

A Metrics-Based Approach to Intrusion Detection System Evaluation for Wireless Sensor Network

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

[†]Research Scholar, IKG PTU, Kapurthala, Punjab. E-mail: rupi_singh76@yahoo.com

[‡]IKG PTU, Kapurthala, Punjab. E-Mail: bal_jatinder@rediffmail.com

Abstract - Metrics are used in identifying the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions. This paper provides a metric based approach that will help administrators of Wireless Sensor Network (WSN) to select the best Intrusion Detection System (IDS) for the sensor network. The metrics discussed in the paper are a subset of the general metric set that particularly impacts WSN intrusion detection issues. A “scorecard” containing the set of metrics and their definitions for WSN is used as the centerpiece of testing and evaluating IDS. The metrics used are general characteristics that are relevant to WSN IDS. The metrics set is divided into three classes, namely Logistical, Architectural, and Performance. Finally, we discuss the results using a preliminary version of the metric scorecard and the opportunities for further work in this area.

Keywords: Metrics, Wireless sensor network, Intrusion detection system, Evaluating, Scorecard.

I. INTRODUCTION

Lord Kelvin said, “If you cannot measure it, you can not improve it”. This fact also applies to Wireless Sensor Network (WSN) or 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 security providers to discern the effectiveness of various components of their security programs. Metrics can help in identifying the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions. Additionally, they may be used to raise the level of security awareness within the network. With knowledge gained through metrics, security managers can better answer hard questions from their executives. Security Metrics that are related to WSN 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.

A new and exciting world has been opened by WSN, its technology is advancing every day and its popularity is increasing. One of the biggest concerns with WSN, however, has been its security. For some time WSN 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 Intrusion Detection System (IDS) [1]. An 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. A WSN IDS performs this exclusively for the WSN. This system monitors traffic on network looking for and logging threats and alerting personnel to respond. Metrics can play an important role in the designing of WSN IDS.

This paper focuses on a metric based approach to evaluate Intrusion Detection technology that is currently popular for WSN. We describe a testing methodology developed to evaluate IDS against a user-definable, dynamically-changing standard. The approach followed in this paper does not compare IDS against each other, but against a standard which is derived from mapping administrator requirements to a standard set of metrics. The generalized approach of this paper will allow systems with any requirements to tailor evaluation of ID technologies to their specific needs. Since evaluation is against a static set of metrics the evaluation may be reused. The standard approach of comparison used in this paper gives us scientific repeatability.

II. WIRELESS SENSOR NETWORK AND INTRUSION DETECTION SYSTEM

WSN are self-configured and infrastructure-less wireless networks to monitor the environment or physical conditions, such as temperature, sound, humidity and so on. WSN cooperatively passes their data gathered through the network to a central location called base station so that the data can be analyzed for further processing. WSN is deployed in the environments that are usually unfriendly and unsafe. WSN has a large number of constraints from which results in new challenges. The sensor nodes have unreliable communication medium and extreme resource limitations which make it very difficult to deploy security mechanism. Figure 1 shows the structure of a typical WSN. Most of the protocols for WSNs in the past assumed that all nodes are trustworthy and cooperative. But this is not the case for many sensor network applications today and a variety of attacks are possible in WSN.

Intrusion detection is the process of detecting unwanted traffic

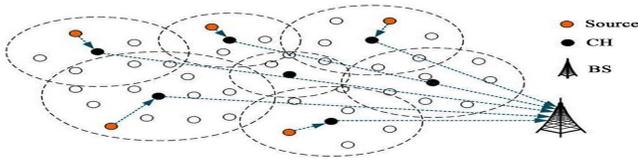


Figure 1: A typical WSN

on a network or a device. IDS can be a software or a hardware that monitors network traffic in order to detect unwanted activity. A WSN IDS is one that can analyze WSN specific traffic, it also includes scanning for external users trying to connect to the network through access points (AP). IDS play important role in securing as networks increasingly support WSN technologies at various points of a topology. An IDS implementation solution is that the sensors should be deployed wherever a WAP is configured so that the majority of attempted attacks can be traced. Detecting the location of an attack is a critical aspect of a WSN IDS where attackers are in close proximity to the WAP, and are physically located in the local areas. WSN IDS can be centralized or decentralized. In centralized IDS network sensors collect and pass frequency data to a centralized management console, where the WSN IDS data are stored and processed for detecting intrusion. On the other hand, a decentralized WSN IDS usually perform activities which are done by both the sensors and the console. Decentralized one is preferable for WSN that are smaller in size, and it is also more cost-effective. When WSNs are larger, a centralized WSN IDS is used for easier management and effective data processing.

