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

Rupinder Singh[†], Dr. Jatinder Singh[‡]

[†]Rupinder Singh, Assistant Prof., P.G. Deptt. of Computer Science and Applications, Khalsa College, Amritsar, Punjab, India.
[‡]Dr. Jatinder Singh, Principal, Golden College of Engg. & Tech., Gurdaspur, Punjab, India.

***Abstract***
***Logistical metrics are used to measure expense, maintainability, and manageability of a wireless IDS. Wireless IDS is used to analyze traffic specific to wireless along with scanning for external users trying to connect to the network through access points and play important role in providing security to wireless network. Design of wireless IDS is a difficult task as wireless technology is advancing every day, Logistic metrics can play an important role in the design of wireless IDS by measuring the areas concern with the logistics of a wireless IDS. In this paper we describes a set of logistic metrics that are relevant to wireless IDS. A "scorecard" containing the set of values is used as the centerpiece of testing and evaluating a wireless IDS. Evaluation of a wireless IDS is done by assigning score to various logistical metrics concern with wireless IDS. We apply our scorecard evaluation methodology 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.***

***Keywords: Logistical Metrics, Wireless, Metrics, IDS, Scorecard.***

## I. INTRODUCTION

Lord Kelvin said "If you cannot measure it, you can not improve it". This fact also applies to wireless network security issues. In order to manage an activity it has to be measured, this is a widely accepted management principle and security falls under this rubric. Metrics can be used as an effective tool by security providers. They can be used to discern the effectiveness of various components of security programs.

A new and exciting world has been opened by wireless. Its technology is advancing every day along with increase in its popularity. However the biggest concern with wireless has been its security. For some time wireless has had very poor, if any, security on a wide-open medium. Along with improved encryption schemes, a new solution to help combat this problem is the Wireless Intrusion Detection System (WIDS). 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 a wireless network. This system monitors traffic on network looking for logging threats and alerting personnel to respond.

Metrics can play an important role in the designing of wireless IDS. Metrics can be used to identify risk level in not taking a given action. They can be used to provide guidance in prioritizing corrective actions and may be used in raising security level within the network. Metrics knowledge can help security managers to better answer the hard questions from their executives. 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].

This paper provides a logistic metrics scorecard based approach to evaluate Intrusion Detection Systems that are currently popular for wireless in the commercial sector. We describe a testing methodology we developed to evaluate wireless IDS by assigning score to various logistical metrics concern with it. The approach followed in this paper do not compare wireless IDS against each other, but against a set of logistic metrics that are 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 logistical metrics, it may be extended for other metrics like
architectural metrics, performance metrics, quality metrics etc. The standard approach of comparison used in this paper also gives us scientific repeatability.

## II. SNORT, AIRDEFENSE GUARD AND KISMET WIRELESS IDS

In order to explain logistic metrics scorecard based evaluation of wireless IDS, we choose three wireless IDS namely Snort-

wireless, AirDefense Guard, and Kismet as these are popular and works on different technology.

### *A. Snort wireless IDS*

Snort wireless is an open source network intrusion detection and prevention system (IDS/IPS) that combines the benefits of signature, protocol, and anomaly-based inspection, and is the most widely deployed IDS/IPS technology worldwide. With millions of downloads Snort has become the de facto standard for IDS/IPS [8]. Snort-wireless allows for custom rules to be created based on framing information from a wireless packet. It also contains rules to attempt to find rogue access points, war drivers, and ad hoc networks.

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 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.

### *B. AirDefense Guard wireless IDS*

Motorola AirDefense Guard is a wireless IDS based on statistically anomalous behavior, signature analysis and protocol assessment policy deviation. AirDefense Guard is able to respond to attacks with Active Defense technology by disconnecting attackers connection to the WLAN.

AirDefense can be used to identity theft by tracking the fingerprints of vendor-specified characteristics along with personal trademarks of authorized users in order to identify intruders in the network. AirDefense can be used to detect Denial-of-Service (DoS) attacks that jams the wireless network. AirDefense can also detect Man-in-the-Middle attacks and ensures that access points can only operate on specified channels and proper protocols are used.

