USER REQUIREMENTS WEIGHT BASED APPROACH TO IDS SELECTION FOR WSN

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 - Intrusion Detection System (IDS) is a network security tools built for detecting vulnerability exploits against attacks in wireless sensor networks (WSNs). The selection of IDS depends on the WSN architecture and application. It is for the administrator to decide which IDS will be the best solution for the sensor network. There is never one solution that works for everything so administrator has to compare the capabilities of each IDS along with budget, knowledge and needs to find one that works best for them. This paper provides a user requirements weight based approach to IDS selection for WSN. We first discuss user WSN IDS requirements and WSN IDS metrics, then for each WSN IDS requirement we match the concern metric(s). User lists their WSN IDS requirements in a partial ordering from least to most important. User requirements are usually stated in a positive form or converted to the positive form. The first requirement (i.e. least important) is assigned the lowest weight (e.g., one) while the remaining requirements are assigned increasing weights in proportion to their relative importance. Once the requirements are weighted, each WSN IDS metric is assigned a weight that is equal to the sum of the weights of the requirements it contributes to. WSN IDS metrics are arranged in descending order where metric with the highest weight is at the top. Appropriate WSN IDS tool may be selected after matching the metrics weight and IDS features.

Keywords: Intrusion detection system; Wireless sensor network; metrics; weight.

I. INTRODUCTION

Security problems are not entirely technical, organization strategy decisions decides about the user’s requirements. The goals, acceptable uses, and constraints on the system are decided by organizational policy regarding security. It is organizational agreement that is going to decide what to monitor, when to alert and whom to alert, or up to what degree of threat a potential intrusion presents. Networking has given rise to the issue of network security. Intrusion Detection Systems (IDS) has emerged as an important security product. 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.

Since wireless sensor network (WSN) is a new technology it also has several vulnerabilities. Products like WSN IDS have come about that address many of these. As variety of WSN IDS are proposed in the literature, it becomes difficult to choose and implement one of them as it’s a complex and time consuming process. This becomes more difficult if the organization does not have a corporate security program. WSN IDS selection decision should not be made quickly, lightly, or without having a firm understanding of the technology, options, or the potential impacts. In this paper, we provide a user requirements weight based approach to IDS selection for WSN. In this approach first all possible user IDS requirements and WSN IDS metrics are listed. Then, for each IDS requirement we find the concern metric(s). User lists their WSN requirements in a partial ordering from least important to most. Requirements are usually stated in positive form or converted to the positive form. 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. Once the requirements are weighted, each IDS metric is assigned a weight that is equal to the sum of the weights of the requirements it contributes to. WSN IDS metrics are arranged in descending order where metric with the highest weight is at the top. Appropriate IDS tool may be selected after matching the metrics weight and WSN IDS features.

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 on a network or a device. IDS can be software or 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

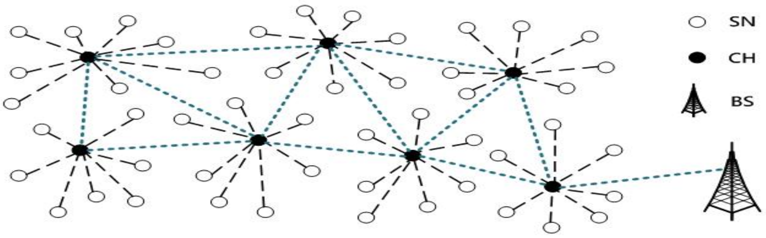


Figure 1: A typical WSN

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. CHOOSING RIGHT WSN IDS

A variety of WSN IDS concepts are available in the literature having different features and capabilities. The decision process for selecting an IDS can be divided into the following steps:

1). Identify the need for IDS by performing risk assessment of the organization.

2). Understanding technical environment of organizations WSN.

3). Perform cost benefit analysis.

4). Apply user requirements weight based approach to choose and implement right IDS.

5). Perform strategic deployment of IDS.

6). Monitoring and maintenance of IDS.

In this paper, we will concentrate only on step 4 of the above mentioned process. The decision of selecting best WSN IDS solution for the network totally depends on its users. One solution is never going to work for everything, therefore the user has to compare the capabilities of each IDS product along with the budget and knowledge which in term will help them in finding the needs for the best solution. User requirements weight based approach involves following steps:

1) Collect user WSN IDS requirements.
2) Assign lowest weight (e.g., one) to least important requirement.
3) Other requirements are assigned increasing weights in proportion to their relative importance. There is also possibility of duplicate weights.
4) Arrange these requirements from least important to most one.
5) Once the requirements are weighted, each IDS metric is assigned a weight that is equal to the sum of the weights of the requirements it contributes to.
6) Arrange IDS metrics in descending order.
7) Select appropriate IDS matching the requirements.