The components of a WSN IDS include Sensors, management logging databases, servers, and consoles. WSN IDSs can be run centralized or decentralized. In centralized systems, the data are correlated at a central location so that the decisions and actions are made based on that data. In decentralized systems, decisions are made at the sensor. The sensor software can be used to detect attacks within the range of the IDS. They also provide features to find out misconfigurations of the nodes, and provide information to manage servers. The software used in sensors may also help to enforce security policies on the sensor nodes, such as providing limited access to WSN interfaces. Various components of WSN IDS are connected to each other through a wired network. The organization's standard networks or separate management network can be used for WSN IDS component communications. A management network or a standard network can be used for controlling the separation between the WSN and wired networks.

WSN IDS is a new technology, so there are a few drawbacks concerned with it. Some Caution should be taken into consideration before applying WSN IDS to an existing sensor network. As it is a new technology, there may be bugs and loopholes in it. WSN IDS technology, which may, weaken the security level of the sensor network, or increase its

vulnerabilities at its worst case. Another drawback with the WSN IDS is its cost, that may be too expensive to afford, particularly when we have a large range of sensor networks, which may need additional sensors to manage the entire network coverage. WSN IDS performance depends on how it is configured by the network administrator. If they are tuned correctly or are pre-configured to find what exactly should on the sensor network, then their function to their optimal capability. However, on the other hand, a WSN IDS can be quite ineffective.

Production of Several false positives or false negatives would present more confusion for the administrator. In general, IDSs are very prone to false alarms, therefore, continues tuning is required for effective intrusion detection. WSN IDS effectiveness depends on administrators who respond after analyzing WSN data gathered by IDS. A WSN IDS may need more resources than wired IDS as it needs to address both the alert data and the responsibility to catch the attackers located by the WSN IDS. The technology of WSN comes with vulnerabilities with which wired networks often not deal, such as authenticating every network sensor. WSN IDS must provide the characteristics such as Confidentiality, Authenticity, Integrity, and Availability if the security of the sensor network is desired. Despite these various downsides with WSN IDS, it can provide a great security solution for a sensor network when it is used effectively and configured properly.

III. Methodology for Evaluation of WSN IDS

A. Developing Scorecard

A "scorecard" containing the set of metrics and their definitions for WSN will be the centerpiece of testing and evaluating WSN IDS. The metrics used are general characteristics that are relevant to WSN IDS. The metrics set has been divided into three classes: Logistical (class 1), Architectural (class 2), and Performance (class 3). The key features to be used for testing are shown in the figure 2.

Well-defined metrics are those that can be observed and reproduced. They are quantifiable, and have the characteristic. Characteristic is the property of metrics by which they can be clearly differentiated by otherwise similar systems. Discrete scoring is the way of assigning values to each metric for a given system. Values zero through four will be used as scores with the discrete values, where higher scores will be interpreted as more favorable ratings. Each metric includes may have low (0), average (2), or high (4) score.

In the case of flexible weighting, any consistent numeric system of weights can be used, which may be discrete or

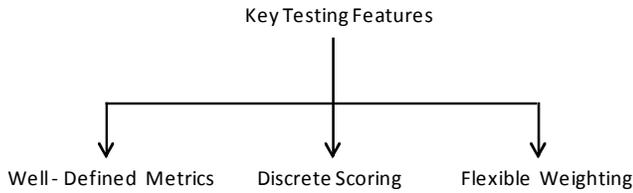


Figure 2: Classifying testing features for metrics

continuous with both the upper or lower limits as defined by the scorer. The weighted score computation is specified in equation 1. Use of the larger range of weighted values will separate the field of products more distinctly. We may also use negative weights to distinguish where a feature is actually counter productive.

$$S_j = \sum_{i=1,3} [\sum_{i=1,n_j} (U_{ij} * w_{ij})] \quad (1)$$

where:

S_j is the weighted overall score for metric. Class j , U_{ij} is the unweighted score for metric i of class j , W_{ij} is a real-valued weight of the ij th metric, n_j is the number of metrics within class j , i is the index of the metrics within the j th class, and j is the metrics class index (logistical = 1, etc)

B. Scorecard Metrics

Next, we will be discussing in greater detail the metrics that are most applicable to WSN IDS. The metrics are grouped together by class, that is followed by a representative metric, including examples of low, average, and high scores. For brevity’s sake, we will not include examples for each metric. The metrics set for WSN IDS will be divided into Logistical (class 1), Architectural (class 2), and Performance (class 3) one as shown in figure 3 and is described below in detail.