### *C. Kismet wireless IDS*

Kismet IDS is an 802.11 layer2 wireless network detector and sniffer. Kismet can work with any wireless card supporting raw monitoring mode, and can be used to sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet IDS also supports plugins that allows sniffing other media such as DECT. Kismet uses data traffic to detect presence of nonbeaconing networks. It identifies standard named networks and hidden networks by passively collecting packets.

Kismet wireless IDS without sending any loggable packets is able to detect the presence of both wireless access points and wireless clients, and associate them with each other. Unlike most other wireless network detectors, Kismet is able to log all sniffed packets and save them in a tcpdump/Wireshark or Airsnort compatible file format. Kismet also captures PPI headers. Kismet can also detect default or "not configured" networks, can probe requests, and can also determine the levels of wireless encryptions used for a given access point. Kismet is also able to supports logging of the geographical coordinates from inputs provided by a GPS receiver.

## III. LOGISTICAL METRICS SCORECARD BASED APPROACH

### *A. Developing Scorecard*

A “scorecard” containing the set of logistical metrics and their definitions for wireless network will be the centerpiece of testing and evaluating wireless IDS [4]. Each metric can have low (0), average (2), or high (4) score, where higher scores will be interpreted as more favorable ratings.

The logistic metrics used are general characteristics that are relevant to wireless IDS. The method used for observing each logistic 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 logistic metrics for wireless IDS.

### *B. Logistical metrics for a wireless IDS*

Logistical metrics are used to measure expense, maintainability, and manageability of a wireless IDS. The common logistic metrics concern with wireless IDS along with their definitions are shown in Table 1. Table 1 includes only the selected logistical metrics. Other logistical metrics that can be included are: Documentation Quality, Available Copy Evaluation, Administration Level, Product Lifetime, Quality of Technical Support etc.

Metrics like Configuration Difficulty, Policy Maintenance, License Management etc. are applicable because products having low scores in these areas would not be easy to use in a distributed environment with multiple sensors. Platform requirements give an indication of the system resources that will be consumed by the wireless IDS in the resource-critical wireless environment.

### *C. Logistical metrics scorecard based approach*

In this section we will apply above mentioned technique to popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. We choose these three for evaluation as they are most widely used and have different ways of working. With table 2 we describe how scores to logistic metrics related to these three wireless IDS are assigned.

Table 1: Selected logistical metrics for a wireless IDS.

| Logistical Metrics | Description |
|---|---|
| Distributed Management | Determining the distribution capabilities of a wireless IDS. It is used to determine up to what extent a wireless IDS supports distributed management. |
| Configuration Difficulty | The difficulties a user faces while installing and configuring a wireless IDS. |
| Policy Management | The difficulty in setting security and intrusion detection policies for a wireless IDS. |
| License Management | The difficulty in obtaining, updating and extending licenses of a wireless IDS. |
| Availability of Updates | The availability of updates of behavior profiles and cost of product upgrades. |
| Platform Requirements | System resources needed to implement a wireless IDS. |
| Copies Downloaded | Describes the popularity of wireless IDS. |

Logistic Metric Distributed Management can be assigned score depending on the following criteria:
Low Score (0): No Distributed Management.
Average Score (2): Sensors are remotely located and report to a centralized management station.
High Score (4): Complete management of all sensors may be done from any sensor.

Table 2: Scorecard for Snort, AirDefense Guard, and Kismet IDS.

| Logistical metrics | Snort-wireless | AirDefense Guard | Kismet |
|---|---|---|---|
| Distributed Management | 2 | 2 | 2 |
| Configuration Difficulty | 4 | 4 | 2 |
| Policy Management | 4 | 4 | 4 |
| License Management | 4 | 2 | 4 |
| Availability of Updates | 4 | 0 | 2 |
| Platform Requirements | 4 | 4 | 4 |
| Copies Downloaded | 4 | 2 | 2 |