User requirements for WSN IDS may be collected by asking following questions to the user:

1) What is the size of the organizations WSN?
2) Whether there is need for complete hardware product, or complete software product, or a combined hardware and software product?
3) Whether the WSN IDS product needed is to be commercial system or open source system?
4) What should be the IDS policy behind intrusion detection?
5) What should be the attack detection capability of IDS?
6) How much it should be difficult to install, configure, and adjust IDS product?
7) What platform and other resources could be provided for proper functioning of IDS?
8) How much performance of IDS is expected?
9) How much reliable should be IDS?
10) How much correct reporting and recovery is expected from IDS product?
11) What should be the interaction of IDS product with the firewall and router?
12) What should be IDS setting as per user environment?
13) How license Management is expected?
14) What and when updates are expected?
15) How much disk space could be provided to store logs and other application data?
16) How much IDS stress tolerance is expected?
17) What kind of wireless cards are used in the network?
18) What network IP range is provided?
19) What compatibility of IDS with other products is expected?
20) What should be the level of administration for IDS?
21) What should be the IDS product lifetime?
22) What kind of technical support is expected?
23) How much clarity of reports is expected?
24) Is information going to be shared?

25) How previous session data is to be recorded?
26) Is there need to extend the network in the future?
27) What should be the maximal input data processing rate of IDS product?

After gathering the WSN IDS user requirements by asking above question, user may be asked to arrange these requirements in an order as per requirement so that appropriate weights may be assigned to the requirements. Depending on the requirements user may leave any of the above questions or may add to the list. Once the requirements are fixed, approach discussed in the paper may be applied for selecting appropriate IDS product.

IV. WSN IDS METRICS

In this section of paper, we will be discussing in greater detail the metrics that are most applicable to WSN IDS. The metrics are grouped together by classes that are 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 2 and is described below in detail.

A. 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.

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.

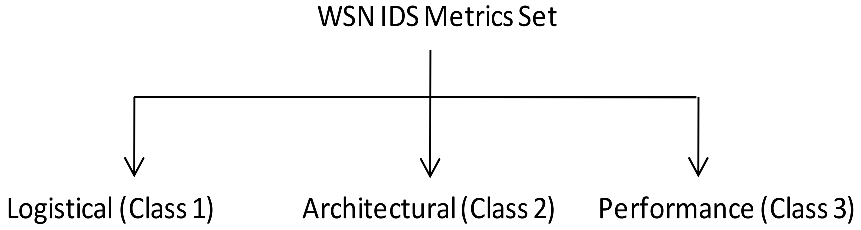


Figure 2: Classification of WSN IDS metrics

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.

B. 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.

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 Rate	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 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.

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

C. 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 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

V. MAPPING USER REQUIREMENTS TO METRIC(S)

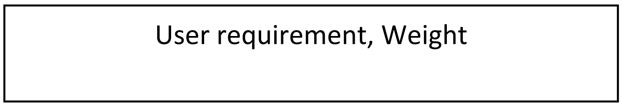
The metrics related with each of possible user requirement are given in table 4. The table indicates what metrics are contributing to fulfil a particular requirement. For example size of user WSN is concern with the metrics Distributed Management, Configuration Difficulty, Platform Requirements, Adjustable Sensitivity, Load

Table 4: User requirements and metrics relation

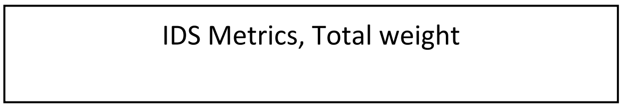
Question number for gathering user requirement	Concerned IDS metric(s)
1	Distributed management, Configuration difficulty, Platform requirement, Adjustable sensitivity, Load balancing, Scalability, Multiple sensor support
2	Configuration difficulty, Platform requirement, Policy management
3	Configuration difficulty, License management
4	Policy management
5	Reordering and stream reassembly, State tracking, Data pool selectability
6	Distributed management, Configuration difficulty, Adjustable sensitivity, User friendliness
7	Distributed management, Platform requirement, Required data storage capacity
8	Distributed management, Induced traffic latency, Throughput, Depth of system’s detection capability, Breadth of system’s detection capability, Reliability of attack detection, Possibility of attack, consistency, Induced traffic latency
9	False positive ratio, False negative ratio, Cumulative false alarm rate
10	Required data storage capacity, Error reporting and recovery
11	Configuration difficulty, Firewall interaction, Router interaction.
12	Configuration difficulty, Policy management, License management, User friendliness
13	License management, Multiple sensor support

14	Availability of updates
15	Distributed management, Platform requirement, Required data storage capacity
16	Compromise analysis, stress handling and point of breakdown, Power, Processing
17	Platform requirement
18	Distributed management, Multiple sensor support, Configuration difficulty
19	Interoperability
20	License management
21	License management, Memory, Distance
22	Availability of technical support
23	Error reporting and recovery
24	Distributed management, Multiple sensor support
25	Session recording and playback
26	Load balancing scalability, Multiple sensor support
27	System throughput

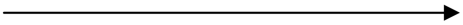
Balancing Scalability, and Multiple Sensor Support as shown in the column corresponding to requirement number 1. The purpose of the table is to help user in making a correct choice to IDS. With figure 3, we provide notations that will be used to represent user requirements and IDS metrics relationship. Figure 3 gives user requirement to IDS metric weighting. Following notations are used to represent weighted user requirements and weighted WIDS metrics relationship example. As in figure 3 metric configuration difficulty gets highest weight, so the IDS product having least difficulty in configuring appears to be the best solution to the user environment in this example. It is also possible that some of the metrics discussed above may not contribute to any of the user requirement. As WSN technology is changing more metrics and questions may be added to the above approach.



