Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

A Metrics Set for Wireless Sensor Networks Intrusion Detection System Evaluation

Er. Harmeet Singh,
SBBSU
Jalandhar, Punjab, India

***Abstract*: Wireless sensor technology has become popular due to its unique features and is advancing every day. This paper describes a set of metrics that are relevant to wireless sensor networks intrusion detection system and can be used for its evaluation. The metrics set will help designers in designing efficient intrusion detection systems for wireless sensor network that are more sensitive to attacks by intruders. The metrics discussed in this paper are general characteristics that are relevant to wireless sensor networks intrusion detection system and only the common ones are discussed. The proposed metrics set will help an administrator of a network to choose the best wireless sensor networks intrusion detection system from a set of IDS systems or to optimize a configuration of a certain wireless intrusion detection system for a given network with a particular topology, sensor nodes capabilities and anticipated types of attack. Finally discussion will be done about the lessons learned using a preliminary version of the metric set and the opportunities for further work in this area.**

***Keywords:* Wireless sensor, Metrics, Intrusion Detection System, Topology, Intruder.**

I. INTRODUCTION

Lord Kelvin said, "If you cannot measure it, you cannot 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.

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 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.

This paper describes a set of metrics that are relevant to wireless sensor networks intrusion detection system and can be used for its evaluation. The metrics set will help designers in designing efficient intrusion detection systems for wireless sensor network that are more sensitive to attacks by intruders. The metrics discussed in this paper are general characteristics that are relevant to wireless intrusion detection system and only the common ones are discussed. In this paper we focus on characteristics of Intrusion Detection technology that is currently popular for wireless network in the commercial sector.

The proposed metrics will help an administrator of a wireless network to choose the best intrusion detection system from a set of systems or to optimize a configuration of a certain intrusion detection system for a given wireless sensor network with a particular topology, sensor nodes capabilities and anticipated types of attack. Finally discussion will be done about the lessons learned using a preliminary version of the metric set and the opportunities for further work in this area.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

II. WIRELESS SENSOR INTRUSION DETECTION SYSTEM

The way Intrusion Detection system (IDS) works on a WLAN is different from how it operates with a traditional LAN. In a wired network there is a full control over what kind of traffic is being transmitted on the wires, but in wireless as air is used as the medium there comes a need to do internal and external monitoring for Wireless Local Area Network (WLAN) [4]. Figure 1 shows how wireless sensor network is connected.

Wireless sensor IDS can be configured to be centralized or decentralized. When centralized, a combination of individual network sensors will collect and pass data to a centralized management console, where the wireless sensor IDS data can be stored and processed for detecting intrusion. On the other hand, a decentralized wireless sensor IDS usually consists of one or more devices that will perform both activities which is done by the sensor and the console.

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.

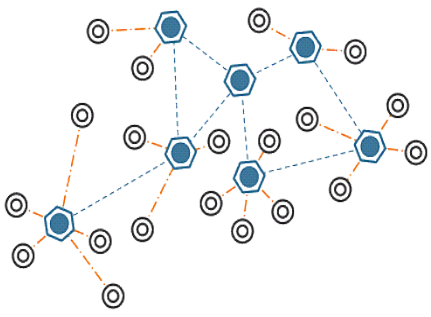

Figure 1: Wireless Sensor Network

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.

Typically, WLANs can cover quite a large physical area so that it can more easily provide more accesses that are convenient to its legitimate users. For this reason, many wireless access points (WAPs) can be set up for a wireless network so that adequate signal strength is available for that area. One general rule when implementing a wireless sensor IDS solution is that sensors should be deployed wherever a WAP is configured. An advantage found by doing this is that the majority of attempted attacks and exploits can be detected when there is a comprehensive coverage of the physical infrastructure of the wireless LAN with wireless sensor IDS sensors at each WAP location. Figure 2 shows placement of wireless sensor IDS in a wireless network.