Snort wireless IDS is assigned an average score (2) for Distributed Management logistic metric as in Snort-wireless networks with higher traffic, load is distributed to several dedicated sensor machines that in turn report to a single alarm database. Periodically attack logs are uploaded to the management station and are stored in a central database. One snort wireless instance is stored on every machine for distributed WLAN. AirDefense Guard wireless IDS consists of distributed sensors and server appliances. All WLAN activities are monitored by remote sensor that sits near 802.11 access points and sends reports back to the server appliance. So, Air Defense Guard is assigned an average score. The Kismet wireless is composed by a "Kismet_server" and a client "Kismet_client". The clients makes communication with the server in order to displays the information collected by server. Kismet wireless is also assigned average score for logistic metric Distributed Management.

Logistic Metric Configuration Difficulty can be assigned score depending on the following criteria:
Low Score (0): Difficult to configure wireless IDS to the network architecture selected by the users.
Average Score (2): Wireless IDS can be configured to the network architecture selected by the users but users cannot create own rules for new attacks.
High Score (4): All of inner workings, configuration files, and rules are laid bare to users, so that users can tune IDS to their specific network architecture and can create own rules for new attacks.

Snort-wireless IDS is assigned a high score for logistic metric Configuration Difficulty as Snore wireless is configurable. All of Snort's inner workings, configuration files, and rules are laid bare to users, so users can tune Snort to their specific network architecture. Not only that, users can also create their own rules for new attacks [6]. AirDefense wireless IDS is assigned a high score for logistic metric Configuration Difficulty as complete WLAN network visibility is provided by AirDefense within one central console with Multi-Vendor/heterogeneous WLAN environment. It enables simplified WLAN management with a lower TCO simplified device configuration tools that provides a cost effective & manageable way to organizations upgrade/migrate to 11n infrastructure. Kismet wireless is not easy to configure as one has to edit the Kismet.conf file for configuration which needs detail knowledge about system and wireless network. So, Kismet wireless is assigned low score for metric Configuration Difficulty.

Logistic Metric Policy Management can be assigned score depending on the following criteria:
Low Score (0): Wireless IDS have poor policy management behind the network to detect intruders.

Average Score (2): Wireless IDS have good policy management behind the network to detect intruders.
High Score (4): Wireless IDS has perfect policy management behind the network to detect intruders.

Wireless Network policy management presents new challenges as there are multiple networks, many types of devices and different groups of mobile workers with varying roles and application requirements. IDS policy manager is a Microsoft Windows based GUI used to manage the Snort configuration file and Snort rules on a sensor [7]. Snort wireless IDS gets a high score for policy management logistical metric as Snort IDS policy manager provides the ability to view, correlate, and report on Snort events, it also adds seamless IDS rule management and deployment. Administrators can quickly view, disable or set suppression a single rule on a single sensor with policy manager. They can deploy a rule change to all Snort sensors while viewing information about an event that is currently triggering, all within the same console view. IDS policy manager adds easy updates and deployment of Snort rules. AirDefense guard has three main categories for policies namely configuration, performance and vendor policy. All policies threshold are configurable to suit a particular enterprise. Therefore AirDefese gets a high score for metric policy management. With a strong wireless policy and proper enforcement, Kismet wireless network can be as secure as the wired equivalent and is therefore assigned high score for metric Policy Management.

Logistic Metric License Management can be assigned score depending on the following criteria:
Low Score (0): Not always possible to manage license policy.
Average Score (2): License can be easily managed.
High Score (4): No license requirement.

Snort is released under the GNU GPL (General Public License), which means it can be used for free, the purpose is to encourage the development of open source software. Reliance on the open source community for developing Snort wireless is an important step in providing a robust wireless intrusion detection system that improves network security. So, snort wireless IDS gets a high score for logistic metric License Management. AirDefense wireless IDS pricing starts at $7,995 for a starter kit with server, five sensors and licenses. License can be easily managed so AirDefense wireless IDS is assigned average score. Kismet is free software distributed under the General Public License (GNU). Kismet wireless gets high score for metric License Management as there is no need of license.

