factors:

? Number of rules ? Power of the machine on which Snort is running ? Speed of internal bus used in the Snort machine ? Load on the network Motorola Air Defense utilizes its 24x7, real-time monitoring of the 802.11a/b/g networks for most accurate intrusion detection of known as well as unknown attacks and does not easily breaks down. Kismet is able to handle stress up to some extent.

Performance metric IDS Throughput can be assigned score depending on the following criteria: ? Low Score (+): Wireless IDS regularly drops packets. ? Average Score (++): Wireless IDS rarely drops packets. ? High Score (+++): Wireless IDS can perform without dropping any packet.

When Snort wireless is working in Inline mode, it works like an Ethernet bridge, that is, in order to monitor a network segment, it has to be inserted transparently with two bridged NICs. With this setup, any packet can flow through the bridge from a network card to the other, unless it matches the drop rules; in that case, the switch opens and blocks the packet. So, Snort wireless drops packet only when it matches the drop rule specified by the user. Studies have shown that Air Defense rarely drops packets. Kismet processes data rate as supported by access point and drops more packets than others.

Performance metric Depth of System's Detection Capability can be assigned score depending on the following criteria: Snort wireless maintains a rule set in order to have the latest detection capabilities. Sourcefire Vulnerability Research Team (VRT) Rules are the official rules of snort wireless. One of the best features of Snort is its rule engine and language. Snort's rule engine provides an extensive language that enables user to write their own rules, allowing them to extend it to meet the needs of their own network. Motorola Air Defense wireless IDS utilizes 24x7, real-time monitoring of the 802.11a/b/g networks for producing most accurate intrusion detection of known and unknown attacks. It has ability to detect 200+ attacks and policy violations [20]. Kismet has less number of attacks detections as compare to snort wireless and Air Defense guard.

Performance metric Reliability of Attack Detection can be assigned score depending on the following criteria: ? Low Score (+): Wireless IDS generates high ratio of false positives to total alarms raised. frames. So, Wireless IDS snort generates high ratio of false negatives to true negatives. Air Defense guard has ability to detect 200+ attacks and policy violations and therefore produces less false positives and it generates low ratio of false negatives to true negatives. Kismet has average Possibility of Attack as it has average false negative ratio.

Performance metric Consistency can be assigned score depending on the following criteria: ? Low Score (+): Wireless IDS has high variations in the performance. ? Average Score (++): Wireless IDS has average variations inthe performance. ? High Score (+++): Wireless IDS has low or no variations in the performance.

In [20] author evaluated two open source network based intrusion detection systems. Snort wireless performed well during tests, but did produce false positives and false negatives. Snort is very lightweight and fast but is limited in its ability to scale in bandwidth per instance. Studies show that Air Defense kismet has average variations in the performance. Performance metric Error Reporting and Recovery can be assigned score depending on the following criteria: ? Low Score (+): Wireless IDS has low or no ability to correctly report and recover.

? Average Score (++): Wireless IDS has average ability to correctly report and recover. ? High Score (+++): Wireless IDS has high ability to correctly report and recover.

Snort wireless generates reports that show what happened during the last day, week or month. -T option of snort wireless is very useful for testing and reporting on the Snort configuration. This option can be used to find any errors in the configuration files. Snort wireless provides tool that gives user a detailed report of actions taken during the update process. SPADE module keeps a record of history data and uses threshold values to report the anomalies. Air Defense guard has flexible alerting and reporting options with integration capabilities into the various Security Information Management (SIM) systems [20]. Error Reporting and Recovery of kismet is poor as compare to snort wireless and Air Defense.

Performance metric Firewall Interaction can be assigned score depending on the following criteria: ? Low Score (+): Wireless IDS has poor interaction with the Firewall systems. ? Average Score (++): Wireless IDS has average interaction with the Firewall systems. ? High Score (+++): Wireless IDS has excellent interaction with the Firewall systems.