1) Logistical Metrics (Class 1): Logistical metrics are used to measure expense, maintainability, and manageability of a WSN IDS. The metrics define applicable to WSN IDS in this area 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.

A detailed example of the logistical metrics for WSN IDS is Distributed Management:

- Low Score: Management of each sensor must be done at the sensor itself.
- Average Score: sensor may be remotely managed, but may have limited or degree of administrative control.
- High Score: Complete management of all sensors may be done from any sensor or remotely. Appropriate encryption and authentication mechanism may be employed.

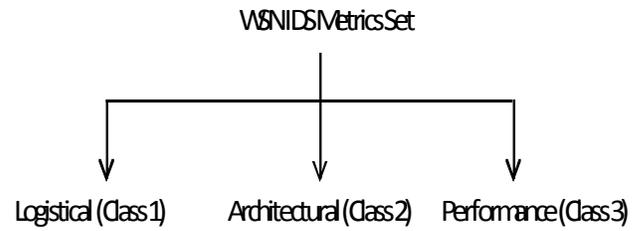


Figure 3: Classification of WSN IDS metrics

Table 1: Selected Logistical Metrics

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

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 WSN IDS in the resource-critical WSN environment.

2) Architectural Metrics (Class 2): Architectural metrics are basically used to compare the intended scope and architecture of the WSN IDS and how they match the deployment architecture. These metrics evaluate the architectural efficiency of the IDS. The metrics defined in this area are shown in Table 2.

Other Architectural metrics that may be included are: Anomaly Based, Misuse Based, Autonomous Learning, Host/OS Security, Interoperability, Package Contents, Process Security, Signature Based, and Visibility etc.

An illustrative example of an architectural metric for WSN IDS is Adjustable Sensitivity:

- Low Score: No Adjustability
- Average Score: Adjustability via static methods

- High Score: Intelligent, dynamic Adjustability

3) **Performance Metrics (Class 3):** Performance metrics are used to measure the ability of a WSN 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 WSN IDS. The metrics defined in this area are shown in Table 3.

Table 3 includes only the selected Performance metrics. Other Performance metrics that can be included are: Analysis of

Table 2: Selected Architectural Metrics

Architectural Metrics	Description
Adjustable Sensitivity	The difficulty of altering the sensitivity of a WSN IDS in order to achieve a balance between false positive and false negative error rates at various times and for different environments.
Required Data Storage Capacity	The amount of disk space needed to store logs and other application data.
Load Balancing Scalability	It measures the ability of a WSN IDS to partition traffic into independent, balanced sensor loads.
Multiple Sensor Support	The cardinality of sensors supported.
Reordering and Stream Reassembly	It is used to find an attack that has been artificially fragmented and transmitted out of order.
State Tracking	This metrics is useful in hardening WSN IDS against storms of random traffic used to confuse it.
Data Pool Selectability	This metrics is used to define the source data to be analyzed for intrusions.
System Throughput	It is used to define the maximal data input rate that can be processed successfully by the WSN IDS.

Table 3: Selected Performance Metrics

Performance Metrics	Description
Observed False Positive Ratio	This is the ratio of alarms that are wrongly raised by the IDS to the total number of detection attempts.
False Negative Ratio	This is the ratio of actual attacks that are not detected by the IDS to the total number of detection attempts.
Cumulative False Alarm	The weighted average of False Positive and False Negative ratios.

Rate	
Induced Traffic Latency	It measures the delay in the arrival of packets at the target network in the presence and absence of a WSN IDS.
Stress Handling and Point of Breakdown	The point of breakdown is defined as the level of sensor network or host traffic that results in a shutdown or malfunction of IDS.
Throughput	This metrics defines the level of traffic up to which the IDS performs without dropping any packet.
Depth of System's Detection Capability	It is defined as the number of attack signature patterns and/or behavior models known to it.
Breadth of System's Detection Capability	It is given by the number of attacks and intrusions recognized by the IDS that lie outside its knowledge domain.
Reliability of Attack Detection	It is defined as the ratio of false positives to total alarms raised.
Possibility of Attack	It is defined as the ratio of false negatives to true negatives.
Consistency	It is defined as the variations in the performance of a WSN IDS.
Error Reporting and Recovery	The ability of a WSN IDS to correctly report and recover.
Firewall Interaction	The ability of a WSN IDS to interact with the Firewall systems.
User Friendliness	The ability of a WSN IDS to configure according to user's environment.
Router Interaction	Degree of interaction of the IDS with the router.
Compromise Analysis	It is the ability to report the extent of damage and compromise due to intrusions.
Induced Traffic Latency	It is the degree to which traffic is delayed by the WSN IDS presence or operation.
Distance	The distance coverage of the IDS in the sensor network.
Memory	The amount of memory required for processing of captured sensor data.
Processing	The processing capabilities of WSN IDS
Power	Power consumption of WSN IDS for transmission and reception of the data in the sensor network and