Logistic Metric Availability of Updates can be assigned score depending on the following criteria:
Low Score (0): No updates available.
Average Score (2): Updates are available at a fixed period.
High Score (4): Updates are available whenever needed.

Snort is constantly updated and maintenance releases out as needed, typically once every few months. Snort rules are updated regularly with new attack signatures that can be downloaded from Snort web site, so Snort wireless IDS again gets a high score for logistic metric Availability of Updates. AirDefense gets a low score for availability of updates as updates are available only after making a purchase. Updates for Kismet wireless are available at fixed period, latest Kismet release is Kismet-2011-03-R2. So, Kismet wireless is assigned average score for metric availability of updates.

Logistic Metric Platform Requirements can be assigned score depending on the following criteria:
Low Score (0): Wireless IDS requires a platform not currently popular.
Average Score (2): Wireless IDS requires few selected platforms.
High Score (4): Wireless IDS runs on multiple platforms.

Snort-wireless runs on multiple platforms including Unix, Linux, and Microsoft Windows. Snort gets a high score for logistic metric Platform Requirements. The AirDefense Services Platform is designed to support any 802.11 a/b/g wireless LAN deployment. Therefore its gets a high score for metric Platform Requirements. Kismet wireless is assigned high score for metric Platform Requirements as Kismet IDS can work with any wireless card supporting raw monitoring mode, and can be used to sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic.

Logistic Metric Copies Downloaded can be assigned score depending on the following criteria:
Low Score (0): Very less download as compare to other wireless IDS.
Average Score (2): Average downloads.
High Score (4): Thousands of downloads each month.

Snort is the most popular and widely used intrusion detection system for wireless network. There are tens of thousands of downloads of Snort each month from the Snort Web site. So, Snort gets a high score for logistic metric Copies Downloaded. AirDefense guard gets an average score for metric Copies Downloaded as it is a paid tool and is less popular than snort. Kismet wireless is also one of the popular wireless IDS with an average number of copies downloaded as it is available under GNU and therefore gets an average score for metric Copies Downloaded. Figure 1 shows score of Snort-wireless, AirDefense, and Kismet IDS.

## IV. CONCLUSION AND FUTURE WORK

A wireless IDS play an important role in detecting unwanted activities on a wireless network. Design of wireless IDS is a difficult task as the technology of design of wireless network is changing at a pace which brings additional challenges in the design of wireless IDS. This paper provides a logistic metrics