There are numerous security-relevant issues that deal with a wireless LAN, and in fact, many of weaknesses can be made more secure. A strong wireless policy needs to be developed and then enforced properly. As a result, WLAN's

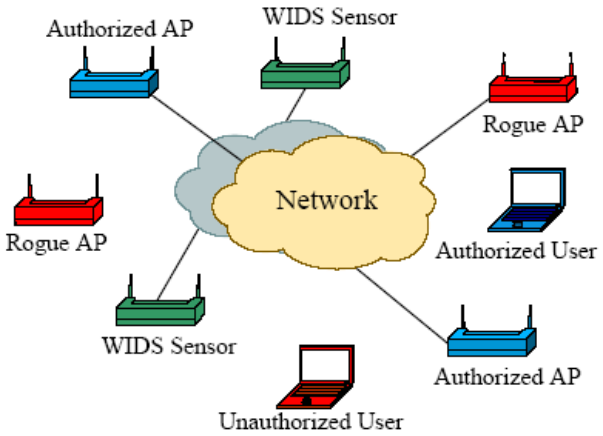

Figure 2: Wireless IDS deployment [5].

vulnerabilities can be mitigated. A wireless sensor IDS can aid in enforcing policies.

III. WIRELESS SENSOR NETWORKS INTRUSION DETECTION SYSTEM METRICS

In this section of paper, metrics that are relevant to wireless sensor network IDS will be discussed in detail. Each metric is given a unique numeric number so that it can be easily accessed. Only the commonly used metrics are discussed.

Metrics Number: M1
Metrics Name: Distributed Management.
Description: It is used to determine the distribution capabilities of IDS. It can be used to determine up to what

extent a Wireless sensor IDS supports distributed management.

Metrics Number: M2
Metrics Name: Configuration Difficulty.
Description: The difficulties a user faces while installing and configuring a wireless IDS.

Metrics Number: M3
Metrics Name: Policy Management.
Description: The difficulty in setting security and intrusion detection policies for a wireless IDS.
Metrics Number: M4
Metrics Name: License Management.
Description: The difficulty in obtaining, updating and extending licenses of a wireless IDS.

Metrics Number: M5
Metrics Name: Availability of Updates.
Description: The availability of updates of behavior profiles and cost of product upgrades.

Metrics Number: M6
Metrics Name: Platform Requirements.
Description: System resources needed to implement a wireless IDS.

Metrics Number: M7
Metrics Name: Adjustable Sensitivity.
Description: The difficulty of altering the sensitivity of a Wireless sensor IDS in order to achieve a balance between false positive and false negative error rates at various times and for different environments.

Metrics Number: M8
Metrics Name: Required data Storage Capacity.
Description: The amount of disk space needed to store logs and other application data.

Metrics Number: M9
Metrics Name: Load Balancing Scalability.
Description: It measures the ability of a Wireless sensor IDS to partition traffic into independent, balanced sensor loads.

Metrics Number: M10
Metrics Name: Multiple Sensor Support.
Description: The cardinality of sensors supported.

Metrics Number: M11
Metrics Name: Reordering and Stream Reassembly.
Description: It can be used to find an attack that has been artificially fragmented and transmitted out of order.

Metrics Number: M12
Metrics Name: State Tracking.
Description: This metrics is useful in hardening Wireless sensor IDS against storms of random traffic used to confuse it.

Metrics Number: M13
Metrics Name: Data Pool Selectability.
Description: This metrics is used to define the source data to be analyzed for intrusions.

Metrics Number: M14
Metrics Name: System Throughput.
Description: It is used to define the maximal data input rate that can be processed successfully by the Wireless IDS.

Metrics Number: M15
Metrics Name: Observed False Positive Ratio.
Description: This is the ratio of alarms that are wrongly raised by the wireless sensor IDS to the total number of transactions.

Metrics Number: M16
Metrics Name: False Negative Ratio.
Description: This is the ratio of actual attacks that are not detected by the wireless sensor IDS to the total number of transactions.

Metrics Number: M17
Metrics Name: Cumulative False Alarm Rate.
Description: The weighted average of False Positive and False Negative ratios.

Metrics Number: M18
Metrics Name: Induced Traffic Latency.
Description: It measures the delay in the arrival of packets at the target network in the presence and absence of a Wireless IDS.

Metrics Number: M19
Metrics Name: Stress Handling and Point of Breakdown.
Description: The point of breakdown is defined as the level of network or host traffic that results in a shutdown or malfunction of IDS.

Metrics Number: M20
Metrics Name: IDS Throughput.
Description: This metrics defines the level of traffic up to which the IDS performs without dropping any packet.

Metrics Number: M21
Metrics Name: Depth of System's Detection Capability.
Description: It is defined as the number of attack signature patterns and/or behavior models known to it.

Metrics Number: M22
Metrics Name: Breadth of System's Detection Capability.
Description: It is given by the number of attacks and intrusions recognized by the IDS that lie outside its knowledge domain.