for processing of data.

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, etc.

An illustrative example of performance metrics for WSN IDS is Observed False Positive Ratio:

- Low Score: WSN IDS generate high Observed false Positive Ratio
- Average Score: WSN IDS generate average Observed false Positive Ratio
- High Score: WSN IDS generate low or no Observed false Positive Ratio

C. Deriving Weights from User Requirements

There is a need to carefully weight the metrics in order to provide meaningful results according to the intended sensor environment where the WSN IDS will function. The weighting of IDS metrics is derived from analysis of the requirements of the prospective WSN IDS procurer. The requirements of the procurer must be clearly defined in order to effectively use the scorecard.

There is flexibility in the actual form of the requirements. The following algorithm developed by G. A. Fink et al. [2] suggests one possible mapping of requirements to a scorecard weighting (Figure 4). In this algorithm administrator first, lists WSN IDS requirements in a partial ordering from least important to most. Requirements are usually stated in positive form or converted to the positive where possible to reduce unnecessary negative weights. Next, the first requirement (i.e. least important) is assigned the lowest weight (e.g., one). Other requirements may be assigned increasing weights in proportion to their relative importance. There is a possibility of duplicate weights as the ordering of requirements is partial. Once the requirements are weighted, each metric is assigned a weight that is equal to the sum of the weights of the requirements it contributes to. The formula given in figure 4 is used to compute Weighted scores for each WSN IDS.

No security problem is purely technical, it depends on the organization policy decisions what are going to be the administrator’s requirements. An organizational policy regarding security states the goals, acceptable uses, and constraints on the system. Without this organizational agreement, it will be impossible to determine what to monitor, when or whom to alert, or the degree of threat a potential intrusion presents. Weighting strategy should reflect accurately the importance of each metric. For WSN, emphasis should be on speed and accuracy of attack recognition and on the ability of the WSN IDS to react automatically via a firewall, router, SNMP, etc. For distributed WSN, the impact of trust among the component is to be taken care of. More future work is needed as far as Mapping of requirements to metric weights is concerned.

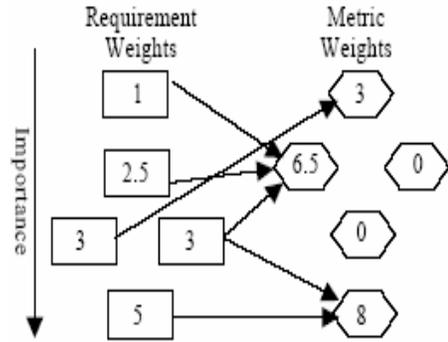


Figure 4: Requirement to Metric Weighting Example

IV. CONCLUSION

A WSN IDS play an important role in detecting unwanted activities on a WSN. The design of WSN IDS is a difficult task as the technology of design of WSN is changing at a pace which brings additional challenges in the design of efficient WSN IDS. This paper provides metrics based approach that can be used for evaluating a WSN IDS in order to find out the areas in which the IDS is weak and needs improvement. In this paper, we define various components and a general architecture of a WSN. The metrics we defined for evaluating WSN IDS are well defined, have discrete scoring, and flexible weighting. For clarification, we classify metrics set into Logistical, Architectural, and Performance one. Although we have tried to find metrics that are important to a WSN IDS, but a lot is required to be done to find out more ones. More metrics and their definitions can be defined as lessons are learned while evaluating a WSN. A few of the metrics discussed in the paper are very difficult (perhaps impossible) to observe for example the metric “observed false negative ratio.” Future work also includes weighting the scorecard metrics according to the environment of a working distributed, WSN.