Snort Sam is a tool used to make Snort work with most commonly used firewalls. It is used to create a Firewall/IDS combined solution. Firewall can be configured to automatically block offending data and addresses from entering system when intruder activity is detected. It is available from http://www.snortsam.net/ where one can find the latest information. The tool consists of two parts: 1. A Snort output plug-in that is installed on the Snort sensor. 2. An agent that is installed on a machine close to Firewall or Firewall itself. Snort communicates to the agent using the output plug-in in a secure way. Air Defense Guard supports stateful Layer 2 and rolebased firewalls and base security policy on the user, group, location, encryption strength, etc. studies show that kismet also has good Firewall Interaction.

Performance metric User Friendliness can be assigned score depending on the following criteria: ? Low Score (+): It is difficult to configure wireless IDS according to user's environment.

? Average Score (++): Wireless IDS can be configured up to some extent according to user's environment. ? High Score (+++): Wireless IDS can be easily configured according to user's environment.

In snort wireless a thorough understanding of what snort. conf file is and how to configure it is essential to a successful deployment of Snort wireless as an IDS in user environment. Snort configuration consists of Global configuration (snort. conf), Optional *.rules file(s), and Additional files. Air Defense Guard is very user friendly as it provides location tracking of the devices on a map, and provides minute by minute granular forensic information for any of the device. Kismet only runs under LINUX and does not have easy to use graphical interface.

Performance metric Router Interaction can be assigned score depending on the following criteria: ? Low Score (+): Wireless IDS has a poor interaction with the router. ? Average Score (++): Wireless IDS has an average interaction with the router. ? High Score (+++): Wireless IDS has excellent interaction with the router.

Depending upon the type of router used, snort wireless can be used on a port. Some routers, like Cisco, allow to replicate all ports traffic on one port where snort machine can be attached. These ports are usually referred to as spanning ports. The best place to install Snort wireless is right behind the firewall or router so that all of the Internet traffic is visible to Snort before it enters any router or hub. Air Defense Guard provides nice router interaction. Kismet does not have good interaction with some of the routers like belking54g.

Performance metric Compromise Analysis can be assigned score depending on the following criteria: In snort wireless snort SnmpPlugin is used to send snmp alerts to network management systems (NMS). The alerts can be traps or informs. This adds to significant power of the NMS by allowing it to monitor security of the network. It also allows snort wireless sensor to exploit the features that are built into the existing network management systems. Air Defense Guard eliminates many of vulnerabilities impacting the security of the wireless network by providing good interaction with SNMP. Kismet provides various utilities for configuring and monitoring of wireless Access Points under Linux using SNMP protocol.

Performance metric Timeliness can be assigned score depending on the following criteria: ? Low Score (+): Wireless IDS takes a lot of time to report the occurrence of an intrusion. ? Average Score (++): Wireless IDS takes average time to report the occurrence of an intrusion. ? High Score (+++): Wireless IDS takes a minimal time to report the occurrence of an intrusion.

Snort wireless is a packet-based system. The basic life of a packet inside snort starts with packet acquisition. Once the packet is inside snort it is passed into the packet decoder. After decoding, the packet is passed on to the pre-processors for normalization, statistical analysis, and some nonrule-based detection. Once the pre-processors are done with the packet it goes into the detection engine, where it is evaluated against all of the rules that were loaded from the configuration file. Finally, the packet is sent off into the output plug-ins for logging and alerting. So, it takes lot of time for snort wireless to detect an attack. Air Defense Guard takes average time for reporting of intrusion as it has 200+ attacks and policy violations detection capability. Studies show that kismet is slow in detection as compare to snort wireless and Air Defense.

17 Conclusion and future work

Wireless IDS are used in detecting unwanted activities on a wireless network. Performance metrics can be used to measure the performance of a wireless IDS within the performance constraints. These metrics measure and evaluate the parameters that impact the performance of the wireless IDS. This paper provides a performance metrics scorecard based approach that can be used for evaluating a wireless IDS in order to find out how it behaves within performance constraints.