Metrics Number: M23
Metrics Name: Reliability of Attack Detection.
Description: It is defined as the ratio of false positives to total alarms raised.

Metrics Number: M24
Metrics Name: Possibility of Attack.
Description: It is defined as the ratio of false negatives to true negatives.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

Metrics Number: M25
Metrics Name: Consistency.
Description: It is defined as the variations in the performance of a Wireless IDS

Metrics Number: M26
Metrics Name: Firewall Interaction.
Description: The ability of a Wireless sensor IDS to interact with the Firewall systems.

Metrics Number: M27
Metrics Name: User Friendliness.
Description: The ability of a Wireless sensor IDS to configure according to user's environment.

Metrics Number: M28
Metrics Name: Router Interaction.
Description: Degree of interaction of a Wireless sensor IDS with the router.
Metrics Number: M29
Metrics Name: Error Reporting and Recovery.
Description: The ability of a wireless sensor IDS to correctly report and recover.

Metrics Number: M30
Metrics Name: Induced Traffic Latency.
Description: It is the degree to which traffic is delayed by the Wireless IDSs presence or operation.

Metrics Number: M31
Metrics Name: Power
Description: Power consumption of WSN IDS for transmission and reception of the data in the sensor network and for processing of data.

Metrics Number: M32
Metrics Name: Processing
Description: The processing capabilities of WSN IDS

Metrics Number: M33
Metrics Name: Memory
Description: The amount of memory required for processing of captured sensor data.

Metrics Number: M34
Metrics Name: Distance
Description: The distance coverage of the IDS in the sensor network.

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

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

IV. CONCLUSION AND FUTURE WORK

Unwanted activities on a wireless sensor network can be detected by a wireless IDS. As the technology of designing wireless sensor networks is changing, there comes a need to design wireless sensor IDS that can work along with wireless networks. This paper provides metrics based approach that can be used for evaluating a wireless sensor network IDS in order to find out the areas in which the IDS is weak and needs improvement.

In this paper we describe what exactly is Wireless sensor IDS and then discuss few common metrics associated with wireless IDS. Although an effert is made to find metrics that are important to a Wireless sensor 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 wireless network. 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 dividing the metrics set into various classes like Logistical metrics, Architectural metrics, Performance metrics etc. so that more accurate definition of each metrics can be defined. A metrics scorecard based approach can be used to assign different scores to wireless sensor IDS under study for their evaluation.

V. REFERENCES

[1] Matthew Gast, 802.11 Wireless Networks: The Definitive Guide, Second Edition, 2005.

[2] William Stallings, Wireless Communications & Networks, 2nd Edition, 2004.

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

[4] Oliver Poblete, An Overview of the Wireless Intrusion Detection System, GIAC Security Essentials Certification (GSEC) PracticalAssignment, 2005. Available at http://www.sans.org/Reading_room/whitepapers/wireless/overview-wireless-intrusion-detection-system_1599

[5] Systems and Network Analysis Center Information Assurance Directorate, 802.11 Wireless LAN Intrusion Detection Systems, Available at http://www.nsa.gov /ia/_files/wireless/802.11_Wireless_LAN.pdf

[6] Reijo Savola, On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.1, January 2010. Available at http://paper.ijcsns.org/07_book/201001 /20100131.pdf

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

[7] Snehal Boob and Priyanka Jadhav, Wireless Intrusion Detection System, International EssentialsCertification (GSEC) Practical Assignment, 2005.Available at http://www.ijcaonline.org/volume5/number8 /pxc3871312.pdf

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

[9] Jamil Farshchi, Wireless Intrusion Detection Systems, Security Article, 2003. Available at http://www.symantec.com/connect/ articles/wireless-intrusion-detection-systems

[10] SANS Institute InfoSec Reading Room, Understanding Intrusion Detection Systems, 2011. Available at http://www.sans.org/readingroom/whitepapers/detection/understanding-intrusion-detection-systems_337

[11] Information Assurance Tools Report, Intrusion Detection Systems,Sixth Edition, September 25, 2009. Available at http://iac.dtic.mil/iatac/download /intrusion _detection.pdf

[12] 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, Issue1, Ver.1: Jul.-Dec., 2011, ISSN : 2249 - 4944 (Print).

[13] Yousef EL Mourabit, Ahmed Toumanari, Anouar Bouirden, 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)