ACKNOWLEDGEMENT

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

REFERENCES

- [1] Snehal Boob and Priyanka Jadhav, “WSN Intrusion Detection System”, International Journal of Computer, Volume 5, No. 8, August 2010.
- [2] 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.
- [3] Nikhil Kumar Mittal, “A survey on Wireless Sensor Network for Community Intrusion Detection Systems,” 3rd International Conference on Recent Advances in Information Technology (RAIT), 2016, pp. 107 – 111.
- [4] D. Udaya Suriya Rajkumar, Rajamani Vayanaperumal, “A leader based intrusion detection system for preventing intruder in heterogeneous Wireless sensor

- network,” IEEE Bombay Section Symposium (IBSS), 2015, pp. 1 – 6.
- [5] Zixin Zhou, Lei Liu, and Guijie Han, “Survival Continuity on Intrusion Detection System of Wireless Sensor Networks,” 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015, pp. 775 – 779.
- [6] Karen Medhat, Rabie A. Ramadan, and Ihab Talkhan, “Distributed Intrusion Detection System for Wireless Sensor Networks,” 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, pp. 234 – 239.
- [7] Prachi S. Moon and Piyush K. Ingole, “An overview on: Intrusion detection system with secure hybrid mechanism in wireless sensor network,” International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015, pp. 272 – 277.
- [8] Okan Can and Ozgur Koray Sahingoz, “A survey of intrusion detection systems in wireless sensor networks,” 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), 2015, pp. 1 – 6.
- [9] Yousef EL Mourabit, Ahmed Toumanari, Anouar Bouriden, Hicham Zougagh, and Rachid Latif, “Intrusion detection system in Wireless Sensor Network based on mobile agent,” Second World Conference on Complex Systems (WCCS), 2014, pp. 248 – 251.
- [10] Ting Sun and Xingchuan Liu, “Agent-based intrusion detection and self-recovery system for wireless sensor networks,” 5th IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT), 2013, pp. 206 – 210.
- [11] Aneel Rahim and Paul Malone, “Intrusion detection system for wireless Nano sensor Networks,” 8th International Conference for Internet Technology and Secured Transactions (ICITST), 2013, pp. 327 – 330.
- [12] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, “A Survey of Intrusion Detection Systems in Wireless Sensor Networks,” IEEE Communications Surveys & Tutorials, 2014, Volume: 16, Issue: 1, pp. 266 – 282.
- [13] Xue Deng, “An intrusion detection system for cluster based wireless sensor networks,” 16th International Symposium on WSN Personal Multimedia Communications (WPMC), 2013, pp. 1 – 5.
- [14] Keldor Gerrigagoitia, Roberto Uribeetxeberria, Urko Zurutuza, and Ignacio Arenaz, “Reputation-based Intrusion Detection System for wireless sensor networks,” a Complexity in Engineering (COMPENG), 2012, pp. 1 – 5.
- [15] Chia-Fen Hsieh, Yung-Fa Huang, and Rung-Ching Chen, “A Light-Weight Ranger Intrusion Detection System on Wireless Sensor Networks,” Fifth International Conference on Genetic and Evolutionary Computing (ICGEC), 2011, pp. 49 – 52.
- [16] Han Bin, “Research of Cluster-Based Intrusion Detection System in Wireless Sensor Networks,” International Conference on Internet Technology and Applications (iTAP), 2011, pp. 1 – 4.
- [17] Luigi Coppolino, Salvatore D'Antonio, Luigi Romano, and Gianluigi Spagnuolo, “An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies,” 5th International Conference on Critical Infrastructure (CRIS), 2010, pp. 1 – 8.
- [18] K. Q. Yan, S. C. Wang, S. S. Wang, and C. W. Liu, “Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network,” 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010, Volume: 1, pp. 114 – 118.
- [19] Abror Abduvaliyev, Sungyoung Lee, and Young-Koo Lee, “Energy efficient hybrid intrusion detection system for wireless sensor networks,” International Conference On Electronics and Information Engineering (ICEIE), 2010, Volume: 2, pp. V2-25 - V2-29.
- [20] Lionel Besson and Philippe Leleu, “A Distributed Intrusion Detection System for Ad-Hoc Wireless Sensor Networks: The AWISSENET Distributed Intrusion Detection System,” 16th International Conference on Systems, Signals and Image Processing, 2009, pp. 1 – 3.
- [21] P. J. Pramod, S. V. Srikanth, N. Vivek, Mahesh U. Patil, and Chandra Babu N. Sarat, “Intelligent Intrusion Detection System (In2DS) using Wireless Sensor Networks,” International Conference on Networking, Sensing and Control, 2009, pp. 587 – 591.