In this paper we provide various performance metrics concern with wireless IDS and a scorecard method for evaluation. Evaluation of a wireless IDS is done by assigning scores to various performance metrics. We use our evaluation methodology to test popular wireless IDS Snort, Air Defense Guard, and Kismet. We define commonly used performance metrics that are important to a wireless IDS, but a lot is required to be done to find out more ones like analysis of intruder intent, clarity of reports, effectiveness of generated filters, evidence collection, information sharing, user alerts, program interaction, session recording and playback, threat correlation, trend analysis, extendibility, adaptability, scalability, overhead, and latency. More performance metrics and their definitions can be defined as lessons are learned while evaluating a wireless network. Future work also includes applying the evaluation methodology to other metrics concern with wireless IDS like logistical metrics, architectural metrics, quality metrics etc. [1] [2]

[1] © 2012 Global Journals Inc. (US)Global Journal of Computer Science and Technology

[2] © 2012 Global Journals Inc. (US)

2012

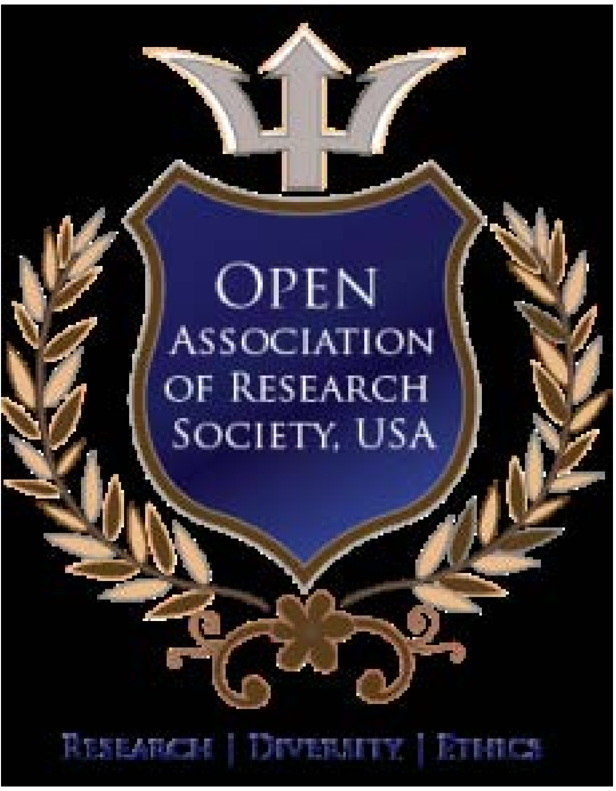
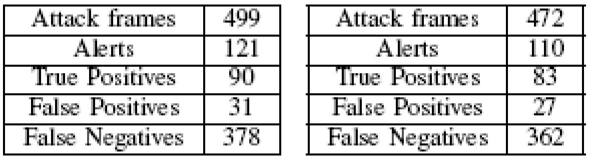


Figure 1: W © 2012

3



Attack frames	499
Alerts	121
True Positives	90
False Positives	31
False Negatives	378

Attack frames	472
Alerts	110
True Positives	83
False Positives	27
False Negatives	362

Figure 2: Table 3 :?

1

Year
2
Volume XII Issue XII Version I
D D D D)
(
Global Journal of Computer Science and Technology

[Note: © 2012 Global Journals Inc. (US)]

Figure 3: Table 1 :

Performance Metrics	Description
False Positive Ratio	
Cumulative False Alarm Rate	

3
Volume XII Issue XII Version I
D D D D) E
(

[Note: signature, and anomaly-based inspection and produces low false positive ratio and gets a high score for this metric [8]. Air Defense guard has ability to detect 200+ attacks and policy violations and therefore produces less false positives. Kismet alert PROBENOJOIN can result excessive false positives while channel hopping is done. False positives are also possible in noisy/lossy situations, it is desirable to disable this alert in some installations [12]. Performance metric False Negative Ratio can be assigned score depending on the following criteria: ? Low Score (+): Wireless IDS generate high False Negative Ratio. ? Average Score (++): Wireless IDS generate average False Negative Ratio. ?]