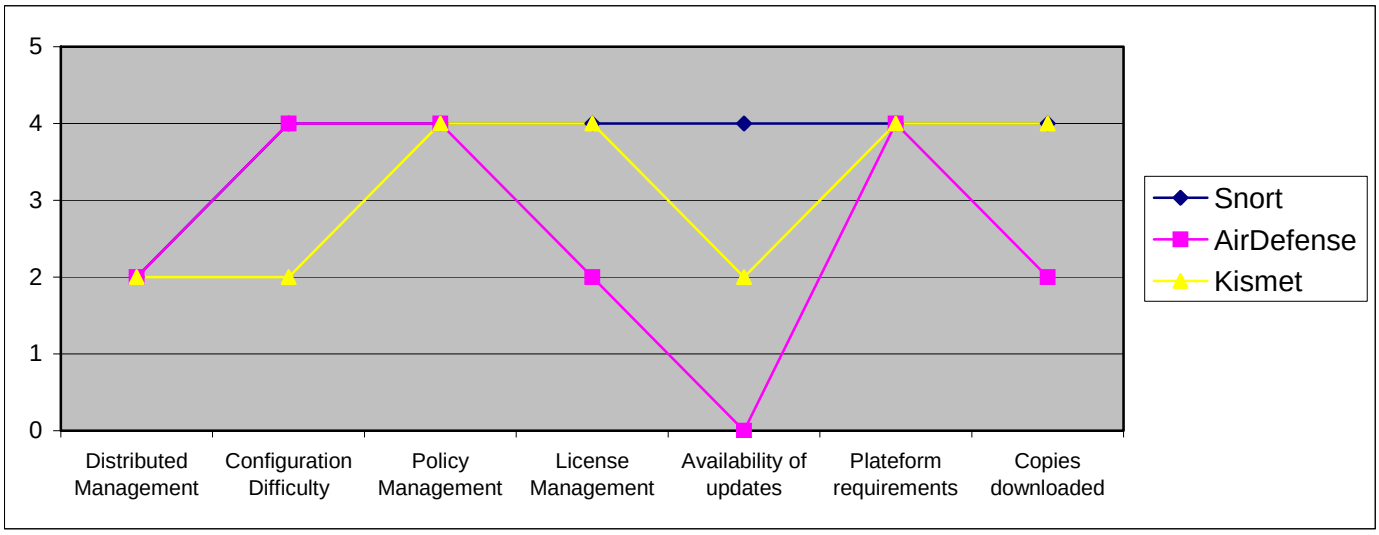


Figure1: Graph showing score of Snort-wireless, AirDefense, and Kismet wireless IDS.

scorecard based approach that can be used for evaluating a wireless IDS in order to find out the areas in which the IDS is weak and needs improvement. Depending upon the requirements of the system these metrics may be given priorities and appropriate wireless IDS may be selected after developing the scorecard.

In this paper we define various logistical metrics concern with wireless IDS and a scorecard method to evaluate a wireless IDS by assigning scores to various logistic metrics. We use our evaluation methodology to test popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. This approach makes it possible for the users to select one of the wireless IDS from a given list depending upon the scorecard generated for various wireless IDS logistic metrics. Although we have tried to find logistic metrics that are important to a wireless IDS, but a lot is required to be done to find out more ones like Documentation Quality, Available Copy Evaluation, Administration Level, Product Lifetime, Quality of Technical Support etc. More logistic metrics and their definitions can be defined as lessons are learned while evaluating a wireless IDS. Future work also includes applying the evaluation methodology to other metrics concern with wireless IDS like architectural metrics, performance metrics, quality metrics etc.

## REFERENCES

[1] Molisch Andres, F. " Wireless Communications ," Second Edition, 2011, Publisher: Wiley, ISBN- 9780470741870.

[2] William Stallings, "Wireless Communications & Networks ," 2nd Edition, Publisher: Prentice Hall, ISBN-10:013191 8354.

[3] Johnny Cache, Joshua Wright and Vincent Liu, "Hacking Exposed Wireless ", Second Edition, 2010, 18351.

[4] Rupinder Singh, Dr. Jatinder Singh, " A Metrics Based Approach to Intrusion Detection System Evaluation for Wireless Network," International Journal of Education and Applied Research (IJEAR) Vol. 1, Issue 1 , Ver. 1: Jul.-Dec., 2011, ISSN : 2249 - 4944 (Print).

[5] G. A. Fink, B. L. Chappell, T. G. Turner, and K. F. O'Donoghue, " A Metrics Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems," WPDRTS,15 – 17 April 2002, Ft. Lauderdale, Florida.

[6] Harrykar Freelance, " HARRYKAR'S TECHIES BLOG Snort , IDS , IPS , NSM , hacking and… beyond, " 31 May 2009.

[7] Rafeeq Ur Rehman, " Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID, " Prentice Hall, ISBN 0-13-140 733-3.

[8] Stephen Northcutt, "Snort 2.1Intrusion Detection," Second Edition, Shroff Publishers, ISBN: 81-7366-894-9.

[9] " SNORT Users Manual 2.9.0, " The Snort Project, March 25, 2011.

[10] J. Gómez , C. Gil, N. Padilla1, R. Baños, And C. Jiménez, " Design of a Snort – Based Hybrid Intrusion Detection System,"S. Omatu et al. (Eds.): IWANN 2009, Part II, LNCS 5518, pp. 515–522, 2009.

[11] Reijo Savola, "On the Feasibility of Utilizing Security Metrics in Software – Intensive Systems," IJCSNS, VOL. 10 No. 1 , January 2010.