Represent each user requirement and its corresponding weight



Represent each IDS metrics and total weight contributed by user requirement



Used to connect user requirements and IDS metrics

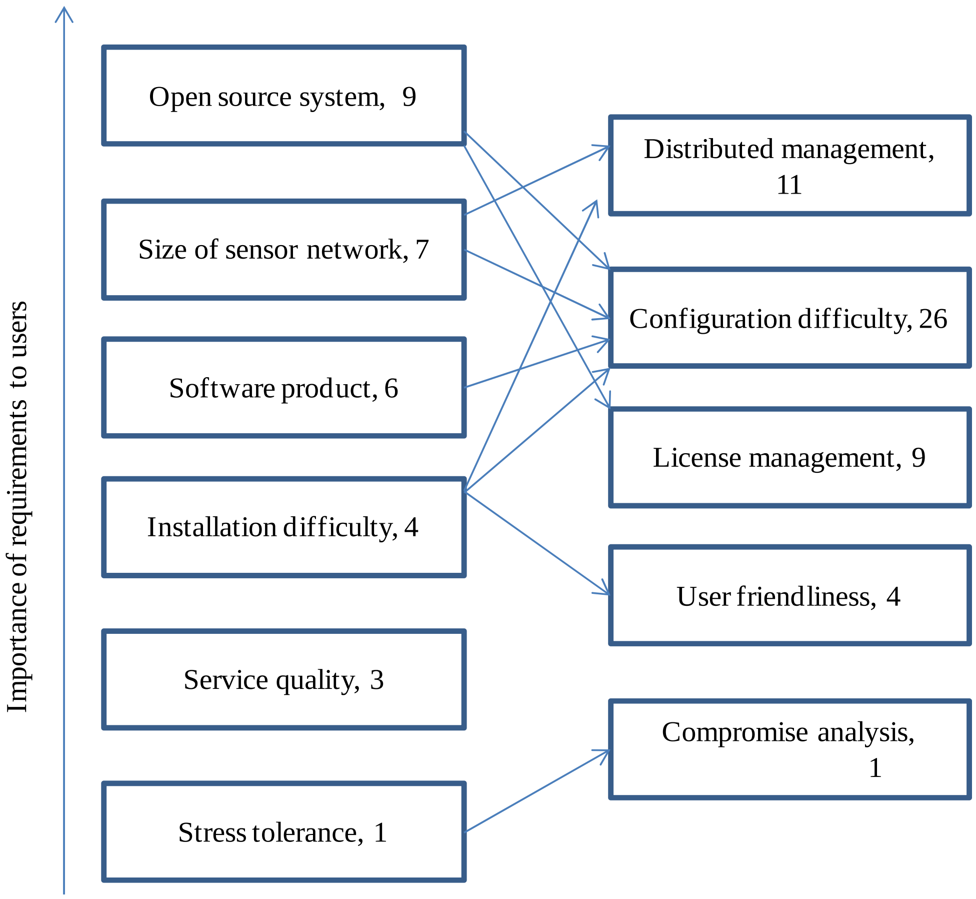

Importance of requirements to users
Open source system, 9
Size of sensor network, 7
Software product, 6
Installation difficulty, 4
Service quality, 3
Stress tolerance, 1
Distributed management, 11
Configuration difficulty, 26
License management, 9
User friendliness, 4
Compromise analysis, 1

Figure 3: User requirement to IDS metric weight example

VI. CONCLUSION AND FUTURE WORK

A variety of IDS concepts are proposed for wireless sensor networks, but it becomes difficult for the user to select one of them that meet their requirements as these concepts differ in features and capabilities. In this paper, we provide a user requirements weight based approach to be used for selecting an IDS concept so that it can be implemented for providing security to sensor network. We describe various steps needed for the selection of IDS and how user requirements may be weighted. We also define various metrics concern with wireless sensor network IDS and how mapping of weighted user requirements to these metrics can be done. Although we tried our best to find out the user requirements and metrics concerned with IDS, but a lot is to be done to find out more. The approach discussed in the paper may be extended by assigning negative and fraction weights to the user requirements so that more accurate selection of IDS can be done.

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 Wiress 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 ireless 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 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.

[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.