Figure 4:

and detecting standard named networks, detecting
hidden networks, and inferring to the presence of
Performance Metrics networks (non-beaconing) via data traffic. Snort wireless AirDefense Performance
False Negative ? Low Score (+): Wireless IDS cannot handle stress
Ratio and easily breakdowns. + ++ ++
2012? Average Score (++): Wireless IDS can handle Cumulative False Alarm Rate ++ ++ ++ stress up to
Year
4 Breakdown and Point of ++ +++++
IDS Throughput ++++++++
Depth of
System's ++++++++
Detection
Capability
Reliability of
Attack Detection ++ +++++
Possibility of
Attack + ++ ++
Consistency ++ ++ ++
Error Reporting
D and Recovery Firewall ++++++++
D
D
D
)
E
(Interaction +++++++++
User
Friendliness ++ ++++
Router
Interaction ++++++++
Compromise
Analysis ++ ++ ++
SNMP
Interaction ++++++++
Timeliness ++ ++ ++

Figure 5:

Figure 6: ?

[(2011)] , Jul.-Dec, 2011. 1.

[(2012)] , June 2012. p. . (Print)

[Freelance et al. (2009)] , Harrykar Freelance , " Harrykar's Techies Blog , Snort , Ids , . . . Ips , Beyond . May 2009. 31.

[Albin (2011)] *A comparative analysis of the snort and suricata intrusion-detection systems*, Eugene Albin . September 2011.

[Singh and Singh] 'A Logistic Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network'. Rupinder Singh , Dr Jatinder Singh . *International Journal of Computer Networks and Wireless Communications (IJCNWC)* 2 (3) .

[Fink et al. (2002)] 'A Metrics -Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems'. G A Fink , B L Chappell , T G Turner , K F O'donoghue . *WPDRTS* April 2002. p. .

[Singh and Singh] 'A Metrics Based Approach to Intrusion Detection System Evaluation for Wireless Network'. Rupinder Singh , Dr Jatinder Singh . *International Journal of Education and Applied Research* (IJEAR)

[David and Benjamin ()] 'A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines'. J David , M Benjamin . *ICDS 2011 : The Fifth International Conference on Digital Society*, 2011. ISBN p. .

[Singaraju et al.] 'A Testbed for Quantitative Assesment of Intrusion Detection Systems Using Fuzzy Logic'. Gautam Singaraju , Lawrence Teo , Yuliang Zheng1 . IWIA'04) 0-7695- 2117-7/04. *Proceedings of The Second IEEE International Information Assurance Workshop*, (The Second IEEE International Information Assurance Workshop)

[Singh and Singh (2012)] 'An Architectural Metrics Scorecard Based Approach to Intrusion BDetection System Evaluation for Wireless Network'. Rupinder Singh , Dr Jatinder Singh . *Global Journal of Computer Science and Technology (GJCST)* June 2012. 12. (Issue 11 Version 1.0)

[Mart´?nez_ et al.] *Beacon Frame Spoofing Attack Detection in*, Asier Mart´?nez_, Urko Zurutuzayz , Roberto Uribeetxeberriay , Miguel Fern´andezy , Jesus Lizarragay , Ainhoa Sernay , I?naki V´elezy . IEEE 802.11.

[Gómez et al. ()] 'Design of a Snort-Based Hybrid Intrusion Detection System'. J Gómez , C Gil , N Padilla1 , R Baños , C Jiménez . *IWANN 2009, Part II*, LNCS S Omatu (ed.) 2009. 5518 p. .

[Rafeeq Ur Rehman] *Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID*, Rafeeq Ur Rehman . Prentice Hall.

[Savola (2010)] 'On The Feasibility of Utilizing Security Metrics in Software Intensive Systems'. Reijo Savola . *IJCSNS International Journal of Computer Science and Network Security* January 2010. 10 (1) .

[PCI Wireless Compliance Demystified Best Practices for Retail] *PCI Wireless Compliance Demystified Best Practices for Retail*, http://www.airdefense.net/PCIpaper.Pdf

[Fayssal] 'Performance analysis Toolset for wireless intrusion detection systems'. Samer Fayssal . *2010 International Conference on High Performance Computing and Simulation (HPCS)*, (Caen, France, ISBN) p. .

[SNORT Users Manual 2.9.0, The Snort Project (2011)] *SNORT Users Manual 2.9.0, The Snort Project*, March 25, 2011.

[Boob and Jadhav (2010)] 'Wireless Intrusion Detection System'. Snehal Boob , Priyanka Jadhav . *International Journal of Computer Applications* August 2010. 5 (8) p. .

[Veseli] *Wireless Intrusion Detection Systems*, Fatbardh Veseli .